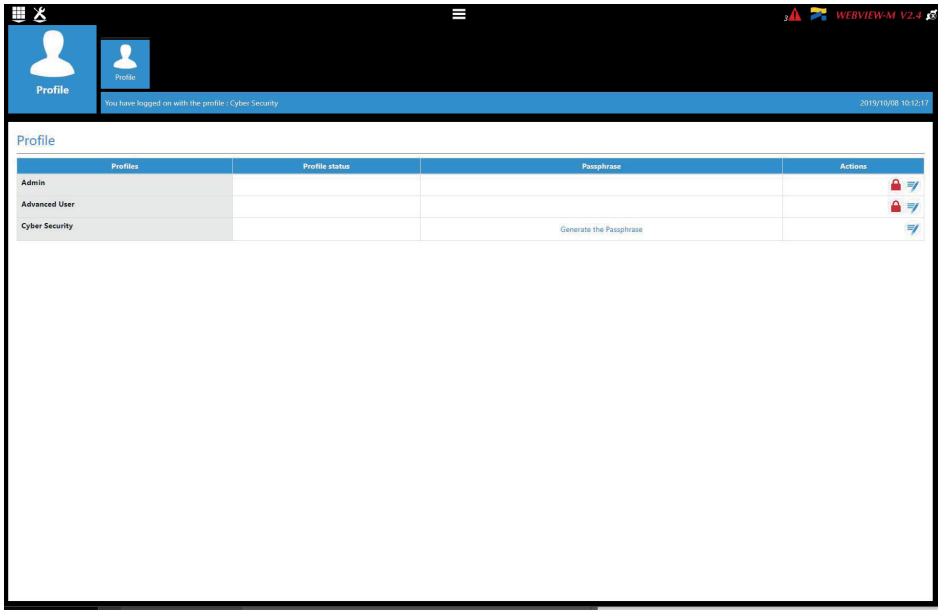
When connecting to the Admin, Advanced User or Cyber security profiles for the first time, it is mandatory to change default passwords. If these passwords are not changed, the "Password alert" alarm will remain active.

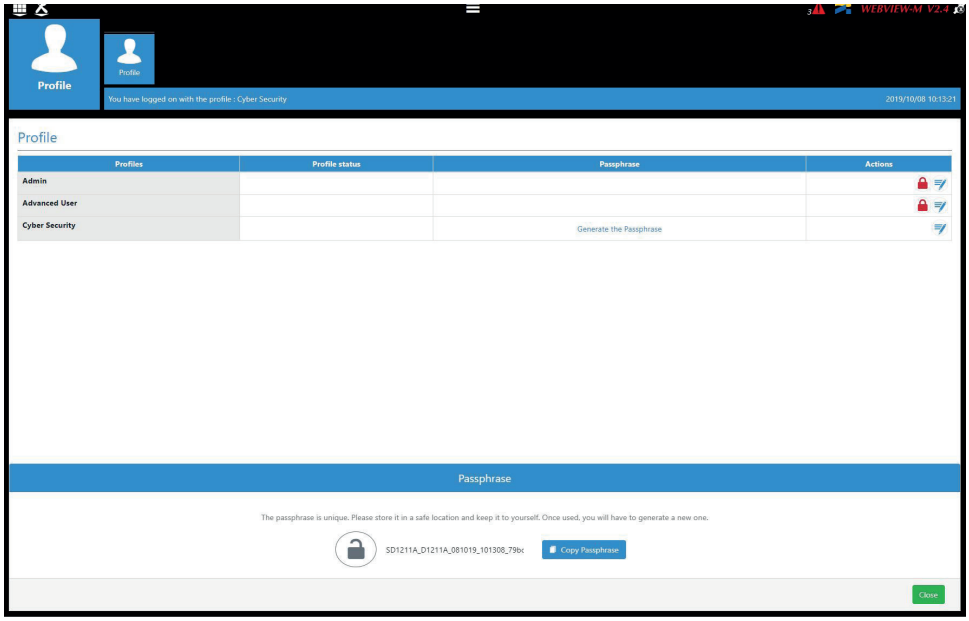
It is highly recommended to change all default passwords right away, especially the password of the Cyber security profile which has the highest privileges including changing passwords for other accounts.

Once passwords have been changed, connect to the Cyber security profile, go to the “Profile” menu and click on “Generate the passphrase”:



Copy the passphrase using the “Copy passphrase” button on the right side of the key, paste it somewhere and keep it safe. This will allow you to recover your password for the Cyber security account, should you lose it.

Account lockout policy: 3 unsuccessful login attempts to the Admin, Advanced User or Cyber security account will lock it for 1 hour. If you do not wish to wait 1 hour, you can reboot the D-50/D-70 display.



If you have forgotten to save the passphrase, the only option left is to reset the D-50/D-70 to factory default settings

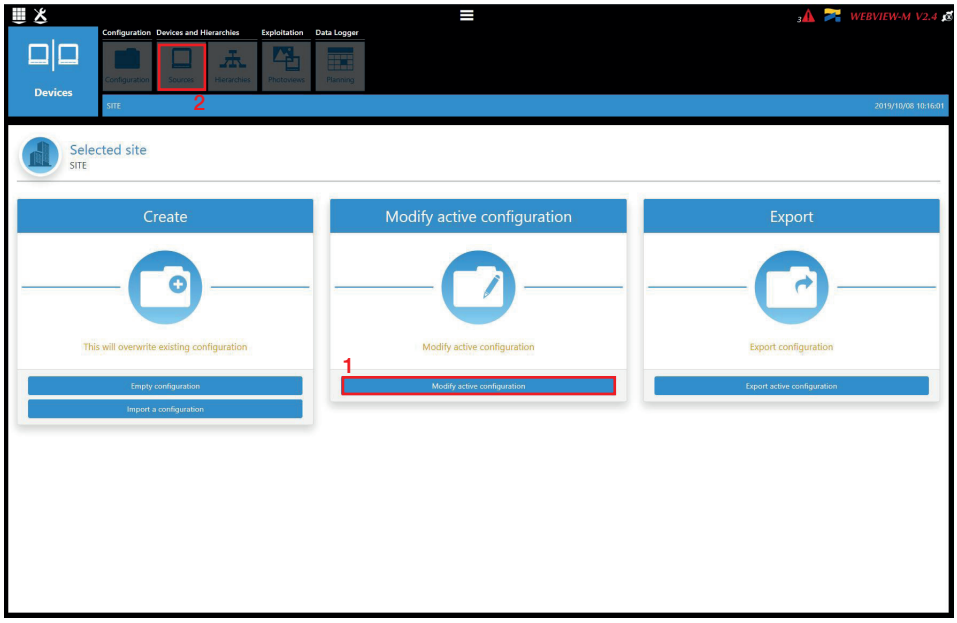
10.2. Admin profile

When connected as Admin, you can access the configuration page by clicking on the “wrench/screwdriver” icon on the top left corner:

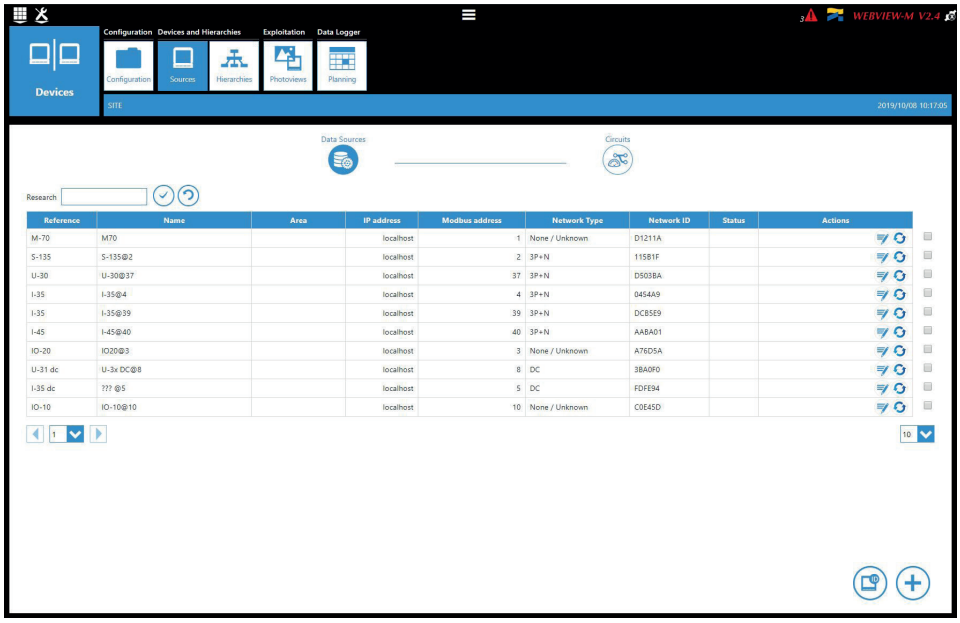
10.2.1. “Devices” tab

- Go to the “Devices” tab:

- Click on “Modify active configuration” (1), and then click on “Sources” (2):



- Click on the “AutoDetect” icon on the right bottom corner to detect and add SOCOMEC devices already present in the D-50/D-70 display’s topology.



- Click on the “+” icon at the right bottom corner for manually adding products one at a time. Adding an M-50/M-70 gateway or D-50/D-70 display will add the entire topology under that gateway or display.

- The various SOCOMEC devices that are supported by WEBVIEW-M are given in the following list:

Gateways

- D-50
- D-50v2
- D-70
- G-30/G-40
- G-50/G-60
- M-50
- M-70

DIRIS B

- B-10
- B-30 RF
- B-30 RS485

DIRIS Digiware

- D-40
- I-30
- I-30 dc
- I-31
- I-33
- I-35
- I-35 dc
- I-43
- I-45
- I-60
- I-61
- IO-10
- IO-20
- S-130
- S-135
- S-Datacenter
- U-10
- U-20
- U-30
- U-31 dc
- U-32 dc

COUNTIS

- Ci
- E03
- E04
- E13
- E14
- E17
- E18
- E23
- E24
- E27
- E28
- E33
- E34
- E43
- E44
- E44R
- E47
- E48
- E53
- ECI32
- ECI3

DIRIS A

- A-10
- A-20
- A-30
- A-40
- A-40 Ethernet
- A-40 Profibus
- A14
- A17
- A17 2In
- A17 THD
- A17 THD In
- A60
- A80

Switches

- ATyS p M
- C55
- C65
- C66

Old DIRIS A

- A10
- A20
- A20v2
- A40v2
- A40v3

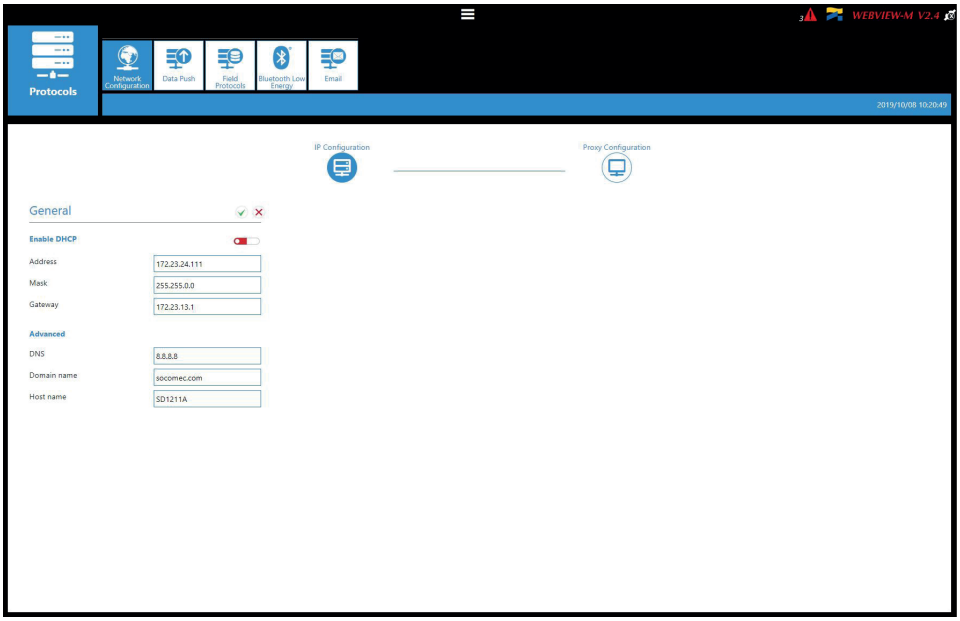
Note: other tabs such as “Hierarchy” and “Photoview” can be configured as well. They offer additional modes for the visualisation and analysis of measurements and consumption.

10.2.2. “Protocols” tab

Once the system is fully configured to visualise measurements and consumption on WEBVIEW-M, the communication protocols which will be used by the D-50/D-70 display to exchange data with an external supervisor (SCADA, Energy Management System, etc.) can be configured from the “Protocols” tab.

- **Network Configuration**

This tab allows you to modify the gateway’s IP configuration:



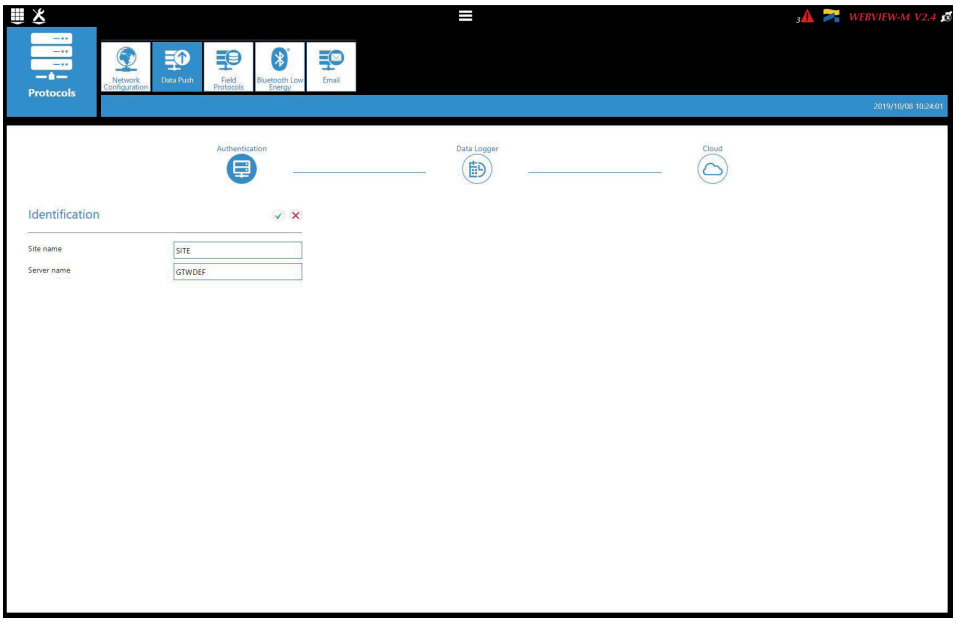
After modifying those parameters, a reboot of the D-50/D-70 display is necessary.

• **Data Push**

- Authentication

▪ Site name: This setting is essential to connect the D-50/D-70 display to a physical location within the project structure. Default Site name is “SITE” and must be changed (in EMS export mode only) or a system alarm will be triggered.

▪ Server name: Unique identifier of the display. The default server name is the NET ID, displayed on the home screen of the D-50/D-70 display.



- Data Logger

▪ Server: To send data files to a remote server, the Administrator selects the FTP(S) server

▪ Destination folder: Enter the remote server directory for receiving the files

▪ Upload log files: Select if you want the display to also send the log file to the remote server

▪ Address: Enter the IP address of the remote server

▪ Port: Enter the software port (usually 20 or 21 for FTP and 990 for FTPS)

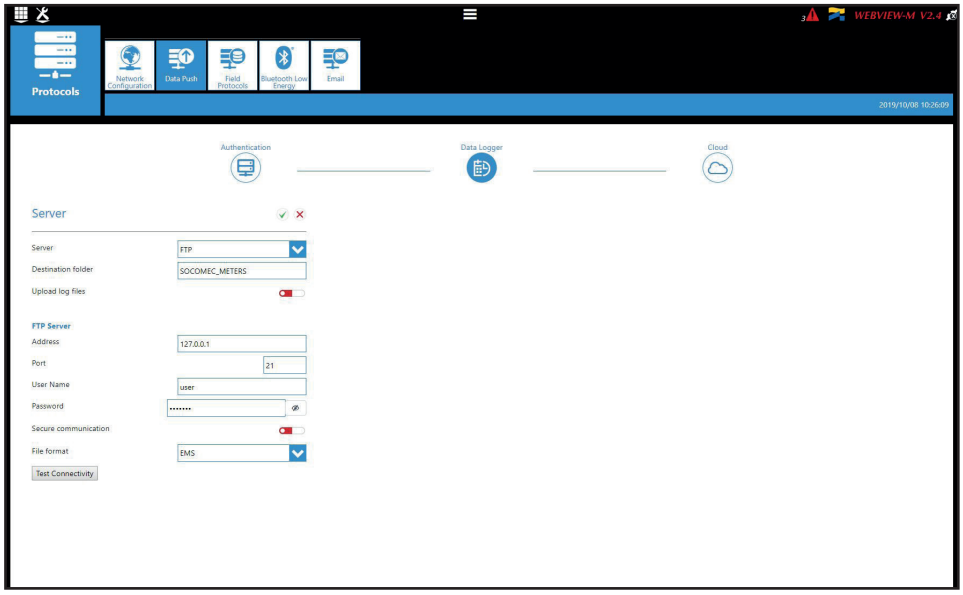
▪ User name: enter the user name the access the remote server. It must be consistent with the User name configured on the FTP server.

▪ Password: enter the password to access the remote server. It must be consistent with the password configured on the FTP server.

▪ Secure communication: open a secure session between the display and the remote server

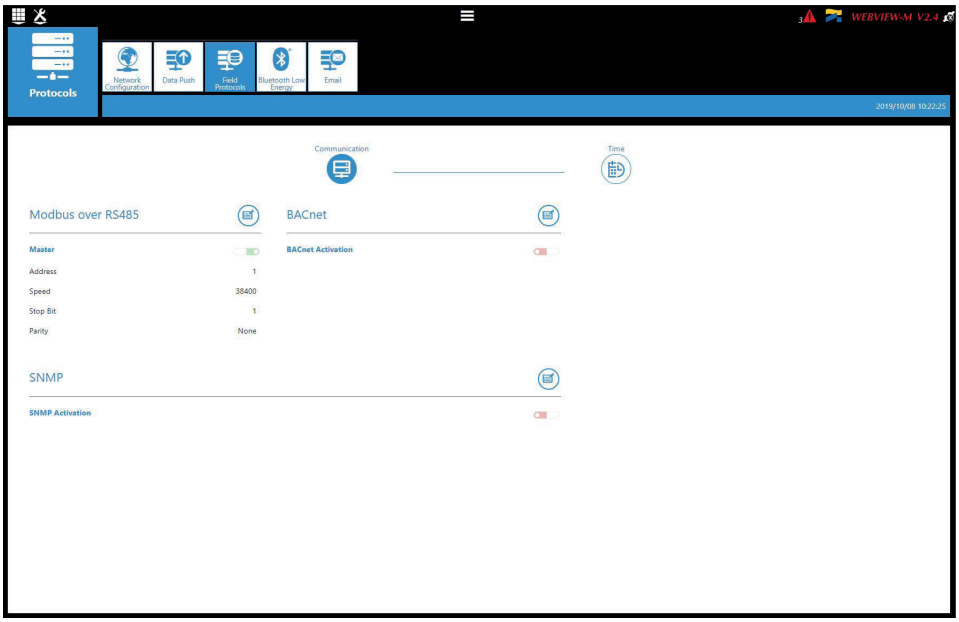
▪ File format: data can be exported in different file formats (CSV and EMS – see appendices 1 and 2). The CSV format is easier to use while EMS is better for importing data into an external energy management software.

▪ Test connectivity: Test the FTP export function



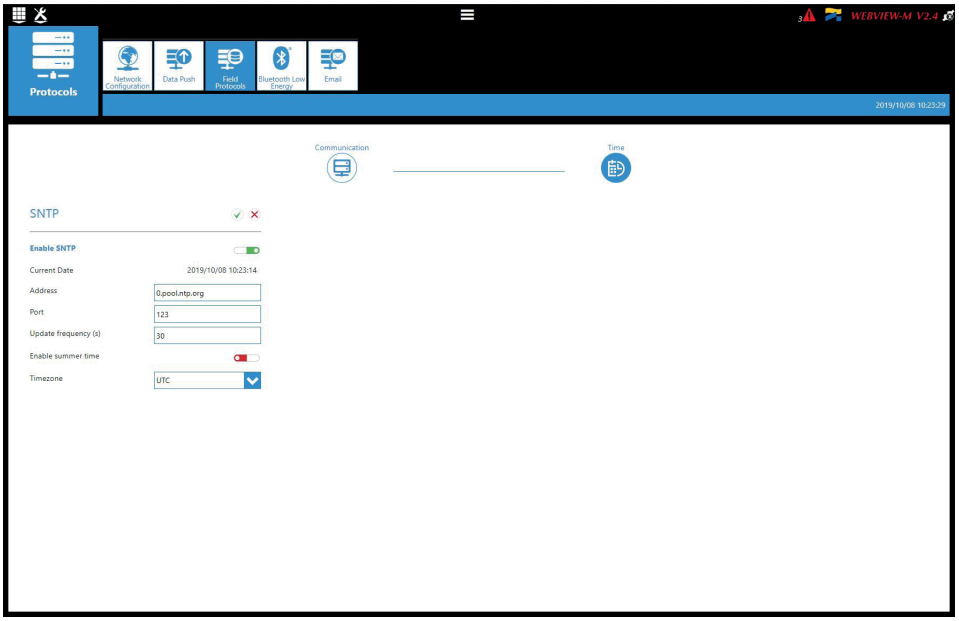
• **Field protocols**

- Communication: allows you to configure the different protocols that the D-50/D-70 display can use to communicate to external energy management systems.



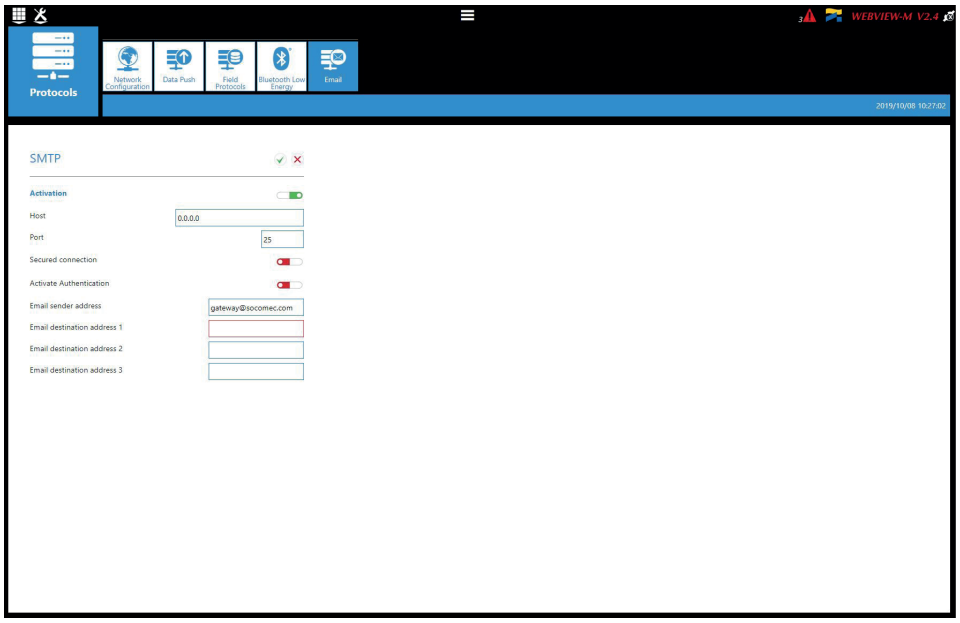
Refer to ANNEX. A and B for more information on BACnet and SNMP communication protocols with the D-50/D-70 display.

- Time: allows you to configure an SNTP server to automatically synchronise the clock of the D-50/D-70 display to an external computer.



• **Email**

This tab allows you to activate and configure email notifications in case of alarms:



- Activation: enable/disable the SMTP email export function
- Host: enter the IP address or name of the SMTP server
- Port: enter the SMTP port
- Secured connection: enable or disable the secured connection (SMTPS)
- Activate Authentication: enable or disable the SMTP authentication. It is possible to activate the authentication, even if the secured connection is disabled.
- User: enter the user name for the authentication
- Password: enter the password for the authentication
- Email sender address: email address used by the D-50/D-70 display to send emails
- Email destination address 1: email address #1 to which email notifications will be sent
- Email destination address 2: email address #2 to which email notifications will be sent
- Email destination address 3: email address #2 to which email notifications will be sent
- Language: language in which emails are sent
- Criticality of alarms to send: choose to send “information” or “Non critical” or “Critical” alarms
- Maximum waiting time: Time to wait to receive the email notification after the alarm is triggered on a device. This allows to limit the number of emails sent by the D-50/D-70 display, especially when the alarm repeatedly changes state.

10.3. Cyber security profile

In addition to the rights of the Admin profile, the Cyber security profile allows you to:

- Manage all profiles and change their passwords. The Cyber security profile it also allows to generate the passphrase for password recovery.
- Implement a Cyber Security policy from a dedicated menu:

10.3.1. Cyber security menu

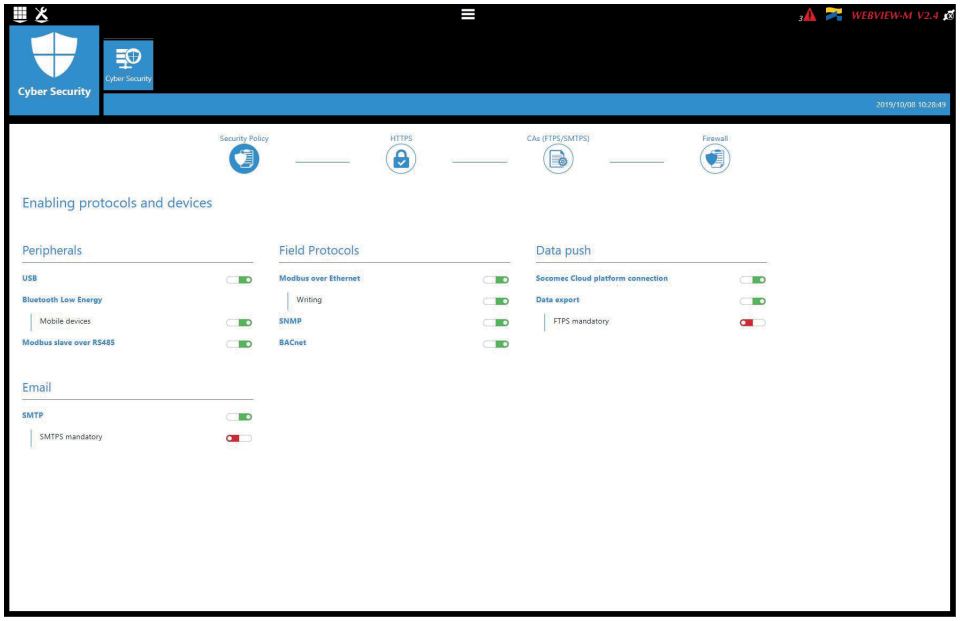
The Cyber Security menu allows you to:

- Define a custom security policy.
- Secure the client-server communication (HTTPS, FTPS, SMTPS).
- Prevent denial-of-service attacks by implementing a firewall in the D-50/D-70 display.

The configuration of Cyber security functions is explained in paragraphs 10.3.1 through 10.3.4.

10.3.2. “Security Policy” tab

DIRIS Digiware D-50/D-70 displays can reduce the attack exposure by disabling certain peripherals or services that are not essential to the customer’s use case.



Peripherals

- USB: disable the USB port of the D-50/D-70 display.
- Bluetooth Low Energy: disable the Bluetooth Low Energy of the D-50/D-70 display.
- Modbus slave over RS485: authorise or disable Modbus communication on the RS485 port of the D-50/D-70 display.

Email

- Make the secure version of SMTP mandatory for email notifications in case of alarm on a connected device.

Field protocols

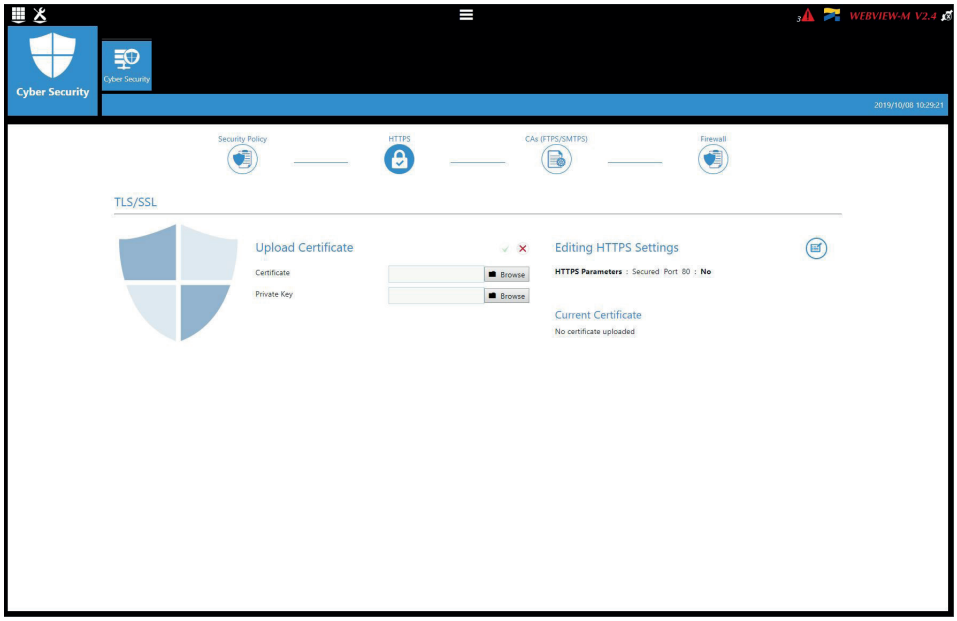
- Modbus Write function: authorise or disable to prevent people from changing settings over Modbus.
- SNMP: allow or disable the use of the SNMP protocol.
- BACnet: allow or disable the use of the BACnet protocol.

Data push

- Socomec cloud platform: authorise or block the export of data to the Socomec platform.
- Data export, FTPS mandatory: force the data export to an FTP server with a secure connection.

10.3.3. “HTTPS” tab

The HTTPS tab allows you to upload a digital certificate to secure the web navigation:



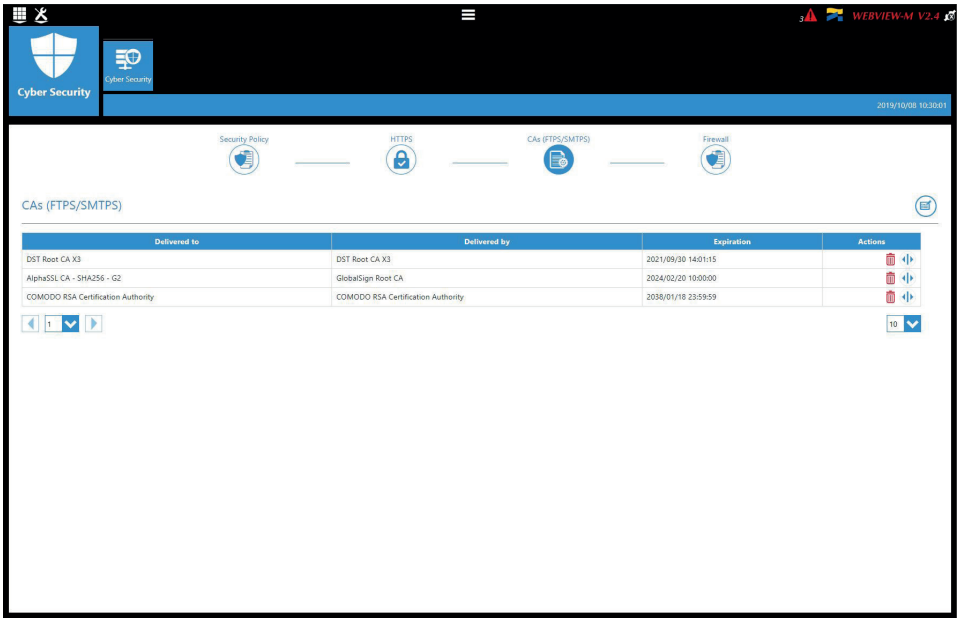
The D-50/D-70 displays will accept a digital certificate under the .pem format. Once a digital certificate and private key has been uploaded, you can edit HTTPS settings to secure the web navigation.

- The D-50/D-70 displays are compatible with RSA and ECDSA (Elliptic Curve Digital Signature Algorithm) digital certificates. The use of ECDSA digital certificates is recommended to optimise the speed of the web navigation.
- The private key size must not exceed 2048 Bits.

10.3.4. CAs (FTPS/SMTPS) tab

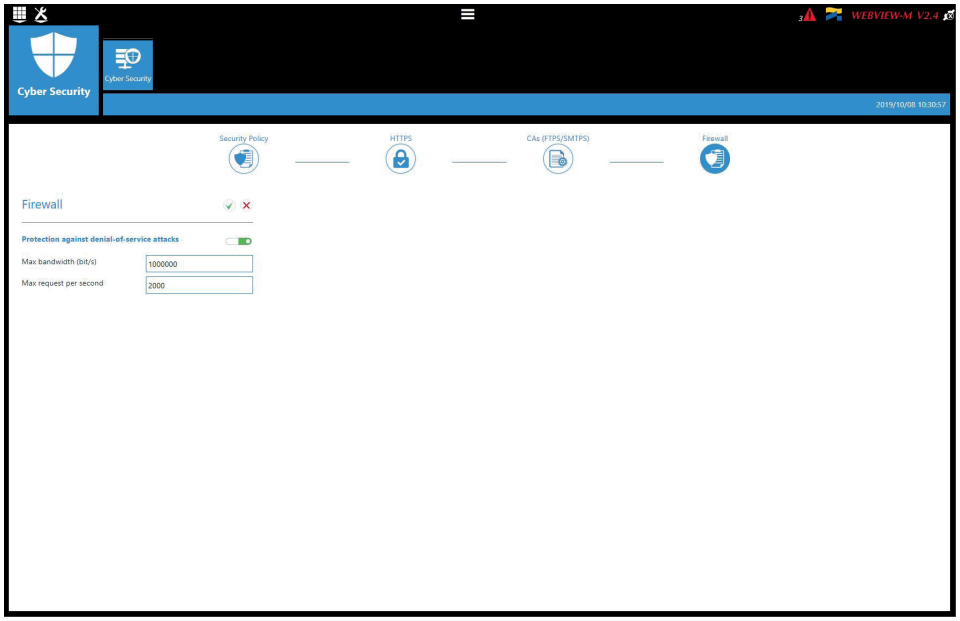
This tab allows you to secure the client (D-50/D-70) to server (FTPS, SMTPS) communication by adding the relevant Certificate Authorities (CA) on the Client side.

Several common Certificate Authorities are already included to the D-50/D-70 display, but the user can add others if necessary.



10.3.5. “Firewall” tab

This tab allows you to implement a firewall to protect against Denial-Of-Service attacks also called Flooding attacks by entering a max bandwidth in kbit/s and a max number of requests per second:

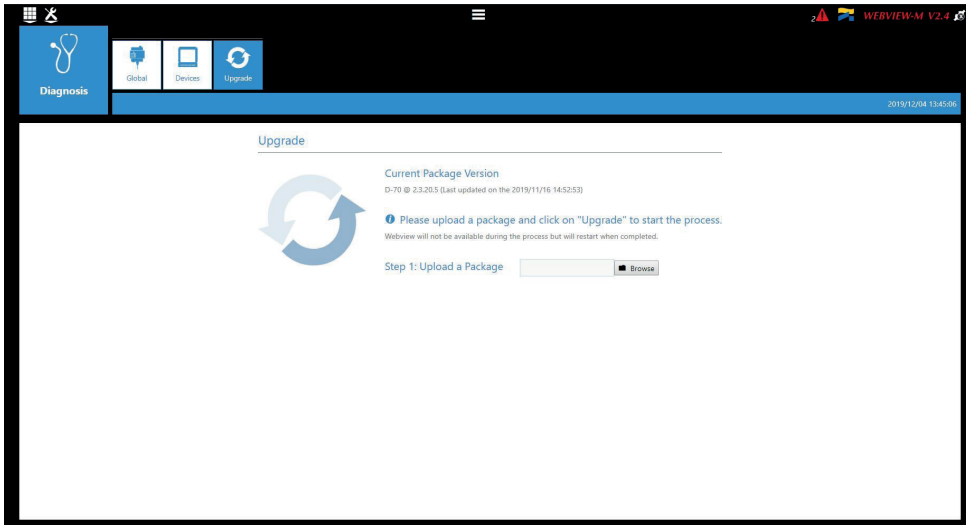


A client exceeding one of the above parameters while communicating to the DIRIS Digiware D-50/D-70 display will be blocked for 30 seconds.

10.3.6. Upgrading the firmware of the D-50/D-70 display

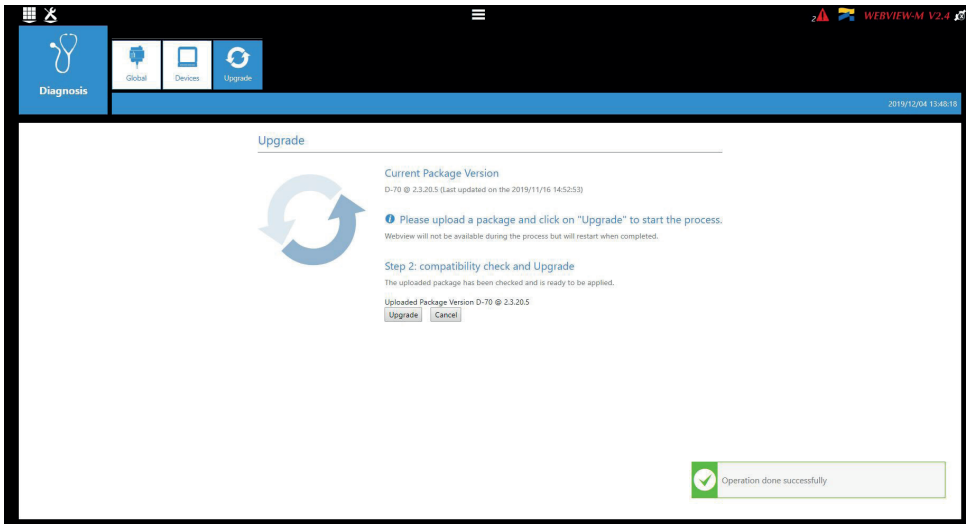
To upgrade the firmware of the DIRIS Digiware D-50/D-70 display, go to the “Diagnosis” menu:

Go to the “Upgrade” tab:

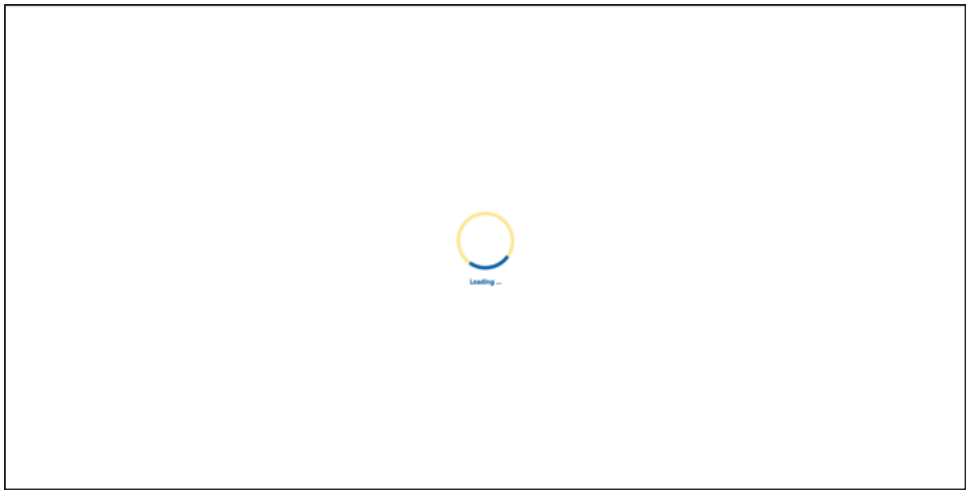


Upload the desired firmware package (.dfu file) by clicking on the “Browse” button.

Wait until the package is loaded, and once package consistency check I finished, click on “Upgrade”:



Once the upgrade is finished, the web page will reload automatically:



10.4. WEBVIEW-M

For more information on the visualisation of measurement data, please refer to the WEBVIEW-M instruction manual, available on the Socomec website at the following link:
https://www.socomec.com/range-software-solutions_en.html?product=/webview_en.html

11. ALARMS

DIRIS Digiware D-50 and D-70 displays collect alarms from downstream devices connected on the Digiware or RS485 bus.

DIRIS Digiware D-50 and D-70 displays also support 8 System alarms. The types of system alarms and the possible causes are listed in the table below:

System alarm #	Alarm type	Description	Possible causes
System alarm 1	Email transmission error	Triggered if the D-50/D-70 display could not send the notification email in case of an alarm.	- Inconsistent password or user name between server and client - Incorrect server information - Server is not available
System alarm 2	SNTP Synchronisation error	Triggered if the D-50/D-70 display could not synchronise its internal clock to the SNTP server.	- Incorrect server information (address, port etc.) - Server is not available
System alarm 3	Modbus slave timeout error	Triggered if the D-50/D-70 display could not communicate with a Modbus slave on the Digiware or RS485 bus.	- Bad RS485 or Digiware connection. - Communication speed on the Digiware bus is too low (38400 by default) - Product is incorrectly requested (wrong Modbus register, …)
System alarm 4	Modbus address conflict	Triggered if the D-50/D-70 display has detected an address conflict among slaves.	A slave's Modbus address must be unique within Digiware and RS485 buses altogether; this alarm will be triggered if 2 slaves have the same Modbus address.
System alarm 5	Product damaged	Triggered if the product is flagged as damaged. Please return the device to Socomec.	- Product has a wrong Network ID, Serial Number or MAC Address - A newer version is available for a slave product
System alarm 6	FTP export error	Triggered if the D-50/D-70 display could not export data to the remote FTP server.	- Inconsistent password or user name between server and client - Gateway does not have permission to write files on FTP server - FTP server unavailable - Site Name is not configured
System alarm 7	Cyber Security alert	Triggered if the D-50/D-70 display detects a cyber security threat.	- Denial-of-service attack caught (client banned) - Expiration of a digital certificate
System alarm 8	Password alert	Triggered if there is an issue with the password of the Admin, Advanced User or Cyber security profile.	- Alarm is active by default until passwords are changed - Alarm is triggered once a year, 15 days before the expiration of one of the passwords and will remain active until they are changed

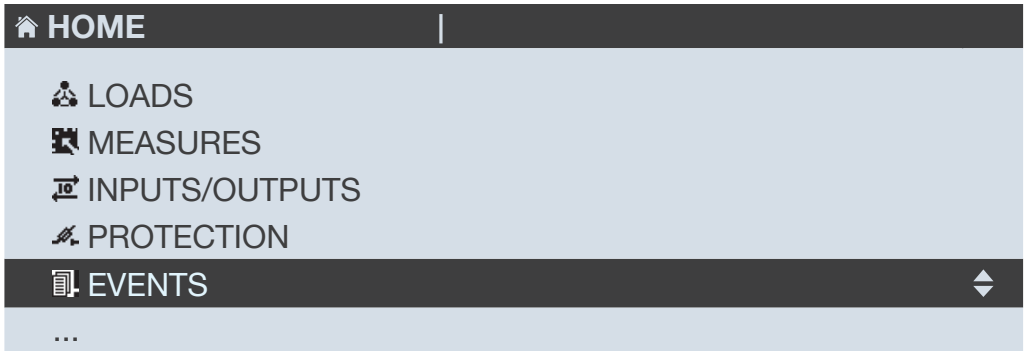
When one or more System alarms are active, the ALARM LED on the front face of the D-50/D-70 display starts blinking.

Alarms are displayed on WEBVIEW-M (for D-70 display only) and a notification will be sent by email if the SMTP(S) feature is enabled.

12. USE

Once the loads are configured, you can visualise the measurements of each load from the "MEASURES" menu.
You can view active and finished alarms from the "EVENTS" menu.

If the "ALARM" LED of the D-50/D-70 display is lit, stable or flashing, it means there is at least one active alarm. Go to the "EVENTS" menu to see which alarms are active.



Note: the "Password Alert" alarm remains active (and the ALARM LED of the D-50/D-70 display blinks) until you change the default passwords of the Admin, Advanced and Cybersecurity profiles on the webserver.

The "Password alert" alarm can also be disabled from the Easy Config System software in the "Alarms" menu of the D-50/D-70.

13. DIRIS DIGIWARE D-50/D-70 TECHNICAL CHARACTERISTICS

13.1. Mechanical characteristics

Type of screen	Capacitive touch-screen technology, 10 keys
Screen resolution	350 x 160 pixels
Front panel protection index	IP65* (IEC 60529)
Weight DIRIS Digiware D-50 / D-70	210 g

* Front face only. The use of a silicone seal may be required to ensure sufficient sealing of the junction between D-50/D-70 display and panel door.

13.2. Communication characteristics

Type of screen	Multipoint remote screen
Ethernet RJ45 10/100 Mbs	Gateway function: - Modbus TCP (max. 16 simultaneous connections) - WEBVIEW-M embedded web server (D-70 only) - BACnet IP - SNMP v1, v2 & v3
SNTP protocol	Updates the screen from an SNTP server. The display updates the connected devices.
SMTP(S) protocol	Sends email notifications from the display.
FTP(S) protocol *Only available with DIRIS Digiware D-70*	Automatically exports data via FTP standard or secure server (consumption curves, load curves, measurement logs)
RJ45 Digiware	Control and power supply interface function
RS485 2-3 wires	Modbus RTU master communication function
USB	Upgrade and configuration via type B micro USB connector
® Bluetooth Low Energy (only with DIRIS Digiware D-50/D-70 BLE versions)	
Use	Visualisation of data from Socomec Bluetooth sensors
Operating frequency	2402 to 2480 MHz
EIRP Power	EIRP Power for CE: 6.23 dBm (measured max average)
Max. Power for FCC/IC	3.15 dBm

13.3. Wireless Characteristics

13.3.1. Canada

This device complies with ISED's licence-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Le présent appareil est conforme aux CNR d' ISED applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Radiation Exposure Statement:

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with greater than 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à plus de 20 cm entre le radiateur et votre corps.

13.3.2. USA

“This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.” (§15.19 (3))

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

13.4. Electrical characteristics

Power supply	24 VDC +/- 15%, Class 2 - 20 W max
Power consumption	2.5 VA
Battery life	10 years with the following typical battery profile over its lifetime: - Product storage: 1 year of full time battery back-up (based on an average storage temperature of 25°C). - Product life: 10 days / year of battery back-up over 9 years
Battery type	3V Lithium cell battery, 48mAh rated capacity

13.5. Environmental characteristics

Use	Indoor
Storage temperature	-40°C … +70°C (IEC 60068-2-1 / IEC 60068-2-2)
Operating temperature	-10°C … +55°C (IEC 60068-2-1 / EN/IEC 60068-2-2)
Humidity	40°C / 95% RH (IEC 60068-2-30)
Pollution degree	2

13.6. EMC characteristics

CHARACTERISTIC	TEST STANDARD	PERFORMANCE CRITERIA	LEVEL
Electrostatic discharges (Contact)	IEC 61000-4-2	B	III
Electrostatic discharges (Air)	IEC 61000-4-2	B	III
Radiated radio-frequency field immunity	IEC 61000-4-3	A	III
Burst immunity	IEC 61000-4-4	B	III
Surge immunity (Common mode)	IEC 61000-4-5	B	III
Surge immunity (Differential mode)	IEC 61000-4-5	NA	NA
Conducted RF immunity	IEC 61000-4-6	A	III
Power magnetic field immunity	IEC 61000-4-8	A	IV / 400 A/m
Dips immunity	IEC 61000-4-11	NA	NA
Conducted emissions	CISPR11	NA	NA
Radiated emissions	CISPR11	Passed	Gr:1 – Class B

ANNEX I. SNMP COMWMUNICATION WITH THE DIRIS DIGIWARE D-50 / D-70

Annex I - 1. SNMP generalities

SNMP stands for Simple Network Management Protocol and is widely used by administrators for an easy network monitoring of devices on IP networks. It works in a client-server communication mode on an Ethernet physical layer.

Once enabled from the Easy Config configuration software, the DIRIS Digiware D-70 display supports SNMP v1, v2 and v3.The D-50 / D-70 is an agent SNMP v1, v2, v3 which responds to queries from managers (also called management stations or supervisors).

The D-50 / D-70 allows access through SNMP of measurement data from SOCOMEC slaves connected via the RS485 bus or the Digiware bus.

Data from the slaves can be reached through a file called “MIB” (“Management Information Base”) under a hierarchical and pre-defined structure. The MIB file of the D-50 / D-70 is named ”socomec-diris-products-mib” and is available from www.socomec.com
The file must be uploaded in the Management station managing your metering system.

The Tree structure of the MIB contains multiple OIDs (Object Identifiers). An OID uniquely identifies and labels a managed object (=parameter from metering devices) in the MIB.

For example, the electrical parameter “Current Inst I1” is identified by one OID. “Current Inst I2” is identified by another one.

COMMON SNMP TERMS	CONSUMPTION CURVES
AGENT	Corresponds to the DIRIS Digiware D-50 / D-70: Interface between the PMDs and the manager
MANAGED DEVICE	The PMDs connected downstream the D-50 / D-70 (ex: I-35, DIRIS B, DIRIS A…)
MIB	Management information base where the OIDs are organized in a hierarchical tree
OID	An object identifier that uniquely identifies and labels a managed object in the MIB hierarchy
COMMUNITY STRINGS	A text that enables the authentication between an agent and the manager
TRAPS	Notifications sent by the agent and received by the manager

Annex I - 2. SNMP functions supported

There are 4 types of SNMP requests supported by the DIRIS Digiware D-50 / D-70:

- **GetRequest:** to retrieve the variable of an OID (I1 Inst for example)
- **GetNextRequest:** to retrieve the variable of the next OID (I2 Inst in this case)
- **GetBulk:** to retrieve multiple variables gathered together
- **SetRequest:** to change the value of one variable such as the state of a Digital output.
- **Traps:** Unlike the above commands which are initiated by the SNMP manager, Traps are initiated by the Agents with no solicitation from the Manager. Traps are notifications to the Manager by the Agent of the occurrence of an event and/or alarm..

Traps are sent by the agent in case one of the following alarms occurs:

- Alarm on a measurement
- Logical alarm (change of status of a Digital input)
- Combination alarms
- PQ events (inrush, voltage swells, voltage sags/dips, voltage interruptions)
- System alarms (Phase Rotation, CT disconnect, VI association)

Traps are sent automatically when the alarm occurs. They will be sent again once the “Trap report frequency” time (entered in Easy Config) is elapsed.

The alarm must be activated in the product (using the configuration software Easy Config) in order for the Traps to be sent. Traps can either be configured for specific hosts or “broadcast” to the whole network. Up to two server IP addresses can be entered in Easy Config for SNMP trap notification of specific hosts.

Annex I - 3. SNMP versions supported

The DIRIS Digiware D-50 / D-70 can use all three versions of SNMP: SNMPv1, v2 and v3.

- **SNMPv1 and v2:**

The identification is based on Read-only and Read-Write Community passwords. They are non-encrypted and are passed over the network in plaintext.

Both passwords have to be entered in the Agent (DIRIS Digiware D-50 / D-70) and the Manager and must be identical.

A matching Read Community allows the Get functions to be executed on the agent.

A matching Read-Write Community also allows the Set function to be executed on the agent.

- The default Read Community V1 password is “public” and the default Read-Write Community V1 password is “Private”.

- The default Read Community V2 password is “publicv2” and the Read-Write Community V2 is “privatev2”.

- **SNMPv3:**

SNMPv3 uses the USM (User-based Security Module) for controlling access to information available via SNMP. This version offers more security using three important features to prevent the interception and deciphering of data:

- A username (called security username)

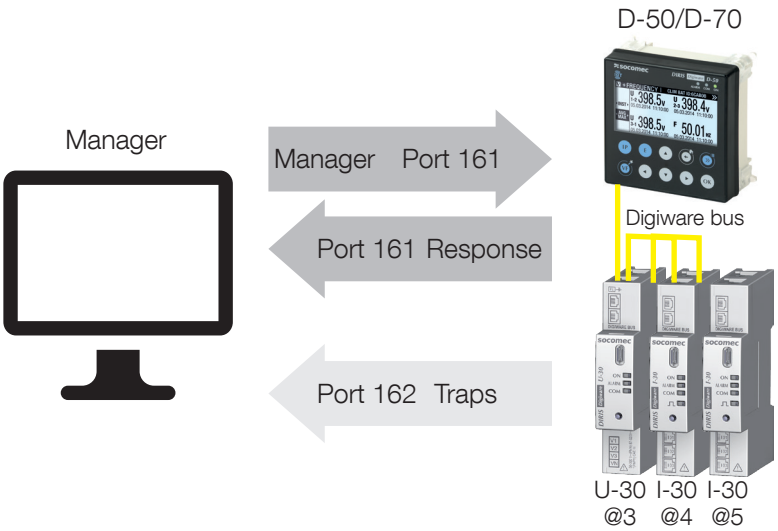
- MD5 and SHA1 authentication protocols to hash the passwords

- DES and AES Privacy protocols to encrypt the data

Annex I - 4. SNMP ports

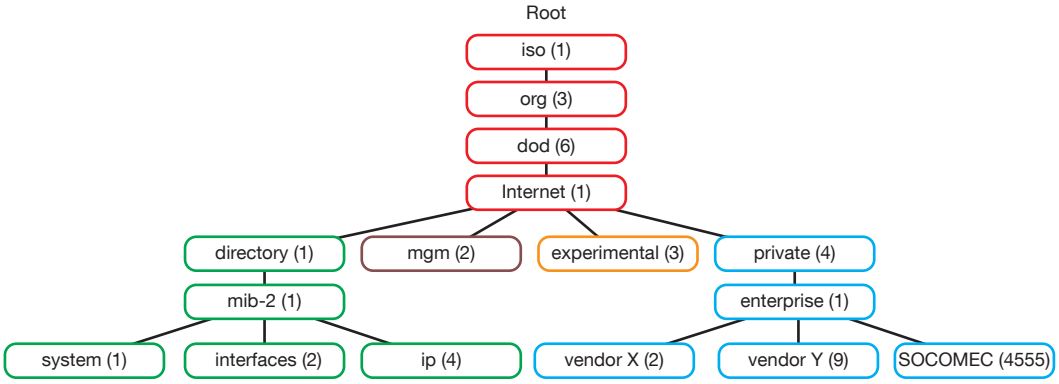
The DIRIS Digiware D-50 / D-70 is configured with standard SNMP ports to receive requests and send notifications:

PORT	DESCRIPTION
161	Used to send and receive requests from the manager.
162	Used by the manager to receive notifications from the agent



Annex I - 5. Retrieving data using the DIRIS Digiware D-50 / D-70 MIB file

The DIRIS Digiware D-50 / D-70 is compliant with MIB-II defined by the MIB standard RFC 1213 which defines the following structure:



OID Tree Example

The standard branches are under the same parent branch structure: 1.3.6.1.4.1

The “Private (4)” group enables vendors to define private branches including the MIB OIDs of their own products. Data related to SOCOMEC metering devices is located under the SOCOMEC enterprise category identified by OID 1.3.6.1.4.1.4555. This implies that all queries from a manager to SOCOMEC agents will start by the base path 1.3.6.1.4.1.4555.

Because the DIRIS Digiware is a multi-circuit system, the DIRIS Digiware D-50 / D-70 creates a dynamic table which depends on the products connected downstream compatible with the DIRIS Digiware D-50 / D-70 and the loads configured on each product.
After adding/deleting a downstream device or a load, make sure to update the topology of the D-70 display. This can be done either directly from the display or from Webview:

- Add or delete a device
- Refresh the loads

Example: The OID for “Current Inst I1” will return a value for all I-xx, B-xx, DIRIS A etc.. On the contrary, the OID for “THD Inst I1” will return “0” for an I-30 or an I-31 module.

This implies that each OID can be associated with several products and several loads.

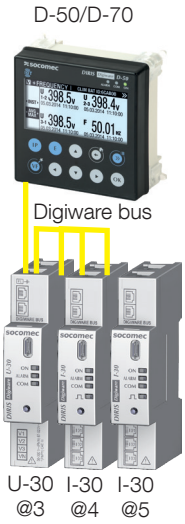
For example the OID for instCurrentI1 is represented by the sequence 1.3.6.1.4.1.**4555.10.20.20.1.10000**.

OID SEQUENCE	DESCRIPTION
4555	“SOCOMEC” enterprise branch
10	“SocomecProducts” table
20	“ProductMetrology” table
20	“InstantaneousTable”
1	Entry (always = 1)
10000	Service ID

This OID is associated with the multiple devices connected downstream the DIRIS Digiware D-50 / D-70.

To identify those multiple devices, the Modbus address and the load number are added to the end of the OID.

Example: Let us consider the following architecture:



PRODUCT	I-30	I-30
MODBUS ADDRESS	4	5
LOAD TYPE	Load 1: 3P + N - 3CT	Load 1: 1P + N - 1CT Load 2: 1P + N - 1CT Load 3: 1P + N - 1CT

The final OID to get the instantaneous current I1 for the I-30 module @ Modbus address 4 for load 1 is:
1.3.6.1.4.1.4555.10.20.20.1.10000.4.1

For the I-30 module @ address 5, there are multiple loads configured. This implies that the Modbus address must be followed by the Load number in the OID.

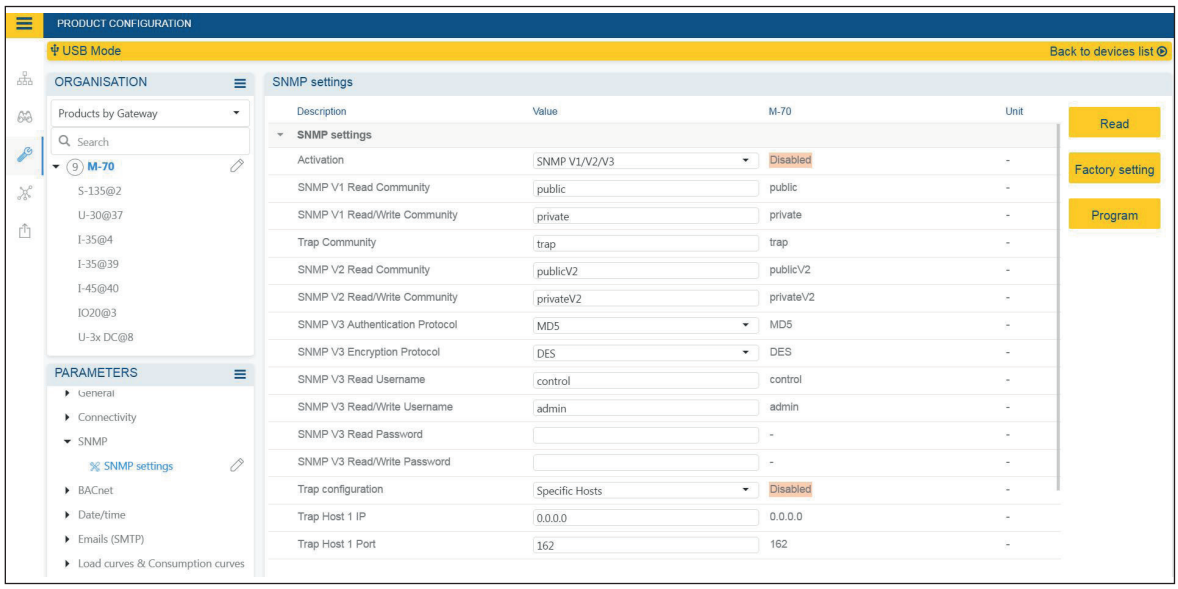
Therefore, the final OID used to request I1 Inst for load 1 of the I-30 @ address 5 is:
1.3.6.1.4.1.4555.10.20.20.1.10000.5.1
The final OID to request I1 Inst for load 2 of the I-30 @ address 5 is **1.3.6.1.4.1.4555.10.20.20.1.10000.5.2**
The final OID to request I1 Inst for load 3 of the I-30 @ address 5 is **1.3.6.1.4.1.4555.10.20.20.1.10000.5.3**

OID SEQUENCE	DESCRIPTION
4555	“SOCOMEC” enterprise branch
10	“SocomecProducts” table
20	“ProductMetrology” table
20	“InstantaneousTable”
1	Entry (always = 1)
10000	Service ID
5	Modbus Address
3	Load number

Note: a request to OID 1.3.6.1.4.1.4555.10.20. 20.1.10001.5 will return “0” because the service ID 10001 corresponds to I2 inst whereas only single-phase loads are configured in the I-30 module @ address 5, which means currents I2 and I3 parameters aren’t used.

Annex I - 6. SNMP configuration via Easy Config System

After logging in to Easy Config System on the DIRIS Digiware D-50 / D-70, you can find the SNMP settings in the SNMP menu, under SNMP settings:



- **Community configuration SNMP V1 & V2:**
  - **SNMP V1 Read Community:** Read-only community string for SNMP v1. Default community string is “public”. It allows a manager to retrieve read-only data from a device connected to the DIRIS Digiware D-50 / D-70.
  - **SNMP V1 Read/Write Community:** Read-Write community string for SNMP v1. Default Read/Write community string is “private”. It allows a manager to write (ex: position of a Digital output) to a device connected to the DIRIS Digiware D-50 / D-70.
  - **Trap Community:** The Trap community string allows the manager to receive notifications in case of an event and/or alarm.
  - **SNMP V2 Read Community:** Read-only community string for SNMP v2. Default community string is “publicV2”. It allows a manager to retrieve read-only data from a device connected to the DIRIS Digiware D-50 / D-70.
  - **SNMP V2 Read/Write Community:** Read-Write community string for SNMP v2. Default Read/Write community string is “privateV2”. It allows a manager to change a setting (ex: position of a Digital output) in a device connected to the DIRIS Digiware D-50 / D-70.

- **SNMP V3 configuration:**
  - **SNMP V3 Authentication Protocol:** If SNPM v3 is activated, you can choose an authentication protocol (MD5 or SHA) to hash your password. For no authentication, select “None”.
  - **SNMP V3 Encryption Protocol:** Choose between DES or AES privacy protocols for the encryption of data messages. For no encryption, select “None”.
  - **SNMP V3 Read Username:** Username enabling authentication for read-only functions.
  - **SNMP V3 Read/Write Username:** Username enabling authentication for read and write functions.
  - **SNMP V3 Read Password:** Password (also passphrase) accompanying the authentication and privacy protocols, and allowing read-only functions. The length of the Read-only authentication & privacy password must be between 8 and 16 characters.
  - **SNMP V3 Read/Write password:** Password (also called passphrase) accompanying the authentication and privacy protocols and allowing read and write functions. The length of the Read-Write authentication & privacy password must be between 8 and 16 characters.
  - **Trap configuration:** Choose to deactivate or activate the traps. If activated, you can choose to broadcast trap notifications to all supervisers on the network or to notify only specific host stations (up to 2).
  - **Trap Host 1 IP:** Enter the IP address of the 1st host station which will receive trap notifications.
  - **Trap Host 1 port:** Enter the port used to send traps for the 1st host station.
  - **Trap Host 2 IP:** Address: enter the IP address of the 2nd host station which will receive trap notifications.
  - **Trap Host 2 port:** Enter the port used to send traps for the 2nd host station.
  - **Trap notification cycle:** Enter the time after which a trap reminder will be sent for active alarms. By default, it is set to 60min.

ANNEX II. BACNET COMMUNICATION WITH THE DIRIS DIGIWARE D-50 / D-70

The DIRIS Digiware D-50 / D-70 supports the BACnet IP protocol.
It acts as a BACnet IP gateway to all devices compatible and connected downstream via RS485 or the Digiware Bus.

The PICS (Protocol Implementation Conformance Statement) of the DIRIS Digiware D-50 / D-70 is available on the Socomec website at www.socomec.com.

Annex II - 1. BACnet Generalities

BACnet provides a method for computer-based control equipment from different manufacturers to be interoperable. BACnet is designed to handle many types of building controls, including HVAC, lighting, security, fire, access control, maintenance, waste management and so forth.

Common terms used in BACnet communication:

Object: Represents a device and its data. Multiple objects type can be available for each device *analog input, binary input…). Each object has a number of properties which fully describe the BACnet object to the network.

Object identifier: Uniquely identifies an object within a BACnet device.

Property: A property describes a BACnet object to the network.

Present value: It is one of the properties of the Analog_Input Object. It represents the current value of an analog input object.

Service: Message type between one BACnet device to another.

BACnet uses a client/server communication mode between devices. Devices communicate between each other using services describing the type of exchange.
A BACnet client is a device that requests a service, and a BACnet server is a device that executes a service.
Data inside a BACnet device is organized as a series of objects, each composed of multiple properties.

Ex: the analog_input object defines a property for present_value, a property for average_value etc…

A BACnet client initiates a request to a BACnet server using a service (ex: read_property) to a specific property (ex: present_value) contained in a BACnet object (ex: analog_input).

Annex II - 2. BACnet Objects

BACnet defines a standard set of “Objects”, each of which has a standard set of “Properties” describing the object and its current status to other devices on the BACnet internetwork. The properties allow for the object to be controlled by other BACnet devices.

BACnet defines 54 objects. Each element of the building control system is represented by one or more objects.
The DIRIS Digiware M-50 / M-70 supports the below Objects:

OBJECT TYPE	EXEMPLE OF USE
Device	To describe the device to the BACnet network.
Analog input	Instantaneous current for phase 1 (I1) measured by a DIRIS Digiware I-xx current module with associated current sensor
Binary input	Status (ON/OFF) of an auxiliary contact
Binary output	Change of status of the output of a DIRIS Digiware IO-10

A list of properties defines each BACnet Object. Properties can be:

- Required by the BACnet specification.
- Optional. In this case, vendors can choose whether to implement them for their devices.
- Proprietary. Vendors can add their own created properties.

Device Object:

Every BACnet device compatible with the DIRIS Digiware D-50 / D-70 must have the Device Object and its associated required properties that fully describe the BACnet device to the network.

Example for the Device Object of the DIRIS Digiware D-50 / D-70:

PROPERTY	BACnet
Object_Identifier (OID)	Required
Object_Name	Required
Object_Type	Required
System_Status	Required
Vendor_Name	Required
Vendor_Identifier	Required
Model_Name	Required
Firmware_Revision	Required
Application_Software_Version	Required
Protocol_Version	Required
Protocol_Conformance_Class	Required
Protocol_Services_Supported	Required
Protocol_Object_Types_Supported	Required
Object_List	Required
Max_APDU_Length_Supported	Required
Segmentation_Supported	Required
APDU_Timeout	Required
Location	Optional
Description	Optional
Local_Time	Optional
Utc_Offset	Optional
Local_Date	Optional
Daylight_Saving_Status	Optional
Active_COV_Subscriptions	Optional
Serial_Number	Optional
Property_List	Optional
Version_Build_Date	Proprietary
Operating_Hour_Counter	Proprietary

The way the OID is assigned to a device (instance number) is the following:

OID = Main OID (= default 100) + ModbusAddress:

- Device with Main OID (100) is the DIRIS Digiware D-50 / D-70 display itself.
- The device with OID (1xx) is the device with the Modbus address xx.

Analog Input Object:

The DIRIS Digiware D-50 / D-70 acts as a BACnet gateway. It provides a number of Analog Input objects which may be available from the devices compatible and connected to the DIRIS Digiware D-50 / D-70.
Whether a device supports an AI object depends on its measurement functionalities.

Ex: The OID for THD_I1 will return 0 for a DIRIS Digiware I-30 module because this parameter is not handled.

The AI object defines 25 properties. The devices compatible and connected downstream the DIRIS Digiware D-50 / D-70 support the following properties:

PROPERTY	BACnet
Object_Identifier	Required
Object_Name	Required
Object_Type	Required
Present_Value	Required
Status_Flags	Required
Event_State	Required
Out_Of_Service	Required
Units	Required
Description	Optional
Reliability	Optional
Min_Pres_Value	Optional
Minimum_Value_Timestamp	Optional
Max_Pres_Value	Optional
Maximum_Value_Timestamp	Optional
Average_Value	Optional
Instantaneous_Timestamp	Proprietary
Average_Timestamp	Proprietary
Max_Average_Value	Proprietary
Max_Average_Timestamp	Proprietary
Min_Average_Value	Proprietary
Min_Average_Timestamp	Proprietary
Harmonics_Row_02	Proprietary
Harmonics_Row_03	Proprietary
Harmonics_Row_04	Proprietary

PROPERTY	BACnet
Harmonics_Row_05	Proprietary
Harmonics_Row_06	Proprietary
Harmonics_Row_07	Proprietary
Harmonics_Row_08	Proprietary
Harmonics_Row_09	Proprietary
Harmonics_Row_10	Proprietary
Energy_Total_Residual	Proprietary
Energy_Total_Hourmeter	Proprietary
Energy_Partial	Proprietary
Energy_Partial_Residual	Proprietary
Energy_Partial_Hourmeter	Proprietary
Energy_Total_Lagging	Proprietary
Energy_Total_Lagging_Res	Proprietary
Energy_Total_Leading	Proprietary
Energy_Total_Leading_Res	Proprietary
Energy_Last_Partial	Proprietary
Energy_Last_Partial_Res	Proprietary
Energy_Last_Partial_Timestamp	Proprietary
Multifluid_Partial	Proprietary
Multifluid_Weight	Proprietary
Instant_Min_Max_Reset	Proprietary
Average_Min_Max_Reset	Proprietary

The way the OID is assigned to an Analog Input Object (instance number) is the following:
OID = LLMM

- with LL = Load # of the device (starting at 1).
- with MM = Index of the measurement type (see Analog Input Measurement List).

For example, Analog Input with OID 204 reflects Phasis/Neutral Voltage V1 of Load 2 of corresponding device.

The table with indexes of the analog input measurement list is given below:

Index	Object Namew	Object Description	Unit	Type	Present + Timestamp	Present Min/Max + Timestamp	Average + Timestamp	Average Min/Max + Timestamp	Harmonics 2 -> 10	Energies Total + Partial + LastPartial	Energies Total Lagging/Leading	Multifluid	Reset Min/Max
0	VystPhN	System Ph-N Voltage	V	Unsigned	•								•
1	VystPhPh	System Ph-Ph Voltage	V	Unsigned	•								•
2	CurrentSyst	System Current	A	Unsigned	•								•
3	Frequency	System Frequency	Hz	Unsigned	•	•	•	•					•
4	VoltPhNV1	Ph-N Voltage V1	V	Unsigned	•	•	•	•					•
5	VoltPhNV2	Ph-N Voltage V2	V	Unsigned	•	•	•	•					•
6	VoltPhNV3	Ph-N Voltage V3	V	Unsigned	•	•	•	•					•
7	VoltPhNVn	Ph-N Voltage Vn	V	Unsigned	•	•	•	•					•
8	VoltPhPhU12	Ph-Ph Voltage U12	V	Unsigned	•	•	•	•					•
9	VoltPhPhU23	Ph-Ph Voltage U23	V	Unsigned	•	•	•	•					•
10	VoltPhPhU31	Ph-Ph Voltage U31	V	Unsigned	•	•	•	•					•
11	CurrentI1	Current I1	A	Unsigned	•	•	•	•					•
12	CurrentI2	Current I2	A	Unsigned	•	•	•	•					•
13	CurrentI3	Current I3	A	Unsigned	•	•	•	•					•
14	CurrentIn	Current In	A	Unsigned	•	•	•	•					•
15	CurrentInba	Current Inba	%	Unsigned	•								•
16	CurrentIdir	Current Idir	A	Unsigned	•								•
17	CurrentIinv	Current Iinv	A	Unsigned	•								•
18	CurrentIhom	Current Ihom	A	Unsigned	•								•
19	CurrentInb	Current Inb	%	Unsigned	•								•
20	PowerApparentNom	Nominal Apparent Power	VA	Unsigned	•								•
21	TotalPowerActive	Total Active Power	W	Signed	•	•	•	•					•
22	TotalPowerRActive	Total Reactive Power	VAr	Signed	•	•	•	•					•
23	TotalPowerApparent	Total Apparent Power	VA	Unsigned	•	•	•	•					•
24	TotalPowerFactor	Total Power Factor	-	Signed	•	•	•	•					•
25	TotalPowerFactorType	Total Power Factor Type	-	Unsigned	•	•	•	•					•
26	PowerActiveP1	P1 Active Power	W	Signed	•	•	•	•					•
27	PowerActiveP2	P2 Active Power	W	Signed	•	•	•	•					•
28	PowerActiveP3	P3 Active Power	W	Signed	•	•	•	•					•
29	PowerRActiveQ1	Q1 Reactive Power	VAr	Signed	•	•	•	•					•
30	PowerRActiveQ2	Q2 Reactive Power	VAr	Signed	•	•	•	•					•
31	PowerRActiveQ3	Q3 Reactive Power	VAr	Signed	•	•	•	•					•
32	PowerApparentS1	S1 Apparent Power	VA	Unsigned	•	•	•	•					•
33	PowerApparentS2	S2 Apparent Power	VA	Unsigned	•	•	•	•					•

Index	Object Namew	Object Description	Unit	Type	Present + Timestamp	Present Min/Max + Timestamp	Average + Timestamp	Average Min/Max + Timestamp	Harmonics 2 -> 10	Energies Total + Partial + LastPartial	Energies Total Lagging/Leading	Multifluid	Reset Min/Max
34	PowerApparentS3	S3 Apparent Power	VA	Unsigned	•	•	•	•					•
35	PowerFactorPF1	PF1 Power Factor	-	Signed	•	•	•	•					•
36	PowerFactorTypeSPF1	sPF1 Power Factor Type	-	Unsigned	•	•	•	•					•
37	PowerFactorPF2	PF2 Power Factor	-	Signed	•	•	•	•					•
38	PowerFactorTypeSPF2	sPF1 Power Factor Type	-	Unsigned	•	•	•	•					•
39	PowerFactorPF3	PF3 Power Factor	-	Signed	•	•	•	•					•
40	PowerFactorTypeSPF3	sPF1 Power Factor Type	-	Unsigned	•	•	•	•					•
41	LoadCurve_ P+	Load Curve Positive Active Power	W	Unsigned	•								•
42	LoadCurve_P-	Load Curve Negative Active Power	W	Unsigned	•								•
43	LoadCurve_ Q+	Load Curve Positive Reactive Power	VAr	Unsigned	•								•
44	LoadCurve_Q-	Load Curve Negative Reactive Power	VAr	Unsigned	•								•
45	LoadCurve_S	Load Curve Apparent Power	VA	Unsigned	•								•
46	THD_I1	THD I1	%	Unsigned	•	•			•				•
47	THD_I2	THD I2	%	Unsigned	•	•			•				•
48	THD_I3	THD I3	%	Unsigned	•	•			•				•
49	THD_In	THD In	%	Unsigned	•	•			•				•
50	THD_V1	THD V1	%	Unsigned	•	•			•				•
51	THD_V2	THD V2	%	Unsigned	•	•			•				•
52	THD_V3	THD V3	%	Unsigned	•	•			•				•
53	THD_U12	THD U12	%	Unsigned	•	•			•				•
54	THD_U23	THD U23	%	Unsigned	•	•			•				•
55	THD_U31	THD U31	%	Unsigned	•	•			•				•
56	A+	Positive Active Energy	Wh	Unsigned	•					•			•
57	A-	Negative Active Energy	Wh	Unsigned	•					•			•
58	ER+	Positive Reactive Energy	VArh	Unsigned	•					•	•		•
59	ER-	Negative Reactive Energy	VArh	Unsigned	•					•	•		•
60	ES	Apparent Energy	VAh	Unsigned	•					•			•
61	Mff	Multifluid feeder	-	Signed	•							•	•

Annex II - 3. BACnet Services

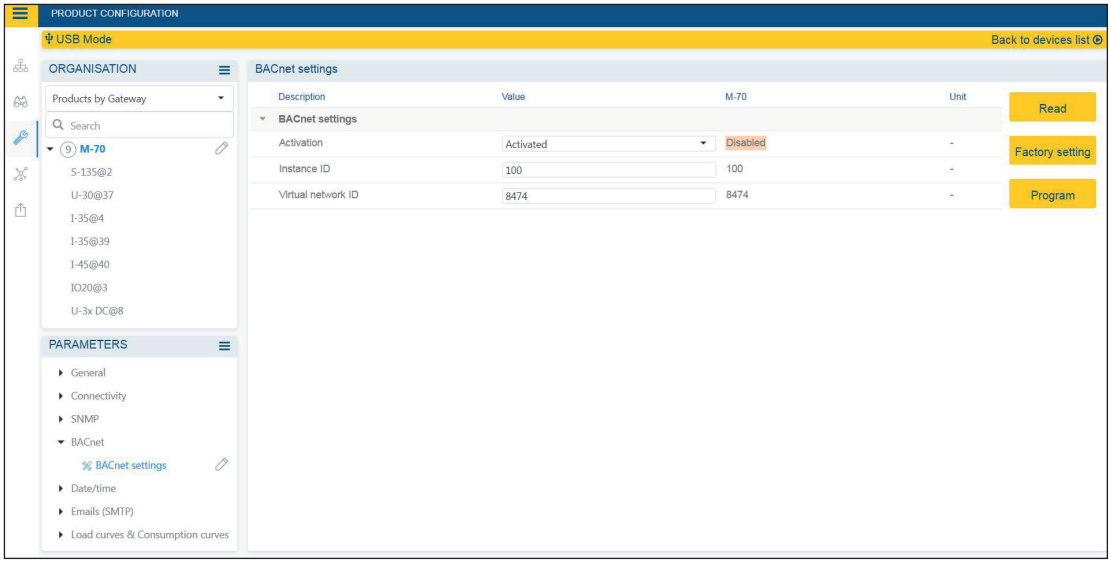
The services define methods for BACnet devices to communicate and exchange data with one another.
The D-50 / D-70 supports the following services:

SERVICE LIST	DESCRIPTION
readProperty	Used by a BACnet device (the client) to ask another BACnet device (the server) to provide the value of one of its object properties
readPropertyMultiple	Used by a BACnet device (the client) to ask another BACnet device (the server) to provide the values of multiple object properties
writeProperty	Used by a BACnet device (the client) to ask another BACnet device (the server) to change the value of one of its object properties
timeSynchronization	Used to broadcast the current time to one or more BACnet servers
who_Has	Asks which BACnet devices contain a particular Object
who_Is	Used by a BACnet client to ask the presence of BACnet servers

Annex II - 4. BACnet IP configuration via Easy Config System

The PICS file (Protocol Implementation Conformance Statement) is available at www.socomec.com

After logging in to Easy Config System on the DIRIS Digiware D-50 / D-70, you can find the BACnet IP settings in the BACnet menu under BACnet settings:



Activation: Enable or disable the BACnet IP function

Main instance ID: 100 by default. It must be unique within the BACnet network.

Virtual network ID: Set the virtual network ID. It must be unique within the BACnet network.

The port used by the DIRIS Digiware D-50 / D-70 for BACnet IP communication is set to 47808 (BAC0 in hexadecimal) and cannot be changed.