Instruction manual
MTL Industrial Network Solutions

May 2021
INM 9471-ET(G) Rev 2

9471-ET(G)

Instrinsically Safe Gigabit Ethernet 4 Port Serial Gateway

Powering Business Worldwide

DECLARATION OF CONFORMITY

A printed version of the Declaration of Conformity has been provided separately within the original shipment of goods. However, you can find a copy of the latest version at -

http://www.mtl-inst.com/certificates

CONTENTS

GENERAL SAFETY INFORMATION

Safety instructions for installation and operating personnel

The operating instructions provided here contain **essential safety instructions** for installation personnel and those engaged in the operation, maintenance and servicing of the equipment.

⚠ WARNING

WARNING !

A 'WARNING' marked in this way is provided for operator and plant safety and MUST be followed.

CAUTION !

A Caution is provided to prevent damage to the instrument.

NOTE

These are used to guide the user in the operation of the instrument.

Before commencing installation or commissioning:

- Read and understand the contents of this manual
- Ensure installation and operating personnel have received adequate training for this task
- Ensure that any operating instructions are fully understood by the personnel responsible.
- Observe national and local installation and mounting regulations (e.g. IEC 60079-14).

⚠ WARNING

WARNING !

These assemblies may not be used in explosion-hazard area applications if they have been used previously in general electrical installations.

⚠ WARNING

WARNING !

The responsibility for planning, installation, commissioning, operation and maintenance, particularly with respect to applications in explosion-hazard areas, lies with the plant operator.

During operation:

- Make the relevant instructions available at all times to the operating personnel.
- Observe safety instructions.
- Observe national safety and accident prevention regulations.
- Operate the equipment within its published specification.
- Servicing, maintenance work or repairs not described in this manual must not be performed without prior agreement with the manufacturer.
- Any damage to this equipment may render its explosion protection null and void.
- No changes to any of the components that might impair their explosion protection are permitted.

If any information provided here is not clear:
Contact **Eaton's MTL product line** or an authorised distributor or sales office.

NOTE

Improper installation and operation of the enclosure can result in the invalidation of the guarantee.

1 FEATURE

- Intrinsically Safe ATEX / IECEx Certification
- 4 Communication Ports – RS232/TTL/485/422 (2 & 4 Wire)
- Dual Port Switch 10/100/1000Mb LAN (daisy-chain capability)
- LAN to Serial
- Modbus/TCP – Modbus/RTU (or ASCII) Protocol
- Versions

  2x Gigabit LAN Ports + 4 Coms

  2x 10/100 LAN/PoEx* Ports + 4 Coms
- CPU Management Feature via Web Pages
- Compact dimensions (W: 42 x H: 160 x D: 140 mm)
- Ex ia IIB T4 Ga, Ex ia [ia Da] IIIC T135°C Db (non-mining),
  Ex ia I Ma (Mining) - ETG version
- Ex ia IIC T4 Ga, Ex ia [ia Da] IIIC T135°C Db (non-mining),
  Ex ia I Ma (Mining) - ET version
- Ta -40ºC to 70ºC
- Zone 1 / Zone 21 mounting
- (Zone 0 / Zone 20 with a suitable Ex ia Power Supply)

**Note* – PoEx is a simple adaptation of the IEEE 802.3af Power over Ethernet (PoE) standard to bring the benefits to the 9400 Range of Hazardous Area devices. This allows two spare pairs in the existing Cat5e cable to distribute the power supply from a 9476 Ethernet Switch (Power Sourcing Equipment – PSE) to each of the devices connected to its five ports (PD – Powered Device). This adaptation is necessary due to restrictions for Hazardous Area use. It is not implied that the device conforms to the 802.3af (PoE) standard.*

2 DESCRIPTION

The 9471-ET(G) is an Intrinsically Safe (IS) Ethernet to Serial 4-Port Communication module suitable for Zone 1 / Zone 21 mounting, (Zone 0 / Zone 20 with a suitable Ex ia Power Supply).

The Module allows existing Intrinsically Safe equipment with an RS485/RS422 or RS232/TTL port to become Ethernet Enabled via a Cat5e/6 cable connection into an IS Ethernet Network (LAN). The unit has 4 serial ports, each one supporting either RS485/RS422 or RS232/TTL depending upon the configuration required. There are 2x RJ45 (LAN) ports that support 10/100/1000 IS Ethernet connections - these allow 'daisy-chaining' of units together.

Power (12V DC) is supplied to the module locally along with Power over Ethernet (PoEx) for the connected devices where required.
Note: PoEx not available on Gigabit ports.

The compact and cost effective design makes it the ideal choice for many applications:

Petrochem

Process Monitoring & Control...

Mining

Underground Communication Links, PLC and Machine Monitoring…

Electrical connections are via cage-clamp and/or screw type plug/socket terminals along with RJ45 type connectors for the Ethernet LAN ports.

3 CONNECTIONS

3.1 DATA & POWER TERMINALS

Power + External IP Rated LEDs (CON1)

Pin	Function	Pin	Function
1	Power In +12V#	**2**	Power In 0V#
3	LAN1 PoEx +12V#	**4**	LAN1 PoEx 0V#
5	LAN2 PoEx +12V#	**6**	LAN2 PoEx 0V#
7		**8**	
9		**10**	
11	0V	**12**	0V
13	LAN1 LED	**14**	LAN2 LED
15	COM1 LED	**16**	COM2 LED
17	COM3 LED	**18**	COM4 LED

#Connect LAN1 OR LAN2 PoEx terminals to Power In terminals to use this function

External IP66 rated LEDs wire down to 0V
Power Ui = 15.4V

3.2 LAN (RJ45) 10/100/1000 BASE-T Ethernet

Pin	10/100 Function	Gigabit Function
1	Tx +	BI_DA+
2	Tx-	BI_DA-
3	Rx +	BI_DB+
4	PoEx +12V*	BI_DC+
5	PoEx +12V*	BI_DC-
6	Rx-	BI_DB-
7	PoEx 0V*	BI_DD+
8	PoEx 0V*	BI_DD-

*PoEx not available on Gigabit ports

3.3 Comms Port Connections

PORT 1 & 2 (CON3)
RS485/422/232/TTL Ports

Pin	Function	Pin	Function
1	1Tx+/A	**2**	1Tx-/B
3	1Rx+	**4**	1Rx-
5	1Tx (RS232)	**6**	0V
7	1Rx (RS232)	**8**	0V
9	2Tx+/A	**10**	2Tx-/B
11	2Rx+	**12**	2Rx-
13	2Tx (RS232)	**14**	0V
15	2Rx (RS232)	**16**	0V

PORT 3 & 4 (CON4)
RS485/422/232/TTL Ports

Pin	Function	Pin	Function
1	3Tx+/A	**2**	3Tx-/B
3	3Rx+	**4**	3Rx-
5	3Tx (RS232)	**6**	0V
7	3Rx (RS232)	**8**	0V
9	4Tx+/A	**10**	4Tx-/B
11	4Rx+	**12**	4Rx-
13	4Tx (RS232)	**14**	0V
15	4Rx (RS232)	**16**	0V

3.4 LED indicators

	OFF	FLASH	ON
PWR (green)	Power Fail	N/A	Power OK
WDG (red/green)	Fault	Green- Healthy (10Hz)	Fault
TX (green)	Idle	Transmitting Serial Data	N/A
RX (red)	Idle	Receiving Serial Data	Fault – RX data polarity is inverted
STAT (red/green)	N/A	Green – Identify module mode	Red (fault) Green (healthy)
RJ45 ACT (yellow)	Ethernet link disconnected	Ethernet link activity	Ethernet link connected
RJ45 1000 (green)	10/100Mbps	N/A	1000Mbps
LAN1 – LAN2 EXT LED	Ethernet link disconnected	Ethernet link activity	Ethernet link connected
Com1 – 4 EXT LED	Idle	TX/RX Data	N/A

4 ORDERING INFORMATION

Part Number	Description	Comments
9471-ETG	**4-Port Serial Gateway (Gigabit)**	**Standard**
9471-ET	4-Port Serial Gateway (10/100 PoEx)	Special Order

Note: Special order items may incur a minimum order quantity

5 DIMENSIONS

Width	42mm
Height	160mm
Depth	140mm
Weight	1500g
Mounting	Din Rail

6 ENVIRONMENTAL

Operating Temperature

-40°C…+70°C

Storage Temperature

-40°C…+70°C

Humidity

0…95% RH, non-condensing

Ingress Protection

Select enclosure to suit application, see certificates for information

7 WASTE REMOVAL INFORMATION

The electronic equipment within must not be treated as general waste. By ensuring that this product is disposed of correctly you will be helping to prevent potentially negative consequences for the environment and human health, which could otherwise be caused by incorrect waste handling of this product. For more detailed information about the take-back and recycling contact Controlled Systems Ltd

8 INSTALLATION

⚠ WARNING	**WARNING !** See Special Conditions of Safe Use in the folllowing section regarding ATEX & IECEx Certification Information before installation

The 12V supply to the module connects via screw terminals 1 + 2 as shown above.

If the unit is being powered using Power over Ethernet (PoEx), it is required that you connect the relevant PoEx power terminals (Con1) to the main power supply pins (Con1), see connections section.

As the 9471 LAN ports support Auto MDI/MDI-X, a straight connected RJ45 Cat5e cable is used to connect to any device.

It is recommended that Cat5e cables for Hazardous Area Zone 1 use are 'Blue' in colour and are of good quality (see accessories section), the Safe Area cables being a colour other than blue to aid identification.

The operating parameters must not exceed those as detailed on the certificate.

This apparatus must only be installed or replaced by a competent person who must ensure existing IS segregation is maintained.

9 ATEX & IECEx CERTIFICATION INFORMATION

The following information is in accordance with the Essential Health and Safety Requirements (Annex II) of the EU Directive 2014/34/EU [the ATEX Directive- safety of apparatus] and is provided for those locations where the ATEX Directive is applicable.

General

a) This equipment must only be installed, operated and maintained by competent personnel. Such personnel shall have undergone training, which included instruction on the various types of protection and installation practices, the relevant rules and regulations, and on the general principles of area classification. Appropriate refresher training shall be given on a regular basis. [See clause 4.2 of EN 60079-17].

b) This equipment has been designed to provide protection against all the relevant additional hazards referred to in Annex II of the directive, such as those in clause 1.2.7. This equipment has been designed to meet the requirements of intrinsically safe electrical apparatus in accordance with EN 60079-0, EN 60079-11 and EN 60079-26.

Installation

a) Reference to the IEC code of practice IEC 60079-14. In addition particular industries or end users may have specific requirements relating to the safety of their installations and these requirements should also be met. For the majority of installations the Directive 1999/92/EC [the ATEX Directive- safety of installations] is also applicable.

b) Unless already protected by design this equipment must be protected by a suitable enclosure against

   i) mechanical and thermal stresses in excess of those noted in the certification documentation and the product specification.

   ii) aggressive substances excessive dust moisture and other contaminants

c) This apparatus is intrinsically safe electrical apparatus and is normally mounted in a hazardous area.

Inspection and maintenance

a) Inspection and maintenance should be carried out in accordance with European, national and local regulations which may refer to the IEC standard IEC 60079-17. In addition specific industries or end users may have specific requirements which should also be met.

b) Access to the internal circuitry must not be made during operation.

Repair

This product cannot be repaired by the user and must be replaced with an equivalent certified product.

Specific Conditions of Use (Special Conditions)

The following conditions relate to safe installation and/or use of the equipment.

8.1 For Group I, the modules shall each be mounted within an enclosure providing a degree of protection of at least IP54.
This shall be in accordance with EN 60529, and the modules installed in a manner that does not impair the existing creepage and clearance distances. The enclosure shall also comply with the appropriate requirements of Clauses 7.4.2 and 7.5, or 8.2 of EN 60079-0.

8.2 For Group II, the RJ45 connectors shall be fitted with either a plug or blanking plug.Alternatively, the module shall be mounted in an enclosure providing a degree of protection of at least IP20.
This shall be in accordance with EN 60529, and the modules installed in a manner that does not impair the existing creepage and clearance distances. The enclosure shall also comply with the appropriate requirements of Clauses 7.4.2 and 7.5, or 8.3 of EN 60079-0.

8.3 For Group III, the module shall be mounted inside a suitably certified enclosure which provides a minimum degree of protection of at least IP54. The module shall be installed in a manner that does not impair the existing creepage and clearance distances.

8.4 The supply to the modules must be derived from a suitably certified, intrinsically safe supply.

8.5 The values of Co and Lo shall apply when one of the two conditions below is given:

- The total Li of the external circuit (excluding the cable) is < 1% of the Lo value, or

- The total Ci of the external circuit (excluding the cable) is < 1% of the Co value.

The above parameters are reduced to 50% when both of the two conditions below are given:

- The total Li of the external circuit (excluding the cable) > 1% of the Lo, and

- The total Ci of the external circuit (excluding the cable) > 1% of the Co.

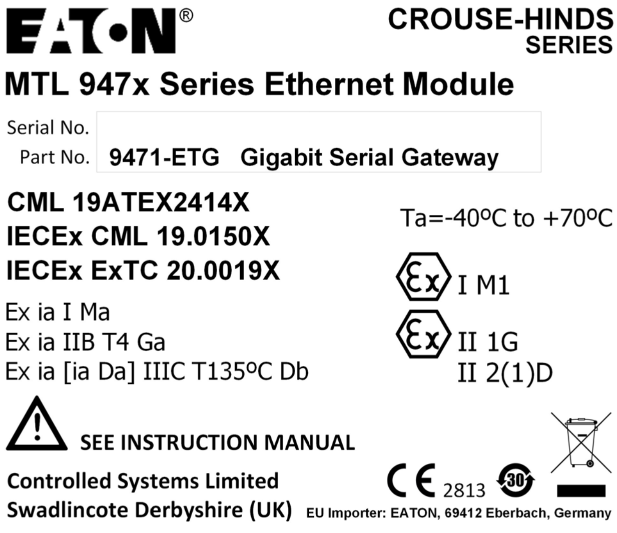
Note: the reduced capacitance of the external circuit (including cable) shall not be greater than 1µF for Group I and IIB/III and 600 nF for IIC.

8.6 The equipment shall be mounted on an earthed metal bracket or housing.

Marking

Each device is marked in accordance with the Directive and CE marked with the Notified Body Identification Number.

9471-ETG Product Label



EATON®

CROUSE-HINDS SERIES

MTL 947x Series Ethernet Module

Serial No.
Part No. 9471-ETG Gigabit Serial Gateway

CML 19ATEX2414X
IECEx CML 19.0150X
IECEx ExTC 20.0019X

Ta=-40ºC to +70ºC

Ex ia I Ma
Ex ia IIB T4 Ga
Ex ia [ia Da] IIIC T135ºC Db

Ex I M1
Ex II 1G
II 2(1)D

SEE INSTRUCTION MANUAL

Controlled Systems Limited
Swadlincote Derbyshire (UK)

CE 2813

EU Importer: EATON, 69412 Eberbach, Germany

10 SPECIFICATION

Power supplies

12VDC IS Power Supply Input
PoEx™ (Power over IS Ethernet)
Typically 12V @ 150mA (Inrush < 400mA)
Ui =15.4V
9492-PS-PLUS recommended

Ethernet

Intrinsically Safe 10/100/1000Base-T

Connector

RJ45 (x2)

Cable Length

Up to 100m Cat5e

11 APPROVALS

Location of Unit

Zone 1, IIB T4 hazardous area (9471-ETG)
Zone 1, IIC T4 hazardous area (9471-ET)

Certification Code

Ex ia IIB T4 Ga (9471-ETG)
Ex ia IIC T4 Ga (9471-ET)
Ex ia [ia Da] IIIC T135°C Db (non-mining)
Ex ia I Ma (M1 mining)
Ta =-40°C to +70°C

Certificate numbers

ATEX (CML 19ATEX2414X)
IECEx (IECEx CML 19.0150X)
QLD (IECEx ExTC 20.0019X

See certificates for further information

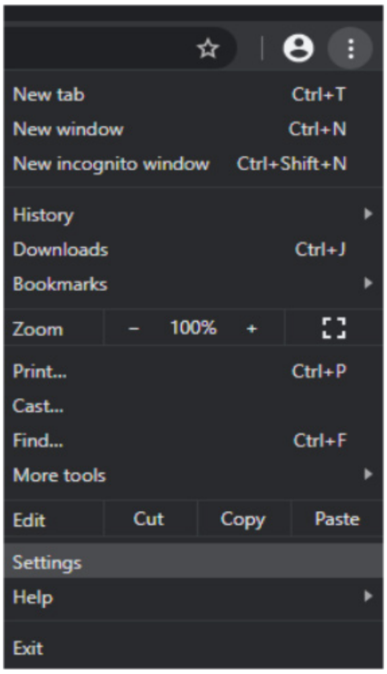
CE

12 CERTIFICATE INSTALLATION

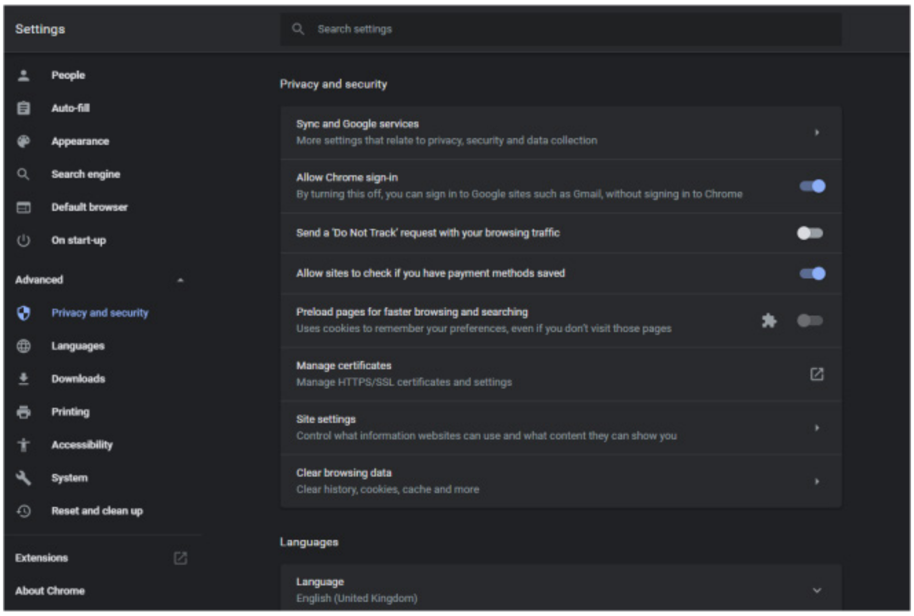
The certificate works on the Hostname of “9471-Gateway”

To be able to view the HTTPS pages of the unit securely you are required to install a SSL certificate. Below are the steps required in the Google Chrome browser (other browser setups are similar).

Click on the 3 dots in the top right corner of the browser



Click Advanced->Privacy and Security-> Manage certificates



Privacy and security

Sync and Google services
More settings that relate to privacy, security and data collection

Allow Chrome sign-in
By turning this off, you can sign in to Google sites such as Gmail, without signing in to Chrome

Send a 'Do Not Track' request with your browsing traffic

Allow sites to check if you have payment methods saved

Preload pages for faster browsing and searching
Uses cookies to remember your preferences, even if you don't visit those pages

Manage certificates
Manage HTTPS/SSL certificates and settings

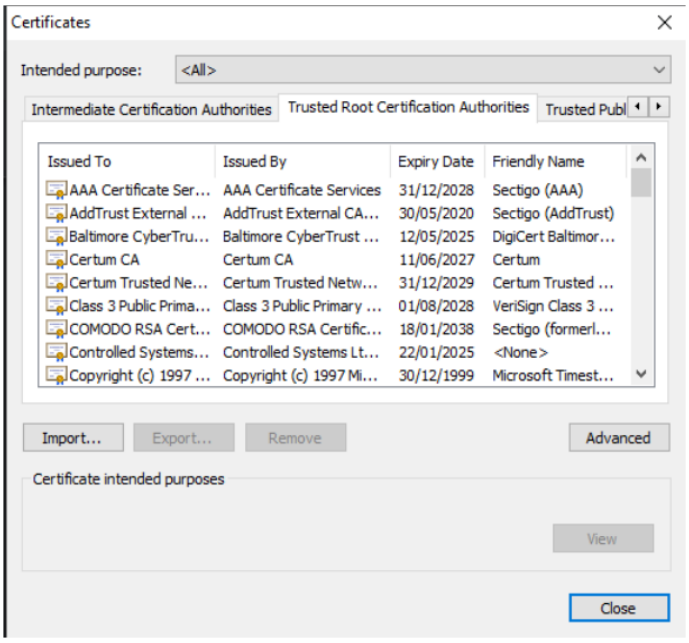
Site settings
Control what information websites can use and what content they can show you

Clear browsing data
Clear history, cookies, cache and more

Languages

Language
English (United Kingdom)

Click on the Trusted Root Certification Authorities Ab and click Insert



Certificates

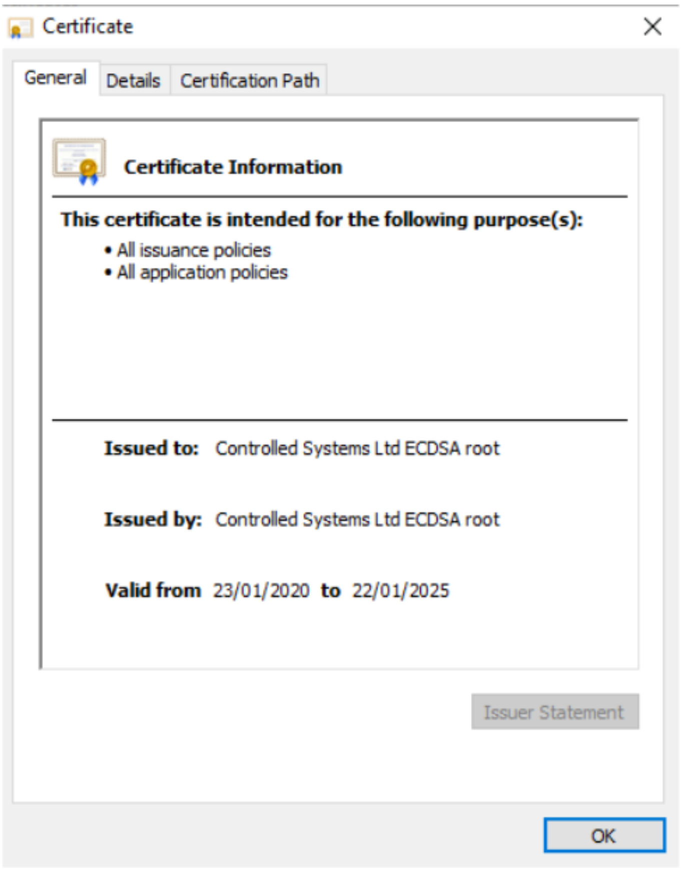
Intended purpose: <All>

Intermediate Certification Authorities | Trusted Root Certification Authorities | Trusted Publ

Issued To	Issued By	Expiry Date	Friendly Name
AAA Certificate Ser...	AAA Certificate Services	31/12/2028	Sectigo (AAA)
AddTrust External ...	AddTrust External CA...	30/05/2020	Sectigo (AddTrust)
Baltimore CyberTru...	Baltimore CyberTrust ...	12/05/2025	DigiCert Baltimor...
Certum CA	Certum CA	11/06/2027	Certum
Certum Trusted Ne...	Certum Trusted Netw...	31/12/2029	Certum Trusted ...
Class 3 Public Prima...	Class 3 Public Primary ...	01/08/2028	VeriSign Class 3 ...
COMODO RSA Cert...	COMODO RSA Certific...	18/01/2038	Sectigo (formerl...
Controlled Systems...	Controlled Systems Lt...	22/01/2025	<None>
Copyright (c) 1997 ...	Copyright (c) 1997 Mi...	30/12/1999	Microsoft Timest...

Browse for the “ca-cert.pem” file and install it.

You will now get and entry in the list of certificates called Controlled Systems Ltd ECDSA root



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: Controlled Systems Ltd ECDSA root

Issued by: Controlled Systems Ltd ECDSA root

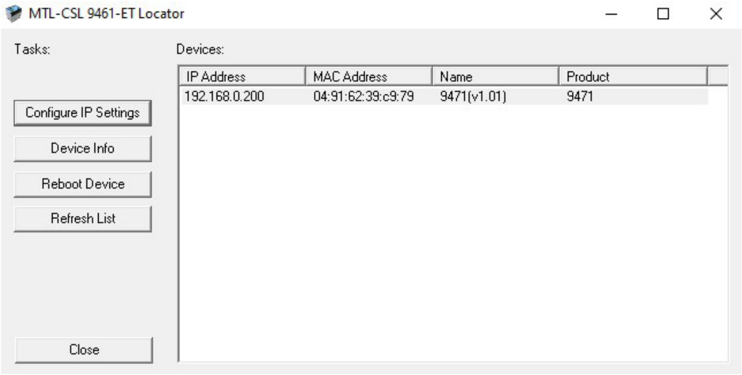
Valid from 23/01/2020 **to** 22/01/2025

13 CONNECTING THE 9471-ET(G) TO A PC/NETWORK

□ Ensure that the 9471 unit is powered by a suitable IS supply, such as the MTL 9492-PS PLUS. PoEx can be used to power the unit via the LAN port if required.

□ The 9471 unit should then be connected to an IS Ethernet Network/PC using a suitable CAT5/6 cable. Either LAN Port 1 or 2 can be used. The other LAN port can be used for daisy chaining units together.

□ Run the 9461-ET Finder.exe program which can be found on the MTL website, this will automatically search for and locate any 9471 units connected to the network.



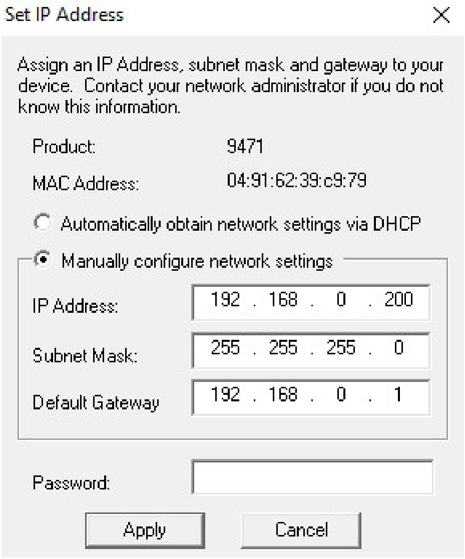
MTL-CSL 9461-ET Locator

Tasks:

Devices:

IP Address	MAC Address	Name	Product
192.168.0.200	04:91:62:39:c9:79	9471(v1.01)	9471

□ Click on the device that you are looking to configure, then click the "configure IP settings" button and this will bring up the following screen



Set IP Address

Assign an IP Address, subnet mask and gateway to your device. Contact your network administrator if you do not know this information.

Product: 9471

MAC Address: 04:91:62:39:c9:79

○ Automatically obtain network settings via DHCP

● Manually configure network settings

IP Address: 192 . 168 . 0 . 200

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway 192 . 168 . 0 . 1

Password:

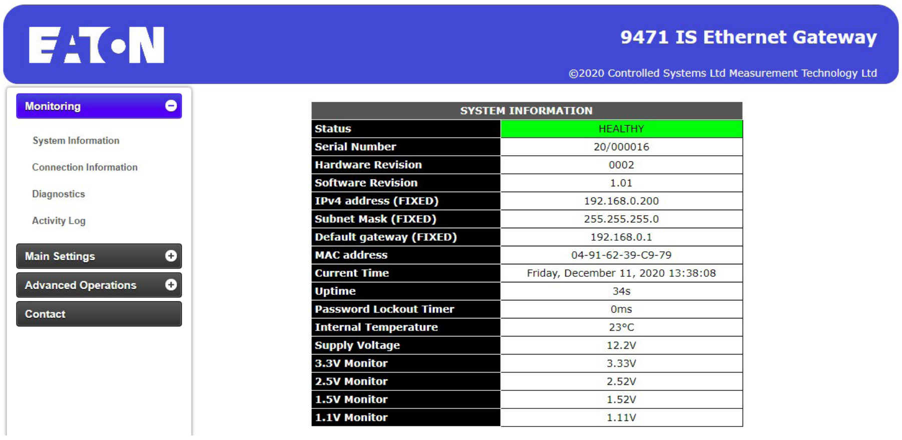
□ Manually type in the settings that you require and then enter the password "CSL". Click the apply button to send the settings to the 9471.

□ Reboot the device by either powering down or by clicking the "reboot" button in the above screen.

□ Once the 9471 is up and running, navigate to the IP Address that has been programmed into the unit using a web browser.

NOTE: The Factory Default IP Address is 192.168.0.200

14 SYSTEM INFORMATION



SYSTEM INFORMATION	
Status	HEALTHY
Serial Number	20/000016
Hardware Revision	0002
Software Revision	1.01
IPv4 address (FIXED)	192.168.0.200
Subnet Mask (FIXED)	255.255.255.0
Default gateway (FIXED)	192.168.0.1
MAC address	04-91-62-39-C9-79
Current Time	Friday, December 11, 2020 13:38:08
Uptime	34s
Password Lockout Timer	0ms
Internal Temperature	23°C
Supply Voltage	12.2V
3.3V Monitor	3.33V
2.5V Monitor	2.52V
1.5V Monitor	1.52V
1.1V Monitor	1.11V

This is the main page of the 9471 and show the main information of the 9471 Gateway

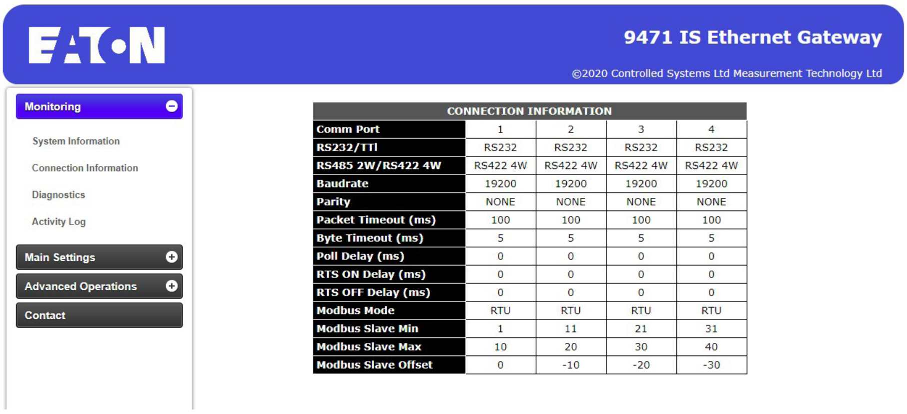
This page show the status of the unit to confirm everything is functioning correctly.

The Password lockout timer indicates the time remaining if the configuration of the unit has been locked out due to the password being entered incorrect 3 or more times.

Hardware and Software version is shown here as well to ensure the latest firmware is being used.

If intermittent problems exist check the Temperature and voltage settings as this may indicate what is wrong.

15 CONNECTION INFORMATION

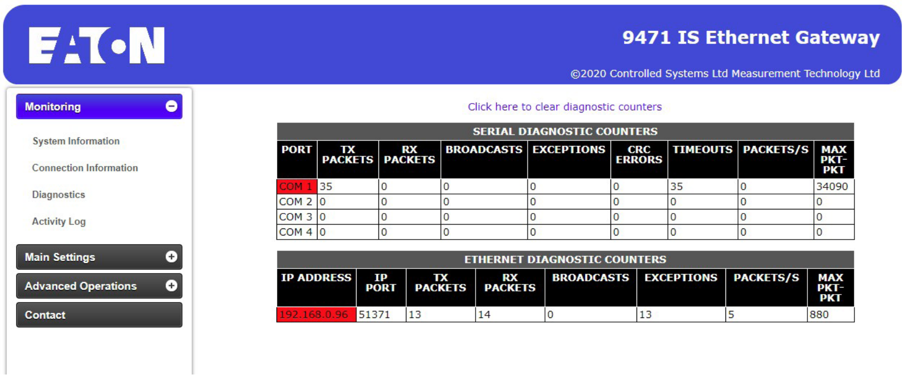


CONNECTION INFORMATION

Comm Port	1	2	3	4
RS232/TTl	RS232	RS232	RS232	RS232
RS485 2W/RS422 4W	RS422 4W	RS422 4W	RS422 4W	RS422 4W
Baudrate	19200	19200	19200	19200
Parity	NONE	NONE	NONE	NONE
Packet Timeout (ms)	100	100	100	100
Byte Timeout (ms)	5	5	5	5
Poll Delay (ms)	0	0	0	0
RTS ON Delay (ms)	0	0	0	0
RTS OFF Delay (ms)	0	0	0	0
Modbus Mode	RTU	RTU	RTU	RTU
Modbus Slave Min	1	11	21	31
Modbus Slave Max	10	20	30	40
Modbus Slave Offset	0	-10	-20	-30

□ This page shows the current configuration of the 4 Comms ports on the 9471

16 COMMUNICATION DIAGNOSTICS



9471 IS Ethernet Gateway

©2020 Controlled Systems Ltd Measurement Technology Ltd

Click here to clear diagnostic counters

SERIAL DIAGNOSTIC COUNTERS

PORT	TX PACKETS	RX PACKETS	BROADCASTS	EXCEPTIONS	CRC ERRORS	TIMEOUTS	PACKETS/S	MAX PKT-PKT
COM 1	35	0	0	0	0	35	0	34090
COM 2	0	0	0	0	0	0	0	0
COM 3	0	0	0	0	0	0	0	0
COM 4	0	0	0	0	0	0	0	0

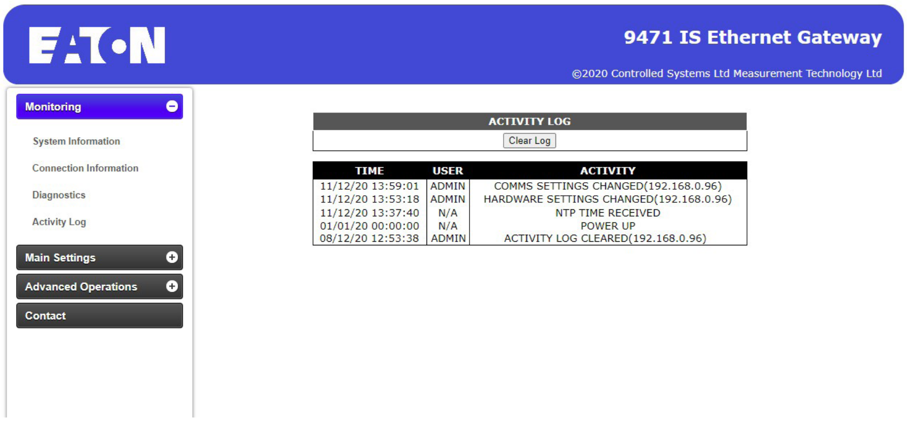
ETHERNET DIAGNOSTIC COUNTERS

IP ADDRESS	IP PORT	TX PACKETS	RX PACKETS	BROADCASTS	EXCEPTIONS	PACKETS/S	MAX PKT-PKT
192.168.0.96	51371	13	14	0	13	5	880

This page shows the counters for all of the LAN connected Modbus/TCP clients as well as the serial ports, this can be useful for fault finding on the network.

The port will turn green once healthy

17 ACTIVITY LOG



ACTIVITY LOG

Clear Log

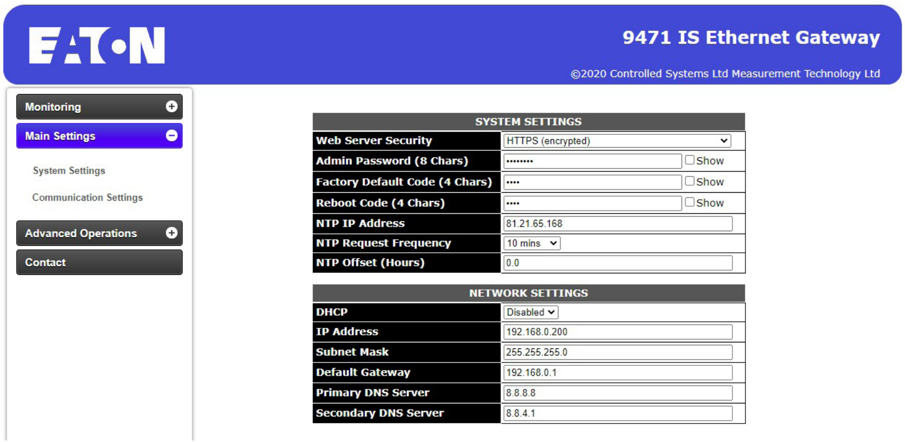
TIME	USER	ACTIVITY
11/12/20 13:59:01	ADMIN	COMMS SETTINGS CHANGED(192.168.0.96)
11/12/20 13:53:18	ADMIN	HARDWARE SETTINGS CHANGED(192.168.0.96)
11/12/20 13:37:40	N/A	NTP TIME RECEIVED
01/01/20 00:00:00	N/A	POWER UP
08/12/20 12:53:38	ADMIN	ACTIVITY LOG CLEARED(192.168.0.96)

This page accessed via the password shows any changes that have occured to the unit. This includes configuration changes, password entered wrong and other useful information.

The Clear Log button will empty the existing log.

NOTE: The Factory Default Password is "Pa55w071" (without quotes)

18 SYSTEM SETTINGS



SYSTEM SETTINGS	
Web Server Security	HTTPS (encrypted)
Admin Password (8 Chars)	•••••••• □ Show
Factory Default Code (4 Chars)	•••• □ Show
Reboot Code (4 Chars)	•••• □ Show
NTP IP Address	81.21.65.168
NTP Request Frequency	10 mins
NTP Offset (Hours)	0.0

NETWORK SETTINGS	
DHCP	Disabled
IP Address	192.168.0.200
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.1

System Settings

Web Server Security

HTTP (clear text) HTTPS (encrypted)

We strongly recommend the use of HTTPS so that the data between browser and 9471 is encrypted

Admin Password

The admin password can be changed here

Factory Default Code

The code entered to allow the unit to factory default can be changed here

Reboot Code

The code entered to allow the unit to reboot can be changed here

NTP IP Address

Enter the IP Address of an NTP server to allow the unit to get the correct time

NTP Request Frequency

This is the frequency that the unit will request the time from an NTP server

NTP Offset

This value can be used to offset the time received from the NTP server. This value is the number of hours the local time is different from Greenwich Mean Time(GMT)

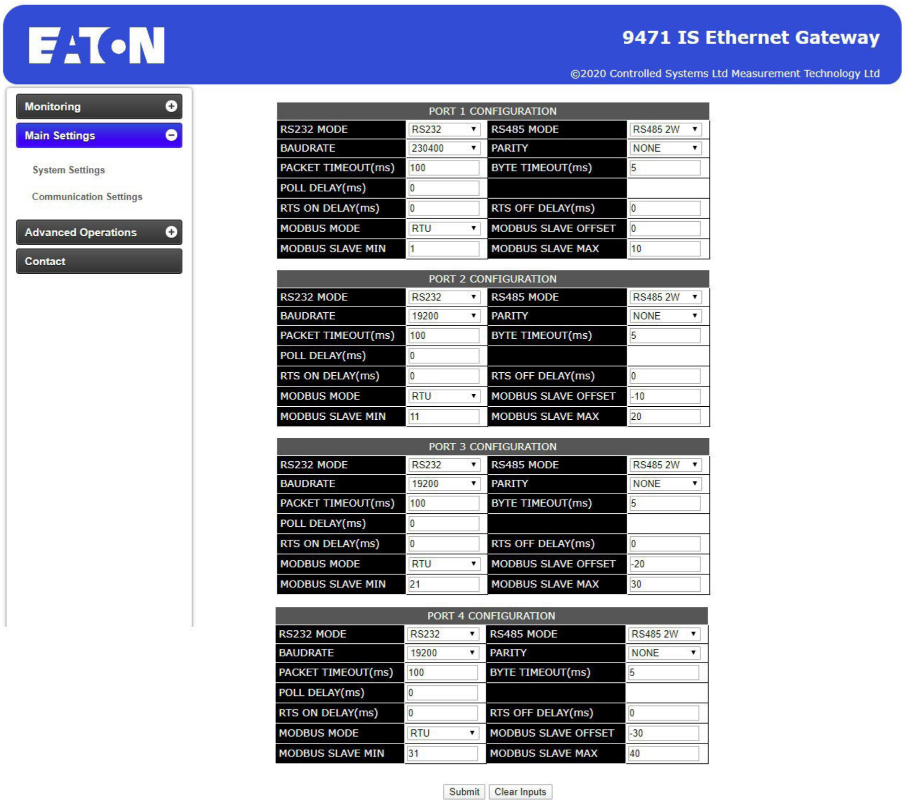
Network Settings

Enter the various settings to allow the 9471 to live on your network architecture. If required DHCP can be setup here and then the unit will be given an IP Address from the Networks DHCP server

Click Submit to save the selection.

NOTE: The Factory Default Password is "Pa55w071" (without quotes)

19 SETTING UP THE 9471 COMS PORTS



PORT 1 CONFIGURATION

RS232 MODE	RS232	RS485 MODE	RS485 2W
BAUDRATE	230400	PARITY	NONE
PACKET TIMEOUT(ms)	100	BYTE TIMEOUT(ms)	5
POLL DELAY(ms)	0		
RTS ON DELAY(ms)	0	RTS OFF DELAY(ms)	0
MODBUS MODE	RTU	MODBUS SLAVE OFFSET	0
MODBUS SLAVE MIN	1	MODBUS SLAVE MAX	10

PORT 2 CONFIGURATION

RS232 MODE	RS232	RS485 MODE	RS485 2W
BAUDRATE	19200	PARITY	NONE
PACKET TIMEOUT(ms)	100	BYTE TIMEOUT(ms)	5
POLL DELAY(ms)	0		
RTS ON DELAY(ms)	0	RTS OFF DELAY(ms)	0
MODBUS MODE	RTU	MODBUS SLAVE OFFSET	-10
MODBUS SLAVE MIN	11	MODBUS SLAVE MAX	20

PORT 3 CONFIGURATION

RS232 MODE	RS232	RS485 MODE	RS485 2W
BAUDRATE	19200	PARITY	NONE
PACKET TIMEOUT(ms)	100	BYTE TIMEOUT(ms)	5
POLL DELAY(ms)	0		
RTS ON DELAY(ms)	0	RTS OFF DELAY(ms)	0
MODBUS MODE	RTU	MODBUS SLAVE OFFSET	-20
MODBUS SLAVE MIN	21	MODBUS SLAVE MAX	30

PORT 4 CONFIGURATION

RS232 MODE	RS232	RS485 MODE	RS485 2W
BAUDRATE	19200	PARITY	NONE
PACKET TIMEOUT(ms)	100	BYTE TIMEOUT(ms)	5
POLL DELAY(ms)	0		
RTS ON DELAY(ms)	0	RTS OFF DELAY(ms)	0
MODBUS MODE	RTU	MODBUS SLAVE OFFSET	-30
MODBUS SLAVE MIN	31	MODBUS SLAVE MAX	40

This page show how you can modify the current settings on each other 4 coms ports and set them up accordingly

The Slave offset allows the user the option of having the same serial slave addressed devices on the 4 ports. It used the sign and offset value to alter the slave address received on the Ethernet before it is passed to the serial port. In the above screenshot, the following config is used;

Port	TCP Slave Addresss	Offset	Serial Slave Address
1	1-10	+0	1-10
2	11-20	-10	1-10
3	21-30	-20	1-10
4	31-40	-30	1-10

The Modbus slave Min and Max sets the TCP slave address limits for that port.

□ Packet Timeout sets the maximum time waiting for the final byte of a reply from a slave. (100ms is typical but may be extended for 'slow' slaves or reduced for 'fast' ones)

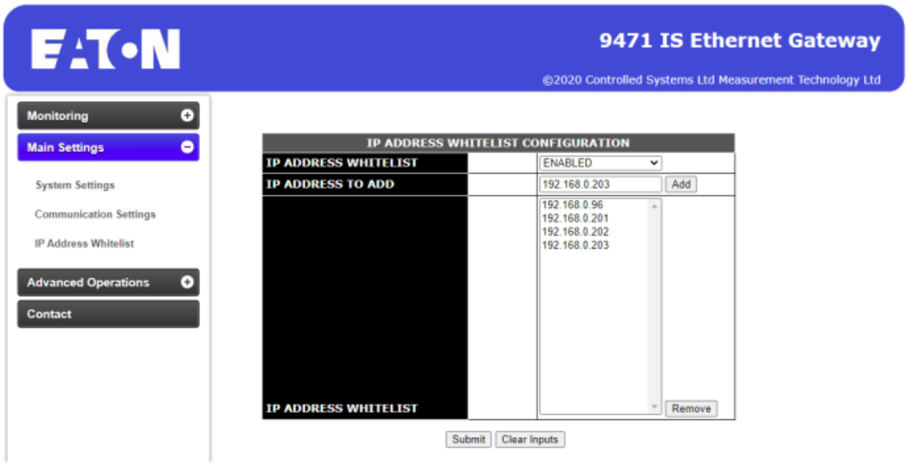
□ Byte Timeout determines the end of a slaves reply as when another byte is not received during this time.(typically set between 2ms and 20ms depending upon Baudrate)

□ Poll Delay slows down the packet rate if required. (Default is 0ms)

□ RTS ON Delay gives a delay after RTS before the packet data is sent, RTS OFF gives a delay after the packet data is sent before releasing RTS signal (typically 0ms to 5ms)

□ Once the settings have been configured, click the submit button. A configuration message will be displayed for 3 seconds before returning back to the main page.

20 IP ADDRESS WHITELIST



IP ADDRESS WHITELIST CONFIGURATION

IP ADDRESS WHITELIST	ENABLED
IP ADDRESS TO ADD	192.168.0.203
IP ADDRESS WHITELIST	192.168.0.96 192.168.0.201 192.168.0.202 192.168.0.203

The Web page above accessed via password allows the user to configure a whitelist of IP addresses. The IP Whitelist is a feature that allows the user to specify what IP Addresses can communicate Modbus through the 9471.

IP Address Whitelist

Enabled / Disabled

This parameter allows the enabling or disabling of the IP whitelist.

We strongly recommend that the IP Whitelist function be used to ensure that the device can only be accessed via authorised devices

IP Address to Add

Enter the IP address of the device you would like to connect and communicate through the 9471 and click Add.

Wildcards in the form of ###.###.###* (e.g. 192.168.0.*) can also be used to allow any device on that subnet to communicate.

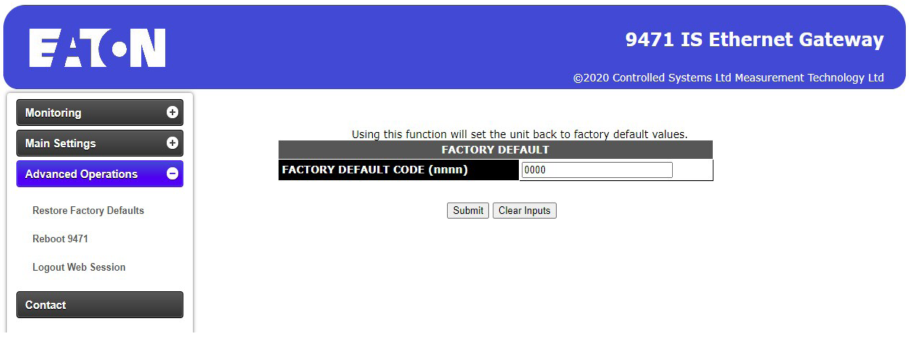
IP Address Whitelist

This list shows the current IP addresses allowed to communicate through the 9471. To remove an entry select it in the list and click Remove.

Click Submit to save the selection.

NOTE: The Factory Default Password is "Pa55w071" (without quotes)

21 RESTORE FACTORY DEFAULTS



Using this function will set the unit back to factory default values.

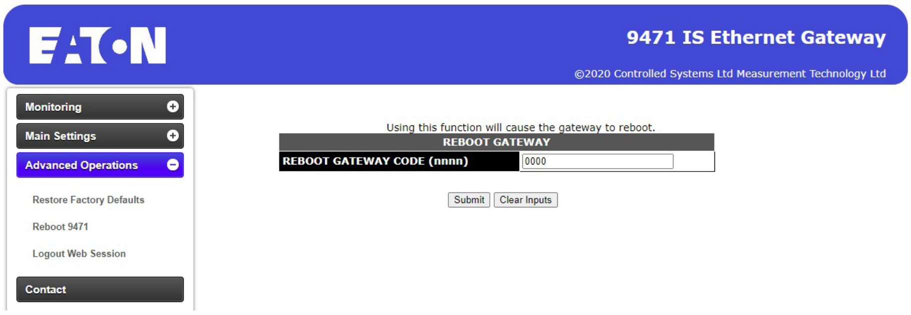
FACTORY DEFAULT	
FACTORY DEFAULT CODE (nnnn)	0000

This page allow the resetting of the unit back to Factory Defaults. To reset enter the factory reset code .

This page is only accessed via a password

The default factory reset code is “DEF

22 REBOOT GATEWAY



Using this function will cause the gateway to reboot.

REBOOT GATEWAY	
REBOOT GATEWAY CODE (nnnn)	0000

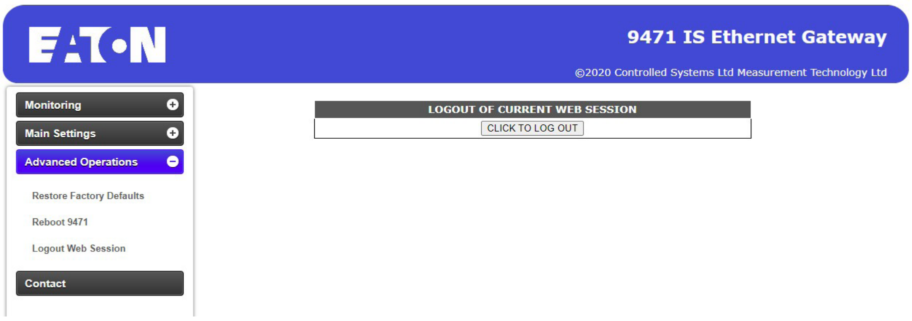
This page allow the rebooting of the unit. To reset enter the reboot device code.

This page is only accessed via a password.

The default reboot code is“4E5E”

NOTE: The Factory Default Password is "Pa55w071" (without quotes)

23 LOGOUT OF CURRENT WEB SESSION



This page logs the current user out of the web session.

It is highly recommended that once finished using the web interface that you log out enforcing that the password will have to be entered next time the unit is accessed.

24 RESET BUTTON

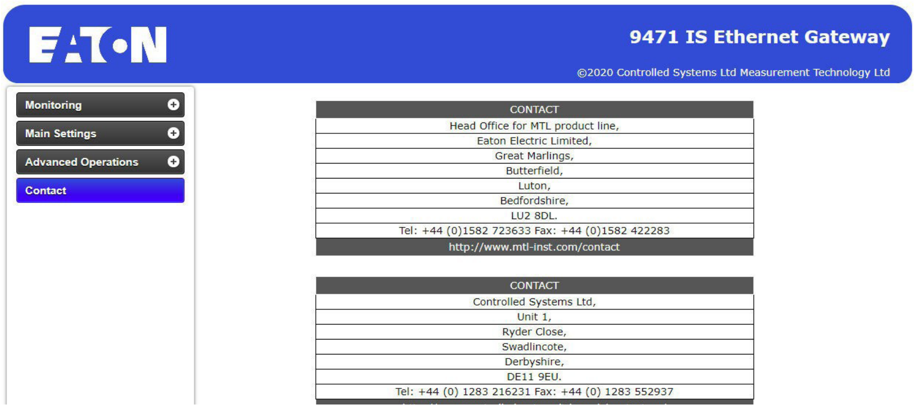
There is a hardware push button that is accessible through the small hole in the front panel, near to the LEDs. This may be needed for example if the password is unknown and you need to factory default the unit to again allow access to configure it.

The button has two functions depending on when it is pressed-

1. Press on power-up = This puts the unit into **Bootloader Mode**, ready for a firmware upgrade. The watchdog LED **flashes red** and the status LED turns **red** also. To exit this mode cycle the power to the unit.

2. Press 1-2 seconds after power-up = Factory Default Mode. This temporarily sets the unit to the defaults described in this manual (IP Address 192.168.0.200, HTTPS etc.). The watchdog LED **flashes green** and the status LED is **red**. The user can then access the webpage at the default IP address (https://192.168.0.200) make any changes to the configuration and save them. If the user cycles power before saving any settings then the unit reverts back to the previously saved settings.

25 CONTACT



CONTACT
Head Office for MTL product line,
Eaton Electric Limited,
Great Marlings,
Butterfield,
Luton,
Bedfordshire,
LU2 8DL.
Tel: +44 (0)1582 723633 Fax: +44 (0)1582 422283
http://www.mtl-inst.com/contact

CONTACT
Controlled Systems Ltd,
Unit 1,
Ryder Close,
Swadlincote,
Derbyshire,
DE11 9EU.
Tel: +44 (0) 1283 216231 Fax: +44 (0) 1283 552937

This page list the contacts for support and offers a quick way to access our websites.

26 APPENDIX A END USER LICENSE AGREEMENT

Eaton

END-USER LICENSE AGREEMENT

Eaton 9471 Instrinsically Safe Gigabit Ethernet 4 Port Serial Gateway

Last Revised Date: 21July 2020

Eaton Corporation owns and operates the Eaton 9471 Instrinsically Safe Gigabit Ethernet 4 Port Serial Gateway software “Product Software”. The following Eaton 9471 Instrinsically Safe Gigabit Ethernet 4 Port Serial Gateway software End-User License Agreement “Agreement” governs the use of this Product Software. Other sites, content or online services owned or controlled by Eaton have their own terms of use/ end-user license agreement and should be reviewed. Eaton licenses the use of the Product Software to you subject to the terms of this Agreement.

IMPORTANT, PLEASE READ THIS AGREEMENT BEFORE REGISTERING, ACCESSING OR USING THE PRODUCT SOFTWARE. THIS AGREEMENT IS A BINDING LEGAL CONTRACT BETWEEN YOU AND/OR THE ENTITY YOU REPRESENT (“AUTHORIZED PARTY”) AND EATON, TOGETHER WITH ITS AFFILIATES ENTITIES AND SUBSIDIARIES. BY CLICKING THE “ACCEPT” BUTTON BELOW, OR BY ACCESSING OR USING THE PRODUCT SOFTWARE, AUTHORIZED PARTY IS AGREEING TO BE BOUND BY THIS AGREEMENT. AUTHORIZED PARTY’S RIGHT TO USE THE PRODUCT SOFTWARE IS LIMITED BY APPLICABLE LAWS IN ITS JURISDICTION.

IF AUTHORIZED PARTY DOES NOT ACCEPT THE TERMS IN THIS AGREEMENT, DO NOT CLICK THE “I HAVE READ AND UNDERSTAND THIS AGREEMENT” CHECKBOX AND THE “CONTINUE” BUTTON AND DO NOT REGISTER, ACCESS OR USE THE PRODUCT SOFTWARE IN ANY WAY.

Description of the Product Software. Configuration Utility Software for Eaton 9471 Instrinsically Safe Gigabit Ethernet 4 Port Serial Gateway The software can be accessed through a web Graphical User Interface (GUI) through an IP Address by physically connecting to the switch.

License. Subject to the terms and conditions of this Agreement, Eaton hereby grants to Authorized Party a limited, non-transferable, non-sublicensable, non-assignable, non-exclusive and revocable license to access and use the Product Software in conjunction with the operation of Eaton products to which the Product Software pertains or other products as described by Eaton in any user guides and manuals **(e.g., INM9471-ET(G)** for access to and use of the Product Software solely for Authorized Party’s own internal business purpose use and only in a manner that is consistent with the terms of this Agreement. In the event Eaton requires Authorized Party to register as an end-user, such license is valid only if the registration is complete and accurate.

Restrictions. This Agreement does not allow Authorized Party to copy, decompile, reverse engineer, disassemble, attempt to derive the source code of, modify, or create derivative works of the Product Software, or any updates or upgrades, or any part thereof. Authorized Party may not use any part of the Product Software to establish any independent data files, databases, compendiums or any other reference materials. Any attempt to do so is a violation of the rights of Eaton. If Authorized Party breaches these restrictions, Authorized Party may be subject to prosecution and damages. The Product Software is intended for adults and by accessing the Product Software, Authorized Party represents that they are of or exceeding the minimum legal age threshold of an adult.

Prohibited Conduct. In connection with the Authorized Party's access to and/or use of the Product Software, the Authorized Party agrees not to:

- Violate any laws or regulations.

- Upload/post anything that imposes an unreasonable or disproportionately large strain on Eaton's network or computer infrastructure.

- Engage in any behavior that is designed to hack into or gain unauthorized access to protected areas of the Product Software and/or Eaton's computers, servers or networks, and/or any computers or systems used by other users of the Product Software.

- Upload/post anything that could destroy, damage, or impair any portion of the Product Software or any computers, systems, hardware, or software used by Eaton or other users.

- Make unauthorized attempts to modify any information stored in the Product Software.

- Make attempts to defeat or circumvent security features, or to utilize the Product Software for any purpose other than its intended purposes.

- Upload/post any unsolicited or unauthorized advertising, promotional materials, spam emails, chain letters, pyramid schemes, or any other form of such solicitations.

- Use any automated technology such as a robot, spider, or scraper to access, scrape, or data mine the Product Software.

- Provide false or misleading information when signing up for a Product Software account or otherwise upload/post any false or misleading information or content through the Product Software.

The previous list of prohibitions is not exclusive or exhaustive. Eaton reserves the right to terminate the Authorized Party's access to the Product Services for any violation of this Agreement.

By accepting this Agreement, the Authorized Party waives and holds harmless Eaton from any claims resulting from any action taken by Eaton during or as a result of Eaton's investigation and/or from any actions taken as a consequence of investigations by either Eaton or law enforcement related to the Authorized Party's use of the Product Services.

Updates and Events outside of Eaton's control. Eaton may update or upgrade the Product Software at any time. Certain functions of the Product Software may be modified or discontinued as a result of any such updates or upgrades. If Eaton elects to provide maintenance or support of any kind, Eaton may terminate that maintenance or support at any time without notice to Authorized Party. The terms and conditions of this Agreement shall govern any upgrades or updates provided by Eaton that replace and/or supplement the original Product Software, unless such upgrade is accompanied by, or references, a separate license agreement in which case the terms of that license agreement shall govern.

Eaton will not be liable or responsible for any failure to perform, or delay in performance of, any of Eaton's obligations under this Agreement that is caused by any act or event beyond Eaton's reasonable control, including but not limited to, acts of God, failure of public or private telecommunications networks, changes in law or regulation, or any other force majeure event or circumstance, whether or not foreseeable.

Proprietary Rights. Eaton owns all rights, title and interest in, and to, without limitation, all intellectual and proprietary rights of any and all featured products or parts, including, but not limited to, any models, data, or formulas exhibited in the Product Software excluding any Open Source Software as defined below that may be contained herein, and, except for the limited license granted to Authorized Party herein, nothing in this Agreement shall be construed to restrict, transfer, convey, encumber, alter, impair or otherwise adversely affect Eaton's ownership or proprietary rights therein or any other of Eaton's information, processes, methodologies, products, goods, services, or materials, tangible or intangible, in any form and in any medium. Authorized Party may not copy, decompile, or reverse engineer any of the products featured in the Product Software.

Open Source and Third-Party Libraries. Certain items of software included with the Product Software may be subject to "open source" or "free software" licenses ("Open Source Software") or third-party proprietary software. Some Open Source Software or proprietary software (collectively, "Third-Party Software") is owned by third parties. Eaton provides the Third-Party Software to You "AS IS" without any indemnities or warranties of any kind. The Open Source Software is not subject to the terms and conditions of this Agreement. Instead, each item of Open Source Software is licensed under the terms of the end user license that accompanies such Open Source Software. Nothing in this Agreement limits Authorized Party's rights under, or grants Authorized Party rights that supersede, the terms and conditions of any applicable end user license for the Open Source Software. To the extent there are any conflicts between the terms of this Agreement and any Open Source Software license corresponding to the open source component(s) of the software included with the Product Software or additional obligations by such Open Source Software license that are not set forth in this Agreement, the terms of the Open Source Software license will control.

Support Services. Eaton or its suppliers and distributors may provide Authorized Party with support services related to the Product Software (**"Support Services"**). Use of Support Services is governed by the policies and programs described in the Documentation, and/or other Eaton-provided materials. Any supplemental materials provided to Authorized Party as part of the Support Services shall be considered part of the Product Software, as applicable, and subject to the terms and conditions of this Agreement.

No Warranty. TO THE EXTENT PERMITTED BY LAW, AUTHORIZED PARTY EXPRESSLY ACKNOWLEDGES AND AGREES THAT USE OF THE PRODUCT SOFTWARE IS AT AUTHORIZED PARTY'S SOLE RISK AND THAT THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY AND EFFORT OF THE PRODUCT SOFTWARE IS WITH AUTHORIZED PARTY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT SOFTWARE AND ANY SERVICES PERFORMED OR PROVIDED BY OR IN CONNECTION WITH THE PRODUCT SOFTWARE ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS, WITH ALL BUGS AND FAULTS AND WITHOUT WARRANTY OF ANY KIND. EATON, ITS AFFILIATES, SUBSIDIARIES, AND AUTHORIZED REPRESENTATIVES HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS OF ANY KIND WITH RESPECT TO THE PRODUCT SOFTWARE AND ANY SERVICES, EITHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING, BUT WITHOUT LIMITATION, ANY IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, OF SATISFACTORY QUALITY, OF FITNESS FOR A PARTICULAR PURPOSE, SECURITY, COMPLETENESS, TIMELINESS, ACCURACY, QUIET ENJOYMENT, TITLE, FREEDOM FROM COMPUTER VIRUSES, AND OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS. NEITHER EATON, NOR ANY OF ITS AFFILIATES OR SUBSIDIARIES, WARRANT THAT THE FUNCTIONS OR SERVICES CONTAINED IN, ACCESSED FROM, PERFORMED BY, DISPLAYED ON, LINKED TO/FROM, OR PROVIDED BY, THE PRODUCT SOFTWARE WILL MEET AUTHORIZED PARTY'S REQUIREMENTS, THAT THE OPERATION OF THE PRODUCT SOFTWARE OR SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, TIMELY, SECURE, OR THAT DEFECTS OR ERRORS IN THE PRODUCT SOFTWARE OR SERVICES WILL BE CORRECTED, OR THAT THE PRODUCT SOFTWARE WILL BE COMPATIBLE WITH ANY

SYSTEM, OR THAT THE PRODUCT SOFTWARE WILL BE FREE FROM WORMS, VIRUSES, MALWARE, TROJAN HORSES, OR OTHER HARMFUL OR DISABLING COMPONENTS. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY EATON, ITS AFFILIATES, SUBSIDIARIES, OR ANY OF THEIR RESPECTIVE AUTHORIZED REPRESENTATIVES SHALL CREATE A WARRANTY. AUTHORIZED PARTY ASSUMES THE ENTIRE COST OF ANY AND ALL NECESSARY REPAIRS IN THE EVENT AUTHORIZED PARTY EXPERIENCES ANY LOSS OR DAMAGE ARISING FROM THE USE OF THE PRODUCT SOFTWARE OR ANY RELATED GOODS OR SERVICES. IF AUTHORIZED PARTY IS DISSATISFIED WITH THIS AGREEMENT, THE PRODUCT SOFTWARE AND/OR ANY RELATED GOODS OR SERVICES, AUTHORIZED PARTY'S SOLE AND EXCLUSIVE REMEDY IS TO DISCONTINUE USING THE PRODUCT SOFTWARE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON APPLICABLE STATUTORY RIGHTS OF A CONSUMER, SO THE ABOVE EXCLUSION AND LIMITATIONS MAY NOT APPLY TO AUTHORIZED PARTY.

Limitation of Liability. TO THE EXTENT PERMITTED BY LAW, IN NO EVENT WILL EATON OR ITS OFFICERS, DIRECTORS, EMPLOYEES, AFFILIATES, SUBSIDIARIES AGENTS, LICENSORS, AUTHORIZED REPRESENTATIVES, ATTORNEYS AND/OR BUSINESS PARTNERS, NOR ANY PARTY INVOLVED IN THE CREATION, PRODUCTION, OR TRANSMISSION OF THE PRODUCT SOFTWARE, BE LIABLE FOR ANY LOSS OR DAMAGE OF ANY KIND WHATSOEVER, INCLUDING, BUT NOT LIMITED TO, ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, STATUTORY, PUNITIVE, ACTUAL, LIQUIDATED, EXEMPLARY, CONSEQUENTIAL OR OTHER DAMAGES, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF REVENUE, LOSS OF DATA, LOSS OF PRODUCTION, LOSS OF GOODWILL, INTELLECTUAL PROPERTY INFRINGEMENT, BUSINESS INTERRUPTION OR LOSS OF USE, PAIN AND SUFFERING, EMOTIONAL DISTRESS OR SIMILAR DAMAGES, OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO AUTHORIZED PARTY'S USE OR INABILITY TO USE THE PRODUCT SOFTWARE, HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT OR OTHERWISE) AND EVEN IF EATON OR THE AFOREMENTIONED PARTIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE EXTENT PERMITTED BY LAW, IN NO EVENT WILL THE COLLECTIVE LIABILITY OF EATON OR THE AFOREMENTIONED PARTIES, REGARDLESS OF THE TYPE OF ACTION, WHETHER IN CONTRACT, TORT, OR OTHERWISE, EXCEED THE GREATER OF $100.00 OR THE AMOUNT THE AUTHORIZED PARTY PAID TO EATON AND/OR THE AFOREMENTIONED PARTIES FOR THE APPLICABLE GOODS OR SERVICES OUT OF WHICH THE LIABILITY AROSE.

Indemnification. Authorized Party agrees to indemnify, defend, and hold harmless Eaton, including its officers, directors, employees, affiliates, subsidiaries, agents, licensors, authorized representatives, attorneys, business partners, and respective successors and assigns (**"Indemnified Parties"**) from and against any and all claims, demands, actions, liabilities, judgments, awards, losses, damages, costs and expenses (including reasonable attorneys' fees, costs of defense, and direct, indirect, punitive, special, individual, consequential, or exemplary damages), Eaton or any of the Indemnified Parties suffer in relation to, arising from, or from the purpose of avoiding, any claim or demand from a third party that relates to Authorized Party's: (a) breach or violation of this Agreement; (b) infringement, misappropriation or any violation of the rights of any other party from use of the Product Software in violation of this Agreement; (c) violation or non-compliance with any applicable law, rule, guidelines, acts, decrees, orders or regulations; (d) use, alteration or export of the Product Software (or any component thereof) in violation of this Agreement; and (e) the use of the Product Software by Authorized Party or any person using Authorized Party's account. Eaton and its affiliates reserve the right to assume the exclusive defense and control of any claims or actions subject to indemnification by Authorized Party and all negotiations for its settlement or compromise, and Authorized Party agrees to fully cooperate with Eaton and its affiliates upon request by Eaton.

Amendments to this Agreement. Eaton may modify, add or remove any of the terms and conditions of this Agreement at its sole discretion at any time without prior notice. Authorized Party will know when a change to this Agreement has been made, as there will be a change to the "Last Revised Date" noted at the start of this Agreement. Any changes will be effective from the Last Revised Date. Authorized Party's continued use of the Product Software after such modifications are made to the Agreement will mean that Authorized Party accepts and agrees to be bound by and comply with such changes and updates.

For Authorized Parties in California. In compliance with California Civil Code § 1789.3, an Authorized Party residing in California has the right to contact Eaton with any complaints or to seek additional information. Such Authorized Party may email Eaton at dataprotection@eaton.com or write to: Attn: Global Data Protection and Privacy Office, Eaton, 1000 Eaton Blvd., Cleveland, OH 44122.

If Authorized Parties in California have any questions or complaints about Eaton they may also contact: The Complaint Assistance Unit of the Division of Consumer Services of the California Department of Consumer Affairs through writing at 400 R Street, Suite 1080, Sacramento, CA 95814, or by telephone at (916) 445-1254 or (800) 952-5210. Hearing impaired persons may call (916) 928-1227 or (800) 326-2297 via TTY device.

Registration. To use the Product Software, Authorized Party must have a valid account with a username and password ("Credentials"). Authorized Party is responsible for maintaining the confidentiality of Authorized Party's username and passwords, and for ensuring that each password is only used by employees granted access to the Product Software on the Authorized Party's behalf. Authorized Party is liable for all transactions and other activities carried out under the Authorized Party's Credentials. Authorized Party agrees to promptly notify Eaton if any password is lost, stolen, disclosed to an unauthorized party, or otherwise may have been compromised. Authorized Party agrees to immediately notify Eaton at mailto:mtltechsupport@eaton.com of any unauthorized use of the Authorized Party's account or any other breach of security in relation to the Product Software known to the Authorized Party. Eaton shall have no liability for any loss or damage arising from the Authorized Party's failure to comply with these requirements. If Eaton suspends or terminates the Authorized Party's account under this Agreement, the Authorized Party acknowledges that all information and content associated with such account will no longer be available to the Authorized Party.

Confidential Information. All information provided in Product Software is Eaton's confidential information. The Authorized Party agrees that it shall not use or disclose Eaton's confidential information without the prior written consent of Eaton, except to share it with the Authorized Party's employees who have a need to know the information and are bound by a duty of confidentiality covering the information that is at least as restrictive as the obligations in this Agreement.

Except for personally identifiable information, the use and disclosure of which is addressed in the Privacy Policy for the Product Software, any and all information and content provided by the

Authorized Party to Eaton is provided on a non-proprietary and non-confidential basis, regardless of whether the information or content is marked or otherwise identified as confidential or proprietary. The Authorized Party agrees that Eaton has a royalty-free, perpetual, irrevocable, worldwide, non-exclusive right and license to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, perform, and display any provided information or content for the purpose of operating and/or marketing the Services or any related services rendered by Eaton. This license includes any right of publicity rights that may be present in the provided information or content.

Intellectual Property. Other than the exceptions referenced in this Agreement and noted elsewhere, all content provided through the Product Software is the sole and exclusive property of Eaton including, but not limited to, all trade names, service marks, trademarks, logos, text, data, documents, messages, pictures, images, video, audio, graphics, links, software and its underlying code, domain names, or other electronic files (referred to hereafter as "**Eaton Content**").

Certain elements of the Product Software including, but not limited to, text, graphics, photos, images, video, audio, color selections, organization and layout, are copyright protected under United States and international copyright laws. Any Eaton Content protected by intellectual property laws may not be copied, republished, posted, modified, edited, transmitted, distributed, used to create derivative works of, or reverse engineered without Eaton's written permission. No information, data, documents, or records found through the Product Software shall be made available as part of a website, app or online location, whether by hyperlink, framing on the internet or otherwise, without the express written consent of Eaton.

The Authorized Party acknowledges that the Authorized Party has no right, title or interest in or to the Product Software and/or any Eaton Content. EATON and MTL947x are trade names and/or marks owned exclusively by Eaton. The Authorized Party shall not use any trade names or marks that are confusingly similar in Eaton's sole opinion without the prior written consent of Eaton, which may be withheld in its sole discretion. Nothing in this Agreement and nothing found through the Product Software shall be construed as a license to use any of Eaton's trademarks, patents, copyrights, or other intellectual property rights.

There may be other content located in the Product Software that is not owned by Eaton, and the Authorized Party should respect those property rights as well. All rights not expressly granted herein are reserved to Eaton.

Termination or Suspension. This Agreement is effective for an unlimited duration unless and until terminated as set forth herein. All rights under the license granted shall terminate automatically without notice from Eaton for failure to comply with any terms or conditions of this Agreement. Upon termination of this Agreement, the Authorized Party shall cease all use of the Product Software, and destroy all copies, full or partial, thereof. Any provision of this Agreement which by its nature must survive the termination of this Agreement in order to give effect to its meaning shall survive such termination.

Miscellaneous. If any provision hereof becomes or is declared by a court of competent jurisdiction to be illegal, unenforceable, or void, this Agreement will continue in full force and effect without said provision. The section titles in this Agreement are for convenience only and have no legal or contractual effect. No failure or delay by Eaton or its affiliates to exercise any right or enforce any obligation shall impair or be construed as a waiver or ongoing waiver of that or any other right or power. Waiving one breach will not be construed to waive any succeeding breach. All waivers must be in writing and signed by the party waiving rights. No provisions in Authorized Party's purchase orders, or in any other business forms employed by Authorized Party, will supersede the terms and conditions of this Agreement.

Export Rules and U.S. Government Restricted Rights. The Authorized Party agrees not to provide access to or use of the Product Software to any citizen of a country to which access or use thereof is barred, or to which exports or shipments are barred, or to anyone on the U.S. Treasury Department's list of Specially Designated National or the U.S. Department of Commerce Denied Person's List or Entity List or any other restricted parties lists by the United States government. Further, the Authorized Party will not shop, transfer or export the Product Software into any country or use the Product Software in any manner prohibited by the United States Export Administration Act or any other export laws, restrictions or regulations (collectively the "**Export Laws**"). In addition, if the Product Software is identified as export controlled items under the Export Laws, the Authorized Party represents and warrants that it is not a citizen of, or otherwise located within, an embargoed nation and that it is not otherwise prohibited under the Export Laws from receiving access to or using the Product Software. All rights to access and use of the Product Software are granted on condition that such rights are forfeited if the Authorized Party fails to comply with the terms of this Agreement.

If the Software is licensed to agencies of the U.S. Government, the Software is a "commercial item" as that term is defined at 48 C.F.R. § 2.101, consisting of "commercial computer software" and "commercial computer software documentation", as such terms are used in 48 C.F.R. § 12.212, and is provided to the U.S. Government only as a commercial end item. Consistent with 48 C.F.R. § 12.212 and 48 C.F.R. §§ 227.7202-1 through 227.7202-4, all U.S. Government End Users acquire the Software with only those rights set forth herein. Contractor/manufacturer is Eaton Corporation, 1000 Eaton Boulevard, Cleveland, Ohio 44122.

Compliance with License and Laws. The Authorized Party agrees to comply with all federal, state, local and foreign laws, regulations, rules and ordinances pertaining to the license granted under this Agreement. In the event that any part of this Agreement is determined to violate any applicable federal, state, local or foreign laws, rules or regulations, then the remaining provisions of this Agreement shall remain in full force and effect and shall be enforced to fullest extent permitted by law.

Governing Law and Interpretation. To the extent not prohibited by law, the Authorized Party agrees that this Agreement and all disputes, claims, actions, suits or other proceedings arising hereunder shall be governed by, and construed in accordance with, the substantive law of the State of Ohio applicable to contracts wholly made and to be performed within the State of Ohio, and to irrevocably submit to the sole and exclusive jurisdiction of the courts of Ohio or the Federal courts of the Northern District of Ohio, and to irrevocably consent to the exercise of personal jurisdiction by such courts and waive any right to plead, claim or allege that Ohio is an inconvenient forum.

Agreement. This Agreement constitutes the entire agreement regarding the use of the Product Software and supersedes any prior or contemporaneous understandings and agreements related to its subject matter.

Any questions regarding this Agreement should be directed to Eaton at:

Eaton
Attn: IP Law Group
1000 Eaton Boulevard
Mail Code 4N
Cleveland, OH 44122

Eaton
Attn: Global Data Protection and Privacy Office
1000 Eaton Boulevard
Cleveland, OH 44122
Email: dataprotection@eaton.com

27 APPENDIX B CYBERSECURITY GUIDELINES

30/01/20

The 9471 has been designed with cybersecurity as an important consideration. A number of features are offered in the product to address cybersecurity risks. These Cybersecurity Recommendations provide information to help users to deploy and maintain the product in a manner that minimizes the cybersecurity risks. These Cybersecurity Recommendations are not intended to provide a comprehensive guide to cybersecurity, but rather to complement customers' existing cybersecurity programs.

Eaton is committed to minimizing the cybersecurity risk in its products and deploying cybersecurity best practices in its products and solutions, making them more secure, reliable and competitive for customers.
The following Eaton whitepapers are available for more information on general cybersecurity best practices and guidelines:

Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):
http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/ content/pct_1603172.pdf

Cybersecurity Best Practices Checklist Reminder (WP910003EN):
http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf

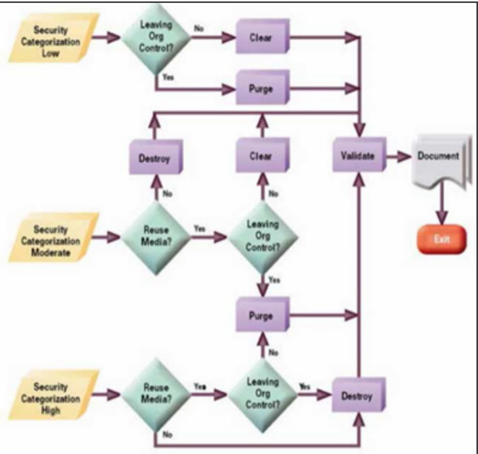
Category	Description
Asset Management	Keeping track of software and hardware assets in your environment is a pre-requisite for effectively managing cybersecurity. Eaton recommends that you maintain an asset inventory that uniquely identifies each important component. To facilitate this, The 9471 unit supports the following identifying information: <Include for hardware>- manufacturer, type, serial number, f/w version number, and location. <Include for software>- publisher, name, version, and version date.
Risk Assessment	Eaton recommends conducting a risk assessment to identify and assess reasonably foreseeable internal and external risks to the confidentiality, availability and integrity of the system | device and its environment. This exercise should be conducted in accordance with applicable technical and regulatory frameworks such as IEC 62443 and NERC-CIP. The risk assessment should be repeated periodically.
Physical Security	An attacker with unauthorized physical access can cause serious disruption to device functionality. Additionally, Industrial Control Protocols don't offer cryptographic protections, making ICS and SCADA communications especially vulnerable to threats to their confidentiality. Physical security is an important layer of defence in such cases The 9471 unit is designed to be deployed and operated in a physically secure location. Following are some best practices that Eaton recommends to physically secure your device: • Secure the facility and equipment rooms or closets with access control mechanisms such as • locks, entry card readers, guards, man traps, CCTV, etc. as appropriate. • Restrict physical access to cabinets and/or enclosures containing The 9471 unit and the associated system. Monitor and log the access at all times. • Physical access to the telecommunication lines and network cabling should be restricted to protect against attempts to intercept or sabotage communications • The 9471 unit supports the following physical access ports. • RJ45 Access to these ports should be restricted.

Category	Description
COTS Platform Security	Eaton recommends that customers harden third-party commercial off-the-shelf (COTS) operating systems or plat- forms that are used to run Eaton applications / products (e.g., third party hardware, operating systems and hyper- visors, such as those made available by Dell, Microsoft, VMware, Cisco, etc.).
	• Eaton recommends that customers refer to the COTS vendor’s documentation for guidance on how to harden these components. • Vendor-neutral guidance is made available by the Center for Internet Security https://www.cisecurity.org/ Irrespective of the platform, customers should consider the following best practices: • Install all security updates made available by the COTS manufacturer. • Change default credentials upon first login. • Disable or lock unused built-in accounts. • Limit use of privileged generic accounts (e.g., disable interactive login). • Change default SNMP community strings. • Restrict SNMP access using access control lists. • Disable unneeded ports & services.
Account Management	Logical access to the system | device should be restricted to legitimate users, who should be assigned only the privileges necessary to complete their job roles/functions. Some of the following best practices may need to be implemented by incorporating them into the organization’s written policies: Ensure default credentials are changed upon first login. The 9471 unit should not be deployed in production environments with default credentials, as default credentials are publicly known. No account sharing – Each user should be provisioned a unique account instead of sharing accounts and passwords. Security monitoring/ logging features in the product are designed based on each user having a unique account. Allowing users to share credentials weakens security. Restrict administrative privileges- Attackers seek to gain control of legitimate credentials, especially those for highly privileged accounts. Administrative privileges should be assigned only to accounts specifically designated for administrative duties and not for regular use.

Category	Description
Account Management (continued)	• Leverage the roles / access privileges to provide tiered access to the users as per the business /operational need. Follow the principle of least privilege (allocate the minimum authority level and access to system resources required for the role). • Perform periodic account maintenance (remove unused accounts). • Ensure password length, complexity and expiration requirements are appropriately set, particularly for all administrative accounts (e.g., minimum 10 characters, mix of upper- and lower-case and special characters, and expire every 90 days, or otherwise in accordance with your organization's policies). • Enforce session time-out after a period of inactivity.
Time Synchronization	Many operations in power grids and IT networks heavily depend on precise timing information. • Ensure the system clock is synchronized an authoritative time source (using manual configuration, NTP, SNTP, or IEEE 1588). Please refer to section 9.7.4 of this manual
Network Security	The 9471 unit supports network communication with other devices in the environment. This capability can present risks if it's not configured securely. Following are Eaton recommended best practices to help secure the network. Additional information about various network protection strategies is available in *Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1].* Eaton recommends segmentation of networks into logical enclaves, denying traffic between segments except that which is specifically allowed, and restricting communication to host-to-host paths (for example, using router ACLs and firewall rules). This helps to protect sensitive information and critical services and creates additional barriers in the event of a network perimeter breach. At a minimum, a utility Industrial Control Systems network should be segmented into a three-tiered architecture (as recommended by NIST SP 800-82[R3]) for better security control. Eaton recommends opening only those ports that are required for operations and protect the network communication using network protection systems like firewalls and intrusion detection systems / intrusion prevention systems. Use the information below to configure your firewall rules to allow access needed for The 9471 unit to operate smoothly The default ports used on The 9471 unit are:= 80 Web Port (HTTP) 443 Secure Web Port(HTTPS)

Category	Description
Remote Access	Remote access to devices/systems creates another entry point into the network. Strict management and validation of termination of such access is vital for maintaining control over overall ICS security. The 9471 unit requires additional hardware to allow Remote Access. This hardware will need securing correctly to ensure security
Logging and Event Management	• Eaton recommends logging all relevant system and application events, including all administrative and maintenance activities. • Logs should be protected from tampering and other risks to their integrity (for example, by restricting permissions to access and modify logs, transmitting logs to a security information and event management system, etc.). • Ensure that logs are retained for a reasonable and appropriate length of time. • Review the logs regularly. The frequency of review should be reasonable, taking into account the sensitivity and criticality of the system | device and any data it processes.
Vulnerability Scanning	Any known critical or high severity vulnerabilities on third party component/libraries used to run software /applications should be remediated before putting the device | system into production. • Eaton recommends running a vulnerability scan to identify known vulnerabilities for software used with the product. For COTS components (e.g., applications running on Windows), vulnerabilities can be tracked on the National Vulnerability Database (NVD), available at https://nvd.nist.gov/. • Keep software updated by monitoring security patches made available by COTS vendors and installing them as soon as possible. *Note: Many compliance frameworks and security best practices require a monthly vulnerability review. For many non-COTS products vulnerabilities will be communicated directly through the vendor site.*
Malware Defenses	Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.

Category	Description
Secure Maintenance	Best Practices Update device firmware prior to putting the device into production. Thereafter, apply firmware updates and soft- ware patches regularly. Eaton publishes patches and updates for its products to protect them against vulnerabilities that are discovered. Eaton encourages customers to maintain a consistent process to promptly monitor for and install new firmware updates. Please check Eaton's cybersecurity website for information bulletins about available firmware and software updates. New firmware for The 9471 unit will be available on the products page on the Eaton website
Business Continuity / Cybersecurity Disaster Recovery	Plan for Business Continuity/Cybersecurity Disaster Recovery Eaton recommends incorporating The 9471 unit into the organization's business continuity and disaster recovery plans. Organizations should establish a Business Continuity Plan and a Disaster Recovery Plan and should periodically review and, where possible, exercise these plans. As part of the plan, important system | device data should be backed up and securely stored, including: Updated firmware for The 9471 unit. Make it a part of standard operating procedure to update the backup copy as soon as the latest firmware is updated. The current configuration. Documentation of the current permissions / access controls, if not backed up as part of the configuration. The following section describes the details of failures states and backup functions:
Sensitive Information Disclosure	Eaton recommends that sensitive information (i.e. connectivity, log data, personal information) that may be stored by The 9471 unit be adequately protected through the deployment of organizational security practices.

Category	Description
Decommissioning or Zeroisation	It is a best practice to purge data before disposing of any device containing data. Guidelines for decommissioning are provided in NIST SP 800-88. Eaton recommends that products containing embedded flash memory be securely destroyed to ensure data is unrecoverable.  Security Categorization Low Leaving Org Control? No Yes Clear Purge Destroy Clear Validate Document No No Exit Security Categorization Moderate Reuse Media? Yes Leaving Org Control? Yes Purge No Security Categorization High Reuse Media? Yes Leaving Org Control? Yes Destroy No Figure 4-1: Sanitization and Disposition Decision Flow *from NIST SP800-88* • **Embedded Flash Memory on Boards and Devices** Eaton recommends the following methods for disposing of motherboards, peripheral cards such as network adapters, or any other adapter containing non-volatile flash memory. • **Clear:** If supported by the device, reset the state to original factory settings. • **Purge:** If the flash memory can be easily identified and removed from the board, the flash memory may be destroyed independently of the board that contained the flash memory. Otherwise, the whole board should be destroyed. • **Destroy:** Shred, disintegrate, pulverize, or Incinerate by burning the device in a licensed incinerator.

28 APPENDIX C CYBERSECURITY REFERENCES

- **[R1] Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):**
  http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf
- **[R2] Cybersecurity Best Practices Checklist Reminder (WP910003EN):**
  http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf
- **[R3] NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015:**
  https://ics-cert.us-cert.gov/Standards-and-References
- **[R4] National Institute of Technology (NIST) Interagency "Guidelines on Firewalls and Firewall Policy, NIST special Publication 800-41", October 2009:**
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf
- **[R5] NIST SP 800-88, Guidelines for Media Sanitization, September 2006:**
  http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819

This page is left intentionally blank

This page is left intentionally blank

Any questions regarding this Agreement should be directed to Eaton at:

Eaton
Attn: IP Law Group
1000 Eaton Boulevard
Mail Code 4N
Cleveland, OH 44122

Eaton
Attn: Global Data Protection and Privacy Office
1000 Eaton Boulevard
Cleveland, OH 44122
Email: dataprotection@eaton.com

CROUSE-HINDS
SERIES

AUSTRALIA
Eaton Electrical (Australia) Pty Ltd,
10 Kent Road, Mascot, New South Wales, 2020, Australia

Tel: +61 1300 308 374 Fax: +61 1300 308 463
E-mail: mtlsalesanz@eaton.com

BeNeLux
MTL Instruments BV
Ambacht 6, 5301 KW Zaltbommel
The Netherlands

Tel: +31 (0) 418 570290 Fax: +31 (0) 418 541044
E-mail: mtl.benelux@eaton.com

CHINA
Cooper Electric (Shanghai) Co. Ltd
955 Shengli Road, Heqing Industrial Park
Pudong New Area, Shanghai 201201

Tel: +86 21 2899 3817 Fax: +86 21 2899 3992
E-mail: mtl-cn@eaton.com

FRANCE
MTL Instruments sarl,
7 rue des Rosiéristes, 69410 Champagne au Mont d'Or
France

Tel: +33 (0)4 37 46 16 53 Fax: +33 (0)4 37 46 17 20
E-mail: mtlfrance@eaton.com

GERMANY
MTL Instruments GmbH,
Heinrich-Hertz-Str. 12, 50170 Kerpen, Germany

Tel: +49 (0)22 73 98 12- 0 Fax: +49 (0)22 73 98 12- 2 00
E-mail: csckerpen@eaton.com

INDIA
MTL India,
No.36, Nehru Street, Off Old Mahabalipuram Road
Sholinganallur, Chennai- 600 119, India

Tel: +91 (0) 44 24501660 /24501857 Fax: +91 (0) 44 24501463
E-mail: mtlindiasales@eaton.com

ITALY
MTL Italia srl,
Via San Bovio, 3, 20090 Segrate, Milano, Italy

Tel: +39 02 959501 Fax: +39 02 95950759
E-mail: chmninfo@eaton.com

JAPAN
Cooper Industries Japan K.K.
MT Building 3F, 2-7-5 Shiba Diamon, Minato-ku
Tokyo, Japan 102-0012

Tel: +81 (0)3 6430 3128 Fax:+81 (0)3 6430 3129
E-mail: mtl-jp@eaton.com

NORWAY
Norex AS
Fekjan 7c, Postboks 147,
N-1378 Nesbru, Norway

Tel: +47 66 77 43 80 Fax: +47 66 84 55 33
E-mail: info@norex.no

RUSSIA
Cooper Industries Russia LLC
Elektrozavodskaya Str 33
Building 4
Moscow 107076, Russia

Tel: +7 (495) 981 3770 Fax: +7 (495) 981 3771
E-mail: mtlrussia@eaton.com

SINGAPORE
Eaton Electric (Singapore) Pte Ltd
100G Pasir Panjang Road
Interlocal Centre
#07-08 Singapore 118523
#02-09 to #02-12 (Warehouse and Workshop)

Tel: +65 6 645 9888 ext 9864/9865
Fax: 65 6 645 9811
E-mail: sales.mtlsing@eaton.com

SOUTH KOREA
Cooper Crouse-Hinds Korea
7F. Parkland Building 237-11 Nonhyun-dong Gangnam-gu,
Seoul 135-546, South Korea.

Tel: +82 6380 4805 Fax: +82 6380 4839
E-mail: mtl-korea@eaton.com

UNITED ARAB EMIRATES
Cooper Industries/Eaton Corporation
Office 205/206, 2nd Floor SJ Towers, off. Old Airport Road,
Abu Dhabi, United Arab Emirates

Tel: +971 2 44 66 840 Fax: +971 2 44 66 841
E-mail: mtlgulf@eaton.com

UNITED KINGDOM
Eaton Electric Limited,
Great Marlings, Butterfield, Luton
Beds LU2 8DL

Tel: +44 (0)1582 723633 Fax: +44 (0)1582 422283
E-mail: mtlenquiry@eaton.com

AMERICAS
Cooper Crouse-Hinds MTL Inc.
3413 N. Sam Houston Parkway W.
Suite 200, Houston TX 77086, USA

Tel: +1 800-835-7075 Fax: +1 866-298-2468
E-mail: mtl-us-info@eaton.com

EATON
Powering Business Worldwide

Eaton Electric Limited,
Great Marlings, Butterfield, Luton
Beds, LU2 8DL, UK.
Tel: + 44 (0)1582 723633 Fax: + 44 (0)1582 422283
E-mail: mtlenquiry@eaton.com
www.mtl-inst.com

Publication No. INM 9471-ET(G) Rev 2 270521
May 2021

EUROPE (EMEA):
+44 (0)1582 723633
mtlenquiry@eaton.com

THE AMERICAS:
+1 800 835 7075
mtl-us-info@eaton.com

ASIA-PACIFIC:
+65 6 645 9888
sales.mtlsing@eaton.com

The given data is only intended as a product description and should not be regarded as a legal warranty of properties or guarantee. In the interest of further technical developments, we reserve the right to make design changes.