

Procon Melco ***sip***⁺ **User Guide**
Issue 2, Apr. 2023

© SYNAPSYS SOLUTIONS LIMITED

All rights reserved. No part of this document may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of the software that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by the information contained in this document.

Printed: Apr. 2023 in England

Contents

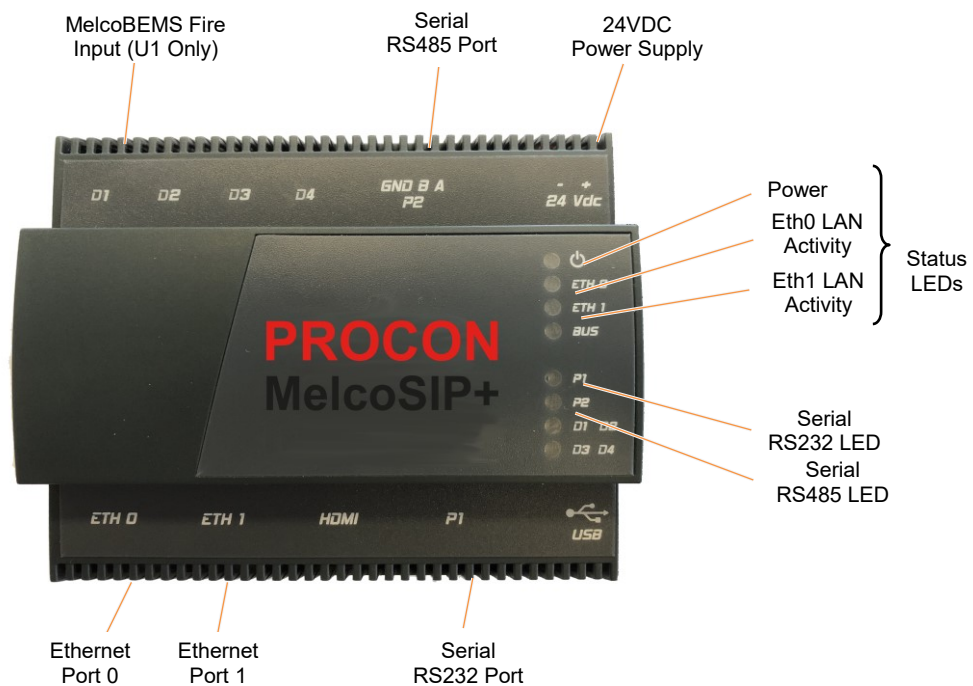
1	INTRODUCTION	1
1.1	THE UNIT.....	3
1.2	SYSTEM OVERVIEW.....	4
2	CONFIGURATION	5
2.1	CONNECT TO THIS PRODUCT	6
2.2	CONFIGURE THE IP SETTINGS.....	8
2.3	CONFIGURE THE GLOBAL SETTINGS.....	11
2.3.1	Change the Site name and SIP name details	11
2.3.1	Change the local Time settings	11
2.3.2	Use the Ping command	12
2.3.3	Use the Reboot.....	12
2.3.4	Installing Webserver certificates	13
2.3.5	Configure the Email Settings	14
2.4	MANAGE DRIVERS	21
2.4.1	Manage the required drivers.....	21
2.4.2	Manage Melco Driver Settings.....	23
2.4.3	Manage BACnetIP Driver settings	26
2.4.4	Manage Data Acquisition Driver Settings	30
2.4.5	Manage ModBus Server/Slave Driver Settings.....	31
2.4.6	Manage MQTT Driver Settings	32
2.4.7	Manage REST Server Driver Settings	34
2.4.8	Manage vIQ Driver Settings.....	34
2.5	DEFINE POINTS.....	39
2.5.1	Define the protocol driver point.....	39
2.5.2	Define Melco Driver Points	40
2.5.3	Define BIC (BACnet Server) Driver Points.....	42
2.5.4	Define Data Acquisition Driver Points	55
2.5.5	Define MQTT Driver Points.....	66
2.5.6	Define REST Server Driver Points.....	70
2.5.7	Define ModBus Server/Slave Driver Points	72
2.5.8	Define vIQ Driver Points	76

2.6	LINK POINTS	97
2.6.1	Link defined points.....	97
2.7	MANAGE CONFIGURATION TRANSFER.....	100
2.7.1	Backup and restore unit configuration	100
3	ORDER CODE	101
3.1	PRODUCT ORDER CODES	101
3.2	ACCESSORIES	101

1 INTRODUCTION

This is a miniature computing platform that can be installed as part of the Building energy Management System (BeMS), and includes a dedicated Mitsubishi Centralised Controller interface. It provides a direct interface between the Mitsubishi Centralised Controller (e.g., AE200 and/or EW50), a BeMS, a third party IoT (MQTT and/or REST) platform and includes a data reporting function.

Remember Energy metering is compulsory for buildings of a floor area >500M². The owner must be able to account for 90% of the consumed energy from each system, i.e., heat, gas, lighting, water, and electricity.



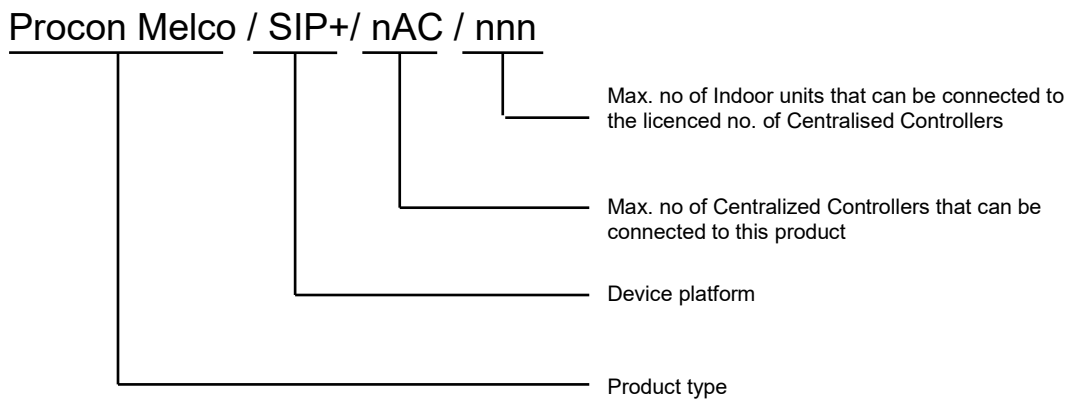
Remember Typically, individual systems (energy control, lighting, boiler, and air conditioning system, etc.) are individually measured for CO₂ accountability. So, installing this unit and combining the individual systems can help an effective BeMS be more energy efficient and comply with April 2006 Part L2 Building Regulations.

It is designed and manufactured to comply with CE Class A, FCC Class A, WEEE (Waste Electrical and Electronic Equipment), RoHS (Restriction of Hazardous Substances) regulations and the identification of a substance as Substance of Very High Concern (REACH).

It also complies with the requirements defined in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility (89/336/EEC). For the evaluation regarding the electromagnetic compatibility, refer to the Declaration of Conformity certificate (available on request).

This product collects values from devices connected to a locally installed Mitsubishi Centralised Controller. This Mitsubishi AC network data is then made available to a BACnet, IoT MQTT, IoT REST Server, ModBus Client/Master (via ModBus Server/Slave driver), and/or Trend BMS via the Ethernet network to control and monitor environmental conditions, i.e., measuring the consumption of specific services (heat, gas, electricity power, airflow, ambient room temperature, humidity, and water) in a building via a controller.

The maximum number of input points permitted is limited according to the product variant licence (see [Order Code](#)), and appropriate hardware (drivers) where applicable.



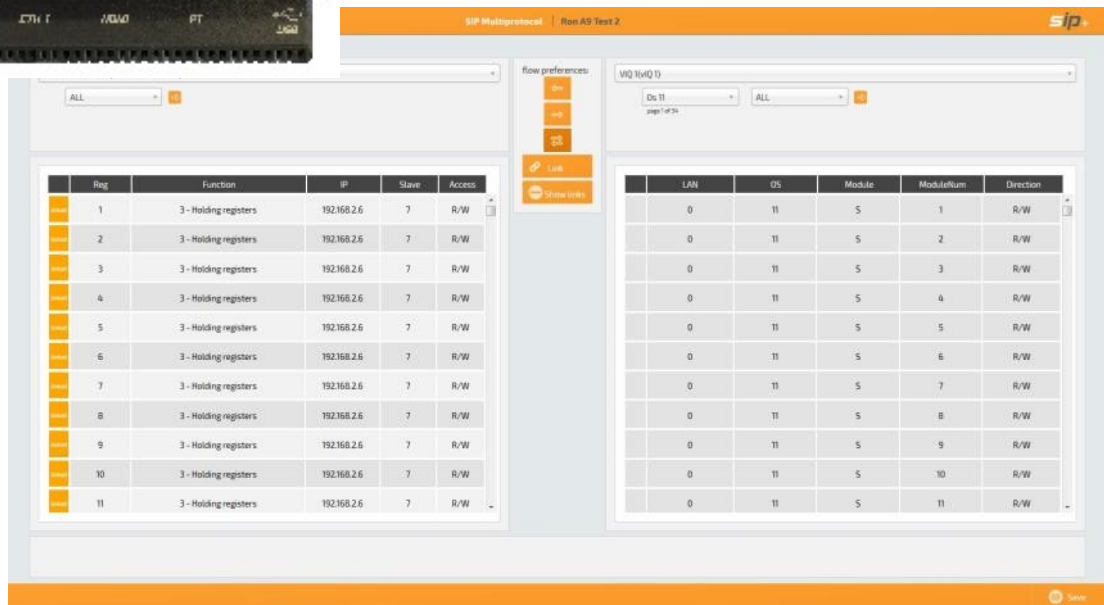
AVAILABLE PROTOCOL/DRIVER	SERIAL	ETHERNET	LICENCED
Melco		Eth0/Eth1	Yes
BACnetIP Server		Eth0/Eth1	No
Data Reporting		Eth0/Eth1	No
IoT: MQTT		Eth0/Eth1	No
IoT: REST Server		Eth0/Eth1	No
ModBus Server/Slave	P1/P2	Eth0/Eth1	No
vIQ (Synapsys Solutions Trend connection)		Eth0	No

1.1 THE UNIT

This product has a smart casing which permits for safe, quick, and simple installation on DIN rail in an enclosure. The hardware includes an internal web-based Configuration pages, designed to simplify the engineering and configuration of the interface, displaying values and reporting alarms. This set of pages simplifies the configuration of communication requirements for each selected driver and allows the value of each input point to be linked to the output points of the selected driver.

It provides a web page used to

- define the connection to the local IP network
- select required drivers, and define the communication requirements for the selected driver
- create/define the required points from the selected driver
- link selected input point of the selected driver to necessary output point of the selected driver
- perform product service/maintenance tasks

The screenshot displays the web-based configuration interface for the Procon MelcoSIP+ unit. The interface is titled 'SIP Multiprotocol | Run AS Test 2' and features a 'sip+' logo in the top right corner. The main content area is divided into two primary sections:

Register Configuration Table:

Reg	Function	IP	Slave	Access
1	3 - Holding registers	192.168.2.6	7	R/W
2	3 - Holding registers	192.168.2.6	7	R/W
3	3 - Holding registers	192.168.2.6	7	R/W
4	3 - Holding registers	192.168.2.6	7	R/W
5	3 - Holding registers	192.168.2.6	7	R/W
6	3 - Holding registers	192.168.2.6	7	R/W
7	3 - Holding registers	192.168.2.6	7	R/W
8	3 - Holding registers	192.168.2.6	7	R/W
9	3 - Holding registers	192.168.2.6	7	R/W
10	3 - Holding registers	192.168.2.6	7	R/W
11	3 - Holding registers	192.168.2.6	7	R/W

Module Connection Table:

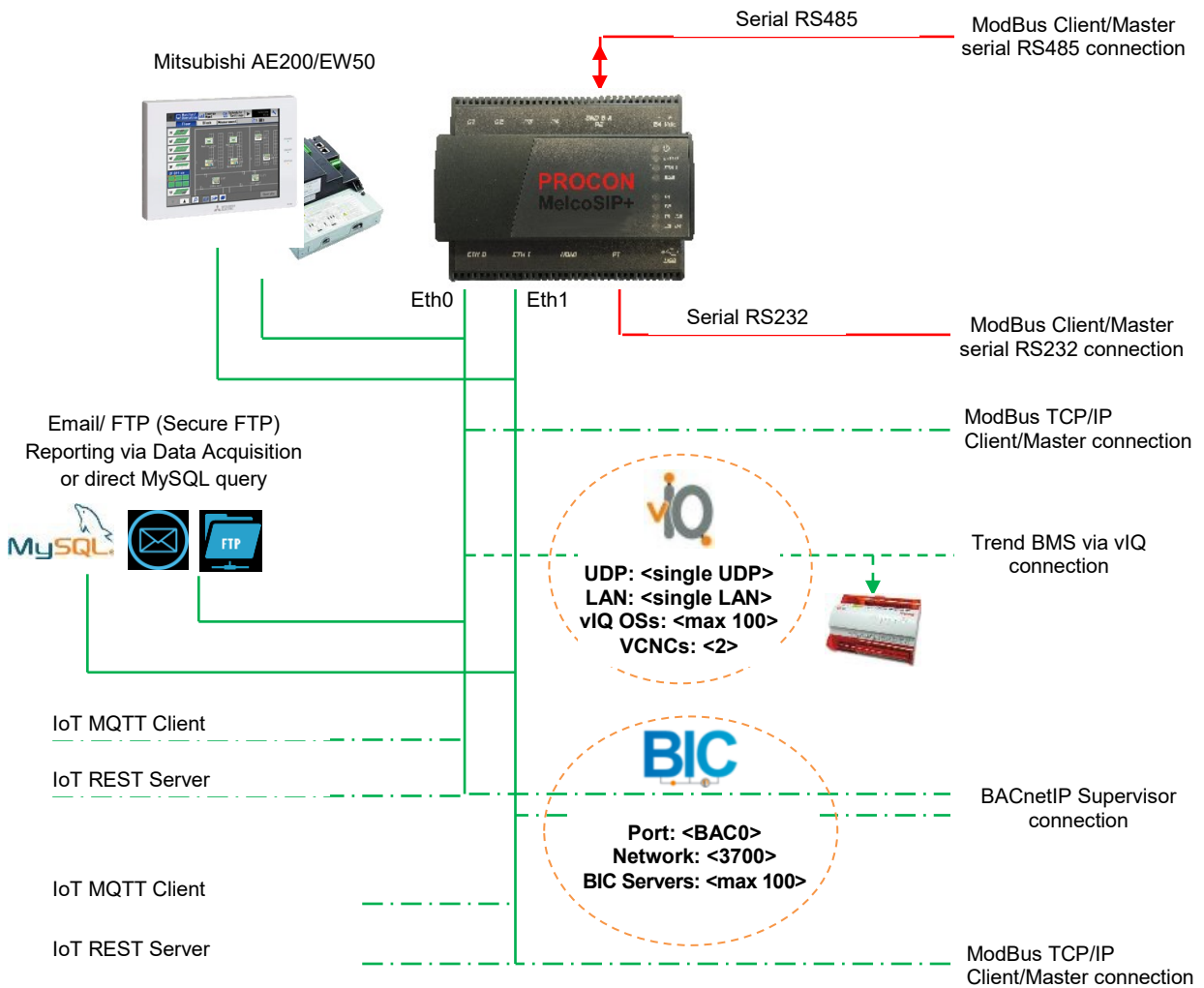
LAN	OS	Module	ModuleNum	Direction
0	11	5	1	R/W
0	11	5	2	R/W
0	11	5	3	R/W
0	11	5	4	R/W
0	11	5	5	R/W
0	11	5	6	R/W
0	11	5	7	R/W
0	11	5	8	R/W
0	11	5	9	R/W
0	11	5	10	R/W
0	11	5	11	R/W

The interface also includes a 'Flow preferences' sidebar with buttons for 'Link' and 'Strip links', and a 'MQ (VQ I)' section with a dropdown menu and a 'page 1 of 24' indicator.

1.2 SYSTEM OVERVIEW

The unit provides a hardware and software connection between devices communicating via an Input protocol and an Output protocol.

Note Any protocols not supplied at start, may be available in future release.



2 CONFIGURATION

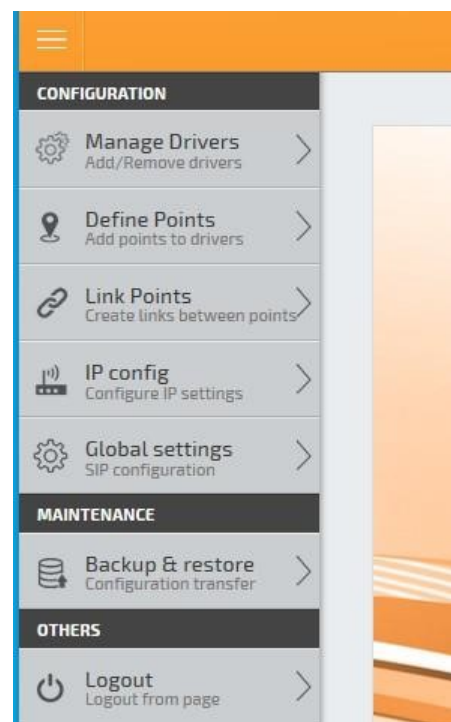
This section describes the process of allowing the data at devices connected to the Mitsubishi Centralised Controller, to be made available to a local BMS network. It explains the specific configuration.

Each product is password protected to prevent unauthorised access to the parameters that define the operation of this product.

The Configuration pages include the

- **Local IP settings** used to configure the unique identity of this product connected to an IP (Internet Protocol) network.
- **Global settings** page used to configure details that relate to the hardware for reporting.
- **Manage drivers** page used to determine the required drivers and configure the communications parameters (**Comms settings**) ensuring compatibility with required protocols.
- **Define points** page used to create/define the Input protocol driver and Data Acquisition driver points, with additional protocol specific parameters to ensure correct values are transferred between Input protocol driver and Data Acquisition driver.
- **Link points** page is used to link an Input protocol driver point to an Output protocol driver point, with appropriate security parameters if necessary.
- **Admin** page used to configure the login security of this product.

Tip! To configure this product, follow the Contents page and/or section headers as a basic level of commissioning instructions.



2.1 CONNECT TO THIS PRODUCT

When this product has been correctly installed the communication protocols and the required parameters must be configured.

Remember If this unit is installed in a system, the controllers must also be configured.

Note Each product is supplied with a default IP address. This is used to identify the product on the IP network, and it must be changed and assigned a unique IP address according to local company network policy.

Before configuring this product, ensure it and the computer are in the same IP range. Typically, a fixed IP address is used because the computer performs communications with individual products. The computers' IP address is displayed on the 'TCP/IP Properties' dialog by selecting,

Start > Control Panel > Network Connections > Local Area Connection > Properties > TCP/IP > Properties

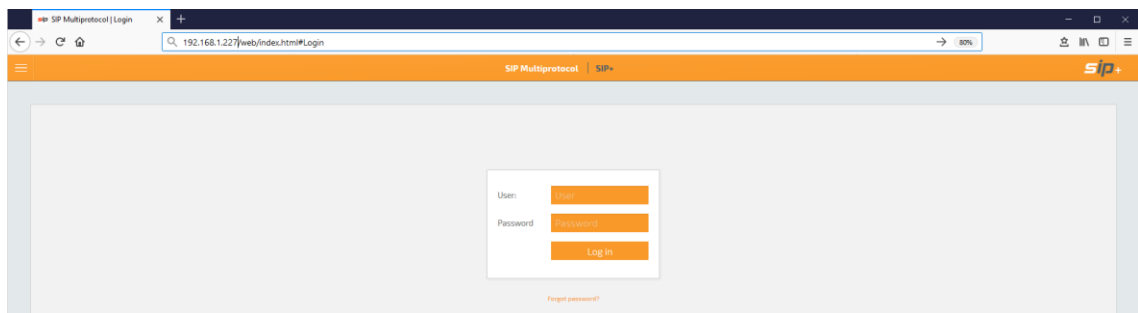
To connect to this product

1. After physically connecting the computer to this product using an appropriate Cat 5e cable, open a web browser application.

Tip! Mozilla Firefox is commonly used by our engineers. Other browsers can be used but may display unexpected problems.

2. Type the required IP address. An IP address must be entered using the standard 32-bit dotted-decimal notation.

Default IP address - **192.168.1.128 (255.255.255.0)**



The 'Login' page will appear.

- ◆ Alternatively, launch the Configuration Tool in the default web browser by selecting

Start > All Programs > Accessories > Run

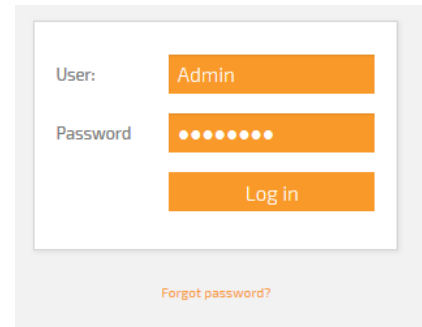
and type the default IP address, including http:// in the dialog that appears. Press 'OK' to confirm.

Note The product can also be installed in a secure site. Type **https://<IP address>** and confirm the secure certification request as necessary.

- ◆ Enter the **'User'** name and **'Password'** and press 'Login' to display the 'Main Menu' options.

Tip!

If the valid **'User'** name and **'Password'** fails to launch the configuration page, check this product is connected and IP communication has been established. Press **'Refresh'** to verify the connection. Clear the web browser cache (generally **<Ctrl>+<Shift>+** will display the **'Delete browsing history'** dialog). Press **'Refresh'** to verify the connection.



- If necessary, acknowledge the **'Time mismatch'** warning dialog. This indicates the time currently set in this product differs from the time currently set in the PC by more than 5 mins.

Note

This warning only appears after the correct Username and password is entered on the **'Login'** page and will not appear again until the browser is reloaded or refreshed.

2.2 CONFIGURE THE IP SETTINGS

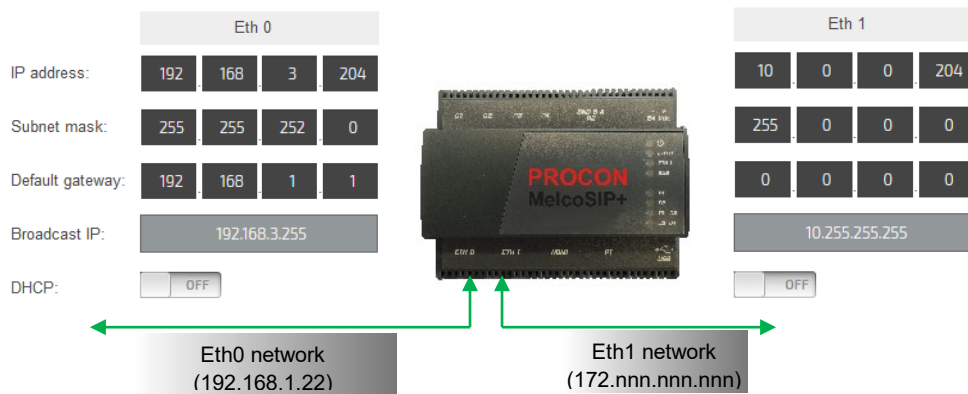
The IP config parameters make this unit compatible with the connected IP network.

1. Press **'IP config'** to display the Transmission Control Protocol and Internet Protocol (TCP/IP) parameters that identify this unit on an IP Network.

Note TCP/IP is the communication protocol used for networks, including the Internet. A specific range of configured IP addresses can be used to group units in networks or subnets.

- ◆ If necessary, change the **'Hostname'**. This is a 15-character label (including '-' and '_') and numbers, assigned to this product and linked to the IP address related to Eth1. The IP address may be derived from the DHCP (**'DHCP enabled'** is)

Tip! The **Hostname** is common across both Eth0 and Eth1 ports.



Note The **'Broadcast IP'** is the logical address used for datagrams to all connected IP devices.

Caution Do NOT define the same IP address subnet range on both Eth0 and Eth1.

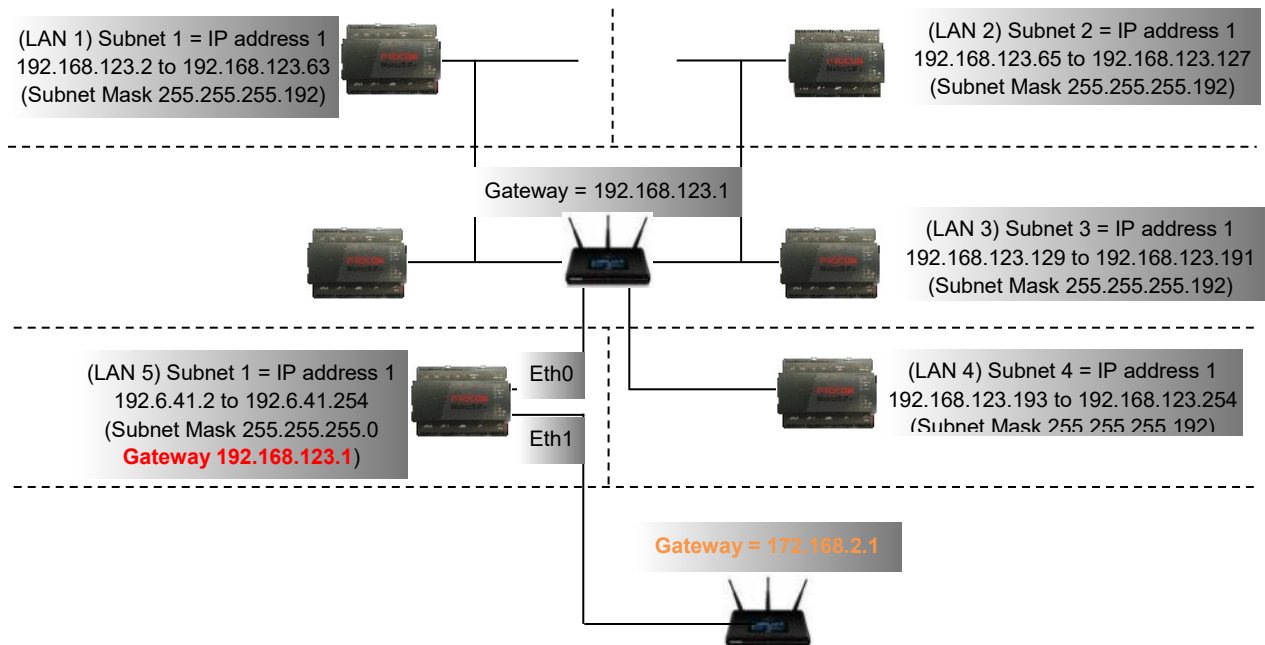
1. Change the 'IP address', 'Subnet mask', and 'Default gateway' of 'Eth1', typically the fieldbus IP address range, (and 'Eth0', typically for the BMS IP address range) according to local network policy.

The IP address provides a unique identification of a product on the IP network. The Subnet Mask is a configurable range of accessible IP addresses, and the Default Gateway is used to direct communications to IP addresses not in the defined Subnet Mask.

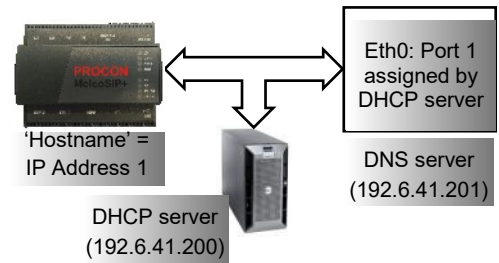
Hostname:	Supp-SIPEMTIF							
	Eth 0				Eth 1			
IP address:	192	168	3	204	10	0	0	204
Subnet mask:	255	255	252	0	255	0	0	0
Default gateway:	192	168	1	1	0	0	0	0
Broadcast IP:	192.168.3.255				10.255.255.255			
DHCP:	<input type="checkbox"/> OFF				<input type="checkbox"/> OFF			

Tip! 'SIP Search' discovers Synapsys Solutions designed products if connected to a compatible IP address range.

Caution Do NOT use the same Subnet range on both Eth0 and Eth1.



DHCP (Dynamic Host Configuration Protocol) configuration. This is a computer networking protocol used by devices (DHCP clients, i.e., this product) on a network to automatically obtain IP address from a DHCP server. When the IP network parameters are assigned by the DHCP server.



Caution

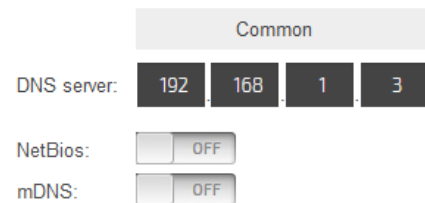
The DHCP Server can be configured to assign an IP address as required. The IP network MUST be managed appropriately by qualified personnel.

- ◆ If necessary, change the **'DNS server'** (Domain Name System), the **'NetBIOS'** (Network Basic Input/Output System) and the **'mDNS'** (multicast DNS).

Tip!

The 'DNS Server' applies to both Eth0 and Eth1 port. Use on site DNS Server where possible.

DNS server (Domain Name System). This is the IP address of the server that manages the translation of the configured **'Hostname'** into an **'IP Address'** that may change if **'DHCP Enabled'** is set .



Remember

The 'DNS server' may need to be configured to support non-Microsoft clients. It may also be integrated with the DHCP Server.

NetBIOS (Network Basic Input/Output System) configuration. This manages the IP address and Hostname (NetBIOS name) resolution of each device via the **'DNS server'**. Typically, this will only be enabled () when multiple products have the same 15-character Hostname.

mDNS (multicast DNS). This is a computer protocol that resolves hostnames to IP addresses within the local.

Caution

Ensure the mDNS hostname includes '.local' when defining a connection to a device which has mDNS enabled, e.g. SIPIP-E3-00-00.local.

Do NOT enable both NetBIOS, and mDNS at the same time.

2. Press **'Save'** to confirm the changes, as necessary.

2.3 CONFIGURE THE GLOBAL SETTINGS

These parameters are used to manage details used to identify each device on the IP network, the source of report files sent via email or FTP and ensure the report timestamps are as correct.

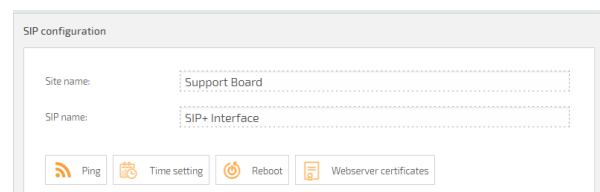
Tip! These parameters can also be changed using the SIP Data Tool.

2.3.1 Change the Site name and SIP name details

- If necessary, configure the 'Site name' and 'SIP name' for identifying this hardware in the browser, and the generated report files.

Site name. Used to identify the site via a web browser and is the first section of the report filename.

SIP name. Used to identify each hardware device via a web browser and is the first section of the report filename.



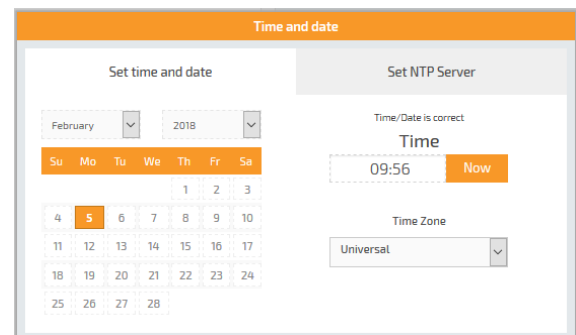
Note Both parameters support a maximum of 64 (UTF-8) characters and numbers.

2.3.1 Change the local Time settings

- Press 'Time setting' to display the hardware applicable clock settings. These values are used for the Timestamp details in the reports derived from the Data Acquisition driver.

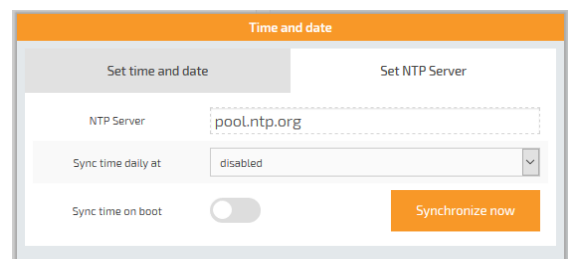
Caution Ensure the time is set correctly, to provide valid reporting data.

- Change the local Time settings on the 'Set time and date page'.
 - Press 'Now' to update the time and date according to the time and date of the PC connected to this hardware.
 - If necessary, set the 'Time Zone' according to the site.



- Alternatively, define an NTP Server on the use 'Set NTP Server' page to manage the local time settings.

Caution Only use 1 (one) means of time synchronisation, e.g product Time zone setting, or NTP Server or BACnet time synchronisation or Trend Timemaster.



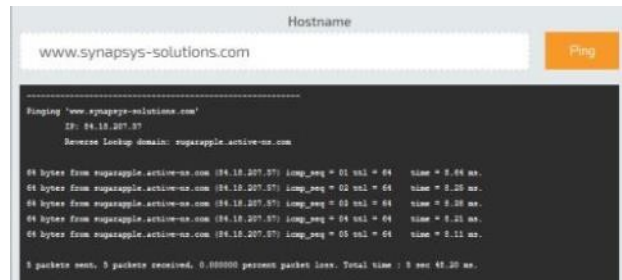
- Press 'Save' to confirm changes.

2.3.2 Use the Ping command

The Ping feature can be used to confirm connectivity to a defined host on an Internet Protocol (IP) network.

1. Press **'Ping'**, to display a page used to confirm the valid IP connection to a specified IP host device.
2. Enter the required web url, IP address or Hostname.
3. Press **'Ping'**, and ensure the dialog shows the number of sent packets matches the number of received packets.

Caution Some IP network may NOT allow the Ping command.



2.3.3 Use the Reboot

The Reboot feature simply performs a power cycle of this device.

2.3.4 Installing Webserver certificates

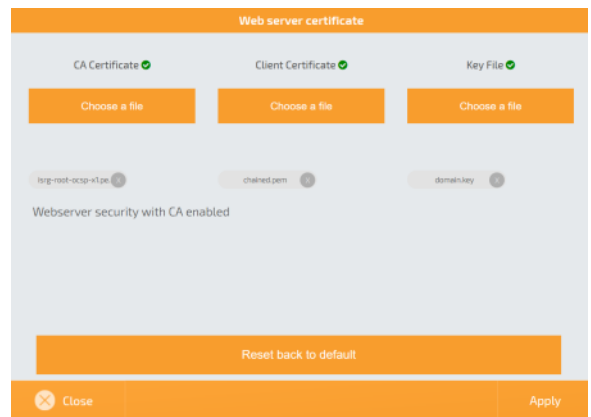
The Webserver certificates feature is used to add compatibility for secure communication using Transport Layer Security (TLS), IP port 443, over a defined domain on a site computer network.

Caution Internet access is required. The site IT team **MUST** provide appropriate https 'base64 pem format' certificates, a valid url for the device, and ensure the site DNS server is set correctly. Do **NOT** distribute certificates without consent from the site IT team.

Remember This hardware is supplied with a self-signed certificate, which only permits secure access to the web page after the user has accepted the risk, as shown in the browser.

1. Press **'Webserver Certificates'** to show a page used to install https certificates applicable to the site domain.
2. Press the appropriate button and select the relevant https security certificate.

- i. Press Client certificate, Choose a file button to show the Open dialog used to locate and select the required Client certificate.



Caution The Client certificate file is used to validate the Key file and CA certificate on selection.

Tip! Choose the Key file first if it includes the Client certificate file, as confirmed by the site IT team.

- ii. Press Key file and CA certificate, Choose a file button to show the Open dialog used to locate and select the required Client certificate.

3. Press **'Apply'** to confirm this certificate and close the page.

Tip! The https web page access can be removed by pressing the **'Reset back to default'** button. The hardware will then use the self-signed certificate. If the hardware fails to respond via https secure web browser access, please have a USB available and contact the office.

4. Use the product hostname, provided by the site IT team, to access this device.

2.3.5 Configure the Email Settings

The **'email settings'** feature is used to define the smtp mail server details required to send (csv) reports to designated email accounts.

The mail process supports standard mail server login process, and OAuth2 authentication standard.

Standard authentication, allowing a simple username and/or password to access the mail server.

OAuth open standard for authentication allowing users to grant third-party access without sharing their credentials. MFA uses a combination of a password, hardware token, and/or a biometric scan to verify the user's identity. OAuth uses tokens to authenticate users.

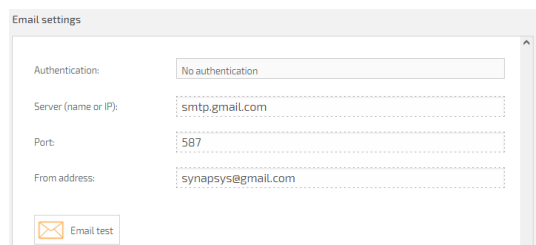
Tip! Having access to the define mail server account, Sent folder, will assist in confirming the test report has been sent.

1. Define the required mail server settings.

Authentication. Used to define the authentication required to send email reports.

- ◆ **No authentication.** Used if the email account on the defined mail server does not require a password.

Server (name or IP). Used to define the mail server used to send reports via email. Set as the Server name, i.e., smtp.gmail.com or local IP address according to local IP Policy.



Tip! A domain mail server (e.g., Office365) or a public mail server (e.g., Gmail, can be used.

Port. Used to define the IP port required to access the defined mail server.

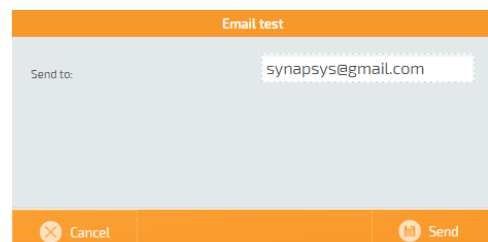
Tip! Typically Port 25 is used for onsite mail server, Port 465 is used for SSL secure encryption connection type and Port 587 is used to TLS (StartTLS) secure encryption connection type.

From address. Used to define the email account in the mail server for sending csv files.

Caution This MUST be a valid/registered email address in the defined mail server.

Email test. Used to launch a page, used to define a mail account that receive a test email, and is used to test the mail server details.

Press the Email test button, enter the mail account used to test the mail server details, and press Send to send the test report.



- ◆ **Login and CRAM-MD5.** Used if the email account on the defined mail server requires a password for the Login to send an email.

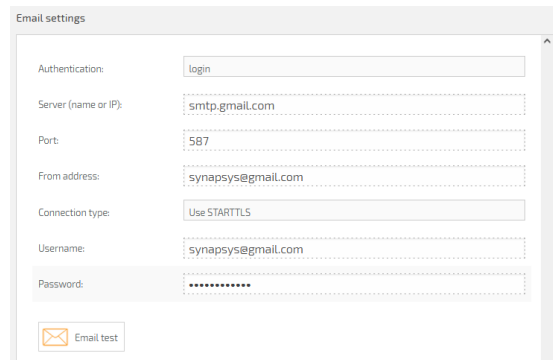
Set mail server details as required.

Server (name or IP). As above.

Port. As above.

Tip!

Typically Port 25 is used for onsite mail server, Port 465 is used for SSL secure encryption connection type and Port 587 is used to TLS (StartTLS) secure encryption connection type.



From address. Shows an email address used to define which device sent the report.

Caution

This MUST be a valid/registered email address if using a local email server.

Connection type. Used to define the secure encryption connection type required by the mail server. Typically, this corresponds to the **Port** settings.

Tip!

Typically Port 25 is used for onsite mail server, Port 465 is used for SSL secure encryption connection type and Port 587 is used to TLS (StartTLS) secure encryption connection type.

Username and Password. Used to define the login credentials required to access the mail account in the defined mail server.

Email test. See above.

- ◆ **Generic OAuth 2.** Used if the email account on the defined mail server requires multi-factor authentication as specified by OAuth2.

Configure mail server as required.

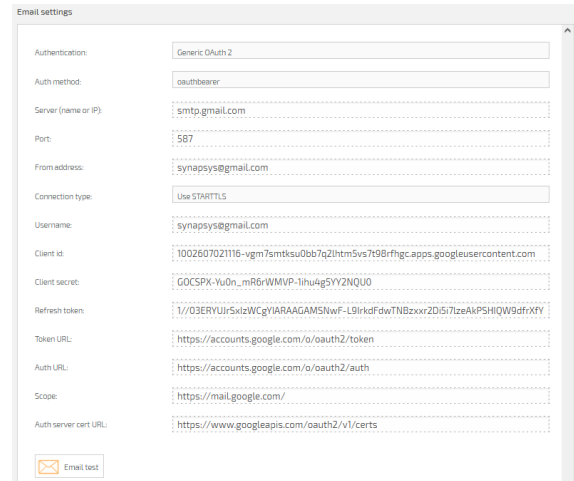
Server (name or IP). As above.

Auth method. Used to define the authentication method required for using the defined mail server.

Port. As above.

Tip!

Typically, Port 25 is used for onsite mail server, Port 465 is used for SSL secure encryption connection type and Port 587 is used to TLS (StartTLS) secure encryption connection type.



From address. Shows an email address used to define which device sent the report.

Caution

This MUST be a valid/registered email address if using a local email server.

Connection type. Used to define the secure encryption connection type required by the mail server. Typically, this corresponds to the **Port** settings.

Username. Used to define the mail account requesting access to the defined mail server.

Tip!

Ensure a valid Username is defined, and is the same as the From address.

Client id. Used to define the string of characters/numbers identifying this device to the mail server. This is provided when configuring the mail server.

Client secret. Used to define the code required to verify/authenticate the **Client id** to the mail server via a string of characters/digits. This ensures the access token request is made only from the configured application, and not from an unauthorised site. This is provided when configuring the mail server.

Refresh token. Used to show the token required to allow the application to access an API and accept new access token.

Token URL Used to define the resource server providing the access token.

Auth URL. Used to define resource server for exchanging an authorization code with an access token.

Scope. Used to define the resource server that specifies what APIs are permitted by this account.

Auth server cert URL. Used to define the resource server certifying the connection to the API.

Email test. See above.

- ◆ **Google OAuth 2.** Used when accessing the Google email account on the defined mail server requires multi-factor authentication as specified by OAuth2.

Caution

Configure the Google mail portal (available from the hyperlink below) before configuring this product mail server settings.

This provides the Client ID and Client secret as required to use the Gmail OAuth 2 authentication and may have already been completed by the site IT team.

<https://console.cloud.google.com/welcome>

Configure the Gmail server as required

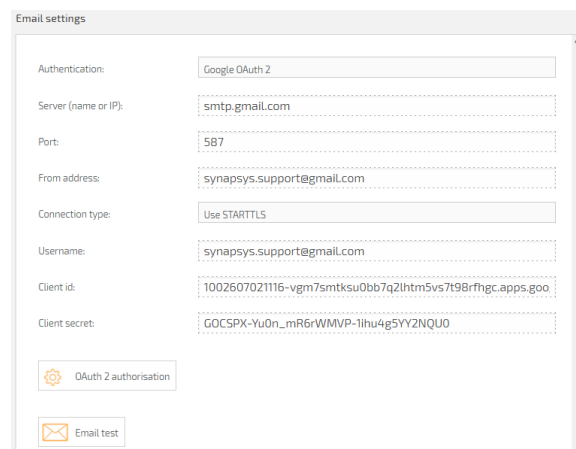
Server (name or IP). As above.

Port. As above.

Tip!

Typically, Port 25 is used for onsite mail server, Port 465 is used for SSL secure encryption connection type and Port 587 is used to TLS (StartTLS) secure encryption connection type.

From address. Shows an email address used to define which device sent the report.



Caution

This MUST be a valid/registered email address if using a local email server.

Connection type. Used to define the secure encryption connection type required by the mail server. Typically, this corresponds to the **Port** settings.

Username. Used to define the mail account requesting access to the defined mail server.

Tip!

Ensure a valid Username is defined.

Client id. Used to define the string of characters/numbers identifying this device to the mail server. This is provided when configuring the mail server.

Client secret. Used to define the code required to verify/authenticate the **Client id** to the mail server via a string of characters/digits. This ensures the access token request is made only from the configured application, and not from an unauthorised site. This is provided when configuring the mail server.

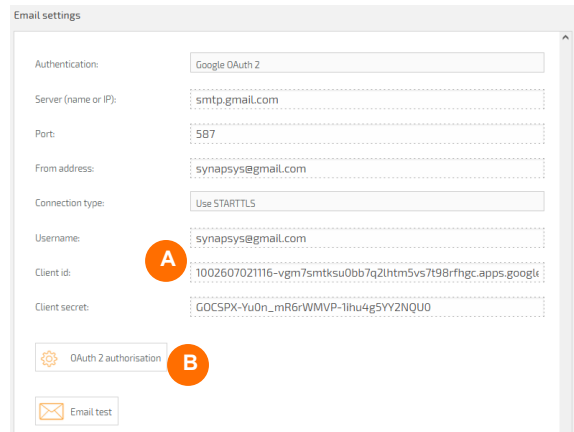
OAuth 2 authorisation. Used to complete the Google Mail server authorisation using the configured Client ID and Client secret to validate this account with the API, see below.

Email test. See above.

To configure **Google OAuth 2** mail server settings, after completing the Google Mail server setup

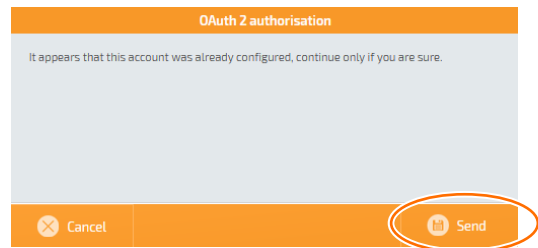
Enter your **Client id (A)** and **Client secret (A)** obtained during the configuration of the Google mail server portal.

Press **Save** to confirm the changes.

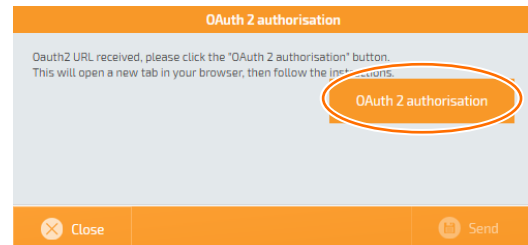


Press **OAuth2 authorisation (B)**, to show a message confirming the mail account is already configured via the Google mail portal.

Press **Send** to overwrite any existing **Client id** and **Client secret** and show a message confirming the OAuth 2 URL has been received.



Press **OAuth 2 authentication** to open a browser and show the Google mail server sign in page.



Tip!

Immediate access is granted if this account is already logged in.

On the web page, ignore the '**Google has not been verified this app**' message and press **Advanced** to show a '**go to (the name of your app) (unsafe)**'. Select '**go to (the name of your app) (unsafe)**' option, read the instructions, press '**Continue**', and wait for the browser to show it is unable to connect.

Ensure the browser shows the product IP Address, edit as necessary.

Example

http://localhost/?code=4/0AWgavddwz... **should** **read**
http://192.168.11.62/?code=4/0AWgavddwz....

Refresh the browser to show the '**Authorization process completed**' message.

Close all unnecessary pages, and test the email process.

- ◆ **Microsoft OAuth 2.** Used if the mail account on the defined Microsoft mail server requires multi-factor authentication.

Caution

Configure the Microsoft Azure portal to provide the Client ID and Client secret as required to use the Microsoft Domain OAuth 2 authentication (available from the link below) before configuring the Microsoft Admin Portal.

<https://portal.azure.com/#home>

Configure the Microsoft Admin portal before configuring this product mail server settings. It may have already been completed by the site IT team.

<https://admin.microsoft.com>

Configure the Microsoft Domain mail server as required

Server (name or IP). As above.

Port. As above.

Tip!

Typically, Port 25 is used for onsite mail server, Port 465 is used for SSL secure encryption connection type and Port 587 is used to TLS (StartTLS) secure encryption connection type.

From address. Shows an email address used to define which device sent the report.

Caution

This MUST be a valid/registered email address if using a local email server.

Connection type. Used to define the secure encryption connection type required by the mail server. Typically, this corresponds to the **Port** settings.

Username. Used to define the mail account requesting access to the defined mail server.

Tip!

Ensure a valid Username is defined.

Client id. Used to define the string of characters/numbers identifying this device to the mail server. This is provided when configuring the mail server.

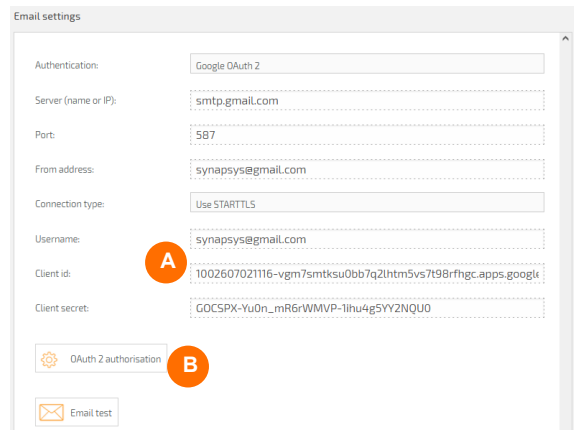
Client secret. Used to define the code required to verify/authenticate the **Client id** to the mail server via a string of characters/digits. This ensures the access token request is made only from the configured application, and not from an unauthorised site. This is provided when configuring the mail server.

- ◆ **OAuth 2 authorisation.** Used to complete the Google Mail server authorisation using the configured Client ID and Client secret to validate this account with the API, see below.
- ◆ **Email test.** See above.

To configure **Microsoft Oauth 2** mail server settings

Enter your **Client id (A)** and **Client secret (A)** obtained during the configuration of the Microsoft Azure portal.

Press **Save** to confirm the changes.



Press **OAuth2 authorisation (B)**, to show a message confirming the mail account is already configured via the Microsoft Azure portal.

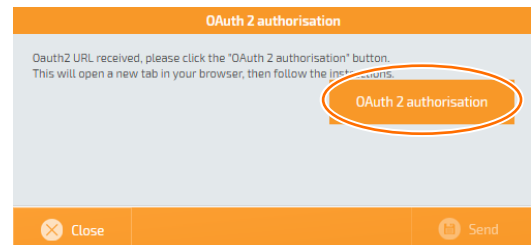
Press **Send** to overwrite any existing **Client id** and **Client secret** and show a message confirming the OAuth 2 URL has been received.

Press **OAuth 2 authentication** to open a browser.



Tip!

Immediate access is granted if this account is already logged in.



The Microsoft Domain Azure portal will show '**Permission requested**', and wait for the browser to show it is unable to connect.

Ensure the browser shows the product IP Address, edit as necessary.

Example

http://localhost/?code=4/0AWgavddwz... **should** **read**
http://192.168.11.62/?code=4/0AWgavddwz....

Refresh the browser to show the '**Authorization process completed**' message.

Close all unnecessary pages, and test the email process.


2.

2.4 MANAGE DRIVERS

The 'Manage Drivers' page is used to get values from parameters in devices connected to a Mitsubishi Electric Centralised Controller via the Melco driver, and allow a required protocol driver, to make these values available to a third-party system, i.e., BACnetIP server, IoT (MQTT/REST server), ModBus Server/Slave (Serial or TCP/IP) or vIQ (Trend BMS).

This product supports a maximum 4 (four) Mitsubishi Melco driver instances, e.g., 1 Melco driver instance per centralised controller, and the following interface drivers, 1 x BACnetIP, 1 x IoT: MQTT/REST Server, 1 x ModBus Server/Slave, and 1 x vIQ (Trend BMS).

2.4.1 Manage the required drivers

1. From the main menu, select 'Manage Drivers' to a page that permits the specification of the required Drivers.
2. Press '' to automatically add a default driver.

Manage drivers

Drivers	Instance	Port	Alias
EMT	1	ETHERNET 0	Dashboard
vIQ	1	ETHERNET 0	UDPS7620
BACnet	1	ETHERNET0	
BACnet MSTP	1	SERIAL2	
Mbus Master	1	Slave Mbus Master 2	
Mbus Master	2	ETHERNET	
Modbus Master	1	ETHERNET	
Modbus Slave	1	SERIAL1	
MQTT Client	1	ETHERNET	
REST client	1	ETHERNET	
Trend	1	ETHERNET	
Modbus Master	2	ETHERNET	

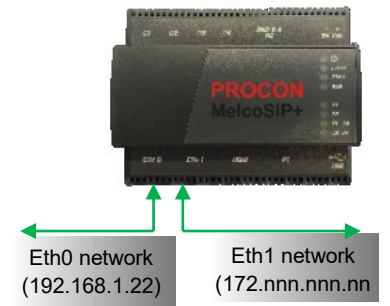
>

3. Select the required Driver from the available options.

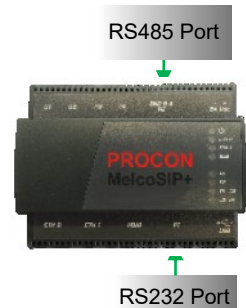
- Select the **'Port'** type related to the specified Driver, e.g., Melco driver with **'Ethernet'** port will communicating with the Mitsubishi Centralised Controller according to the subnet range of the selected IP port.


Caution **The Trend BMS network (connected via the vIQ driver) MUST be physically connected to 'Eth0' and in a compatible IP address range.**

- Select Ethernet for the connection via either **'Eth0'** or **'Eth1'** port.



- Select Serial 1 for the connection via the RS232 port. Used for ModBus Slave Serial Master supporting RS232 connectivity.
- Select Serial 2 for the connection via the RS485 port. Used for ModBus Slave Serial Master supporting RS485 connectivity.



- If necessary, type a meaningful label in the **'Alias'** field. This is to provide a simple method of identifying the purpose of the corresponding driver.
- Press  to show a page used to define the communications setting according to the selected driver and port combination.

2.4.2 Manage Melco Driver Settings

When 'Driver' is **Melco** and the 'Port' is 'Ethernet' set the Melco comms settings.

Each Melco driver supports a connection to 1 (one) Mitsubishi Centralised controller, e.g., 1 x AE200 and 2 x EW50 (150 indoor units max) is total of 3 x Melco drivers.

Tip! Synapsys Solutions products terminate and re-establish the IP connection to allow other products to query the device.

On the 'Settings', if necessary, change the **IP Address**, **VFC type**, **New setting comparison**, **Polling Interval**, and **Energy** parameters, used to define the slave communications requirements.

IP Address. Used to define the centralised controller providing M-Net device values.

VFC type. Used to determine the VFC (Volt-Free Contact) action required to assert the fire alarm. Set **Make on fire** to close the VFC and assert a fire alarm via the 'Forced-Off' message to the centralised controller. Set **Break on fire** to open the VFC and assert a fire alarm via the 'Forced-Off' message to the centralised controller.

IP address:	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="1"/> <input type="text" value="1"/>
VFC type:	<input type="text" value="Make on fire"/>
New setting comparison:	<input type="text" value="On"/>
Polling interval:	<input type="text" value="30 seconds"/>
Energy:	<input type="text" value="Disabled"/>

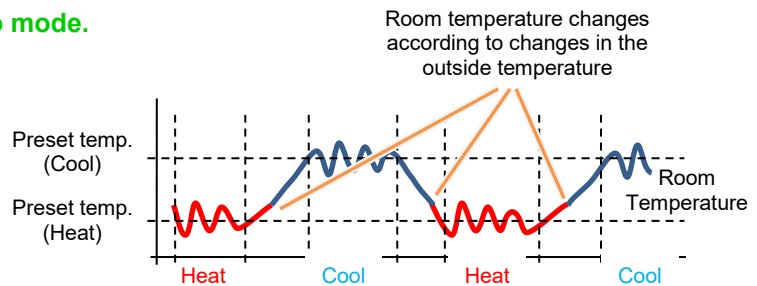
Tip! Ensure the VFC is connected to the U1 port. The VFC type sends the 'Forced-Off' Set command to the centralised controller every 5secs. While the 'Forced-Off' is Set all connected indoor units are switched off and all remote-controllers are disabled until the 'Forced-Off' Reset command is issued. This ensures that any subsequent 'Forced-Off' command sent via the linked interface driver is not overridden.

Dual setpoint. Used to define the operation of centralised controller as single Setpoint mode, i.e., as per Mitsubishi AG150 and earlier AC controllers, or dual Setpoint mode, i.e., as per the Mitsubishi AE200. When the operation mode is set to the Auto (dual set point) mode, two pre-set temperatures (one each for cooling and heating) can be set. Depending on the room temperature, indoor unit will automatically operate in either the Cool or Heat mode and keep the room temperature within the pre-set range. Set **'On'** when the compatible centralised controller is in Auto mode and when the operation mode is set to Auto or Setback and all indoor units support two setpoint temperatures for Cool mode and Heat mode. Set **'Off'** when the centralised controller is in Auto mode and when the operation mode is set to Auto or Setback any indoor unit on the M-Net does not support two setpoint temperatures.

Caution **The Dual Setpoint mode function is supported only when all connected indoor units, remote controllers, and system controllers in the given group features the function.**

Tip! **Refer to Mitsubishi Centralised controller documentation, for details about Dual Setpoint functionality.**

Example **Dual Setpoint in Auto mode.**

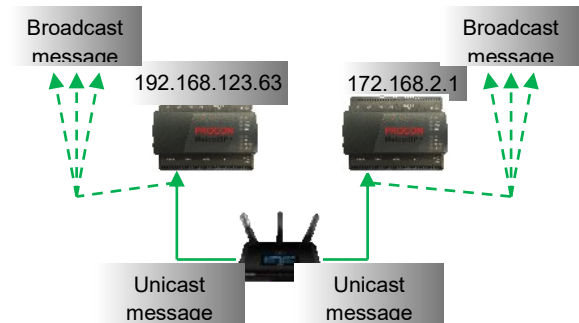


2.4.3 Manage BACnetIP Driver Settings

When 'Driver' is 'BACnet', the 'Port' is either Ethernet 0 or Ethernet 1, configure the BACnetIP comms settings.

Remember This product only permits 1 (one) BACnet driver instance.

BBMD enable. Used to allow this device to receive a unicast 'Who-is' message from a device on a different subnet range and send a 'Who-is' broadcast message to devices in this subnet range. It is used in conjunction with the 'BDT List' and 'FD List' pages shown beside the 'Settings' option.



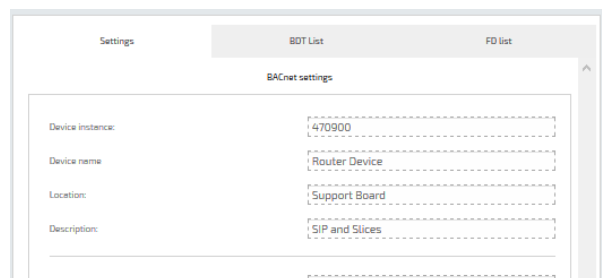
Tip! IP routers do NOT permit broadcast messages. A BBMD (BACnet Broadcast Message Device) sends a unicast message to the specified BBMD device on the other subnet range.

Note A 'Who-is' message is sent by other BACnet devices that need to acquire the address information of other devices without creating more network traffic. Other BACnet devices respond with an 'I-am' message. This hardware automatically send an 'I-am' message on start-up.

On the 'Settings', if necessary, change the hardware BACnet 'Device instance', 'Device name', 'Location' and 'Description' settings.

Device instance (range 0 to 4194303), Used to identify this device in the BACnetIP network via a numeric reference.

Tip! Use the first 4 digits as a reference to the BACnet network, i.e., Network 4709 is Device instance 4709000.



Device name. Used to identify this device in the BACnetIP network via a Human readable identifier.

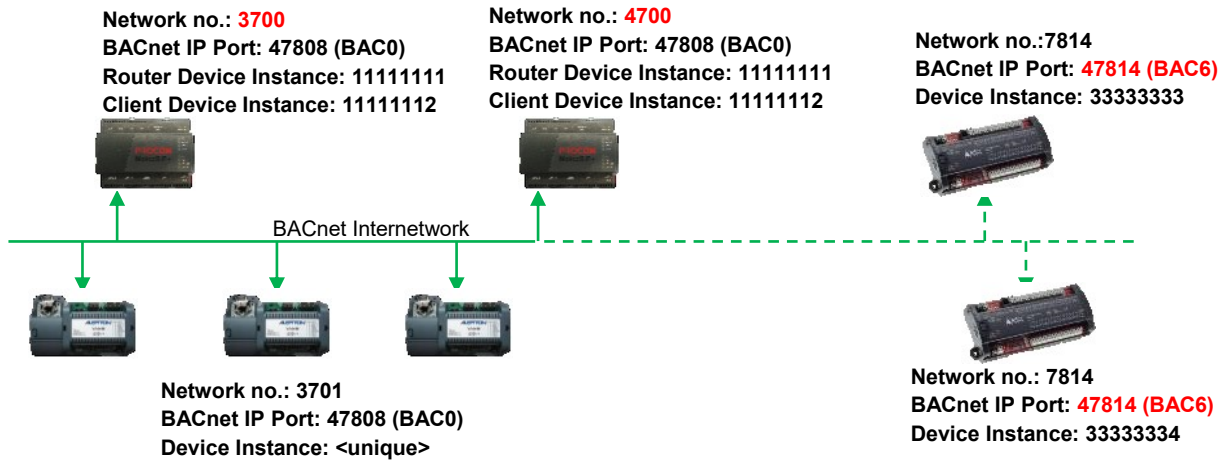
Caution Use third party BACnet explorer to ensure the 'Device instance' and the 'Device name' is unique.

Location. A freeform location text used to indicate the physical location of this product in the BACnet/IP based control system.

Description. A freeform text field.

On the 'Settings', if necessary, change the hardware BACnet '**Network number**', '**BACnet IP Port**', '**DCC Password**', '**Time sync**' and '**Accept object changes from BACnet**' settings.

Network number (range 1 to 65534, default: 0)) and '**BACnet IP Port**' (range 0 to 65535, default: 47808(BAC0)). Used to define the connection of this device and the virtual BACnet client device on the BACnetIP network.



Caution Ensure a unique '**Network number**' is configured for each product on the BACnetIP network and all devices that need to communicate with each other are using the same '**BACnetIP Port**'.

DCC Password. Used to permit the DCC (Device Communication Control) and RD (Reinitialise Device) operations.

Time sync. Used to enable/disable a time synchronization broadcast message from a Time Master device (client) to adjust the time and date in this device.

Accept object changes from BACnet (i.e., Read Only). Used to enable/disable changes to Object instance values in this device.

Description:	<input type="text"/>
Network number:	<input type="text" value="3708"/>
BACnet IP port:	<input type="text" value="47808"/>
DCC password:	<input type="text"/>
Time sync:	<input checked="" type="checkbox"/>
Accept object changes from BACnet:	<input checked="" type="checkbox"/>
When in min:	<input type="text" value="0"/>

Who-is min and **Who-is max** (Service Parameters). Used to define the range of addresses that are expected to respond to the **'Who-is'** message sent from this device.

APDU Timeout' and **APDU retries**. Used to define the number of ms this device will wait until repeating the request, and the number attempts the request will be made respectively.

Tip! Only set **'Slow mode'** following instruction from Synapsys Solutions.

Points failure threshold. Used to define the number of consecutive failed requests from a device to determine when a communications failure state is indicated.

ACCEPT OBJECT CHANGES FROM BALANCE: ON

Who is min:

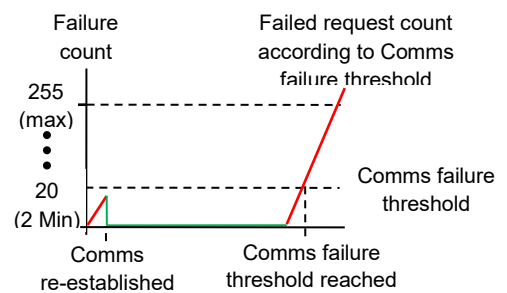
Who is max (max 4194303):

APDU timeout (milliseconds):

APDU Retries:

Slow mode: OFF

Points fail treshold:



On the 'BDT List', change as necessary

- ◆ Press 'BDT List' manage the BBMD references for devices on different subnet ranges.

Press '+' to add a BBMD reference. Enter the BACnet BBMD IP Address.

If necessary, change the Remote UDP (BACnet network number).

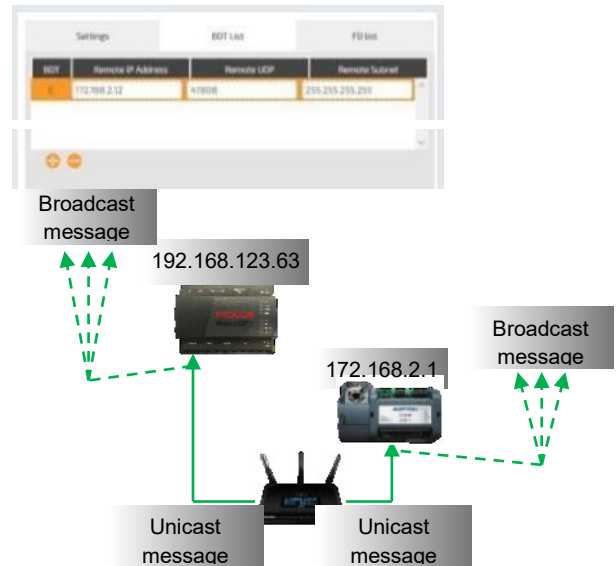
Tip!

The 'Remote subnet' should remain at 255.255.255.255. This will allow the broadcast 'Who-is' message across the entire 'Remote IP Address' range.

Press '-' to remove a selected BBMD reference.

Caution

Ensure the BACnet Device on the other subnet range is suitable.



On the 'FD List', change as necessary

- ◆ Press 'FD List' (Foreign Device List) showing a list of devices on different subnet ranges, the TTL (Time To Leave) and Seconds Remaining.

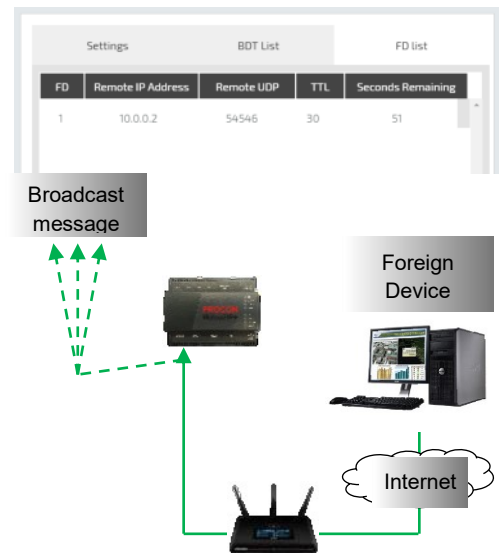
Note

The details will be removed when the TTL has occurred.

- ◆ Press 'Cancel' or 'OK' as appropriate.

Caution

Appropriate IT rules will be required for inbound BACnet connectivity.



2.4.4 Manage Data Acquisition Driver Settings

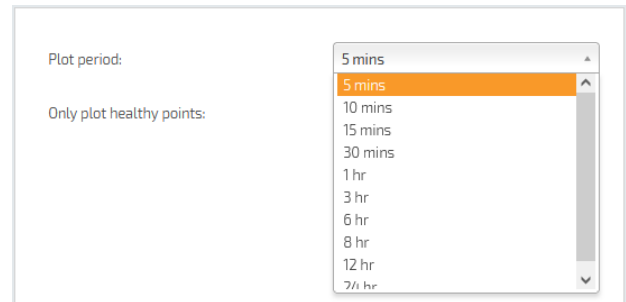
When the driver is 'Data Acquisition' and the 'Port' is 'Ethernet', set the Data Reporting settings.

On the 'Settings', if necessary, change the 'Plot period', and the 'Only plot healthy points' to define the data reporting file constraints.

Plot period. Used to define when the value is logged to the database.

Tip!

The relationship between the Plot period and the total number of datapoints being plotted determines the amount of historic data that is stored.

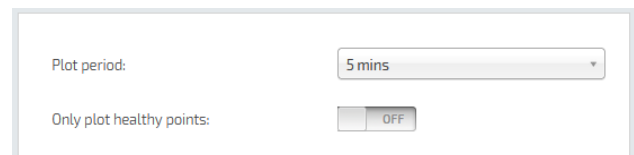


Plot period: 5 mins
5 mins
10 mins
15 mins
30 mins
1 hr
3 hr
6 hr
8 hr
12 hr
7 1/2 hr

Only plot healthy points. Used to set a report field to null/empty if the data source fails to provide a value.

Tip!

A synchronised timestamp and a real timestamp are logged in the internal database.



Plot period: 5 mins
Only plot healthy points: OFF

- Press 'Cancel' or 'OK' as appropriate.

Caution

Ensure the Data Acquisition reporting time is after 02:00 to allow all AE200 energy data to be processed.

2.4.5 Manage ModBus Server/Slave Driver Settings

When 'Driver' is **ModBus Slave** and the 'Port' is

- 'Serial 1' set the RS232 comms settings
- 'Serial 2' set the RS485 comms settings

When 'Driver' is **ModBus Slave** and the 'Port' is 'Ethernet' set the ModBus TCP/IP comms settings

On the 'Settings', if necessary, change the **Port number** and **TCP Timeout** parameters are used to define the slave communications requirements.

Remember **ModBus TCP/IP is an Ethernet network. Multiple masters are permitted but are dependent on connected servers/slaves.**

Port number (default: 502). Used to define the IP Port used for ModBus TCP/IP comms with this ModBus Slave driver.

Tip! **Ensure PC firewall is not preventing Modbus TCP/IP comms via port 502.**

Connection type:	TCP/IP
Port number:	<input type="text" value="502"/>
TCP server timeout (seconds)	<input type="text" value="180"/>

TCP server Timeout. Used to define the required number of seconds necessary to determine when this hardware considers the ModBus TCP/IP Master has disconnected.

When 'Driver' is 'ModBus Slave' and the 'Port' is 'Serial 1', configure the ModBus RS232 comms settings, or if the 'Port' is 'Serial 2' set the ModBus RS485 comms settings.

Remember **ModBus RS232 is a single Master to a single slave connection. ModBus RS485 driver is a daisy-chained network of up to 32 unique slave addresses.**

- ◆ If necessary, select the required **'Baudrate'**, **'Parity'**, **'Data bits'**, and **'Stop bits'**. These values must be the same as the connected slave.

Connection type:	RS232
Baudrate:	<input type="text" value="9600"/>
Parity:	<input type="text" value="None"/>
Data bits:	<input type="text" value="8"/>
Stop bits:	<input type="text" value="1"/>

Baud: Data transmission speed in bps (bits per second).

Parity: Request Packet checking.

Data bits: Number of bits used for the data.

Stop bits: Number of bits used to signify the end of the ModBus message.

2.4.6 Manage MQTT Driver Settings

When 'Driver' is 'MQTT' the 'Port' is Ethernet, configure the IoT: MQTT comms settings.

Caution MQTT requires an MQTT Broker. This can be an independent device, or available from the cloud-based application.

Tip! An MQTT connection to Goggle IoT core requires TLS connection using CA certificate. This is generated when creating a Key Pair. The Key pairs can be created using OpenSSL following the guidance given on the Google IoT documentation.

<https://cloud.google.com/iot/docs/how-tos/credentials/keys> --- "Generating an RS256 key with a self-signed X.509 certificate"

On the 'Settings', if necessary, change the 'Client ID', 'Broker Address', 'IP Port', 'Version', 'Keep Alive', and 'Batch Publishing' parameters are used to define the requirement of the connection to the MQTT Broker, and are available from the provider.

Tip! The MQTT Broker connection details are available from the provider.

Client ID. Used to identify this device to the MQTT Broker.

Example Google IoT Core uses
`projects/{project-id}/locations/{cloud-region}/registries/{registry-id}/devices/{device-id}`

Broker Address. Used to identify the MQTT Broker being used, according to the MQTT host name or IP address. This configuration is dependent on the Broker.

Example Google IoT Core uses
`mqtt.googleapis.com`

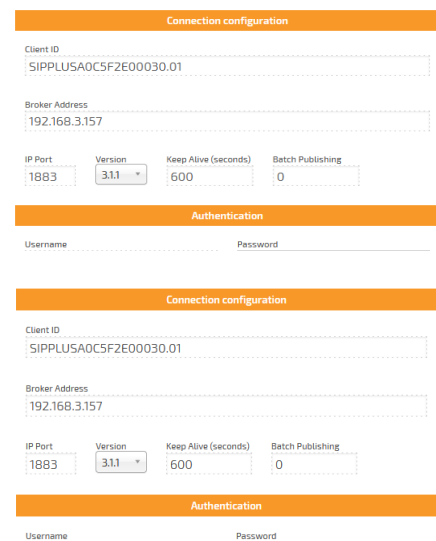
IP Port. Used to define the IP network port used for the MQTT protocol connection. Default: 1883.

Caution When using TLS encryption, change IP Port to '8883'.

Version. Used to define the MQTT specification version required to connect to the Broker.

Keep Alive (Seconds). Used to define the period of inactivity in seconds until a 'Keep alive' message is sent to the Broker.

Batch Publishing. Used to define the number of seconds before the last recorded values are Published as a single payload to the Broker.



The image shows two screenshots of a configuration interface. The top screenshot is titled 'Connection configuration' and contains the following fields: Client ID (SIPPLUSA0C5F2E00030.01), Broker Address (192.168.3.157), IP Port (1883), Version (3.1.1), Keep Alive (seconds) (600), and Batch Publishing (0). Below this is an 'Authentication' section with fields for Username and Password. The bottom screenshot is identical to the top one, showing the same configuration details.

On the 'Settings', if necessary, change the 'Username', 'Password', 'TLS', and 'CERT/PSK' parameters are used to define the required authentication for the connection to the MQTT Broker.

Tip! The Authentication details should be available from the provider.

Username. Used to identify the user requiring access to the MQTT Broker. This configuration is dependent on the MQTT Broker.

Example Google IoT Core uses

`google-iot-core.jwt`

Microsoft Azure uses

`"{iothubhostname}/{device_id}/?api-version=2018-06-30"`

where the `iothubhostname` is the full name of the IoT Hub and the `device_id` is the client id (as per above).

Password. Used to define the password related to the User requiring access to the MQTT Broker. This configuration is dependent on the MQTT Broker.

Example Google IoT Core uses

`{project-id}`

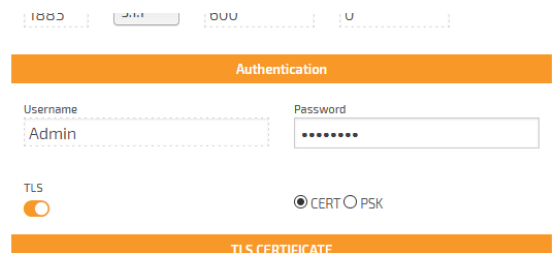
Microsoft Azure uses

SAS Token, refer <https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-mqtt-support>

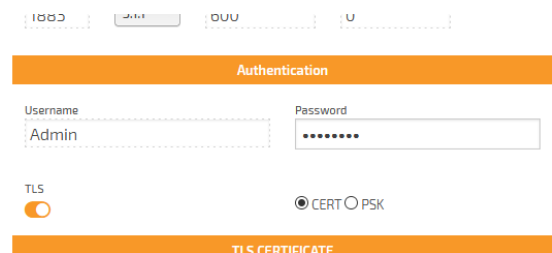
TLS. Used to define the encryption required for compatibility with the Broker. If enabled (*On*) the TLS security encryption is required by the Broker, and certification will be necessary. If disabled (*Off*) the MQTT does NOT require TLS encryption.

CERT or PSK. Used to allow the configuration of the selected TLS security encryption. Enable **CERT** to show each of the forms of certification, and the required password option. Enable **PSK** to show the Pre Shared ID and Pre Shared Key certification option.

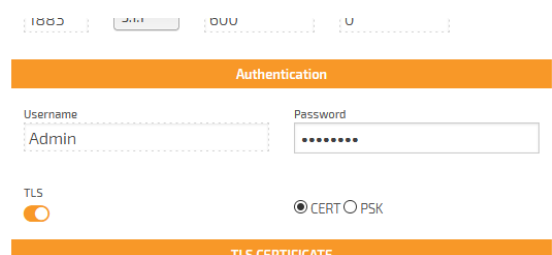
Tip! The necessary TLS security certificates are dependent on the Broker and should be available from the provider.



The screenshot shows a configuration interface with a top navigation bar containing 'Home', 'Settings', 'Device', and 'User'. Below this is an 'Authentication' section with a 'Username' field containing 'Admin' and a 'Password' field with masked characters. The 'TLS' section has a radio button for 'On' selected and 'CERT' selected under the 'CERT/PSK' options. A 'TLS CERTIFICATE' section is visible below.



This screenshot is identical to the one above, showing the 'Authentication' and 'TLS' configuration options in the MQTT Broker settings.



This screenshot is identical to the previous ones, showing the 'Authentication' and 'TLS' configuration options in the MQTT Broker settings.

2.4.7 Manage REST Server Driver Settings

When the Driver is 'REST server', the 'Port' is Ethernet, configure the REST comms settings.

https: Defines the type of connection, standard or secure, to the REST client on local IP network. Set *On* to connect via a secure http (https:) using port 443. If *Off* a standard http connection using port 80 is used.



Caution Compatibility with https: networks, requires a secure http certificate and key file. A self-signed certificate is loaded by default. Device dedicated certificates can be uploaded via the Global settings page.

2.4.8 Manage vIQ Driver Settings

When the driver is 'vIQ' and the 'Port' is 'Ethernet 0' set the vIQ comms settings.

On the 'Settings', if necessary, change the **VCNC** (Virtual Communications Node Controller), parameters '**Node(s)**', '**Port(s)**', and '**Timeout(s)**' to configure the 'vIQ' Trend LAN connection to the Trend network.

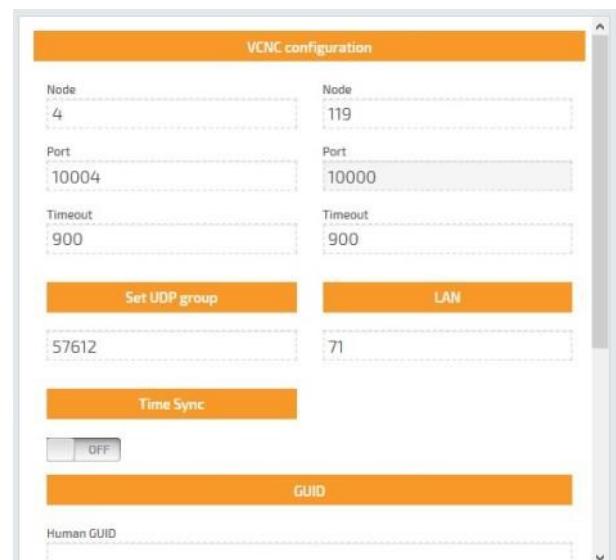
Tip! vIQ does not include modules that count towards the licence limit when used as a connection to the Trend Internetwork.

Node. Used to define a **VCNC** node (1 (one) to 119) for this connection to this Trend LAN on the Trend network.

Caution A Node is equivalent to an OS that is represented by the corresponding OS in the Trend BMS and MUST be unique. Node 2, Node 3, and Node 10 are reserved.

Port. Used to define a **VCNC** IP Port number related to the Node (1 (one) to 119) for this connection to this Trend LAN on the Trend network.

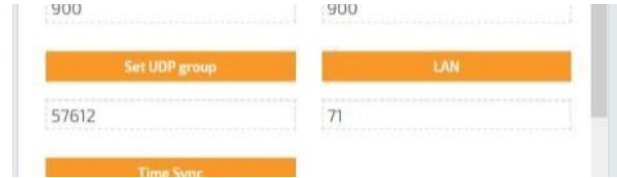
Tip! When adding multiple products to a single Trend LAN, increase the lowest 'Node' and 'Port' number by 1 (one), but decrease the highest 'Node' and 'Port' number by 1 (one).



Timeout. Used as a countdown timer to determine when the connection to the defined UDP group has failed.

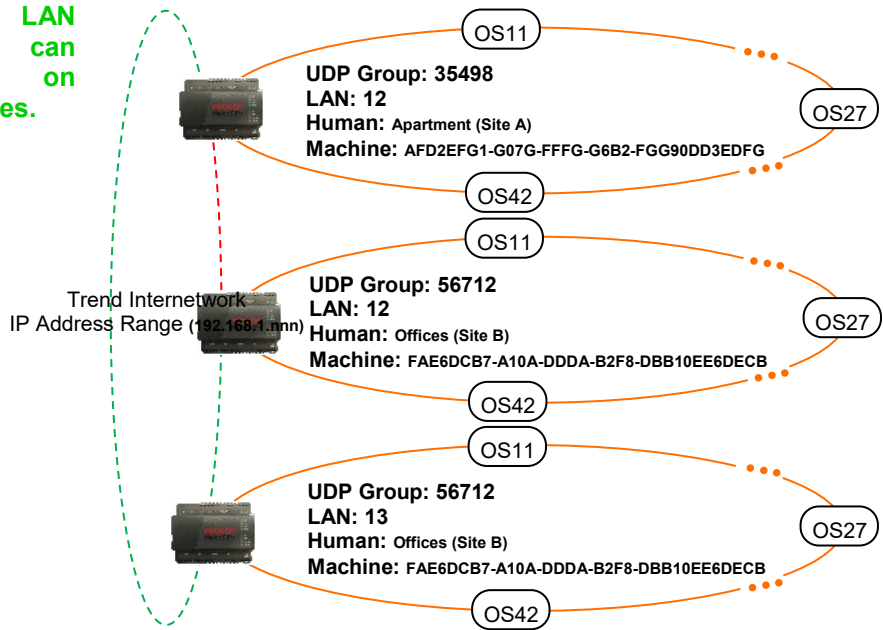
On the 'Settings', if necessary, change the 'Set UDP group', and 'LAN' to define network of compatible Trend devices.

UDP (User Datagram Protocol/group number). Used to establish low-latency and loss-tolerating connections with other Trend devices in the group, on the compatible IP address range.



Tip!

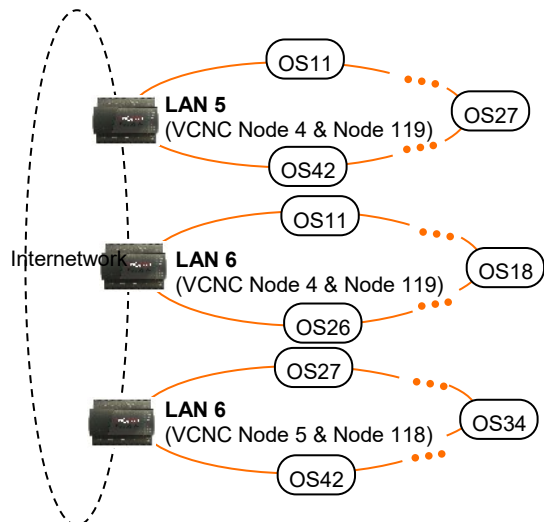
The same LAN number can appear on separate sites.



LAN. Used to identify a group of devices on the Trend network via a numeric reference.

Note

An Internetwork is a communication link between Trend LANs, (Local LAN is local to the connection, and Remote LAN a Local Area Network (LAN) accessed from the reference device via the Internetwork). A Trend LAN is a number of connected nodes; each node is used to connect a LAN, i.e., the VCNC port.



On the 'Settings', if necessary, change the 'Time Sync', used to provide compatibility with a Trend TimeMaster.

Time Sync. Used to allow the internal date/time to be controlled by a Trend Timemaster. Enable (On) the 'Time Sync' to allow the Trend Timemaster to update the internal time settings. If disabled (Off) the Trend Timemaster will NOT change the internal time settings.

Set UDP group: 57612 LAN: 16

Time Sync: ON

GUID: Support

Caution **Do NOT configure an NTP Server if using the SIP+ Time zone setting, BACnet time synchronisation or Trend Timemaster.**

On the 'Settings', if necessary, change the 'GUID', to provide a meaningful location name for asserted Trend alarms.

Human GUID. Used to identify the Trend BMS site that this product is assigned to.

Machine GUID. Used as a unique site identifier and must be identical in each device.

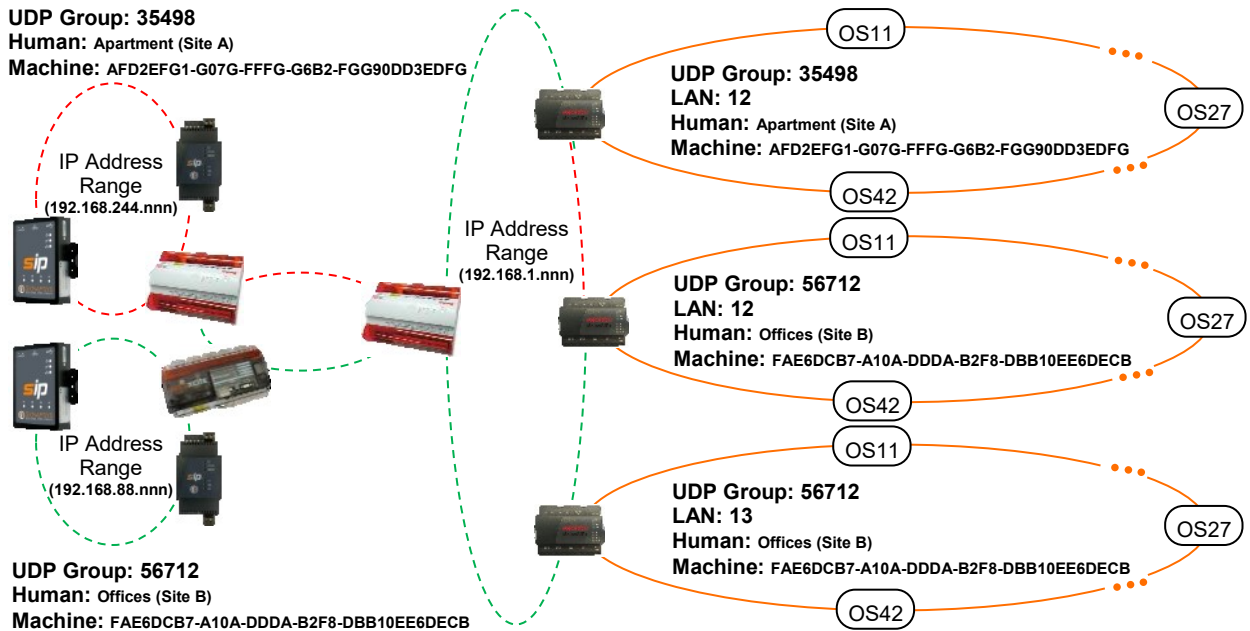
Time Sync: ON

GUID: Support

Human GUID: Support

Machine GUID: FAE6DE7D-A2D0-F13C-C65A-DBC470E6F22D

Trend network status



Caution **The GUID MUST be configured to ensure module labels are shown in multi-site system.**

The **Trend network status** parameters are used to show the current state of the Trend network.

Trend network status. Used to display a dialog showing the status of the system, LAN, and Internetwork. It can be used to diagnose and indicate network problems.

Tip! This  button is also available from the Trend Client driver when vIQ is the connection type.

PARAMETER	DESCRIPTION
System Uptime	The amount of time this product has been operating, i.e. since this product was last turned on or rebooted.
Lan OK Time	The amount of time the Lan has been successfully communicating on the Trend network, i.e., since the last build process was successful.
Lan Status	The current condition of the Lan corresponding to this product and the time remaining until a 'Timeout' will occur.
	Lan POWERUP The Lan build process is starting.
	Lan DEAF The comms with other Trend network devices is not applicable (only 1 (one) device in Lan) or not available (more than 1 (one) device in Lan, see ' <i>Lan BROKEN</i> ').
	Lan BROKEN A comms failure with other devices on the Lan. Typically, due to a timeout caused by Ethernet wiring or connection problem, an IP address that is sending but not receiving messages, duplicate OS numbers from identified IP address on the Lan or when a Lan is changed, i.e., identified IP address is added or removed.
	Lan BUILT The Lan build process is successful.
	Lan OK! Successful Lan comms are detected if product is not alone on local Lan or if it can communicate with other devices on the local Lan.
Last Lan Message	The last message from describing the Lan status, see 'Lan Status'.

continued...

PARAMETER	DESCRIPTION										
continued...											
Internetwork OK Time	The amount of time the Internetwork has been successfully communicating, i.e. since the last Internetwork build process was successful.										
Internetwork Status	The current condition of the Internetwork assigned to this product and the time remaining until a 'Timeout' will occur.										
	<table border="0"> <tr> <td>Internetwork POWERUP</td> <td>The Internetwork build process is starting.</td> </tr> <tr> <td>Internetwork DEAF</td> <td>The comms with other Trend network devices is not applicable (only 1 (one) device in Internetwork) or not available (more than 1 (one) device in Internetwork, see '<i>Internetwork BROKEN</i>').</td> </tr> <tr> <td>Internetwork BROKEN</td> <td>An Internetwork comms failure. Typically, due to a timeout caused by an Ethernet wiring or connection problem, duplicate Lan numbers from an identified IP address on the Internetwork or when the Internetwork is changed, i.e., identified IP address is added or removed.</td> </tr> <tr> <td>Internetwork BUILT</td> <td>The Internetwork build process is successful.</td> </tr> <tr> <td>Internetwork OK - Timeout in <i>nn</i></td> <td>Successful Internetwork communications and number of seconds until Timeout is detected, i.e., when '<i>nn</i>' shows '00'.</td> </tr> </table>	Internetwork POWERUP	The Internetwork build process is starting.	Internetwork DEAF	The comms with other Trend network devices is not applicable (only 1 (one) device in Internetwork) or not available (more than 1 (one) device in Internetwork, see ' <i>Internetwork BROKEN</i> ').	Internetwork BROKEN	An Internetwork comms failure. Typically, due to a timeout caused by an Ethernet wiring or connection problem, duplicate Lan numbers from an identified IP address on the Internetwork or when the Internetwork is changed, i.e., identified IP address is added or removed.	Internetwork BUILT	The Internetwork build process is successful.	Internetwork OK - Timeout in <i>nn</i>	Successful Internetwork communications and number of seconds until Timeout is detected, i.e., when ' <i>nn</i> ' shows '00'.
Internetwork POWERUP	The Internetwork build process is starting.										
Internetwork DEAF	The comms with other Trend network devices is not applicable (only 1 (one) device in Internetwork) or not available (more than 1 (one) device in Internetwork, see ' <i>Internetwork BROKEN</i> ').										
Internetwork BROKEN	An Internetwork comms failure. Typically, due to a timeout caused by an Ethernet wiring or connection problem, duplicate Lan numbers from an identified IP address on the Internetwork or when the Internetwork is changed, i.e., identified IP address is added or removed.										
Internetwork BUILT	The Internetwork build process is successful.										
Internetwork OK - Timeout in <i>nn</i>	Successful Internetwork communications and number of seconds until Timeout is detected, i.e., when ' <i>nn</i> ' shows '00'.										
Last Internetwork Message	The last message from describing the Internetwork status, see 'Internetwork Status'.										

Tip! If necessary, use 'SIP Search' to ensure IP Addresses are unique. Use Trend 'ipTool' to ensure Lan numbers (and VCNC Node numbers where necessary) are unique.

- Press 'Save' to confirm changes.

Tip! Use the context menu and select 'Delete Driver' to remove any driver(s) that is NOT required.



2.5 DEFINE POINTS

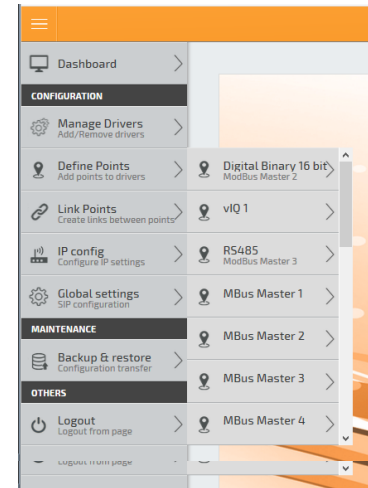
The 'Define points' page is used to configure required input points related to the selected protocol driver and expected output (BACnet server and/or Trend BMS) driver points.

2.5.1 Define the protocol driver point

1. From the main menu, select '**Define Points**' to show the next menu that permits the selection of a configured Driver.
2. Select the required driver to show the driver related configuration pages.

Caution **Unlink points before changing an existing 'Defined Points' configuration and then re-link.**

Do NOT link multiple drivers together, e.g., Mitsubishi Melco to vIQ Sensor to REST Server point.



2.5.2 Define Melco Driver Points

This page is used to discover supported Mitsubishi Centralised controller point types on the compatible IP network and define the parameters to be linked for reporting.

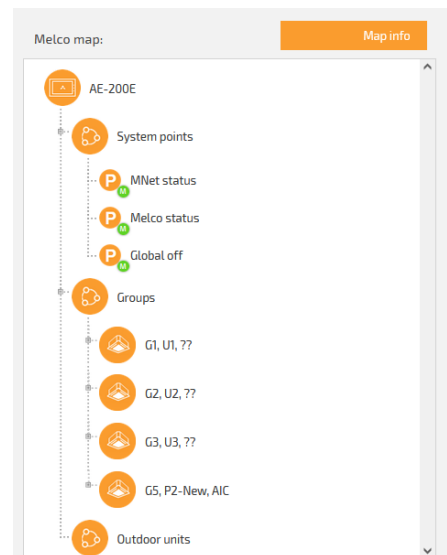
Caution **Ensure Dual Setpoint is disabled if any indoor unit connected to the centralised controller has only a single setpoint.**

This product does not support QAHV and CAHV units.

1. If the driver is Melco, a single Mitsubishi centralised controller as defined on **'Manage Drivers'** page can be discovered. This will display all available System points, Groups, and Outdoor unit points.
2. Discover all devices connected to the centralised controller at the IP address defined in the Manage driver page.
 - i. Select **'Map empty'** and press **'Refresh'** to discover all devices/points available from the centralised controller.
 - ii. Press the disc to expand the required point types, e.g., **'System points'**, **'Groups'** (inc. **Units, Un**) or **'Outdoor units'**, and show available parameters.

Tip! **Use 'Delete' to remove Melco map. This can be used to confirm connectivity with the centralised controller and will not affect the configuration of this product.**

Press 'Map info' to show the current state of the Melco Map.



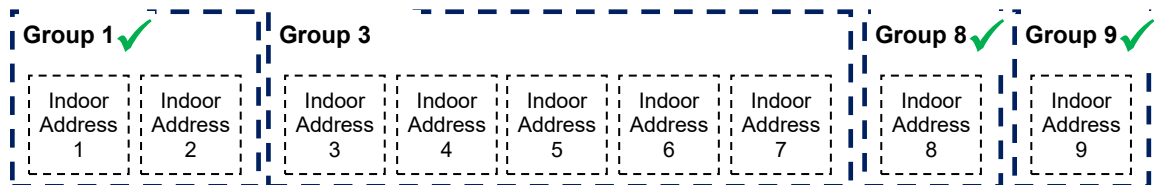
OBJECT TYPE	DESCRIPTION
System points	Shows specific parameters that relate to the AC system
Groups	Shows specific parameters that relate to units/devices in a configured Group of devices on the M-Net network
Outdoor units	Shows specific parameters that relate to outdoor AC devices on the M-Net network

- iii. Press the disc to expand the required ‘Groups’ (e.g., G1, U1) to show the Group indoor unit parameter labels.

Tip! Press the disc to show individual indoor unit Error Code parameter.

Caution The AC network configuration MUST adhere to the Mitsubishi criteria, i.e., the Group number MUST be the lowest indoor unit address.

Example Valid Indoor Unit/Group addressing



- iv. Drag the required AC network device points to the table, as below. A message confirms the point is added to the configuration. Each column is automatically populated according to the AC network device type and can be edited as required.

Tip! The ‘Name’ column shows a unique label, automatically generated relating to the centralised controller details, i.e., <Group no.><Device parameter>.

Remember Alternatively, manually edit the row indicated by ‘>’ if required AC network device points are already known and/or ‘Duplicate/move’ if a similar point(s) already exist.

Melco map: Map info

- G3, U3, 77
- G5, P2-New, AIC
- Room temperature
- Temperature setpoint
- Mode
- Fan speed
- On/Off
- Air direction
- Inhibit
- Filter sign
- U5, AIC

Point list:

	Group	Unit	Type	Melcopoint	Access	Name
	5	-	AIC-IC	Room temperature	R/O	G5 Room temperature
	5	-	AIC-IC	Temperature setpoint	R/W	G5 Temperature setpoint
	5	-	AIC-IC	Mode	R/W	G5 Mode
	5	-	AIC-IC	Fan speed	R/W	G5 Fan speed
	5	-	AIC-IC	On/Off	R/W	G5 OnOff
	5	-	AIC-IC	Air direction	R/W	G5 Air direction
	5	-	AIC-IC	Inhibit	R/W	G5 Inhibit
	5	-	AIC-IC	Filter sign	R/W	G5 Filter sign
	5	5	Unit	Error code	R/O	G5 U5 Error code
						>

Tip! Use the ‘Map mismatch’ button to indicate any configured AC network device points that are NOT available in the current ‘Melco map’.

- 3. Press ‘Save’ to confirm changes.

2.5.3 Define BIC (BACnet Server) Driver Points

The BACnet Server Driver is the Synapsys Solutions BACnet BMS compatible software. It provides a connection to the BACnetIP network, via the defined network details configured in the Manage Driver, Comms settings. This driver supports interfacing to a maximum 100 BACnet BICs (BACnet Integrated Controllers). Each BIC will appear as an individual BACnet controller.

Caution This product will NOT get values from devices connected on a BACnet BMS.

To create a virtual BACnet (server)

1. Press **'Add'** to display a page required to define the required BACnet Server device details. Each virtual BACnet server supports a full range of BACnet Object types and parameter, Notification classes and Trendlogs.

Tip! A **'Device instance'** and **'Device name'** is automatically set according to previously defined BACnet Router and any existing BACnet servers.



Press **'Delete'** to remove the selected BACnet Server device and any configured BACnet Object types.

Press **'Edit'** to show page used to change the selected the 'Device instance', 'Device name', 'Location' and/or 'Description'.

Press **'Duplicate'** to show a page used to duplicate the selected BACnet Server device and any configured BACnet Object types.

- i. If necessary, edit the 'Device instance', 'Device name', 'Location' and/or 'Description'.

Device instance. This is a maximum 6-digit unique numeric reference that identifies this device on the BACnetIP control system. Initially derived from the Device Instance defined in the Manage Drivers>Comms settings.

Device Name. Unique readable text related to the unique **Device instance**.

Caution Ensure the **'Device instance'** and **'Device name'** are unique.

Location. This freeform location text is used to indicate the physical location of these virtual BACnet servers in the BACnetIP based control system and can be read by the communication partners.

Description. This is a maximum 30-character password used to identify this device, i.e. First Floor.

2. Create the required BACnet Object types for interfacing to a BACnetIP control system. Each Object type has a unique set of properties, according to the type of value, i.e., an analogue read only, read/write, or write only, binary read only, read/write, or write only or multistate read only, read/write, or write only.

OBJECT TYPE	COPY/PASTE REF	DESCRIPTION
Analogue Input	0-AI-analog input	A numeric input value, i.e., a sensor. Read from (R/O) this device by a BACnetIP control system
Analogue Output	1-AO-analog output	A numeric, i.e., a louvre position. Write to (W/O) this device by a BACnetIP control system
Analogue Value	2-AV-analog value	A numeric control input/output value, i.e., a room setpoint. Read from and Write to (R/W) this device by a BACnetIP control system
Binary Input	3-BI-binary input	A single-bit Boolean (True/False, On/Off, or 1/0) input value, i.e., a switch. Read from (R/O) this device by a BACnetIP based control system
Binary Output	4-BO-binary output	A single-bit Boolean (True/False, On/Off, or 1/0) output value, i.e., a relay. Write to (W/O) this device by a BACnetIP control system
Binary Value	5-BV-binary value	A single-bit Boolean (True/False, On/Off, or 1/0) control input/output value, i.e., a control system parameter. Read from and Write to (R/W) this device by a BACnetIP control system
Multistate Input	13-MI-multistate input	A numeric input value showing the current state in the process, i.e., refrigerator's On, refrigerator's Off, and Defrost state. Read from (R/O) this device by a BACnetIP control system
Multistate Output	14-MO-multistate output	A numeric output value defines the next state in the process, i.e., turn refrigerator On, turn refrigerator Off. Write to (W/O) this device by a BACnetIP control system
Multistate Value	19-MV-multistate value	A numeric control input/output value, i.e., a control system parameter. Read from and Write to (R/W) this device by a BACnetIP control system

Tip! Use the Copy/Paste option to populate the appropriate number of BACnet Servers devices, including the DeviceInstance (CoIA), DeviceName (CoIB), DeviceDescription (CoIC), DeviceLocation (CoID), ObjectType (CoIE), ObjectInstance (CoIF), ObjectName (CoIG), ObjectDescription (CoIH), and Units (CoII) details. Columns A to G are compulsory. DeviceInstance limited 0 – 4194302. DeviceName limited 1 – 63 characters. DeviceDescription limited 1 – 253 characters. DeviceLocation limited 0 – 63 characters. ObjectType can be shown as in table above. ObjectInstance limited 0 – 4194302. ObjectName limited 1 – 63 characters. ObjectDescription limited 1 – 253 characters. Units limited 0 - 65535 (use conversion table).

Caution Ensure Device and Object are unique where necessary, the paste function does not validate duplicates. Using the Copy/Paste option will break all existing links.

CONFIGURE THE ANALOGUE OBJECT TYPES

BACnet Analogue Object types include AI (Analogue Input), AO (Analogue Output) and AV (Analogue Value).

BACnet AI Object type instance provides a read only analogue value to the BACnetIP control system.

BACnet AO Object type instance provides a write only analogue value to the BACnetIP control system.

BACnet AV Object type instance provides a read and write analogue value to the BACnetIP control system.

Caution Each Object Type Instance number **MUST** be unique in this virtual BACnet Server.

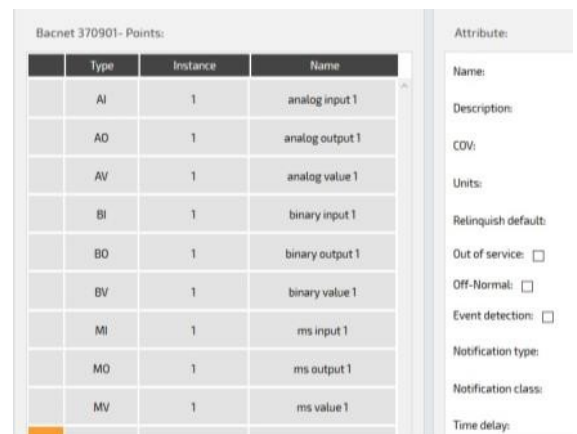
To configure AI, AO, and/or AV Object types

1. Press '>' to insert a pre-configured index row, and change the 'Type' to an AI, AO, and/or AV instance as necessary.

Type. The required Object types.

Instance. The unique numeric reference for this Object type instance. Used to identify the required parameter according to the configured **Object name**. Edit as necessary.

Object name. Readable text identifying this Object type instance. Edit as necessary.



Bacnet 370901- Points:			Attribute:
Type	Instance	Name	Name:
AI	1	analog input 1	Description:
AO	1	analog output 1	COV:
AV	1	analog value 1	Units:
BI	1	binary input 1	Relinquish default:
BO	1	binary output 1	Out of service: <input type="checkbox"/>
BV	1	binary value 1	Off-Normal: <input type="checkbox"/>
MI	1	ms input 1	Event detection: <input type="checkbox"/>
MO	1	ms output 1	Notification type:
MV	1	ms value 1	Notification class:
			Time delay:

2. Edit the Object type instance '**Attributes**'. These are used to define the constraints of the corresponding Object type instance.

- i. Configure the Object type instance '**Attributes**'.

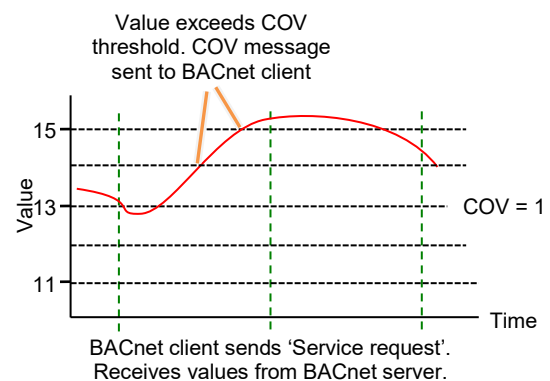
Object name. A unique readable name for this Analogue Object type instance, also shown in the '**Name**' column.

Description. Readable text for this Object type instance, i.e. First Floor.

COV (Change of Value). A threshold value used to determine when this BACnet device sends a COV message to the BACnetIP control system, i.e., if the value has changed by 1 or more, a COV message is sent.

Note

Typically, BACnet servers wait for a BACnetIP control system to request data before responding, but this optional BACnet property sends a COV message when the COV threshold is exceeded.



Tip!

COV is a sub-set of the 'Alarm and Event Services'.

Units and Unit types. Defines a required measurement, i.e., Units = energy, and the required term of measurement, i.e. kilowatt hours.

Relinquish default (AO and AV only). A fallback value used as the present value to resolve command conflicts when connection to the BACnetIP control system fails and the '**Out of service**' is false.

Tip!

The Relinquish default parameter only applies to AO and AV Object types.

Out of service. Shows the Present Value can be overwritten by the BACnetIP control system.

- ii. Configure the **Notification class** requirements. This defines the parameters used to determine when a value will be included in the related Notification class Event or Alarm log.

Off-Normal, Fault, Normal. Defines the '**Event enabled**' types of state that will be logged an Event or Alarm. Set the required parameter as necessary.

Event detection. Shows the enabled type of states will be logged an Event or Alarm. Set 'On' to log the enabled Off-Normal, Fault, and/or Normal states as an Event or Alarm.

Notification type. Defines the type of notification applied to the '**Event enabled**' types of state, Off-Normal, Fault, and/or Normal states. The Event or Alarm type of notification can be used to filter the configured '**Event enabled**' types of state.

Remember

Configure the 'Notification classes' to ensure the 'Event enabled' types are logged correctly.

Notification class. Identifies the **Notification class** handling the event-initiating object.

Time delay. Defines the number of seconds that must elapse before an Event or Alarm will be logged in the related **Notification class**. Only values that exceed the defined **High limit** and **Low limit** and exceed this 'Time delay' will be logged in the related **Notification class**.

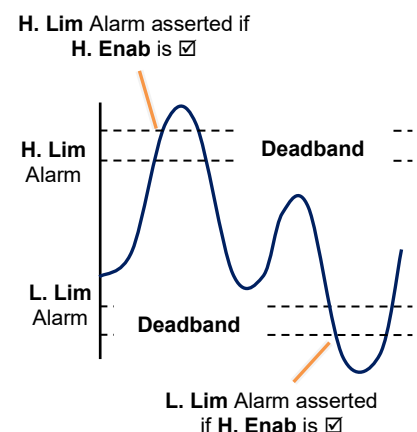
High limit and **Low limit.** Defines the high alarm limit and/or the low alarm limit. This is used to define the upper and/or lower limits of the value recorded from the parameter. If a limit is exceeded the corresponding alarm in the BACnetIP control system will only be asserted if '**(High limit) Enable**' and/or '**(Low limit) Enable**' is enabled ()

Remember

A configured low alarm limit value must be less than the defined high alarm limit.

(High limit) Enable and **(Low limit) Enable.** Determines the value exceeding the specified criteria will/will not assert an Event or Alarm. If necessary, enable () the high alarm limit ('**(High limit) Enable**') and/or low alarm limit ('**(Low limit) Enable**'). Defines the high alarm and low alarm indication in the BACnetIP control system, when the value recorded from the parameter asserts an alarm state determined by the value defined in '**High limit**' and/or '**Low limit**'. If this field is disabled () an alarm state will not be indicated.

DeadBand. A range of input values that can reduce the frequency of Event or Alarm occurrences if the value fluctuates around the '**High limit**' and/or '**Low limit**'.



CONFIGURE THE BINARY OBJECT TYPES

BACnet Binary Object types include BI (Binary Input), BO (Binary Output) and BV (Binary Value).

BACnet BI (Binary Input) Object type instance provides a read only binary state to the BACnetIP control system.

BACnet BO (Binary Output) Object type instance provides a write only binary state to the BACnetIP control system.

BACnet BV (Binary Value) Object type instance provides a read and write binary state to the BACnetIP control system.

Caution **The Object Type Instance number MUST be unique in this virtual BACnet Server.**

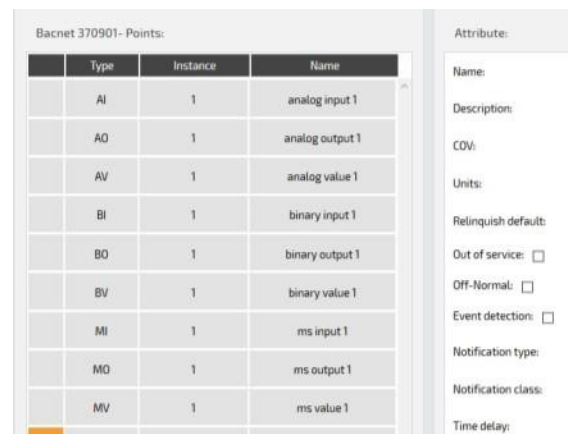
To configure BI, BO, and/or BV Object types

1. Press '>' to insert a pre-configured index row, and change the 'Type' to a BI, BO, and/or BV Object type as necessary.

Type. The required Object Type.

Instance. The unique numeric reference for this Object type instance. It is used to identify the required parameter according to the configured **Object name**. Edit as necessary.

Object name. The unique readable name for this Object type instance. Edit as necessary.



Type	Instance	Name
AI	1	analog input 1
AO	1	analog output 1
AV	1	analog value 1
BI	1	binary input 1
BO	1	binary output 1
BV	1	binary value 1
MI	1	ms input 1
MO	1	ms output 1
MV	1	ms value 1

Attributes:

Name:

Description:

COV:

Units:

Relinquish default:

Out of service:

Off-Normal:

Event detection:

Notification type:

Notification class:

Time delay:

2. Edit the Object type instance '**Attributes**'. These are used to define the constraints of the corresponding Object type instance.
 - i. Configure the Object type instance '**Attributes**'.

Object name. A unique readable name for this Binary Object type instance, also shown in the '**Name**' column.

Description. Readable text identifying this Object type instance. Edit as necessary, i.e. First Floor.

Inactive Text and Active Text. The intended effect of Inactive and Active state of the present value, i.e. Inactive: Fan 1-Off, Active: Fan 1-On. Enter text for each option, as necessary.

Polarity. Indicates the relationship between the physical Input state and the logical state of the present value, i.e. if Polarity: Normal, the Active state of the present value and the physical Input state will be the same, but if Polarity: Reversed, the Active state of the present value and the physical Input state will be the opposite.

Out of service. Shows the Present Value can be overwritten by the BACnetIP control system.

- ii. Configure the **Notification class** requirements. As per Analogue Object types.

Off-Normal, Fault, Normal (BI and BV only). As per Analogue Object types.

Event detection. As per Analogue Object types.

Notification type. As per Analogue Object types.

Remember

Configure the 'Notification classes' to ensure the 'Event enabled' types are logged correctly.

Notification class. As per Analogue Object types.

Time delay. As per Analogue Object types.

Alarm value. The state used to determine the alarm condition.

Caution

Ensure the combination of Inactive Text and Active Text, and Polarity are set correctly to assert the necessary alarm.

CONFIGURE THE MULTISTATE OBJECT TYPES

BACnet Multistate Object types include MI (Multistate Input), MO (Multistate Output) and MV (Multistate Value).

BACnet MI (Multistate Input) Object type instance provides a read only numeric reference for 2 (two) or more states to the BACnetIP control system.

BACnet MO (Multistate Output) Object type instance provides a write only numeric reference for 2 (two) or more states to the BACnetIP control system.

BACnet MV (Multistate Value) Object type instance provides a read and write numeric reference for 2 (two) or more states to the BACnetIP control system.

Caution **The Object Type Instance number MUST be unique in this virtual BACnet Server.**

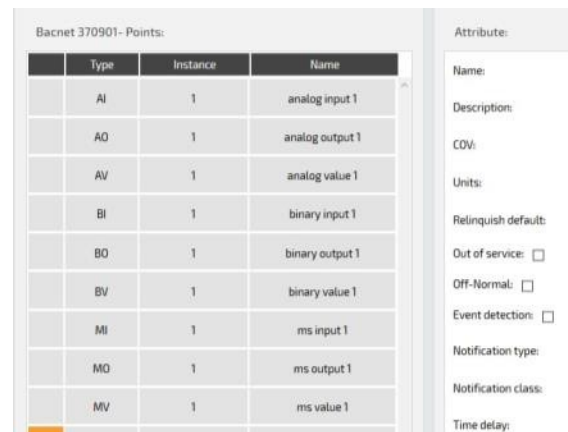
To configure MI, MO, and/or MV Object types

1. Press '>' to insert a pre-configured index row, and change the 'Type' to a MI, MO, and/or MV Object type as necessary.

Type. The required Object Type.

Instance. The unique numeric reference for this Object type instance. Used to identify the required parameter according to the configured **Object name**. Edit as necessary.

Object name. The unique readable name for this Object type instance. Edit as necessary.



Type	Instance	Name
AI	1	analog input 1
AO	1	analog output 1
AV	1	analog value 1
BI	1	binary input 1
BO	1	binary output 1
BV	1	binary value 1
MI	1	ms input 1
MO	1	ms output 1
MV	1	ms value 1

Attribute:

Name:

Description:

COV:

Units:

Relinquish default:

Out of service:

Off-Normal:

Event detection:

Notification type:

Notification class:

Time delay:

2. Edit the Object type instance '**Attributes**'. These are used to define the constraints of the corresponding Object type instance.

- i. Configure the Object type instance '**Attributes**'.

Object name. A unique readable name for this Object type instance, also shown in the '**Name**' column.

Description. Readable text identifying this Object type instance. Edit as necessary, i.e. First Floor.

Number of states. The required number of states related to the present value, i.e., 3 = 1: Hand, 2: Off, 3: Auto. Enter number of states required, as necessary.

State Text. The intended effect of each defined state related to the present value, i.e., 3 = 1: Hand, 2: Off, 3: Auto. Enter required text for each option, as necessary.

Relinquish default (MO and MV only). A fallback state used as the present value to resolve command conflicts when connection to the BACnetIP control system fails and the '**Out of service**' is false.

Tip! **The Relinquish default parameter only applies to MO and MV Object types.**

Out of service. Shows the Present Value can be overwritten by the BACnetIP control system.

- ii. Configure the **Notification class** requirements (MI and MV only). As per Analogue Object types.

Off-Normal, Fault, Normal. As per Analogue Object types.

Event detection. As per Analogue Object types.

Notification type. As per Analogue Object types.

Remember **Configure the 'Notification classes' to ensure the 'Event enabled' types are logged correctly.**

Notification class. As per Analogue Object types.

Time delay. As per Analogue Object types.

Alarm value. The state used to determine the alarm condition.

Caution **Ensure the combination of State Text, and Alarm Value are set correctly to assert the necessary alarm.**

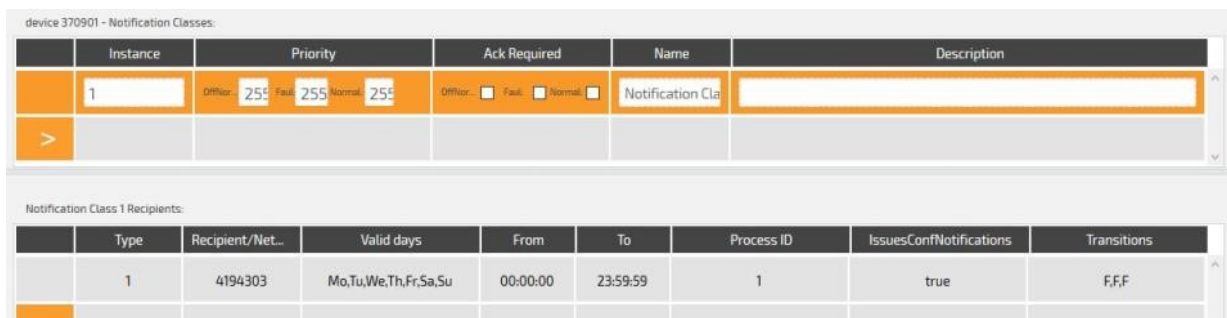
CONFIGURE THE NOTIFICATION CLASS OBJECT TYPES AND RECIPIENTS

BACnet '**Notification Class**' (NC) Object types are used to send Event or Alarm message to a recipient on the BACnet control system. When a BIC shows a present value that has been defined as operating outside the required criteria, a notification object would be used to inform the defined recipient within the BACnet control system that an Event or Alarm has occurred.

Caution **The Object Type Instance number MUST be unique in this virtual BACnet Server.**

To configure NC Object types

1. Select the required BACnet Server, and press '>' to insert a pre-configured index row and change the parameters as necessary.



device 370901 - Notification Classes:								
Instance	Priority			Ack Required			Name	Description
1	Off-normal: 255	Fault: 255	Normal: 255	Off-normal: <input type="checkbox"/>	Fault: <input type="checkbox"/>	Normal: <input type="checkbox"/>	Notification Cla	
>								
Notification Class 1 Recipients:								
Type	Recipient/Net...	Valid days	From	To	Process ID	IssuesConfNotifications	Transitions	
1	4194303	Mo,Tu,We,Th,Fr,Sa,Su	00:00:00	23:59:59	1	true	F,F,F	

2. Edit the Object type instance parameters. These are used to define the constraints of the corresponding Object type instance.

Instance. The unique '**NC**' Object type Instance number. Used to identify a configuration defining specific Event/Alarm message criteria. Edit as necessary.

Priority. The level of importance for Off-normal, Fault, and/or Normal Events, 0 (low) to 225 (high). Used to ensure a specific Event/Alarm with critical time constraints are not delayed. Edit as necessary.

Ack required. Shows an acknowledgement for Off-normal, Fault, and/or Normal Events from the BACnet control system is required.

Name. A unique '**NC**' name for the Object type instance.

Description. Readable text identifying this Object type instance. Edit as necessary, i.e. First Floor.

- Press '>' to insert a '**NC**' Recipient details associated with the selected '**NC**'. These are used to determine, when and where Event/Alarm will be shown.

Type. A BACnet identifier of the Recipient showing the Event/Alarm.

Recipient/Network. The Event/Alarm recipient as determined by the 'Type' configuration and defined in the '**Recipient Attributes**'.

Days. The days of the week when an Event/Alarm will be passed to the BACnet recipient defined in the 'Type' and 'Recipient/Network' configuration as defined in the '**Recipient Attributes**'.

From and To. The start and stop time of the day, when an Event/Alarm will be passed to the BACnet recipient defined in the 'Type' and 'Recipient/Network' configuration as defined in the '**Recipient Attributes**'.

Process ID. The Event/Alarm recipient order when more than one recipient is used, i.e., Process ID 1, Process ID 2, etc as defined in the '**Recipient Attributes**'.

IssuesConfNotifications. A confirmation message from BACnet recipient is required, as defined in the '**Recipient Attributes**'.

Transitions. An Event/Alarm notification will occur when the values has changed between the enabled conditions as defined in the '**Recipient Attributes**'.

Select the required '**NC**' Recipient row to show the '**Recipient Attributes**'. Edit as necessary.

Event Days. The days of the week when the Event/Alarm can be sent. Set *On*, an Event/Alarm will be sent to the BACnet Recipient. Set *Off*, an Event/Alarm will be sent to the BACnet Recipient.

From and To. The start and stop time of the day when the Event/Alarm can be sent. Set *On*, an Event/Alarm will be sent to the BACnet Recipient. Set '**From**' (e.g., 08:00) and '**To**' (e.g., 20:00) with a time according to the 24-hour clock.

Type. A BACnet identifier of the Recipient showing the Event/Alarm. Edit as necessary.

- ◆ If '**Device**', define the unique numeric Device Instance number to determine the Recipient showing the Event/Alarm.
- ◆ If '**Address**', define the '**Net number**' and '**MacToIP(Hex)**' to determine the Recipient showing the Event/Alarm.

Tip!

'Net number' is the BACnet Network number and 'MacToIP(Hex)' is the BACnet device IP address and BACnet port displayed in hex.



The screenshot shows a configuration form with the following fields and values:

- Event days:** Mo, Tu, We, Th, Fr, Sa, Su (all checked)
- From:** 00:00:00
- To:** 23:59:59
- Recipients:**
 - Type:** address
 - Process:** ProcessID: 1
- Net number:** 0
- MacToIP(Hex):** COA80BD6BAC0
- IssuesConfNotifications:**
- Transitions:**
 - Off-normal:
 - Fault:
 - Normal:

Process ID. The Event/Alarm recipient order when more than one recipient is required. Set the number in order of priority required by the recipients.

IssuesConfNotifications. A confirmation message from BACnet recipient is required. Set *On*, a confirmation messages is expected from the recipient. Set *Off*, a confirmation messages is not expected from the recipient.

Transitions. An Event/Alarm notification will occur when the values has changed between the enabled conditions. Set **Off-Normal, Fault** and/or **Normal On**, an Event/Alarm notification will be sent to the recipient. Set **Off-Normal, Fault** and/or **Normal Off**, an Event/Alarm notification will not be sent to the recipient.

CONFIGURE THE TRENDLOG OBJECT TYPES

The Trendlog object (like Trend Plot data) monitors and records changes in the behaviour of an individual supported object type over time. The Trendlog object collects sample values at timed intervals or only upon changes in the given value.

Tip! Useful for diagnosing behavioural characteristics, i.e., unexpected room air temperature changes.

To configure Trendlog Object types

1. Select the required BACnet Server, and press '>' to insert a pre-configured index row, in the Trendlog List' and change the parameter attributes as necessary.

Instance. The unique numeric reference for this Trendlog Object type instance. Edit as necessary.

Name. The unique readable name for this Trendlog Object type instance. Edit as necessary.



Trendlog List: +	
Instance	Name
1001	Trendlog 1001
>	

- ◆ Press '+' to automatically create Trendlogs associated with selected Object types.
- ◆ Select 'Delete' from the available menu option to remove the selected Trendlog.

2. Edit the Trendlog Object type instance '**Attributes**'. These are used to define the constraints of the corresponding Object type instance.

Name. Used to define unique readable name for this Object type instance, also shown in the '**Name**' column. Edit as necessary.

Description. Used to define readable text identifying this Object type instance, i.e. First Floor. Edit as necessary.

Source Type. Used to define the Object type being monitored by the Trendlog. Edit as necessary.

Source Instance. Used to define the unique numeric reference for the Object type being monitored by the Trendlog. Edit as necessary.

TL Type. Used to define how a value will be included in this Trendlog according to the defined action. If '**Poll**' the value is added to this Trendlog according to the defined interval (see **Interval** below). If '**Trig**' the value is added to this Trendlog according to change of value.

TL Instance. Used to define the unique numeric reference for this Trendlog Object type instance. Edit as necessary.

Enable. Used to define how this Trendlog will be used. If *On*, this Trendlog Object will be including values according to the '**TL Type**'. If *Off*, this Trendlog is NOT including values.

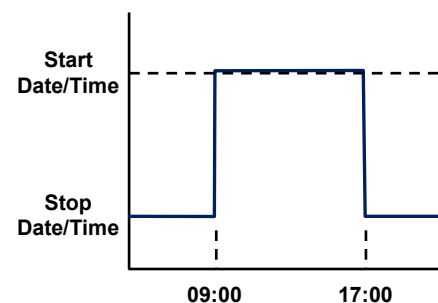
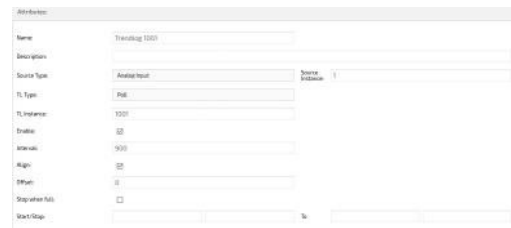
Interval. Used to define the number of seconds between logging the associated Object type in this Trendlog. Edit as necessary.

Align (Intervals). Used to define that a clock-aligned periodic logging is enabled. If clock-aligned periodic logging is enabled and the value of Log Interval is a factor of a second, minute, hour, or day, then the beginning of the period specified for logging shall be aligned to the second, minute, hour, or day, respectively.

Offset (Intervals). Used to define the delay in ms from the beginning of the period specified for logging until the actual acquisition of a log record begins.

Stop when full. Shows if historic values will be overwritten or not. If *On*, values will stop being added to the Trendlog when it is full. If *Off*, historic values will be overwritten by the latest values.

Start/Stop. Shows when the Trendlog will be active. Set '**Date**' using the calendar option and '**Time**' as hh:mm:ss for the '**Start**' period, and Set '**Date**' using the calendar option and '**Time**' as hh:mm:ss for the '**Stop**' period.



2.5.4 Define Data Acquisition Driver Points

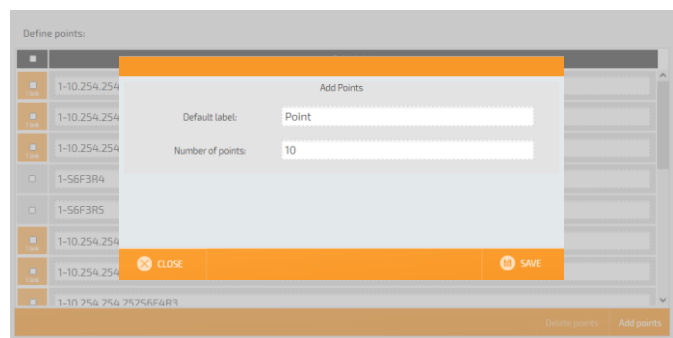
This page is used to define the required Datapoint labels (according to the licence limit) and, if necessary, assign to required groups via the Group mode option.

Note Group mode is used for the 'Single File Grouped' report.

Tip! Before starting, make a note of total number of points required for reporting.

1. If the driver is Data Acquisition (Basic mode), press 'Add points'. This displays the 'Default label' and 'Number of points' options.

Default label. Used to prefix the automatically generated Data Acquisition Datapoints labels e.g., 'Point' to give a default Datapoint label of 'Point nn'.



Tip! Amend the 'Label prefix' for each new range of Data Acquisition Datapoints labels to provide a specific identification.

Label the Data Acquisition Datapoints in the same order as the defined parameters from the fieldbus protocol drivers were configured.

Number of points. Used to define the required number of Data Acquisition Datapoints which will be available for reporting or via a MySQL query.

Note Use 'Copy/Paste' if configuration was performed off site. A configuration spreadsheet is available from Synapsys Solutions Technical Support.

Caution Label prefixes will be overwritten if labels are obtained automatically from the linked prefixes.

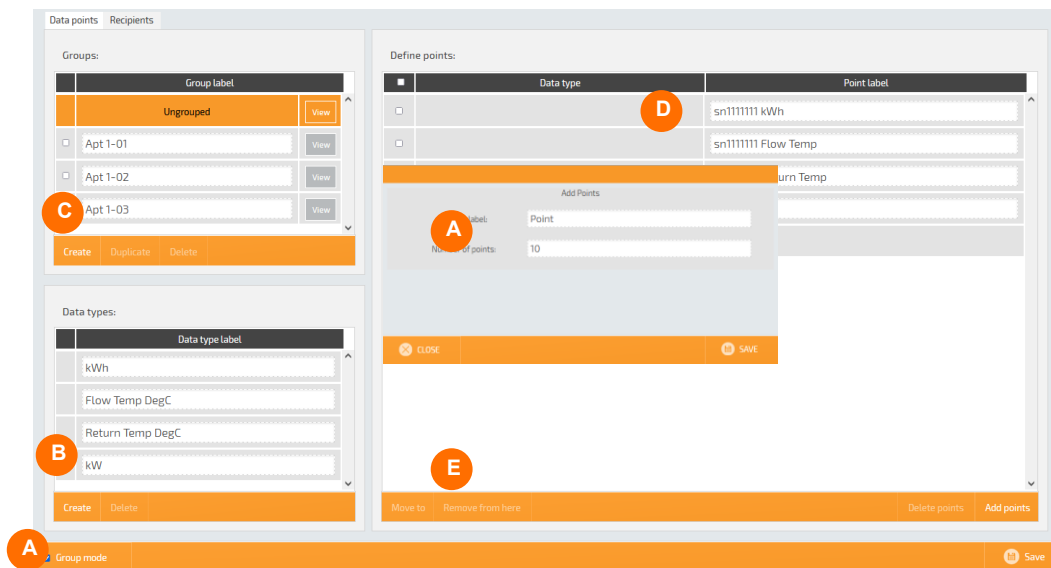
USE GROUP MODE

The Group mode option is used to assign the values from a determined range of identical parameters to a user defined group to support the Single File Grouped report format.

Tip! Using Group mode can make data analysis easier. Points can also be grouped via a defined data type.

1. If the driver is Data Acquisition (Group mode is Enabled) (A), press 'Add points' to the 'Default label' and 'Number of points' options.

Tip! New Datapoints are added to 'Ungrouped'.



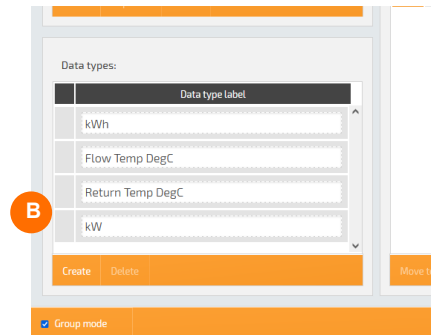
Default label. Used to prefix the automatically generated Data Acquisition Datapoints labels e.g., 'Point' to give a default Datapoint label of 'Point nn'.

Tip! Amend the 'Label prefix' for each new range of Datapoints labels to provide a specific identification.

Label the Datapoints in the Data Acquisition protocol driver in the same order as the defined parameters from the fieldbus protocol drivers were configured.

Number of points. Used to define the required number of Data Acquisition Datapoints which will be available for reporting or via a MySQL query.

2. Add a **'Data type label'** (B). Used to define Data type to be associated with a specific Datapoint in a specific Group when using the Single File Grouped report format.
 - iii. Press **'Create'** to add a default Data type label row.
 - iv. Select the **'Data type label'** and edit as necessary. This label will be an option in the Define points Data type list.
 - ◆ If necessary, select the Data type that is not required, and press Delete.



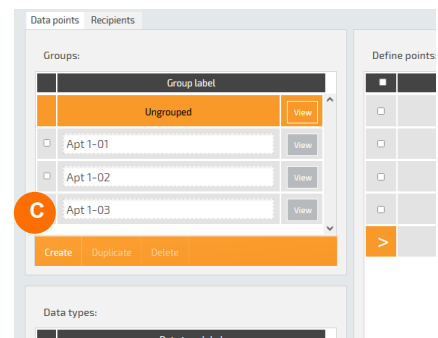
3. Add a **'Group'** (C). Used to define a Group label for 1 (one or more) defined Data type labels when using the Single File Grouped report format.

View. Used to show the Datapoints assigned to the selected Group.

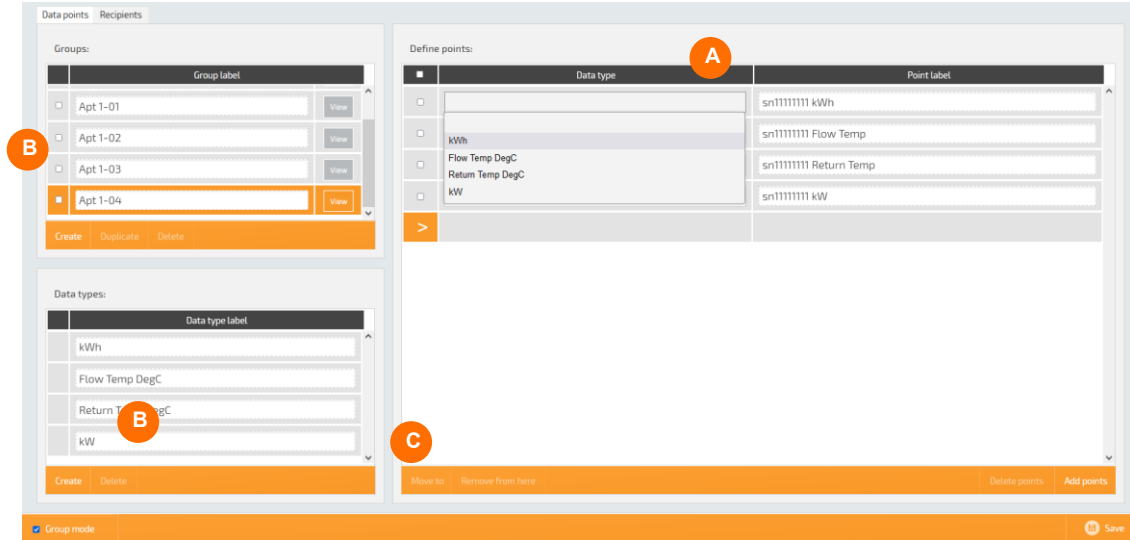
If necessary, use the tick box to select a Group that is not required, and press Delete.

Tip!

To ensure a clear report filename, use a unique, meaningful name for the Datapoint and Group labels and Data type labels.

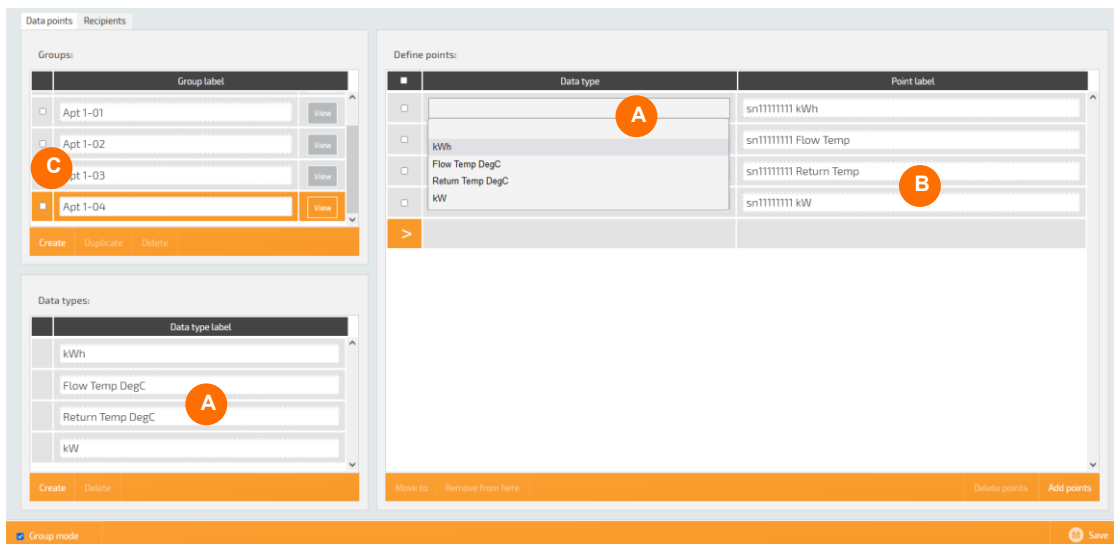


4. In 'Define points', assign the Datapoint to the required Groups.



- v. Use the tick box to select Datapoints (A), then use the tick box to select a Group (B) for the selected Datapoints and press the '**Move to**' (C) button.
- vi. Press View to confirm the Datapoints have been moved to the selected Group.
If necessary, use the tick box to select a Group that is not required, and press Delete.

5. Use the Data type drop down (A) to select the data type for the selected datapoint (B) in the group displayed.



MANAGE RECIPIENTS AND REPORTS

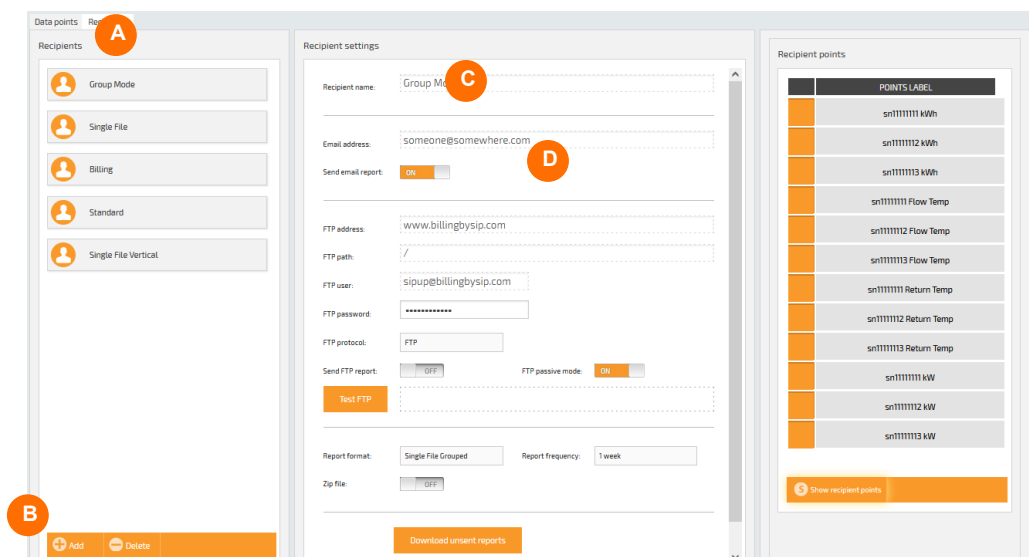
The Recipients page is used to define the 'Recipients', 'Recipient settings' (including 'Recipient name', 'Report type', 'Report format' and 'Recipient points').

1. Select 'Recipients' (A). Shows the page used to configure the reporting requirements of that recipient.
2. Press 'Add' (B) to create a new FTP or email report recipient.

If necessary, select the Recipient, that is not required, and press Delete.

Caution Use unique names to avoid files being overwritten.

3. In 'Recipient settings', edit as necessary.

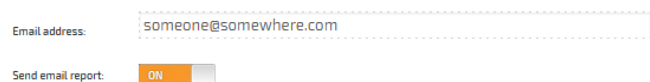


Recipient name (C). Used to provide a unique name for a defined FTP or email report recipient.

Note The 'Recipient name' is used within the filename when the 'Single File', 'Single File Vertical', or 'Single File Grouped' report format are selected.

Email address (D). Used to define the email address receiving reports. Edit as necessary.

Send email report (D). Used to control email reporting. If *On*, reports will be emailed via the email server define in the Global settings. If *Off*, email reporting is disabled.



Remember A valid email account is required, according to the mail server settings defined in the Global Settings page.

FTP Address. Used to define the home directory in the Fully Qualified Address or the IP Address of the FTP Server receiving reports for the selected recipient. Edit as necessary.

Tip!

Non-standard ports can be used.

File path. Used to define any additional Directory structure used. Edit as necessary.

FTP user and FTP password. Used to define the FTP Server login credentials.

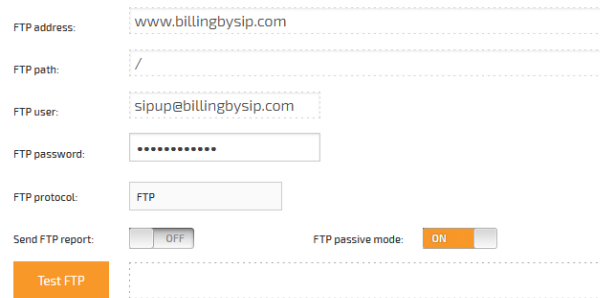
Send FTP report. Used to control FTP reporting. If *On*, reports will be transferred using FTP to the defined FTP Server. If *Off*, FTP is disabled.

FTP Protocol. Used to define the FTP Protocol required by the FTP Server. Set *FTP*, to use plain FTP (unsecure), *FTPS*, to use FTP with TLS security, and *SFTP* to use FTP with SSH security.

Tip!

Use 'Test FTP' to send a test file using the FTP details entered.

Use a third-party FTP Client to prove connectivity to defined FTP Server.

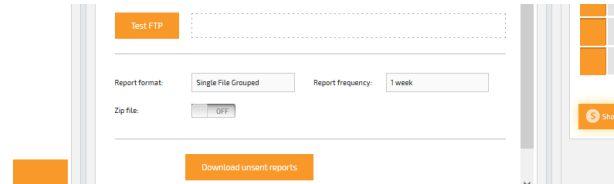


The screenshot shows a configuration form with the following fields and values:

- FTP address: www.billingbysip.com
- FTP path: /
- FTP user: sipup@billingbysip.com
- FTP password: [masked with dots]
- FTP protocol: FTP
- Send FTP report: OFF (checkbox)
- FTP passive mode: ON (checkbox)
- Test FTP: [button]

- In the Report settings, edit as necessary.

Report format. Used to define the report format required by the Recipient. The selected Report format shows additional related parameters.



- ◆ **Standard.** Generates a single report file per Datapoint, with the default filename (milliseconds since last report). The content includes Time stamp (Col:A), Value (Col:B) as logged in the internal MySQL database, and Point name (Datapoint Label, Col:C).

Example

	A	B	C
1	Time stamp	Value	Point name
2	31/07/2018 00:15	23	L1O1S1 - Sensor 1
3	31/07/2018 00:30	23	L1O1S1 - Sensor 1
4	31/07/2018 00:45	23	L1O1S1 - Sensor 1
5	31/07/2018 01:00	23	L1O1S1 - Sensor 1
6	31/07/2018 01:15	23	L1O1S1 - Sensor 1
7	31/07/2018 01:30	23	L1O1S1 - Sensor 1

Report Frequency. Used to define when the selected reports are sent.

ZIP each file. Used to control the compression requirements for individual .csv (Comma Separated Variable) reports. If *Off*, each individual report will be sent as a .csv file. If *On*, each individual .csv report will be sent in a compressed .zip file.

ZIP all file. Used to control the compression requirements of all .csv (Comma Separated Variable) reports. If *Off*, all report will be sent as a .csv file. If *On*, all .csv reports will be sent in a single compressed .zip file.

Meaningful filename. Used to manage the **Standard** report filename. If *Off*, the report filename is derived from the number of milliseconds since last report. If *On*, the report filename is derived by <Site name>_<SIP name>_<Datapoint label>_<Report period>.

Synchronised timestamps Used to define the timestamp in the report. If *Off*, the report will show the real time the value was logged in the database, e.g. 00:01, 00:17, ..., 23:33, 23:41. If *On*, the report will show the timestamp synchronised to the defined Plot period, e.g. Manage drivers>Data Acquisition>Plot period shows 15mins, the timestamp would show 00:00, 00:15, ..., 23:30, 23:45.

- ◆ **Single File.** Generates a single report file for all Datapoints with the filename derived from <Site name>_<SIP name>_<Recipient>_<Report date>. The content includes driver defined plot interval Time stamp (Col:A) and Datapoint labels (Row:1).

Example

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
1	Time stamp	L1O1S1 - Sensor 1	L1O1S2 - Sensor 2	L1O1	L1O1	L1O1	L1O1	L1O1	L1O1	L1O1	L1O1	L1O1	L1O1	L1O1	L1O1	L1O1	L1O1	L1O1	L1O1	L1O1	L1O1
2	31/07/2018 00:15	23	24.5	0	100	0	60	0	0	0	19.5	23	2	2	12	0	60	5	1800	60	
3	31/07/2018 00:30	23	24.5	0	100	0	60	0	0	0	19.5	23	2	2	12	0	60	5	1800	60	
4	31/07/2018 00:45	23	24.5	0	100	0	60	0	0	0	19.5	23	2	2	12	0	60	5	1800	60	
5	31/07/2018 01:00	23	24.5	0	100	0	60	0	0	0	19.5	23	2	2	12	0	60	5	1800	60	
6	31/07/2018 01:15	23	24.5	0	100	0	60	0	0	0	19.5	23	2	2	12	0	60	5	1800	60	
7	31/07/2018 01:30	23	24.5	0	100	0	60	0	0	0	19.5	23	2	2	12	0	60	5	1800	60	
8	31/07/2018 01:45	23	24.5	0	100	0	60	0	0	0	19.5	23	2	2	12	0	60	5	1800	60	
9	31/07/2018 02:00	23	24.5	0	100	0	60	0	0	0	19.5	23	2	2	12	0	60	5	1800	60	

Report Frequency. Used to define when the selected reports are sent.

Tip!

Do not set greater than Daily.

ZIP file. Used to control the compression requirements of the .csv (Comma Separated Variable) report. If *Off*, the report will be sent as a .csv file. If *On*, the .csv reports will be sent in a single compressed .zip file.

- ◆ **Billing/Half Hourly Log.** Generates a single report file per Datapoint, with the filename derived from <MAC - Auto included>_<Site name>_<SIP name>_<Datapoint label>_<Report period> (milliseconds since last report). The content includes 30 minute TimeStamp (Col:A), DataValue (Col:B) as logged in the internal MySQL database, and MeterID (Datapoint Label, Col:C).

Example

	A	B	C
1	TimeStamp	DataValue	MeterID
2	17/04/2023 13:00	3005	E016B0-Synapsys_Office_HM_kWh_11600501
3	17/04/2023 13:30	3005	E016B0-Synapsys_Office_HM_kWh_11600501
4	17/04/2023 14:00	3005	E016B0-Synapsys_Office_HM_kWh_11600501
5	17/04/2023 14:30	3005	E016B0-Synapsys_Office_HM_kWh_11600501
6	17/04/2023 15:00	3005	E016B0-Synapsys_Office_HM_kWh_11600501
7	17/04/2023 15:30	3005	E016B0-Synapsys_Office_HM_kWh_11600501
8	17/04/2023 16:00	3005	E016B0-Synapsys_Office_HM_kWh_11600501
9	17/04/2023 16:30	3005	E016B0-Synapsys_Office_HM_kWh_11600501

Date separator. Used to define how the date and time Timestamp is shown in the report. If -, the date and time Timestamp will be shown as 01-01-2000 00:00. If /, the date and time Timestamp will be shown as 01/01/2000 00:00.

Data Period. Used to define the time frame of data included in the report.

Tip!

Ensure the end timestamp is before the Send at time.

Send at. Used to define the time (on the hour) the report will be sent.

- ◆ **Single File Vertical.** Generates a single report file for max 50 Datapoints with the filename derived from <Site name>_<SIP name>_<Recipient>_<Report date>. The content includes Time stamp (Col:A, repeated for each Datapoint label), Value (Col:B) as logged in the internal MySQL database, and Point name (Datapoint Label, Col:C).

Example

	A	B	C
1	Time stamp	Value	Point name
2	31/07/2018 00:10	23	L1O1S1 - Sensor 1
3	31/07/2018 00:25	23	L1O1S1 - Sensor 1
4	31/07/2018 00:30	23	L1O1S1 - Sensor 1
5	31/07/2018 00:35	23	L1O1S1 - Sensor 1
6	31/07/2018 00:40	23	L1O1S1 - Sensor 1
7	31/07/2018 00:45	23	L1O1S1 - Sensor 1
8	31/07/2018 00:50	23	L1O1S1 - Sensor 1
9	31/07/2018 23:25	23	L1O1S1 - Sensor 1
10	31/07/2018 23:40	23	L1O1S1 - Sensor 1
11	31/07/2018 23:55	23	L1O1S1 - Sensor 1
12	31/07/2018 00:10	24.5	L1O1S2 - Sensor 2
13	31/07/2018 00:25	24.5	L1O1S2 - Sensor 2
14	31/07/2018 00:40	24.5	L1O1S2 - Sensor 2

Caution Limit Single File Vertical reports to 50 Datapoints max when reporting to Synapsys Solutions EBIS platform.

Tip! Add Recipients to accommodate each range of 50 Datapoints and ensure the Global Settings>Site name include the last 6 digits of the MAC address.

Report Frequency. Used to define when the selected reports are sent.

Tip! Do not set greater than Daily.

ZIP file. Used to control the compression requirements of the .csv (Comma Separated Variable) report. If *Off*, the report will be sent as a .csv file. If *On*, the .csv reports will be sent in a single compressed .zip file.

Synchronised timestamps Used to define the timestamp in the report. If *Off*, the report will show the real time the value was logged in the database, e.g. 00:01, 00:17, ..., 23:33, 23:41. If *On*, the report will show the timestamp synchronised to the defined Plot period, e.g. Manage drivers>Data Acquisition>Plot period shows 15 minutes, the timestamp would show 00:00, 00:15, ..., 23:30, 23:45.

- ◆ **Single File Grouped.** Generates a single report file for all Datapoints with the filename derived from <Site name>_<SIP name>_<Recipient>_<Report date>. The content includes Site name (Col:A), SIP name (Col:B), Group name (Col:C), Time stamp (Col:D), Value (Col:E to Col:last configured datatype) according to the configured group Datatypes.

Example

	A	B	C	D	E	F	G	H	I
1	Site name	SIP name	Group	Time stamp	Energy kWh	Gas m3	Gas kWh	Water m3	Power kW
2	Synapsys	SIP+	Group 1	31/07/2018 00:15	23	24.5	0	100	0
3	Synapsys	SIP+	Group 1	31/07/2018 00:30	23	24.5	0	100	0
4	Synapsys	SIP+	Group 1	31/07/2018 00:45	23	24.5	0	100	0
5	Synapsys	SIP+	Group 1	31/07/2018 01:00	23	24.5	0	100	0
6	Synapsys	SIP+	Group 1	31/07/2018 01:15	23	24.5	0	100	0
7	Synapsys	SIP+	Group 1	31/07/2018 01:30	23	24.5	0	100	0
8	Synapsys	SIP+	Group 1	31/07/2018 01:45	23	24.5	0	100	0
9	Synapsys	SIP+	Group 1	31/07/2018 02:00	23	24.5	0	100	0

Tip! Suitable when logging the same parameters/units from several devices.

Report Frequency. Used to define when the selected reports are sent.

Tip! Do not set greater than Daily.

ZIP file. Used to control the compression requirements of the .csv (Comma Separated Variable) report. If *Off*, the report will be sent as a .csv file. If *On*, the .csv reports will be sent in a single compressed .zip file.

- ◆ **Network Health.** A single file showing the overall reliability of Trend modules being polled via the Trend Client driver with less than configured % success rate is listed.

Example

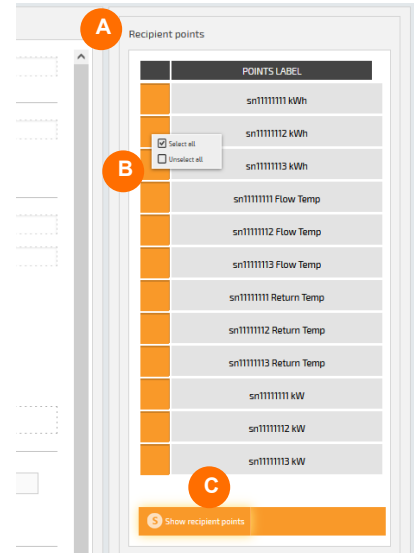
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	A
1	Synapsys	SIP+		Health report	#####																								
2																													
3	Overall success ratio	50%		Hour	00 to 01	01 to 02	02 to 03	03 to 04	04 to 05	05 to 06	06 to 07	07 to 08	08 to 09	09 to 10	10 to 11	11 to 12	12 to 13	13 to 14	14 to 15	15 to 16	16 to 17	17 to 18	18 to 19	19 to 20	20 to 21	21 to 22	22 to 23	23 to 24	
4	Successful requests	206926		Hourly success ratio	N/D	N/D	N/D	N/D	N/D	N/D	N/D	N/D	N/D	N/D	N/D	98%	99%	99%	99%	99%	37%	8%	8%	9%	9%	9%	9%	9%	
5	Total requests	406625																											
6																													
7																													
8	Points with success under	100%																											
9	L2101151 - Sensor 1	50%																											
10	L2101152 - Sensor 2	50%																											
11	L2101153 - Sensor 3	50%																											
12	L2101154 - Sensor 4	50%																											
13	L2101155 - Sensor 5	50%																											
14	L2101156 - Sensor 6	38%																											
15	L2101157 - Sensor 7	38%																											

5. In 'Recipient settings' (A), edit as necessary.
 - i. Select the required Recipient from the list.
 - ii. Select each Datapoint (B), as necessary.
Use the context menu to 'Select all' or 'Unselect all' if necessary.

Tip!

Keyboard shortcuts can make this easier.

Use the 'Show recipient points' (C) button to filter the list of Datapoints assigned to the selected Recipient.



DATA ACQUISITION DATABASE QUERIES

The SIP+ Data-IF uses a MySQL database to store data that is recorded directly from the defined source. This data is stored in 'Read only' database objects ('Data' and 'DataPoints' tables). Each 'table' is a collection of related data entries.

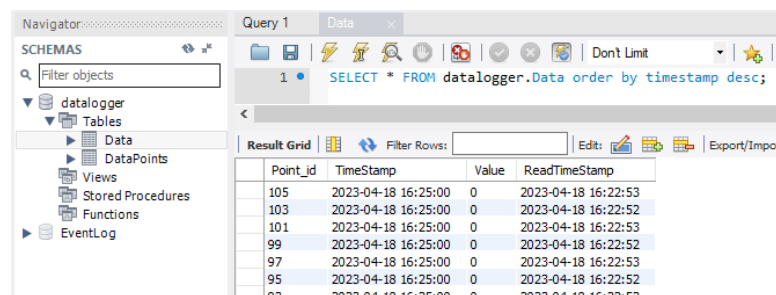
Note Databases are useful when storing information and allows quick and easy interrogation of the data using MySQL queries.

Tip! To perform read only MySQL queries, use Username 'Datalogger', and password 'Datalogger'. A schema is available on request.

The amount of historic data retained in the Data Acquisition driver database is calculated as, number of datapoints & the logging interval (max 162 days), e.g.,

10 Datapoints x 15-minute intervals = 180 days reduced to max 162 days.

Example



2.5.5 Define MQTT Driver Points

The MQTT Driver uses a Publish and Subscribe method of transferring data related to defined Topics. An MQTT Broker is required, but this can be part of the MQTT platform, i.e., Microsoft AWS, or Google IoT hub.

Data can be transferred as plain text or JSON topics, with the payload structure determined by the configuration on this page.

Caution MQTT points affect the available points limit.

To create MQTT points

1. Press '>' to insert a pre-defined row. Edit as necessary.

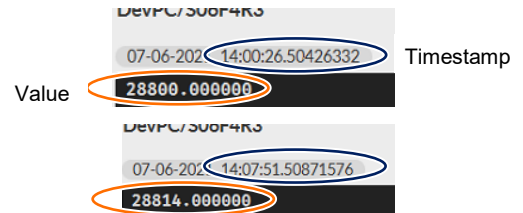
MQTT DEFINE POINTS							
On/Off	Topic	Property	COV	QOS	Retain	Access	
	Polling Topic		Polling Command		Interval		
▼	DevPC/S06F1R1		0	0	Off	R/W	
○ Polling	Polling Topic		Polling Command		Interval		
▶	DevPC/S06F2R1		0	0	Off	R/O	
▶	DevPC/S06F3R1		0	0	Off	R/W	

Topic. Used to define the case-sensitive Topic parameter being Published to the Broker and/or Subscribed from the Broker.

Example Unique Topic only.

Each Payload (plain text) shows the value according to the timestamp.

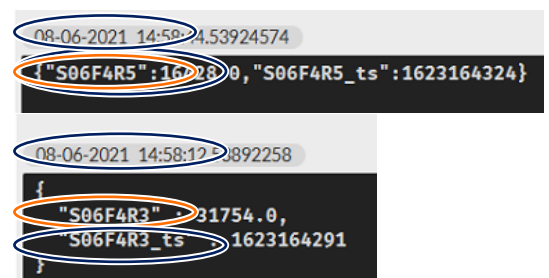
Each Payload (JSON Format) shows the value according to the timestamp.



Example Unique Topic with multiple Property parameters.

Each Payload (plain text) shows the value according to the timestamp.

Each Payload (JSON Format) shows the value according to the timestamp.

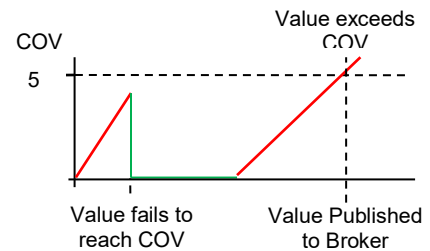


Tip! A 'get' command in second MQTT Client can be used to see all values and Topics in a single payload.

Property. Used in conjunction with the Topic. If all Topics are unique, every updated value will be an individual payload between this product and the Broker.

Tip! All changed values can be sent as an individual payload if the Property is the same for all Topics.

COV. Used to define when a value will be published to the Broker. If 0 (zero), every change will be published to the Broker, if not 0, the value MUST change by at least the specified amount before the payload it attempted.

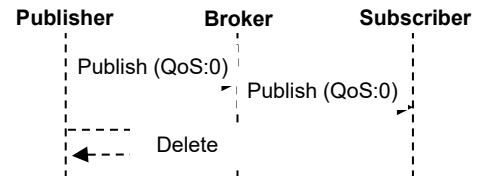


QoS (Quality of Service). Used to define level of reliability expected for a specific MQTT Topic via the Publisher or Subscriber.

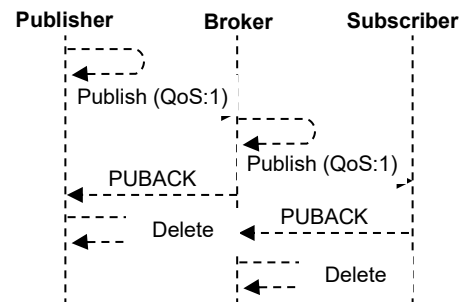
When the QoS used by the Publisher is greater than the QoS used by Subscriber, the QoS of server forwarding messages uses the Subscriber QoS.

When the QoS used by the Publisher is less than the QoS used by Subscriber, the QoS of server forwarding messages uses the Publisher QoS.

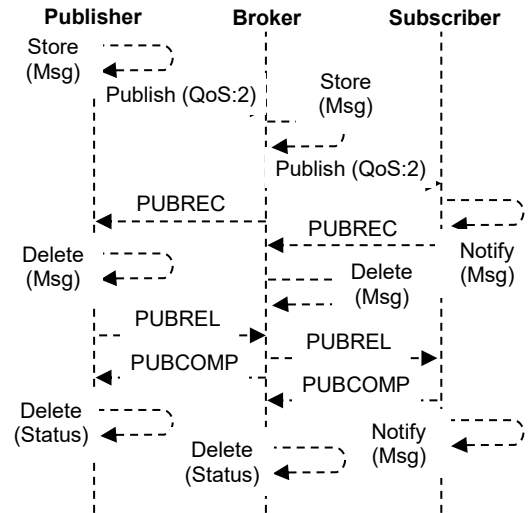
If 0 (At most once), the payload is sent, and a response is not expected.



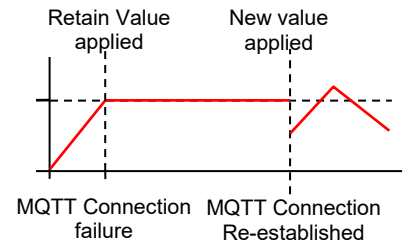
If 1 (At least once), the payload is sent, and a response is expected. The payload will be resent if there is no response. This can guarantee that the payload will arrive at least once, but it cannot guarantee that the message is repeated.



If 2 (Exactly once), the Publisher and Subscriber payload is sent, and a response is expected with message loss and duplication are unacceptable.



Retain. Used to instruct the Broker to use the last successful value for a specified topic. When a new client subscribes to a topic, they receive the last message that is retained on that topic.



Access. Used to define what is allowed to occur at the parameter linked to this Topic, i.e. W/O published to Broker only, R/W Published to Broker and Subscribed from Broker, or R/O Subscribed from Broker only.

2. Select '**Delete**' from the available menu option to remove the selected Topic.

CONFIGURE THE MQTT POLLING TOPIC

The Polling Topic is only necessary depending on the third-party Publishing device. It is an extension to a configured MQTT Topic, and used to control the periodic polling of an MQTT Broker that is being Published to by a third party MQTT Client, rather than the continuously passing the payload with the MQTT Broker.

To create configure the Polling Topic

1. Expand the existing MQTT Topic to show the Polling Topic parameters.

MQTT DEFINE POINTS						
	Topic	Property	COV	QOS	Retain	Access
	On/Off	Polling Topic	Polling Command		Interval	
Linked	▼ DevPC/S06FIR1		0	0	Off	R/W
	⊙ Polling	S06FIR1 get	get		300	
Linked	▶ DevPC/S06FIR2		0	0	Off	R/W

Polling. Used to control the Polling Topic. If disabled, the Polling Topic will not be polled. If enabled, the Polling Topic will be polled at the defined 'Interval'.

Polling Topic. Used to define a separate MQTT Topic to send the polling command that the device requires, e.g., a destination Topic that may only be applicable to the device being polled.

Polling Command. Used to define a specific word or string that is sent to the third-party device that requires the data.

Interval (ms). Used to determine the how frequently the Polling Topic will be polled, e.g., 300ms.

Tip! Use the Copy/Paste option to populate the appropriate number of MQTT Topic, Property, COV, QOS, Retain, Access, On/Off, Polling Topic, Polling Command, and Interval details.

Caution Using the Copy/Paste option will break all existing links.

2.5.6 Define REST Server Driver Points

The REST Server Driver is the Synapsys Solutions REST API compatible software. It provides values via a REST connection across an IP network using an OAuth 2.0 authentication.

To create REST Server points

1. Press **'Client Admin'** to display a page required to define an available connection to this device.
2. Define the connection details.

- i. Press **'Add'** to display a page used to create a connection and define all the required connection credentials.



Client name. Used to show a Human readable text identifying for connection by a third party. Edit as necessary. Max 3 REST Clients are permitted.

Permission. Used to provide permitted privileges for connection by a third party. Set **'Write'** and **'Read'** (*On*) to allow the connected third party to write and/or read the configured parameters. If (*Off*), third party is not allowed to write and/or read the configured parameters. Edit as necessary.



- ii. Press **'Save'** to confirm and show connection details required by third party connection.

Client id and **Client Secret.** A machine id code generated internally for connection by a third party, and the corresponding pass code for requesting an access 'Bearer' token.

Tip! **The Client id and Client Secret can be used as authentication for requesting the access 'Bearer' token by the third-party connection, if required.**

- iii. Press **'Get token'** to provide an access 'Bearer' token. This is the 'Bearer' token required by the third party to read and write values to the REST points defined internally.

Caution **The third party must include the access 'Bearer' token in the Authorization header when making requests.**

- iv. Press **'Save'** to confirm connection details. Close the page.

Tip! **Use the** to select a connection that can be removed. Press **'Delete'** to remove selected connection.

3. Press '>' to insert a pre-defined row. Edit as necessary.

These points can be used to make value from a linked point available to a third-party connection.



	URI	Access
<input type="checkbox"/>	/rest/ S01R01F3RoomTemp	R/O
<input type="checkbox"/>	/rest/ point2	W/O

URI. Identifies the REST point to the third-party connection. Edit as necessary.

Access. Defines the type of operation permitted to this REST point, dependant on the point linked.

Tip! Use the to select a REST point that can be removed. Press 'Delete' to remove selected REST point.

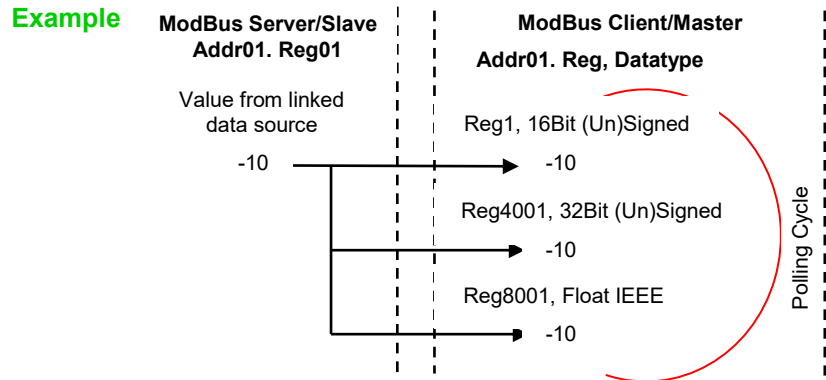
4. Press **'Save'** to confirm changes.

2.5.7 Define ModBus Server/Slave Driver Points

The ModBus Server/Slave Driver is used to provide values from the linked source point available to a ModBus Client/Master, i.e., PLC, or SCADA system.

Each product supports addresses 1 to 247, with register Base 1 (ModBus).

The ModBus Server/Slave makes each register value available as all datatypes at the same time.



REGISTER RANGE IN CLIENT/MASTER	REGISTER DATATYPE IN CLIENT/MASTER	MAX REGISTERS PER ADDRESS
1-2000	16Bit Signed	1-2000
2001-4000	16Bit Unsigned	
4001-6000	32Bit Signed	1-1000
6001-8000	32Bit Signed/Unsigned	
8001-10000	32Bit Float IEEE	

Datatype Registers restart at 1 for each Function Code (1-Coils, 2-Inputs, 3-Holding Registers, and 4-Input Registers)

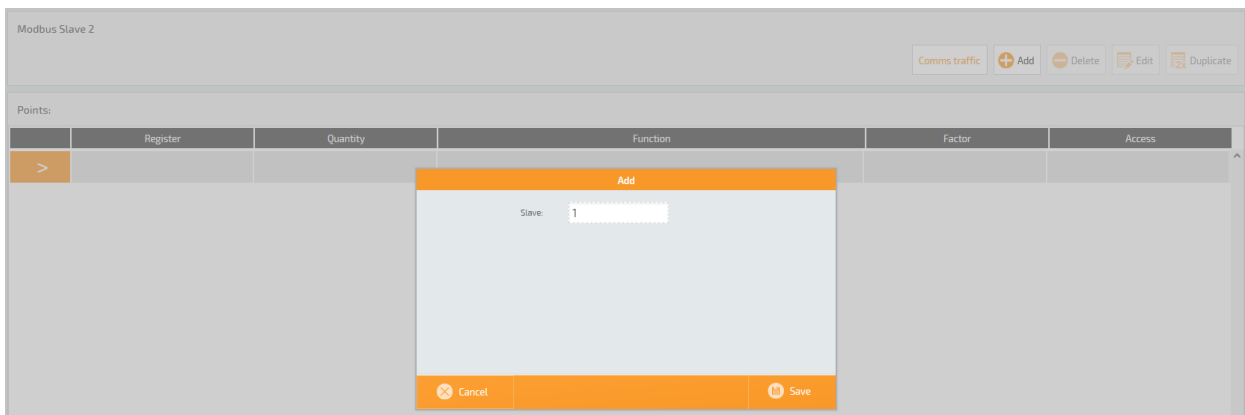
Example Configured ModBus Server/Slave Registers are automatically available.

SERVER/SLAVE REG/BASE	CLIENT/MASTER 16BIT SIGNED/UNSIGNED	CLIENT/MASTER 32BIT SIGNED/UNSIGNED	CLIENT/MASTER FLOAT32IEEE
1	1/2001	4001/6001	8001
2	2/2002	4003/6003	8003
3	3/2003	4005/6005	8005
to	to	to	to
1000	1000/3000	6000/8000	10000
to	to	N/A	N/A
2000	2000/4000	N/A	N/A


Caution Max 2000 16bit registers or 1000 32bit registers per server/slave, per Function Code.


To create ModBus Servers/Slaves and registers

1. Press **'Add'** to display a page required to specify the required server/slave address.
2. Enter the required server/slave address and press **'Save'** to confirm. This will add a default configuration.



Press  to delete the existing server/slave address and any configured registers.

Press  to show page used to change the existing server/slave address.

Press  to show a page used to duplicate the selected server/slave address and registers to one or more server/slave addresses.

- i. Enter the required server/slave address.

Tip! A range of servers/slaves addresses can be defined, i.e. 2-10, 14, 25.

- ii. Press **'Add'** to list the server/slave addresses to be added to the Define Points page.



Tip! Use the **'☑'** to select slave addresses that can be removed from the list of requested slave addresses. Press **'Delete'** to remove selected server/slave addresses.

- iii. Press **'Save'** to confirm this list of new server/slave addresses.

3. Press '>' to insert a pre-defined row. Edit as necessary.

Register	Quantity	Function	Factor	Access
1	1	1 - Coils	1	R/W
1	1	2 - Inputs	1	R/O
1	1	3 - Holding registers	1	R/W
1	1	4 - Input registers	1	R/O

Reg. Used to define the ModBus Server/Slave register that will show a value from the linked point. Edit as necessary.

Qty. Used to define a number of sequential ModBus register, i.e., register (00)21 and Qty 5 will give registers (00)21 to (00)25 inclusive.

Tip! To avoid confusion, ensure Qty is 1. Set the ModBus Client/Master to poll continuous registers where appropriate.

Function. Used to define the type of value provided by the source point. Each function (type of action) is identified by a group of specific memory addresses, i.e., coils, inputs, holding registers, and input registers. Each message (communication packet) includes a function code in the range of 1 to 55 Hex (1 to 255 decimal), but a function code in the range of 80 to 55 Hex (128 to 255 decimal) are reserved for exception responses.

FUNCTION (CODE)	DEC ADDR.	DESCRIPTION
-----------------	-----------	-------------

Coils (01)	1 - 10000	A single-bit Read/Write (R/W) Boolean (True/False, On/Off, or 1/0) ModBus register value, e.g., controlling a State.
Inputs (02)	10001 - 20000	A single-bit Read Only (R/O) Boolean (True/False, On/Off, or 1/0) ModBus register value, e.g., showing a State.
Holding registers (03)	40001 - 50000	A 16-bit word Read/Write (R/W) Integer/Float IEEE ModBus register value, e.g., controlling a condition.
Input registers (04)	30001 - 40000	A 16-bit word Read Only (R/O) Integer/Float IEEE ModBus register value, e.g., showing a condition.

Tip! The 'Comms traffic' page is used to validate the outgoing and incoming messages to/from the ModBus Client/Master and verify the response to a specific request.

Factor. Used to apply a scaling factor to a value from the linked point before the ModBus Client/Master polls the register.

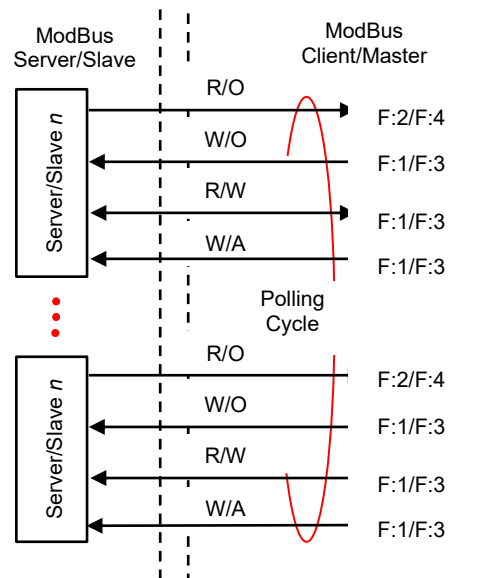
Tip! To avoid confusion, ensure Factor is 1.

Access. Used to define the type of operation applied to the selected register.

Note R/O, R/W and W/O operations are performed when a value has changed. The 'write-always' (W/A) access type provides a write command every cycle. This can be used to continually write the same value to the register, e.g., perform a heartbeat function.

Tip! To avoid confusion, ensure use R/W for Function 1 & Function 3, & R/O for Function 2 and Function 4.

4. Press **'Save'** to confirm changes.



2.5.8 Define vIQ Driver Points

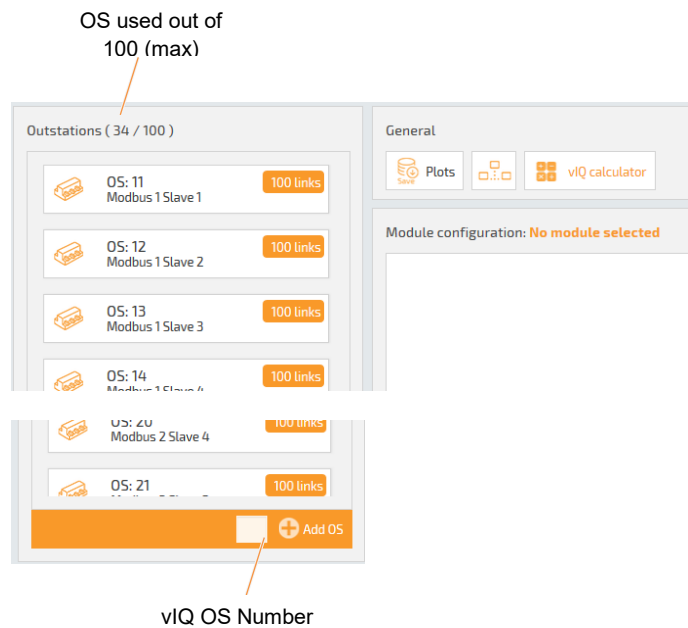
The vIQ Driver is the Synapsys Solutions Trend BMS compatible software. Each vIQ OS appears as an individual Trend controller.

Each product supports 100 vIQ OSs.

To create an vIQ OS

1. Define the required vIQ OS number in the appropriate field.
2. Press **'Add OS'** to include a default vIQ OS with the defined vIQ OS number in the list above.

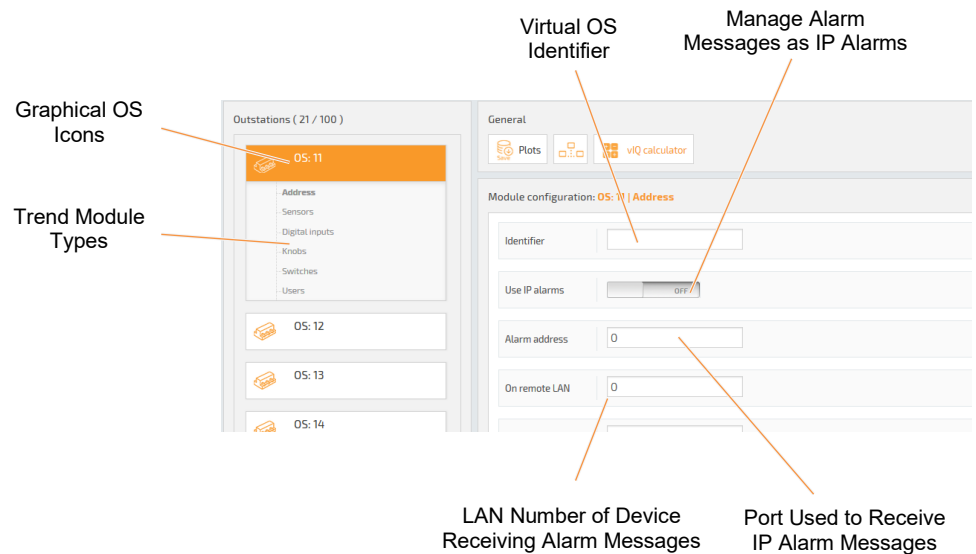
Tip! Number of existing Links per vIQ OS are shown.



CONFIGURE THE ADDRESS MODULE

The 'Address Module' page displays information relating to the module selected from the graphical list of OS icons already created using the OS network window.

Note The device receiving alarm messages can be identified using the 'Alarm Address' and 'On Remote LAN' fields, or the 'IP' and 'Port' fields if 'Use IP Alarms' is enabled.



Caution Identifier does not support '\ / ({ ; , : ' invalid characters.

To configure the module details

1. Configure the **'Address Module'** details. This page provides parameters used to identify each individual OS and configure the alarm message transmission path.
 - i. Select the required OS from the list of graphical icons and press **'Address Module'** if the Address Module details are not displayed.
 - ii. Configure the alarm message transmission path.

Tip! The text above the Module type buttons identifies the selected out-station.

- ◆ If necessary, enter text in the **'Identifier'** field. This identifies the OS associated with the defined slave in this product and BeMS.

Use standard alarm message transmission (default **'Alarm address'** and **'On remote LAN'** values define a local connection).

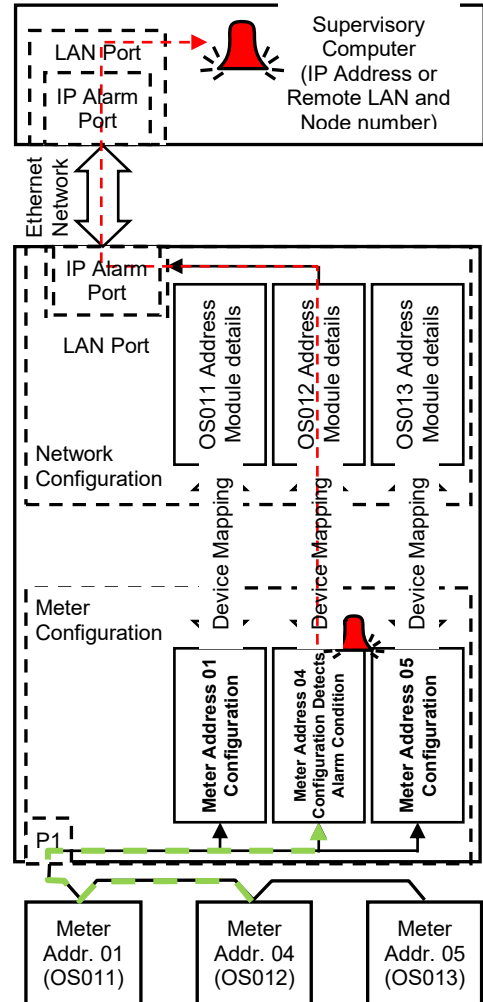
Enter the **'Alarm Address'** number. This identifies the device on the Ethernet network used to display alarms generated by the third-party devices on the network. Enter the **'On Remote LAN'** number. This identifies the LAN that includes the device on the Ethernet network used to display asserted alarms.

Alternatively, use IP alarm message transmission (default **'Use IP alarms'**, **'IP address'** and **'Port'** values define a local connection).

Enable IP alarms (Internet Protocol), i.e., **'Use IP alarms'**. This allows the transmission of IP alarm signals, but not Trend alarms, to the BeMS. Enter the **'IP address'**. This identifies the device on the BeMS that will receive alarms messages. Enter the **'Port'** number. This identifies the internal port used to receive IP alarm messages.

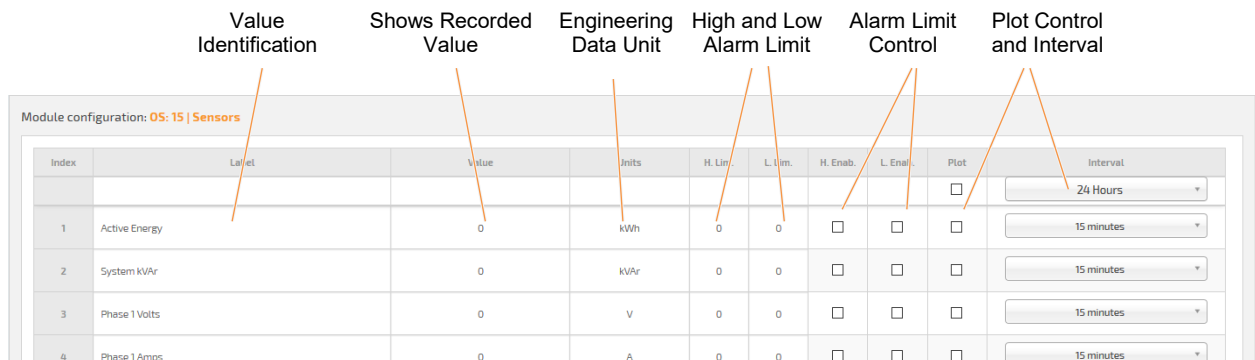
Note The IP address must be configured according to local company network policy.

3. Press **'Save'** to confirm changes.



CONFIGURE A SENSOR MODULE

The **'Sensors'** page displays read-only Integer values in the specified engineering units recorded by the corresponding third-party device. The parameters on this page are also used to define and enable required alarm levels and determine the plot intervals.



Index	Label	Value	Units	H. Lim.	L. Lim.	H. Enab.	L. Enab.	Plot	Interval
1	Active Energy	0	kWh	0	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	24 Hours
2	System KVAr	0	KVAr	0	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	15 minutes
3	Phase 1 Volts	0	V	0	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	15 minutes
4	Phase 1 Amps	0	A	0	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	15 minutes

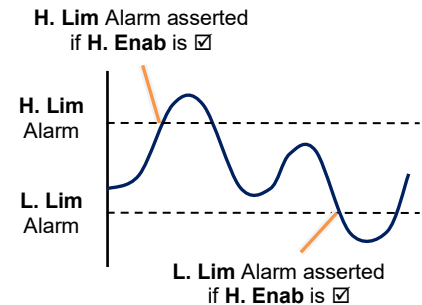
To configure a Sensor module

1. Press **'Sensors'** to display the Sensor module configuration page.
 - i. Enter text (40 characters max) used to identify the associated parameter in the **'Label'** field. This is used to identify the parameter in the BeMS. It should be a concise description of the parameter.

Caution Identifier does not support '\ / ({ ; , : ' invalid characters.

- ii. Inspect the **'Value'** field. This displays the value recorded from the parameter defined in the **'Link points'** page.
- iii. Enter the appropriate engineering data value type in the **'Unit'** field. This appears in the BeMS and is used to identify the engineering data value, i.e. A (amps) if scaling a value measuring a mA signal.

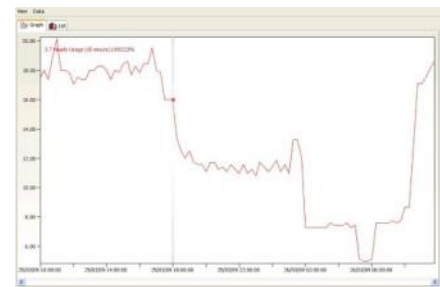
- ◆ If necessary, enter a value used to specify the high alarm limit in 'H. Lim.' and/or the low alarm limit in 'L. Lim.'. This is used to define the upper and/or lower limits of the value recorded from the parameter. If a limit is exceeded the corresponding alarm in the BeMS will only be asserted if 'H. Enab.' and/or 'L. Enab.' is enabled ()



Remember A configured low alarm limit value must be less than the defined high alarm limit.

- ◆ If necessary, enable () the high alarm limit ('H. Enab.') and/or low alarm limit ('L. Enab.'). This control the high alarm and low alarm indication in the BeMS, when the value recorded from the parameter asserts an alarm state determined by the value defined in 'H. Lim.' and/or 'L. Lim.'. If this field is disabled () an alarm state will not be indicated.
- ◆ If necessary, enable () the plot function. This allows the Trend graph in the BeMS to plot 1000 value records from the parameter. If this field is disabled () a Trend will not be generated.

Note A Trend is a graphical representation of a value from a defined point at regular time periods. The period is synchronised to the real-time clock in this product. The Trend Sensor module appears as the value in Plots page of Trend BeMS.



Tip! Plot data logged in this product can be recorded by the Trend Supervisor (963) before it is overwritten using the RECORDAUTO_COMPACT action or RECORDAUTO_PRECISION action. This is automatically run when Buffer Ready Events (BBUF) are received from this product. Refer to Trend Controls documentation for details.

- ◆ If necessary, select the required plot interval, from 1 minute to 24 hours. This defines the period between each plot of the corresponding recorded value on the Trend graph in the BeMS.

Tip! Press 'Copy/paste data' button to display a dialog. Use 'Copy to clipboard' to add all the module information (excluding Values) to the computer clipboard or click the right-hand mouse button in the white square and select 'Paste' from the context menu to add copied information to the Module page. Module information can be edited using .CSV editing software, e.g., Microsoft Excel.

4. Press 'Save' to confirm changes.

CONFIGURE A DIGITAL INPUT MODULE

The **'Digital Inputs'** page displays read-only Boolean values recorded by the parameter in the corresponding third-party device. The parameters on this page are used to enable required alarms and inspect and control the status of a specific engineering data value from this product.

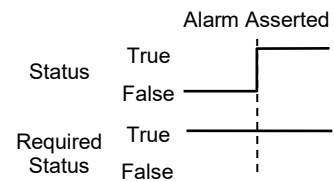
Module configuration: 05.15 Digital inputs Value		Shows Current Digital Value	Alarm Control	Shows Required Digital Value	
Index	Identification Label		Value	Alarm enable	Required status
1			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

To configure the Digital Input

1. Press **'Digital Inputs'** to display the Digital Input module configuration parameters.
 - i. Enter text (40 characters max) in the **'Label'** field. This is used to identify the parameter in the BeMS. It should be a concise description of the parameter.

Caution **Identifier does not support '\ / ({ ; , : ' invalid characters.**

- i. Inspect the **'Status'** field. This displays the current condition of the recorded Digital Input value.
 - ◆ If necessary, enable () the alarm detection state in **'Alarm enable'**. This controls the alarm indication when the recorded value asserts an alarm state, determined by the **'Required Status'**. If this field is disabled () an alarm state will not be indicated.
 - ◆ If necessary, define the required alarm indication state in the **'Required Status'** field. A healthy state is shown if **'Status'** is (1, True, Enabled, or On), and **'Required Status'** is (0 (zero), False, Disabled, or Off). An unhealthy state (alarm state asserted) is shown if the **'Status'** and the **'Required Status'** are the same.

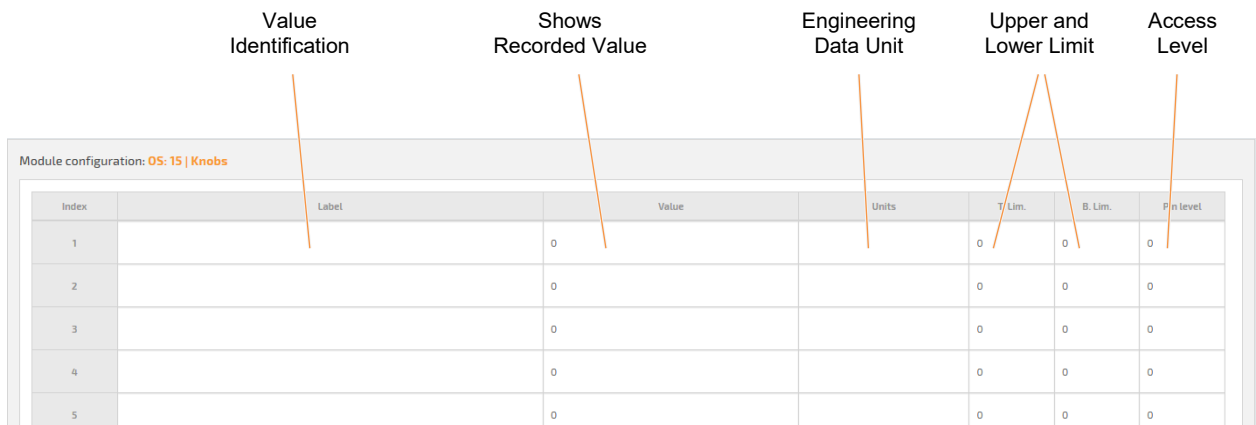


Tip! Press **'Copy/paste data'** button to display a dialog. Use **'Copy to clipboard'** to add all the module information (excluding Status) to the computer clipboard or click the right-hand mouse button in the white square and select **'Paste'** from the context menu to add copied information to the Module page. Module information can be edited using .CSV editing software, e.g., Microsoft Excel.

2. Press **'Save'** to confirm changes.

CONFIGURE A KNOB MODULE

The 'Knobs' page displays read and write Integer values in the specified engineering units recorded by the parameter in the corresponding third-party device. The parameters on this page are used to configure the authorisation level required to inspect and/or control a specified Knob Module value within the defined limits.



Module configuration: 05:15 | Knobs

Index	Label	Value	Units	T. Lim.	B. Lim.	Pin level
1		0		0	0	0
2		0		0	0	0
3		0		0	0	0
4		0		0	0	0
5		0		0	0	0

To configure a Knob module

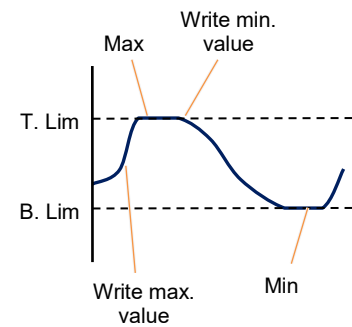
1. Press 'Knobs' to display the Knob module configuration page.
 - i. Enter text used to identify the parameter in the 'Label' field. This is used to identify the value in this product and the BeMS. It should be a concise description value.

Caution Identifier does not support '\ / ({ ; , : ' invalid characters.

- ii. Inspect the 'Value' field. This displays the value recorded from the parameter defined in the 'Link points' page.

Note If an authorisation level has been configured, an appropriate pin number must be entered correctly before a write command to this module type can be confirmed.

- iii. Enter the appropriate engineering data value type in the '**Unit**' field. This appears in the BeMS and is used to identify the engineering data value recorded, i.e. A (amps) if scaling a value measuring a mA signal.
- ◆ If necessary, enter a value used to specify the maximum value allowed in '**T. Lim.**' and/or minimum value allowed in the '**B. Lim.**'. This is used to define the maximum and/or minimum value that can be written to the parameter using the corresponding engineering units.
- iv. Enter the required '**Pin level**' number. This is the authorisation level used to prevent un-authorised access to the engineering data. A '**Pin level**' number should already have been configured via the '**Users**' page (see [Configure the Pin Level Authorisation](#)).




Tip! Press '**Copy/paste data**' button to display a dialog. Use '**Copy to clipboard**' to add all the module information (excluding Values) to the computer clipboard or click the right-hand mouse button in the white square and select '**Paste**' from the context menu to add copied information to the Module page. Module information can be edited using .CSV editing software, e.g., Microsoft Excel.

2. Press '**Save**' to confirm changes.

CONFIGURE A SWITCH MODULE

The '**Switches**' page displays read and write Boolean values that have been recorded by parameter in the corresponding third party device. The parameters on this page are used to inspect and/or control the status and authorisation level.



Index	Label	Status	Pin Level
3		<input type="checkbox"/>	0
4		<input type="checkbox"/>	0
5		<input type="checkbox"/>	0
6		<input type="checkbox"/>	0
7		<input type="checkbox"/>	0

To configure the switch

1. Press '**Switches**'. This displays the Switch module configuration parameters.
 - i. Enter text used to identify the parameter in the '**Label**' field. This is used to identify the parameter in the controller. It should be a concise description of the parameter.

Caution Identifier does not support '\ / ({ ; , : ' invalid characters.

- ii. Inspect the '**Status**'. This shows the current condition of the corresponding parameter in the 'Switch' module, where is 1, True, Enabled or On.

Note If an authorisation level has been configured, an appropriate pin number must be entered correctly before a write command to this module type can be confirmed.

- iii. Enter the required '**Pin level**' number. This is the authorisation level used to prevent unauthorised access to the parameter. A Pin level number should already have been configured via the '**Users**' page (see [Configure the Pin Level Authorisation](#)).

Tip! Press 'Copy/paste data' button to display a dialog. Use 'Copy to clipboard' to add all the module information (excluding Status) to the computer clipboard or click the right-hand mouse button in the white square and select 'Paste' from the context menu to add copied information to the Module page. Module information can be edited using .CSV editing software, e.g., Microsoft Excel.

2. Press '**Save**' to confirm changes.

CONFIGURE THE PIN LEVEL AUTHORISATION

A maximum of six authorisation levels, Pin Levels, and associated Pin Numbers can be configured via the **'Users'** page which is displayed when **'Users'** is selected. Each **'Pin Level'** determines the minimum level of authorisation required to change module parameters. Any **'Pin Level'** of 94 or below only permits changes to the values on **'Knobs'** pages and status on the **'Switches'** pages. However, a **'Pin Level'** of 95 or above permits changes to all module parameters, and includes **'Labels'**, **'Units'** and changing the Pin Numbers that are assigned to a Pin Level less than current Pin Level.

Caution Values will not appear on the 'viQ pages' if a 'Pin number' is configured, but the 'Trend security' on protocol dependant web page is not.

Module configuration: 05: 15 | Users

Index	Pin number	Pin level
1		0
2		0
3		0

To configure the authorisation levels

1. Press **'Users'** to display the Pin Level configuration page. Each 'Pin Level' is associated with a 'Pin Number' that is used to confirm the current users' authorisation to change the edited parameter.

- i. Enter a **'Pin level'** number in the range 0 to 99. This number is an authorisation level relating to the **'Pin Number'**.


Tip! Always configure an administrative 'Pin Level' first (Pin Level 99).

- ii. Enter a maximum 4-digit security number in the **'Pin Number'** field. This number is used to confirm the user is allowed to change a module parameter using 'Text comms'.

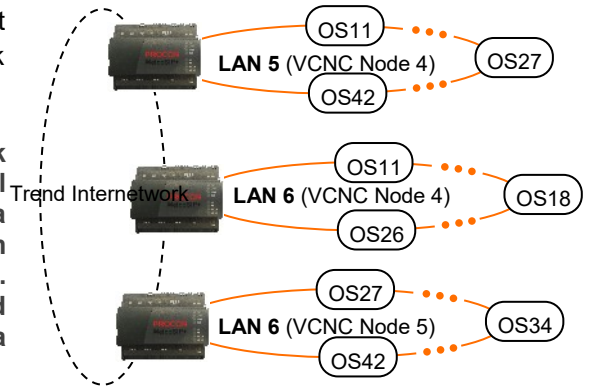
Note Text comms enables user-entered read and write requests to module parameters.


2. Press **'Save'** to confirm changes.

VERIFY TREND NETWORK STATUS

Use the  button to show a page displaying the status of the system, LAN and Internetwork. It can be used to diagnose and indicate network problems.

Note An Internetwork is a communication link between Trend LANs, (Local LAN is local to the connection, and Remote LAN a Local Area Network (LAN) accessed from the reference device via the Internetwork). A Trend LAN is a number of connected nodes; each node is used to connect a LAN, i.e., the VCNC port.



- Press  to display the 'Network Status' dialog.

PARAMETER	DESCRIPTION
System Uptime	The amount of time this product has been operating, i.e. since this product was last turned on or rebooted.
Lan OK Time	The amount of time the Lan has been successfully communicating on the Trend network, i.e., since the last build process was successful.
Lan Status	The current condition of the Lan corresponding to this product and the time remaining until a 'Timeout' will occur.
	Lan POWERUP The Lan build process is starting.
	Lan DEAF The comms with other Trend network devices are not applicable (only 1 (one) device in Lan) or not available (more than 1 (one) device in Lan, see 'Lan BROKEN').
	Lan BROKEN A comms failure with other devices on the Lan. Typically, due to a timeout caused by Ethernet wiring or connection problem, an IP address that is sending but not receiving messages, duplicate OS numbers from identified IP address on the Lan or when a Lan is changed, i.e., identified IP address is added or removed.
	Lan BUILT The Lan build process is successful.
	Lan OK! Successful Lan comms are detected if product is not alone on local Lan or if it can communicate with other devices on the local Lan.


continued...

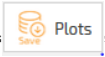
PARAMETER	DESCRIPTION
continued...	
Last Lan Message	The last message from describing the Lan status, see 'Lan Status'.
Internetwork OK Time	The amount of time the Internetwork has been successfully communicating, i.e., since the last Internetwork build process was successful.
Internetwork Status	The current condition of the Internetwork assigned to this product and the time remaining until a 'Timeout' will occur.
Internetwork POWERUP	The Internetwork build process is starting.
Internetwork DEAF	The comms failure with other Trend network devices is not applicable (only 1 (one) device in Internetwork) or not available (more than 1 (one) device in Internetwork, see ' <i>Internetwork BROKEN</i> ').
Internetwork BROKEN	An Internetwork comms failure. Typically, due to a timeout caused by an Ethernet wiring or connection problem, duplicate Lan numbers from an identified IP address on the Internetwork or when the Internetwork is changed, i.e., identified IP address is added or removed.
Internetwork BUILT	The Internetwork build process is successful.
Internetwork OK - Timeout in <i>nn</i>	Successful Internetwork communications and number of seconds until Timeout is detected, i.e., when ' <i>nn</i> ' shows '00'.
Last Internetwork Message	The last message from describing the Internetwork status, see 'Internetwork Status'.

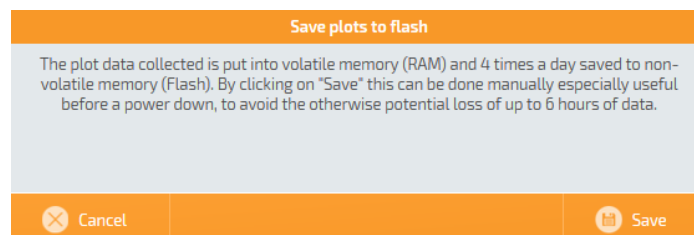
- If necessary, correct any issues that may be indicated.

Tip! If necessary, use 'SIP Search' to ensure IP Addresses are unique. Use Trend 'ipTool' to ensure Lan numbers (and VCNC Node numbers where necessary) are unique.

SAVE PLOTS TO FLASH

The  button is used to display a dialog that provides the functionality to save the current vIQ OS plot values. Saving these values ensures all selected plot data is included when a **'Backup'** is performed. The plot data will be automatically loaded when a **'Restore'** is performed.

1. Press  to display the **'Save plots to flash'** dialog.
2. Press **'Save'** to save the current plot data immediately. This can prevent the loss of data before using the 'Restore' function.

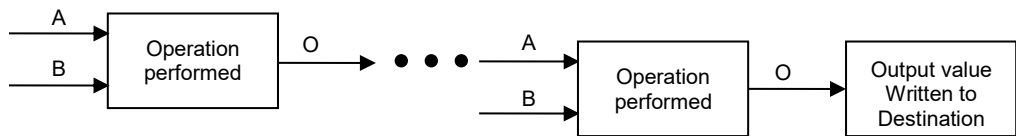


Note Plot data is saved to flash at regular 6 hours intervals, 00:00, 06:00, 12:00 and 18:00. Performing this operation does not affect this function.

Caution **Rebooting or removing the power from this product before all plot data is saved may corrupt plot data files or cause loss of essential energy data. It takes about 1.5 secs to save a plot data file, and approximately 20 mins to save the maximum 1024 plot data files.**

USE THE VIQ CALCULATOR

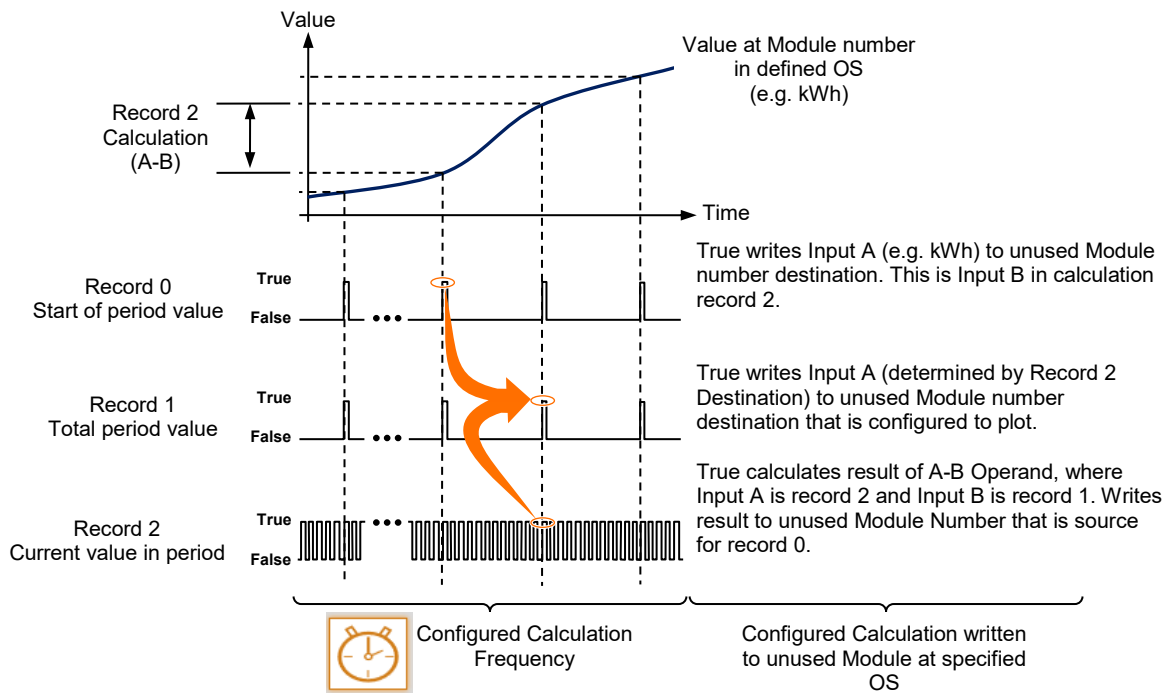
The vIQ Calculator page allows the user to influence an output value to a specified Module type by performing a sequence of up to 5 operations at specified intervals. Each operation is constructed using a combination of values sourced from a defined Module number at a specified OS or a user defined fixed value.



Note
A and B - Fixed Value or vIQ Module Value
O - Output (Result of A and B)

The final operation provides an output that should be written and stored at an unused Module number in the defined OS. This may be the partial result of a combination of multiple vIQ Calculations which produces a completed result at a scheduled frequency. This is useful when investigating energy usage.

Example This example shows 2 vIQ Calculations that provide partial results for a third vIQ Calculation. Index 0 shows the total usage over the last configured calculation period and writes the value to an unused Module number at a defined out-station. Index 1 shows the starting usage from second unused Module number at a defined out-station. Index 2 calculates the total usage at configured intervals.



This page provides sections that,

- identify each calculation,
- show the sequence of operations combined for a selected calculation,
- configure the frequency of a selected calculation and each operation (e.g., A+B, A-B, etc.) in the calculation.

Note **The Calculator supports a maximum of 1000 calculations.**

The screenshot displays the configuration interface for a calculator. It is divided into three main sections:

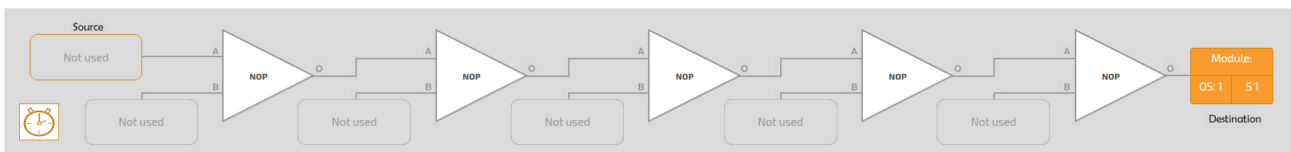
- Calculations Table:** A table with columns for Index, Label, and Frequency. It contains one entry: Index 1, Label 'Calculation 1', and Frequency 'Every 10 seconds'.
- Frequency configuration:** Two dropdown menus for 'Frequency type'. The first is set to 'Every given seconds' and the second is set to '10'.
- Graphical Operation Icons:** A flow diagram starting from a 'Source' module (OS: 11, S1) and ending at a 'Destination' module (OS: 43, S1). The flow consists of a sequence of operations: 'A / B', followed by three 'NOP' (No Operation) blocks, and finally 'A * B'. Each operation block has a 'Value' field set to '1000'. Below each operation block is a 'Not used' button.

Annotations with orange lines point to the 'Calculations Table', 'Frequency Schedule or Operation', and 'Graphical Operation Icons'.

CREATE THE VIQ CALCULATION

Each vIQ Calculation is referenced using an 'Index' number and is performed at intervals determined by the configured 'Frequency' schedule. The 'Index' number is identified by a 'Label' that can be edited to clarify the purpose of the individual vIQ Calculation.

Remember **The Calculator supports a maximum of 1000 calculations.**



To create a vIQ Calculation table,

The vIQ Calculation table is used to assign an Index number to a specific calculation and provides a simple means of tracking the calculations. It will also show the total number of calculations configured in this product.

Tip! **Press 'Calculator' to refresh the page. This will ignore unsaved changes and restore the page to the last known configuration. Press 'Go back' to return to the 'vIQ' driver Define points page.**

1. Create a blank vIQ Calculation.

Press 'Add Calculation' to add a blank vIQ Calculation using the next available Index number.

Index	Label	Frequency
1	Energy at Start of period	Every 10 seconds
2	Calculation 2	Never


Alternatively,

- ◆ drag calculations to list in a specific sequence
- ◆ select 'Select all' or 'Unselect all' from the available menu option as necessary
- ◆ select 'Delete' from the available menu option to remove the selected calculations
- ◆ select 'Move to' to re-order the list of current calculations
- ◆ press 'Wizard' to create a specific number of calculations (see [Replicate an Existing vIQ Calculation](#)).

Note **All Index numbers will be automatically re-numbered.**


- If necessary, change the text in the 'Label' field used to identify the calculation.

Tip! **Use a brief description to clearly indicate the purpose of the calculation.**

Note **The Frequency of a blank calculation is scheduled to 'Never', i.e., it will not run.**
Use the  in the graphical vIQ Calculation to display parameters that configure frequency schedule.

CONFIGURE THE VIQ CALCULATION

A vIQ Calculation can be used to perform a calculation using a value sourced from a defined Module number in a specified out-station or a user defined fixed value which produces an output value that can be written to a defined Module Type. Each vIQ Calculation Index corresponds to a configured sequence of 5 graphically represented operations displayed below the vIQ Calculation Index table.

Note Each vIQ Calculation can be scheduled using parameters that are displayed when the  is pressed.

Tip! An area below the graphical vIQ Calculation displays information that may be useful configuring a vIQ calculation.

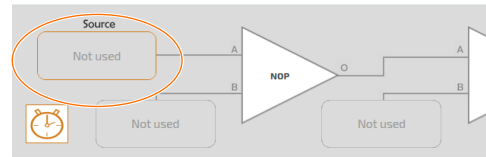
To configure a vIQ Calculation

1. Select the required vIQ Calculation.

This displays a sequence of 5 operations. Each mathematical operation is pre-configured as a **'No Operation'**, i.e., the input value will remain unchanged.

2. Configure the Input values. Input values can be sourced from a defined Module number in a specified OS or can be a user defined fixed value. Starting at the Source,
 - i. Configure **Source** (Input A) value type.

Select the Source (Input A) operand configuration icon to display the parameters used to define the Source Input A value.



Define the origin of Input A value by selecting a **'Fixed value'** (user defined value) or **'Module'** (Module number in a specified out-station) **'Operand type'**.

If **'Fixed value'** is selected, enter the required value at the 'Fixed value' parameter.

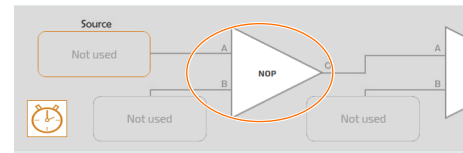
If **'Module'** is selected, define the required OS number at **'OS'**, define the number of the Module at **'Module number'** and select the corresponding type of Module at **'Module type'**.



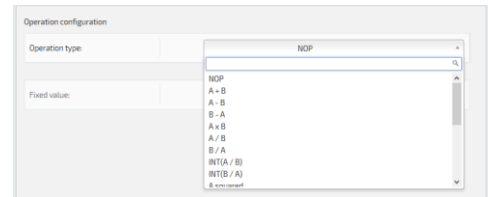
Tip! All this information should be available on the configuration web pages.

ii. Configure the mathematical operation.

Select the Input B operand configuration icon to display the parameters used to configure the mathematical operation.



Select the mathematical operation used to determine the output using the values derived from Input A and Input B at the '**Operation type**'.



Note

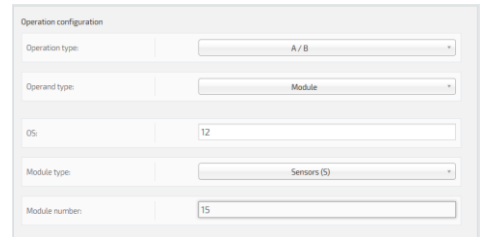
Input A is already defined from the Source or previous operation.

OPERATION TYPE	DESCRIPTION
NOP	Input value is unchanged, No Operation
A + B	Add A and B (e.g., 9 + 3 = 12)
A - B	Subtract B from A (e.g., 9 - 3 = 6)
B - A	Subtract A from B (e.g., 3 - 9 = -6)
A x B	Multiply A by B (e.g., 9 x 3 = 27)
A / B	Divide A by B (e.g., 9.3 ÷ 3 = 3.1)
B / A	Divide B by A (e.g., 3 ÷ 9 = .333)
INT(A / B)	Divide A by B (e.g., 9.3 ÷ 3 = 3), whole integers, no decimal places
INT(B / A)	Divide B by A (e.g., 3 ÷ 9 = 0), whole integers, no decimal places
A squared <A ² >	Multiply A by A (e.g., 9 x 9 = 81)
A cubed <A ³ >	Multiply A by A by A (e.g., 9 x 9 x 9 = 729)
A to the power of B <A ^B >	Multiply A by A using B to define the power ratio (e.g., if B = 5, sum 9 ⁵ = 9 x 9 x 9 x 9 x 9 = 59,049)
2 to the power of A <2 ^A >	Multiply 2 by 2 using A to define the power ratio (e.g., if A = 9, sum 2 ⁹ = 2 x 2 x 2 x 2 x 2 x 2 x 2 x 2 x 2 = 512)
10 to the power of A <10 ^A >	Multiply 10 by 10 using A to define the power ratio (e.g., if A = 9, sum 10 ⁹ = 10 x 10 x 10 x 10 x 10 x 10 x 10 x 10 x 10 = 1 000 000 000)
B to the power of A <B ^A >	Multiply B by B using A to define the power ratio (e.g., A = 9, sum 3 ⁹ = 3 x 3 x 3 x 3 x 3 x 3 x 3 x 3 x 3 = 19,683)
Square root of A	A = n ² (e.g., 9 = 3 x 3)
A % B	A% of B (e.g., 50% of 200 = 100)
Truncate A	Ignores decimal places (e.g., Truncate 9.333 = 9)
A Modulus B	Divide A by B and display the remaining value (e.g., if 10 ÷ 3 = 3 + remainder 1, then 10 Modulus 3 = 1)

Define the origin of Input B value by selecting a 'Fixed value' (user defined value) or '**Module**' (Module number in a specified out-station) '**Operand type**'.

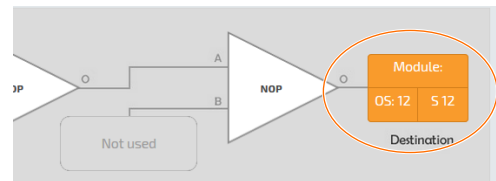
If '**Fixed value**' is selected, enter the required value at the 'Fixed value' parameter.

If '**Module**' is selected, define the required Out-station number at '**OS**', define the number of the Module at '**Module number**' and select the corresponding type of Module at '**Module type**'.



Tip! All this information should be available on the VIQ Driver 'Define Points' page.

- iii. Press '**OK**' to confirm changes.
 - ◆ If necessary, configure the remaining mathematical operations as required using the previous instructions.
3. Configure the destination OS and module type used to display the output value.
 - i. Select the **Destination OS/Module Type** configuration icon to display the parameters used to identify the OS and module type used to display the output value.
 - ii. Enter the required OS number at '**OS**', the number of the module at '**Module number**' and select the corresponding type of module at '**Module type**' (Sensor (S), Digital Input (I), Knob (K), or Switch (W)).
 - iii. Press '**OK**' to confirm changes.



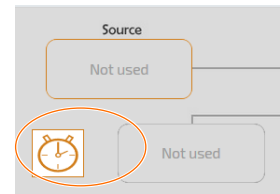
Tip! All this information should be available on the VIQ Driver 'Define Points' page.

CONFIGURE THE 'FREQUENCY' SCHEDULE

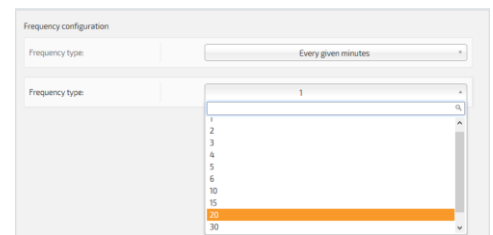
The '**Frequency**' schedule determines the time period between repeating the selected vIQ Calculation. A vIQ Calculation can be configured to occur at a pre-defined time period or at a user defined time period.

To configure the 'Frequency' schedule

1. Select the '**Frequency**' configuration icon to display parameters that configure calculation schedule. Calculations can be configured to occur at a pre-defined time period or a user defined time period.
 - i. Select a pre-defined or user defined time schedule in '**Calculation frequency**'.



A pre-defined schedule performs the calculation at specific occurrences, i.e. '**At first run**', '**At midday**', '**At midnight**', '**A new month**', '**A new year**' or '**Never**'. The calculation will not be performed if '**Never**' is selected.



A user defined schedule performs the calculation at regular periods, i.e. '**Every given seconds**', '**Every given minutes**', '**Every given hours**', or '**Every given days**' determined by the value configured in '**Parameter**', i.e. if '**Parameter**' is 10, and '**Calculation frequency**' is 'Every given hours' the calculation will be performed at regular intervals of 10 hours.

- ii. Press '**OK**' to confirm changes.
2. Press '**Save**' to confirm changes.

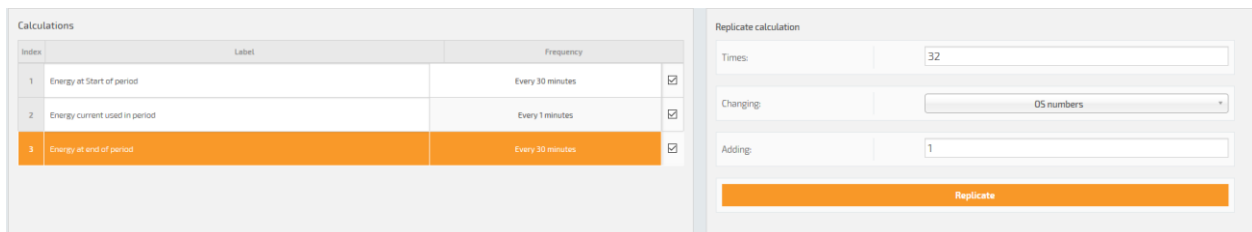
REPLICATE AN EXISTING VIQ CALCULATION

An existing vIQ Calculation will perform a sequence of mathematical operations that are also applicable or similar to the requirements of other vIQ Calculations. By replicating a selected a calculation, the corresponding sequence of mathematical operations can be automatically assigned to a defined out-station and module in each calculation record.

Example This shows the automatic configuration of out-station numbers when replicating an existing vIQ Calculation record. This can also apply to module numbers.

To replicate an existing vIQ Calculation

1. Replicate the selected vIQ Calculation record.
 - i. Press **'Wizard'** to display the parameters used to configure how the selected vIQ Calculation must be adjusted.
 - ii. Select the Calculations that are to be replicated.
 - iii. Enter the number of calculations to be added to the vIQ Calculation table in **'Replicate'**. The additional calculation records are automatically populated using the selected vIQ Calculation.



Index	Label	Frequency	
1	Energy at Start of period	Every 30 minutes	<input checked="" type="checkbox"/>
2	Energy current used in period	Every 1 minutes	<input checked="" type="checkbox"/>
3	Energy at end of period	Every 30 minutes	<input checked="" type="checkbox"/>

Replicate calculation

Times:

Changing:

Adding:

Replicate

Select **'OS numbers'** or **'Module numbers'** in **'Changing'**. This determines the numerical references that are adjusted when the vIQ Calculation corresponding to the selected calculation record is replicated, i.e. if **'OS numbers'** is selected, all numerical out-station references in each mathematical operation is offset by the value defined in **'Adding'**, or if **'Module numbers'** is selected, all numerical Module references in each vIQ Calculation are offset by the value defined in **'Adding'**.

Enter a value in **'Adding'**. This determines the offset for the numerical references defined in **'Changing'** when the selected calculation record is replicated, i.e. if this value is **'2'** and **'OS numbers'** is selected, all numerical out-station references in each vIQ Calculation are offset by the **'2'**.

Tip! Enter a minus (-) number in **'Adding'** to decrease the **'OS numbers'** or **'Module numbers'** defined in **'Changing'**.

- iv. Press **'Replicate'** to perform the request changes.
2. Press **'Save'** to confirm changes.

2.6 LINK POINTS

The 'Link points' page is used to associate 1 (one) protocol driver Input point to another designated driver, i.e., Melco driver to BACnetIP server, Data Acquisition and/or Trend server.

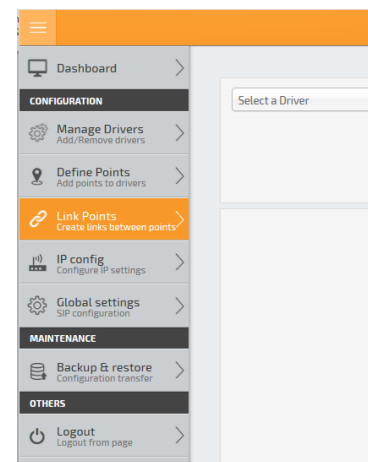
Caution Do NOT link multiple drivers together, e.g., Mitsubishi Melco to vIQ Sensor to REST Server point.

2.6.1 Link defined points

All existing defined points are listed according to the Driver type.

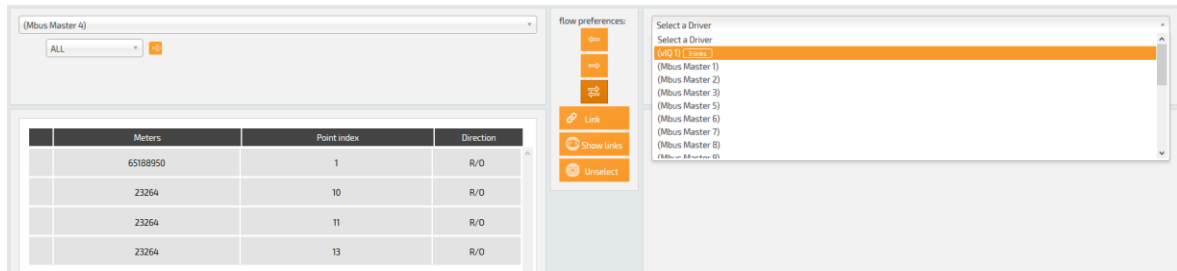
- Select 'Link points' and select the required driver to show the driver related configuration pages.

Caution Always create a second link from the source parameter, e.g., Mitsubishi Melco to vIQ Sensor and Mitsubishi Melco to REST Server point.



LINK POINTS BETWEEN DRIVERS

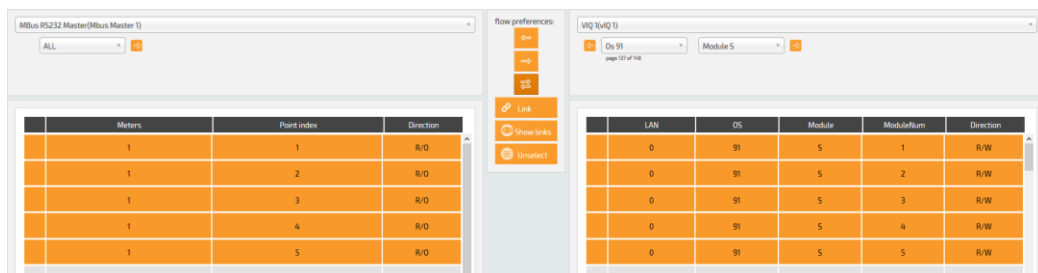
The 'Link points' page shows 2 (two) tables that allow the defined points from 1 (one) driver to be linked to the defined points in the other driver.



1. Select the required drivers.
 - i. Select the required driver on the left to show a list of the existing 'Define points' for the selected driver.
 - ii. Select the require driver on the right to show a list of the existing 'Define points' for the selected driver.

Tip! Use the available filters to ensure specific 'Defined points' are shown.

2. Select the required points from the drivers.
 - i. Select the required points on the left from the list of existing 'Define points' for the selected driver.
 - ii. Select the required points on the left from the list of existing 'Define points' for the selected driver.



Tip! The number of points selected is shown below the list of points.

Press '**Unselect**' to remove all currently selected '**Defined points**'.

- iii. Define the 'Flow preference' to determine the read only/write only flow of data between the 2 (two) lists of points.

Caution The 'Flow preference' **MUST** be selected according to the read only/write only flow of data between the 2 (two) lists of points.

- ◆ Press **'Link'** to show a page used to verify and confirm the link between the selected **'Defined points'**.

Ensure the points are correctly linked, and press **'Manage links'** to confirm the link.

	meter	index	links	LAN	OS	Module	ModuleNum
<input type="checkbox"/>	1	1	on	0	91	5	1
<input type="checkbox"/>	1	2	on	0	91	5	2
<input type="checkbox"/>	1	3	on	0	91	5	3
<input type="checkbox"/>	1	4	on	0	91	5	4
<input type="checkbox"/>	1	5	on	0	91	5	5
<input type="checkbox"/>	1	1	on	0	11	5	1
<input type="checkbox"/>	1	2	on	0	11	5	2

Tip! To remove the link between **'Defined points'** that are not necessary, enable the points that are not required and press **'Delete'**.

- ◆ Press **'Show Link'** to show a page displaying all existing link between the selected **'Defined points'**.

Ensure the points are correctly linked, and press **'Manage links'** to confirm the link.

	meter	index	links	LAN	OS	Module	ModuleNum
<input type="checkbox"/>	1	1	on	0	91	5	1
<input type="checkbox"/>	1	2	on	0	91	5	2
<input type="checkbox"/>	1	3	on	0	91	5	3
<input type="checkbox"/>	1	4	on	0	91	5	4
<input type="checkbox"/>	1	5	on	0	91	5	5

Tip! To remove the link between **'Defined points'** that are not necessary, enable the points that are not required and press **'Delete'**.

3. Press **'Save'** to confirm changes.


2.7 MANAGE CONFIGURATION TRANSFER

The main menu page provides access to the **'Backup and restore'** function.

2.7.1 Backup and restore unit configuration

The **'Back up'** function allows a copy of the configuration in this product to be protected in a secure environment that prevents un-authorized access and/or damage. It creates a backup of the configuration to a defined media/location which can be used to restore this product configuration to a previous state.

Tip!

Use  ('Save Plots' in the 'Define points>vIQ Driver') before performing a 'Back up'. This ensures the latest plot values are saved and may prevent the loss of data before using the 'Restore' function.

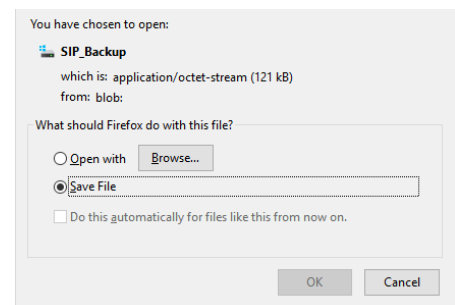
- A **'Backup file'** will restore the site configuration following a serious data loss, i.e. disaster recovery
- An **'Update file'** (available from Technical Support or website) will update the product firmware to improves functionality.

To create a backup file

- Press **'Backup'** to automatically collate the configuration data ready for creating a backup file. When completed a confirmation dialog appears.
- Select **'Save file'** and press **'OK'** to confirm the backup file must be downloaded and launch a browse dialog.
- Locate the required back up destination, i.e. a hard drive, writable CD or DVD, network location, or a removable drive and press **'Save'** to confirm the operation.

Tip!

Adjust the browser settings to allow the file to be saved to any destination required, e.g., use **'Always ask you where to save files'** in Firefox.



To restore a backup or update file

- Press **'Restore'** to show the dialog.
- Locate and select the required back up or update file.
- Confirm selection and wait for the hardware to apply the file and completely reboot.

3 ORDER CODE

3.1 PRODUCT ORDER CODES

ORDER CODE	DESCRIPTION
MelcoBEMS/SIP+/1AC/50	1 Melco driver connecting to an AE200 or EW50 collecting data from max 50 indoor units
MelcoBEMS/SIP+/2AC/100	2 Melco drivers (1 per Centralised controller) connecting to an AE200 or EW50 collecting data from max 100 indoor units
MelcoBEMS/SIP+/3AC/150	3 Melco drivers (1 per Centralised controller) connecting to an AE200 or EW50 collecting data from max 150 indoor units
MelcoBEMS/SIP+/4AC/200	4 Melco drivers (1 per Centralised controller) connecting to an AE200 or EW50 collecting data from max 200 indoor units

3.2 ACCESSORIES

ORDER CODE	DESCRIPTION
PSU/24VDC/nA	24V DC nA Power Supply
SYN/ESWn	Unmanaged Ethernet switch with 'n' x 10/100BaseT(X) ports

Intentionally left blank