

ioPAC 6500 Series User Manual

Version 1.1, October 2025

www.moxa.com/products



© 2025 Moxa Inc. All rights reserved.

ioPAC 6500 Series User Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

© 2025 Moxa Inc. All rights reserved.

Trademarks

The MOXA logo is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

- Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.
- Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.
- Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.
- This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. About This Manual	5
Revision History	5
Relevant Models	5
Package Contents	6
Usage Scenarios	6
Hardware and Software Requirements	7
Safety Precautions	7
Additional Resources	8
2. Product Overview	9
Technical Data	9
Physical Dimensions	22
LED Definition	31
I/O Pin Definitions	43
3. Hardware Installation.....	46
Mounting the Unit	46
Horizontal Installation	47
Installing the System on the DIN Rail	48
Unmounting the System from a DIN Rail	50
Grounding the System.....	52
Wiring System and Field Power.....	53
System Power.....	53
Field Power.....	53
Wiring Ethernet Ports	54
Wiring Serial Port(s).....	54
Wiring the Fiber Port(s)	54
100/1000BaseSFP (mini-GBIC) Fiber Port.....	54
Connecting Expansion Module	55
Wiring I/O Channels.....	57
Inserting the microSD™ Card	61
Powering on the Unit.....	62
Mode Switch	62
Reset Button: Reset Origin Device	63
4. Software Configuration.....	64
Connecting the Web Interface	64
Dashboard.....	65
System Configuration	66
Maintenance	72
Diagnostic	74
Certificate	77
Security	79
Logging in by Console Port.....	87
5. IINxpress	90
Menu and Toolbar	91
Build New Project	93
ioPAC 6500 Project	93
Network Scan	95
Empty Project	97
ioPAC 6500 Configuration	97
Home	98
System	110
Diagnostic	113
Log Manager.....	114
Account Manager.....	115
Firmware Update.....	118
Service Settings	119
System Status	133
Library Manager	133
POU	134

GVL	136
6. Switch Module Configuration	138
About this Chapter	138
Meanings of the Symbols in the Web Interface Configurations.....	138
Configuration Reminders	140
Getting Started	141
Log in by Web Interface	141
Log In by RS-232 Console	143
Log In by Telnet.....	145
Web Interface Configuration	147
Device Summary.....	148
System	152
Port	185
Layer 2 Switching.....	193
Network Redundancy	219
Management.....	238
Security	244
Diagnostics.....	280
Industrial Applications.....	302
Maintenance and Tool	307
A. Activate and Transfer the IINxpress.....	313
Activate the IINxpress.....	313
Transfer the Activation Code Between IINxpress.....	315
B. Account Privileges List of 65M-5011M (Managed Switch Module)	317
Account Privileges List.....	317
C. Event Log Description of 65M-5011M (Managed Switch Module).....	319
Event Log Description	319
D. SNMP MIB File of 65M-5011M (Managed Switch Module)	322
Standard MIB Installation Order	322
MIB Tree	323
E. Security Guidelines of 65M-5011M (Managed Switch Module).....	324
Installation	324
Physical Installation	324
Account Management.....	324
Vulnerable Network Ports	325
Operation	325
Maintenance	326
Decommission	327
F. SFP Module List of 65M-5011M (Managed Switch Module)	328

1. About This Manual

In this chapter, we explain the scope of and how to use this document.

Revision History

Version	Change	Date
v1.0	First release	2024-11-27
v1.1	Add 5290, 3800H, 5801. Updating Services, Software Configuration	2025-08-01

Relevant Models

This document only applies to the models listed below.

Model Name	Description
65M-CPU14-IEC-CT-T	Control CPU Module with IEC61131 programming, 3-in-1 serial port x 2, 10/100/1000 Ethernet port x 2
65M-PW0075-CT-T	Power module, 24 VDC, 75 W
65M-5011M-CT-T	Layer 2 managed Ethernet switch module 100/1000 Fiber x 2 + 10/100/1000 RJ45 x 8
65M-5290-CT-T	Expansion module, RJ45 x 2, SFP x 2, Combo Port
65M-1900-CT-T	32 DI module, 24 VDC, with 8CH/10 KHz counter mode
65M-2901-CT-T	32 DO module, 24 VDC, with 8CH pulse-out mode
65M-3600-CT-T	16 AI modules 0-20 mA/4-20 mA
65M-3610-CT-T	16 AI modules 1 to 5 VDC/0 to 10 VDC/-10 to 10 V
65M-3800H-CT-T	8 AI module 4-20 mA with HART
65M-4820-CT-T	8 AO group isolation modules 4-20 mA/1 to 5 VDC
65M-5801-CT-T	8 serial module RS232/422/485-2w
65M-BMPW01-CT-T	Power module backplane 1 slot
65M-BMPW02-CT-T	Power module backplane 2 slots
65M-BMCM01-CT-T	Communication or networking module backplane 1 slot
65M-BMCM02-CT-T	Communication or networking module backplane 2 slots
65M-BMCP01-CT-T	CPU module backplane 1 slot
65M-BMCP02-CT-T	CPU module backplane 2 slots
65M-BMIO02-CT-T	I/O module backplane 2 slots
65M-BMIO04-CT-T	I/O module backplane 4 slots
65M-TB-1900-CT-T	Terminal block for 32 DI modules, 24 VDC, with 8CH/10 KHz counter mode
65M-TB-2901-CT-T	Terminal block for 32 DO modules, 24 VDC, with 8CH pulse-out mode
65M-TB-3600-CT-T	Terminal block for 16 AI modules 4-20 mA
65M-TB-3610-CT-T	Terminal block for 16 AI modules 1 to 5 VDC/0 to 10 VDC
65M-TB-4820-CT-T	Terminal block for 8 AO group isolation modules 4-20 mA/1 to 5 VDC
65M-TB-3800H-CT-T	Terminal block for 8 AI module 4-20 mA with HART
65M-TB-5801-CT-T	Terminal block for 8 serial modules

Package Contents

The following items are included in the product package.

- The 65M module device
- Quick installation guide (Printed)
- Pinout card (65M-TB Series only)
- Warranty card

Usage Scenarios

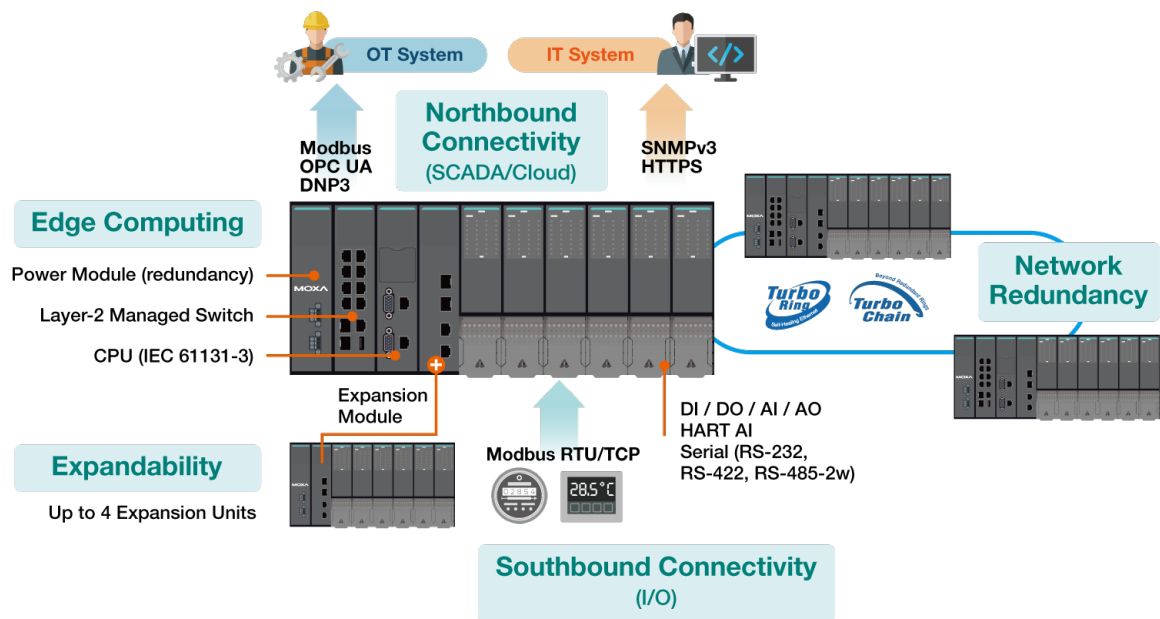
The ioPAC 6500 Series is designed with 6C core competencies.

- Control: the ability to perform precision control
- Communication: the ability to support protocols to connect to other devices or systems
- Computing: the ability to execute the program that is not related to precision control
- Connectivity: the wired, wireless interface, which is supported by the ioPAC 6500 Series
- Cloud: the ability of cloud connectivity and cloud edge computing
- Cybersecurity: the ability to protect the users' device, information, and data

The major functions of the ioPAC 6500 Series are categorized into 5 groups.

- Southbound: the I/O and the protocols to collect the data from other devices
- Northbound: the protocols to deliver the data to other systems
- Computing: the ability to process the data and event
- Networking: the ability to enhance the network reliability
- Expandability: the ability to have more I/O points





Hardware and Software Requirements

You will need the following hardware and software to use the ioThinX 6500 Series.

- A power source that provides 12 to 48 VDC, and power wires
- A PC running a Windows OS with Chrome installed and an Ethernet cable
- IINxpress software utility (Refer to the IINxpress chapter for more details.)

Safety Precautions

Observe the following safety precautions when installing and using the ioPAC 6500 Series:



DANGER

Never work on the device while the power source is switched on. Disconnect all power sources to the device before performing installation, repair, or maintenance work.



DANGER

Disconnect the power when you want to remove or replace components or disconnect equipment unless the area is free of ignitable substances.

- If you connect or disconnect the Removable Terminal Block when field power is applied, an electrical arc can occur. This could cause an explosion when installed in hazardous locations. Ensure that power is removed, or the area is nonhazardous before installation.
- If you connect or disconnect wiring while the power is on, an electrical arc can occur. This could cause an explosion in hazardous environments. Ensure that power is removed, or the area is nonhazardous before installation.
- Do not disconnect the unit unless the power has been disconnected, or the area is nonhazardous. In a hazardous area, the unit must be powered down before removing it.



WARNING

This unit is sensitive to Electrostatic Discharge, which can cause internal damage and affect operations. Follow these guidelines when you handle this unit:

- Touch a grounded object to discharge potential static.
- Wear an approved grounding wristband.
- Do not touch connectors or pins on component boards.
- Do not touch circuit components inside the equipment.
- Use a static-safe workstation, if available.
- Store the device in static-safe packaging when not in use.



WARNING

Check the voltage supplied by the power source. Make sure the voltage provided by the power source matches the voltage required by the device.



WARNING

Check the voltage or current of the sensors or loads. Make sure the voltage and/or current shown on the sensors or loads correspond to the specifications of your 45M module before you connect the device.



WARNING

Connect your device to an earthed ground.



CAUTION

Do not use the device if the device is already damaged. Replace defective or damaged devices to ensure that your devices function properly.



CAUTION

Do not repair the device yourself. If your device needs to be repaired, return the device to Moxa's customer service department. Attempting to repair the device yourself could invalidate the device's warranty.

Additional Resources

Refer to the following documents for additional information.

- Datasheets for the following products:
 - ioPAC 6500 Series

2. Product Overview

In this chapter, we summarize each ioPAC 6500 Series device.

Technical Data

Common Specifications

System Performance

Maximum Unit(s): 1 (Control unit)

Maximum Expansion Unit (s): 4 (Expansion units)

Maximum Power backplane in control unit: 1 (1-slot or 2-slot)

Maximum CPU backplane in control unit: 1 (1-slot or 2-slot)

Maximum Communication backplane in control unit: 1 (1-slot or 2-slot)

Maximum I/O backplane in control unit: 2 (2-slot or 4-slot)

Physical Characteristics

Housing: Plastic

Mounting Options

DIN-rail Mounting: Default

Rack Mounting: Supported (with optional kit)

Environmental

Operating Temperature: -40 to 75°C (-40 to 167°F, airflow is required in an environment over 65°C)

Storage Temperature: -40 to 85°C (-40 to 185°F, package included)

Relative Humidity: 5 to 95% (non-condensing)

IP Protection: IP20

Operating Altitude: Up to 2000 meters

Standard and Certifications

EMC:

EN 55032/35

EN 61000-6-2/6-4

EMI:

CISPR 32

FCC Part 15B Class A

EMS:

IEC 61000-4-2 ESD: Contact: 4 kV; Air: 8 kV

IEC 61000-4-3 RS: 80 MHz to 1 GHz: 10 V/m

IEC 61000-4-4 EFT: DC Power: 1 kV; Signal: 1 kV

IEC 61000-4-5 Surge: DC Power: 0.5 kV L-N, 1 kV L/N-PE; Signal: 1 kV; IO: 0.5 kV

IEC 61000-4-6 CS: DC Power: 10 Vrms; Signal: 10 Vrms

IEC 61000-4-8 PFMF: 30 A/m

Safety: UL 61010-1, UL 61010-2-201

Shock: IEC 60068-2-27

Half Sine Wave:

Acceleration: 15 g

Duration Time: 11 ms

Vibration: IEC 60068-2-6

DIN-rail Mounted: 7 mm peak-peak (p-p) (2 to 8.42 Hz), 1 g (8.42 to 150 Hz)

Rack Mounted (with optional kit): 7 mm peak-peak (p-p) (2 to 8.42 Hz), 0.5 g (8.42 to 150 Hz)

Package vibration / drop test: STA-1A

Warranty

Warranty period: 5 years

Details: See www.moxa.com/tw/warranty

65M-CPU14-IEC-CT-T

Controller

CPU: ARM Cortex-A53 Quad-core 1.6 GHz

DDR SDRAM: 4 GB

Storage (eMMC): 8 GB (4 GB reserved for users)

NVRAM: 512 kB MRAM for data logger

OS: Moxa Industrial Linux

Automation Language: IEC 61131-3

Physical I/O Capacity: 512 points

Interface

Ethernet Ports: Auto-sensing 10/100/1000 Mbps ports (RJ45 connector) x 2

Serial Ports: RS-232/422/485 ports x 2, software selectable (DB9)

Console Ports: RS-232 (TxD, RxD, GND), 4-pin header output (115200, n, 8, 1)

Mode Switch: Remote, Run, Stop

microSD slot: 1 (function reserved)

Reset button: 1

Ethernet

LAN: 2 x 10/100/1000 Mbps, 2 MACs (IPs), RJ45

Magnetic Isolation Protection: 1.5 kV magnetic isolation

Serial

No. of Ports: 2, DB9

Serial standard: RS-232, RS-422, RS-485-2w

Baudrate: 300, 1200, 1800, 2400, 4800, 9600, 19200, 28800, 38400, 57600, 115200 bps

Data Bits: 8

Stop Bits: 1, 2

Parity: None, Even, Odd

Flow Control: RTS/CTS, XON/XOFF

Serial Signals

RS-232: TxD, RxD, RTS, CTS, DTR, DSR, DCD, GND

RS-422: Tx+, Tx-, Rx+, Rx-, GND

RS-485-2w: Data+, Data-, GND

RS-485-4w: Tx+, Tx-, Rx+, Rx-, GND

Power Parameters

Input Current: 0.8 A @ 12 VDC

Physical Characteristics

Dimensions: 42 x 177 x 134.8 mm (1.65 x 6.97 x 5.31 in)

Weight: 625 g (1.38 lb)

MTBF

Time: 1,830,589 hrs

Standard: Telcordia SR332

65M-PW0075-CT-T

System Power

Input Voltage: 24 VDC; 21.6 to 26.4 VDC

Input Current: 4 A (max.)

Inrush Current: 20 A (max.)

Input Internal Fuse Rating: 10 A

Output Voltage: 12 VDC

Output Current: 6.25 A (max.)

Output Power: 75 W (max.)

Output Hold Up Time: 10 ms (min.)

Output Startup Delay Time: 100 ms (max.)

Output Over Voltage Protection: 15.6 V (max.)

Output Over Current Protection: 9 A (min.)

Efficiency: 87%

Isolation: 3k VDC (input to output), 3k VDC (system-to-field power)

Field Power

Input Voltage: 24 VDC; 21.6 to 26.4 VDC

Input Current: 3 A (max.)

Input Internal Fuse Rating: 8 A

Output Voltage: Input voltage minus 0.4 VDC (max. matching-diode drop at 3 A)

Output Current: 3 A (max.)

Output Over Voltage Protection: 29 V (max.)

Output Over Current Protection: 5 A (min.)

Physical Characteristics

Dimensions: 42 x 177 x 149.4 mm (1.65 x 6.97 x 5.88 in)

Weight: 713 g (1.57 lb)

MTBF

Time: 2,847,774 hrs

Standard: Telcordia SR332

65M-5011M-CT-T

Ethernet Interface

10/100/1000BaseT(X) Ports (RJ45 connector): 8

Auto MDI/MDI-X connection

Auto-negotiation speed

Full/Half-duplex mode

100/1000BaseSFP Ports: 2

Standards:

IEEE 802.3 for 10BaseT, IEEE 802.3u for 100BaseT(X), IEEE 802.3ab for 1000BaseT(X), IEEE 802.3z for 1000BaseX, IEEE 802.3x for flow control, IEEE 802.3ad for port trunk with LACP, IEEE 802.1Q for VLAN Tagging, IEEE 802.1D-2004 for Spanning Tree Protocol, IEEE 802.1w for Rapid Spanning Tree Protocol, IEEE 802.1p for Class of Service, IEEE 802.1X for authentication

Ethernet Software Features

Filter: GMRP, GVRP, GARP, 802.1Q VLAN, IGMP Snooping v1/v2/v3, IGMP Querier

Management: IPv4/IPv6, Flow control, Back Pressure Flow Control, DHCP Server/Client, ARP, RARP, LLDP, Port Mirror, Linkup Delay, SMTP, SNMP Trap, SNMP Inform, SNMPv1/v2c/v3, RMON, TFTP, SFTP, HTTP, HTTPS, Telnet, Syslog, Private MIB, fiber check

MIB: P-BRIDGE MIB, Q-BRIDGE MIB, IEEE8021-SPANNING-TREE-MIB, IEEE8021-PAE-MIB, IEEE8023-LAG-MIB, LLDP-EXT-DOT1-MIB, LLDP-EXT-DOT3-MIB, SNMPv2-MIB, RMON MIB Groups 1, 2, 3, 9

Redundancy Protocols: STP, RSTP, Turbo Ring v2, Turbo Chain, Ring Coupling, Dual-Homing, Link Aggregation

Security: Broadcast storm protection, Rate Limit, Trust access control, Static Port Lock, MAC Sticky, HTTPS/SSL, SSH, RADIUS, TACACS+, Login and Password Policy

Time Management: SNTP, NTP Server/Client, NTP Authentication

Protocols: IPv4/IPv6, TCP/IP, UDP, ICMP, ARP, RARP, TFTP, DNS, NTP Client, DHCP Server, DHCP Client, 802.1X, QoS, HTTPS, HTTP, Telnet, SMTP, SNMPv1/v2c/v3, RMON, Syslog

Switch Properties

MAC Table Size: 16 K

Jumbo Frame Size: 9.216 KB

Max. No. of VLANs: 256

VLAN ID Range: VID 1 to 4094

IGMP Groups: 512

Priority Queues: 4

Packet Buffer Size: 1 MB

Serial Interface

Console Port: RS-232 (Tx/D, Rx/D, GND), 8-pin RJ45 (115200, n, 8, 1)

Input/Output Interface

Buttons: RESET Button

USB Connector: USB Type A (only supports the ABC-02-USB from Moxa)

Power Parameters

Input Current: 0.9 A @ 12 VDC

Physical characteristics

Dimensions: 42 x 177 x 131.5 mm (1.65 x 6.97 x 5.18 in)

Weight: 660 g (1.46 lb)

Environmental

Operating Temperature:

-40 to 75°C (-40 to 167°F)

-40 to 65°C (-40 to 149°F) with SFP module installed

NOTE: Proper airflow is required in an environment over 65°C.

MTBF

Time: 3,104,403 hrs

Standard: Telcordia SR332

65M-5290-CT-T

Ethernet Interface

Port Interfaces: RJ45 Ports x 2, SFP Fiber Ports x 2

Protocol: Proprietary

Power Consumption

System Power: 0.38 A @ 12 VDC

Physical characteristics

Dimensions: 42 x 116 x 130 mm (1.65 x 4.57 x 5.12 in)

Weight: 501 g (1.1 lb)

MTBF

Time: 2,800,019 hrs

Standard: Telcordia SR332

65M-1900-CT-T

Digital Input

Number of Channels: 32

Input Type: Current Sink (internal or external sensor supply for dry contact)

Input Pulse Width: 50 μ s (min.)

Internal Field Circuit Supply (only for dry contact):

Voltage: 24 VDC; 22.8 to 25.2 VDC

Current: 125 mA (max.) (Only for dry contact)

Input ON Voltage: 11 to 30 VDC

Input OFF Voltage: 0 to 5 VDC

Input Current: 2.35 mA $\pm$ 20 % per channel (at Input ON Voltage)

Input Filtering: Software configurable

Isolation: 3k VDC (signal to system)

Counter

Number of Channels: 8 (Channel 1 to 8, group configurable by software)

Counting Frequency: Square wave 0 to 10 kHz

Frequency Measurement: No

Counter Size: 32 bits

Diagnostic

Input Wire-Break Detection:

Input Current < 50 μ A

Detection Delay Time: 20 ms (typ.)

Internal Field Circuit Supply Detection: 17.5 VDC (typ.); 16 to 19 VDC

Power Consumption

System Power: 0.068 A @ 12 VDC

Field Power:

0.019 A @ 24 VDC (without field circuit supply)

0.115 A @ 24 VDC (32 channels dry contact with internal field circuit supply)

Physical characteristics

Dimensions: 42 x 116 x 130 mm (1.65 x 4.57 x 5.12 in)

Weight: 253 g (0.56 lb)

MTBF

Time: 2,057,118 hrs

Standard: Telcordia SR332

65M-2901-CT-T

Digital Output

Number of Channels: 32

Output Type: Current source

Common Power Input Voltage: 24 VDC; 19.2 to 28.8 VDC

Common Power Input Current: 6.4 A (max.)

Load Current:

200 mA / 1 channel (typ.)

500 mA / 1 channel (max.)

Leakage Current: 0.11 mA (max. at OFF State)

Load Resistance Range: 48 to 8k Ω

Protection:

Output short-circuit protection

Common power input over voltage protection

Inductive load shutdown voltage protection

Isolation: 3k VDC (signal to system)

Pulse

Number of Channels: 8 (Channel 1 to 8, group configurable by software)

Pulse Duration: 500 μ s (min.)

Diagnostic

Output Wire-Break Detection:

Output Current < 3 mA (ON state);

Output Load Impedance > 58 K Ω (OFF state)

Output Short-Circuit Detection: Output current > 0.87 A (typ.); 0.64 to 1.2 A

External Power Detection: 17.5 VDC (typ.); 16 to 19 VDC

Fail-Safe Configuration: Hold last / Fail-safe state

Power Consumption

System Power: 0.068 A @ 12 VDC

Field Power: 0.01 A @ 24 VDC

Physical characteristics

Dimensions: 42 x 116 x 130 mm (1.65 x 4.57 x 5.12 in)

Weight: 254 g (0.56 lb)

MTBF

Time: 2,007,795 hrs

Standard: Telcordia SR332

65M-3600-CT-T

Analog Input

Number of Channels: 16 (8 channels per group)

Input Mode:

0 to 20 mA

4 to 20 mA

Permitted Overload on Inputs: ± 30 mA

IO type: Differential

Internal Loop Power Supply (only for 2-wire connection):

Voltage: 24 VDC; 22.8 to 25.2 VDC

Current: 200 mA/Group (max.)

Resolution: 16 bits

Measurement Resolution:

2 μ A (0 to 20 mA)

1.6 μ A (4 to 20 mA)

Conversion Time: 100 ms

Normal Mode Rejection Ratio: > 60 dB @ 60 Hz ; conversion time: 100 ms

Common Mode Rejection Ratio: > 90 dB @ 60 Hz ; conversion time: 100 ms

Accuracy:

$\pm 0.1\%$ Full-scale range @ 25°C

$\pm 0.3\%$ Full-scale range @ -40 to 75°C

Input Resistance: 250 Ω

Isolation:

3k VDC (signal to system)

1k VDC for 1 min. (group to group)

Diagnostic

Internal Loop Power Detection: 17.5 VDC (typ.); 16 to 19 VDC

Input Wire-Break Detection: Yes, (4 to 20 mA mode only, detection delay time: 0.8 s (max.))

Input Short-Circuit Detection: Yes

Input Underflow / Overflow Detection: Yes

Power Consumption

System Power: 0.073 A @ 12 VDC

Field Power:

0.053 A @ 24 VDC (without internal loop power)

0.466 A @ 24 VDC (16 channels 20 mA current input with internal loop power)

Physical characteristics

Dimensions: 42 x 116 x 130 mm (1.65 x 4.57 x 5.12 in)

Weight: 267 g (0.59 lb)

MTBF

Time: 1,686,798 hrs

Standard: Telcordia SR332

65M-3610-CT-T

Analog Input

Number of Channels: 16 (8 channels per group)

Input Mode:

0 to 10 V

1 to 5 V

Permitted Overload: ± 12 V

IO type: Differential

Resolution: 16 bits

Measurement Resolution:

1 mV (0 to 10 V)

0.4 mV (1 to 5 V)

Conversion Time: 100 ms

Normal Mode Rejection Ratio: > 60 dB @ 60 Hz ; conversion time: 100 ms

Common Mode Rejection Ratio: > 90 dB @ 60 Hz ; conversion time: 100 ms

Accuracy:

$\pm 0.1\%$ Full-scale range @ 25°C

$\pm 0.3\%$ Full-scale range @ -40 to 75°C

Input Resistance: > 1 M Ω

Isolation:

3k VDC (signal to system)

1k VDC for 1 min. (group to group)

Diagnostic

Input Wire-Break Detection: Yes (detection delay time: 1.6 s (max.))

Input Underflow / Overflow Detection: Yes

Power Consumption

System Power: 0.069 A @ 12 VDC

Field Power: 0.038 A @ 24 VDC

Physical characteristics

Dimensions: 42 x 116 x 130 mm (1.65 x 4.57 x 5.12 in)

Weight: 250 g (0.55 lb)

MTBF

Time: 1,885,953 hrs

Standard: Telcordia SR332

65M-3800H-CT-T

HART Analog Input

Number of Channels: 8

Channel Enable/Disable: Yes

Input Mode: 4 to 20 mA

Permitted Overload on Inputs: 30 mA

IO type: Differential

Internal Loop Power Supply (only for 2-wire connection):

Voltage: 24 VDC; 22.8 to 25.2 VDC

Current: 500 mA (max.)

Resolution: 16 bits

Measurement Resolution: 1.6 μ A (4 to 20 mA)

Conversion Time: 100 ms

Accuracy:

$\pm 0.1\%$ Full-scale range @ 25°C

$\pm 0.3\%$ Full-scale range @ -40 to 75°C

Input Resistance: 250 Ω

Isolation:

3k VDC (signal to system)

1k VDC for 1 min. (group to group)

HART

Number of HART Modem: 1

Data Update Time: 1 sec/field device

Operation Type: Primary client

Topology: Point-to-point

HART Enable/Disable: Yes

Diagnostic

Internal Power Detection: 17.5 VDC (typ.); 16 to 19 V DC

Internal Wire-Break Detection: Yes

Input Wire-Break Detection: Yes

Input Short-Circuit Detection: Yes

Power Consumption

System Power: 0.072 A @ 12 VDC

Field Power:

0.05 A (max.), 24 VDC (without using internal loop power)

0.25 A (max.), 24 VDC (8 channels 4 to 20 mA input using internal loop power all in 20 mA)

0.66 A (max.), 24 VDC (internal loop power supply at 500 mA)

Physical characteristics

Dimensions: 42 x 116 x 130 mm (1.65 x 4.57 x 5.12 in)

Weight: 262 g (0.58 lb)

MTBF

Time: 1,016,573 hrs

Standard: Telcordia SR332

65M-4820-CT-T

Analog Output

Number of Channels: 8 (4 channels per group)

Output Mode:

0 to 10 V

1 to 5 V

0 to 20 mA

4 to 20 mA

IO type: Differential

Resolution: 16 bit

Output Resolution:

0.1 mV (0 to 10 V)

0.4 mV (1 to 5 V)

2 μ A (0 to 20 mA)

1.6 μ A (4 to 20 mA)

Output Refresh Time: 16 ms

Output Step Response Time: 1 ms (max.)

Accuracy:

$\pm 0.1\%$ Full-scale range @ 25°C

$\pm 0.3\%$ Full-scale range @ -40 to 75°C

Output Load Impedance:

$\geq 1\text{ K}\Omega$ (0 to 10 V/1 to 5 V)

$\leq 750\ \Omega$ (0 to 20 mA/4 to 20 mA)

Isolation:

3k VDC (signal to system)

1k VDC for 1 min. (group to group)

Diagnostic

Output Wire-Break Detection: Yes, for Current Mode

Output Short-Circuit Detection: Yes, for Voltage Mode

Fail-Safe Configuration: Hold last/Fail-safe state

Power Consumption

System Power: 0.069 A @ 12 VDC

Field Power:

0.022 A @ 24 VDC (without external load)

0.266 A @ 24 VDC (4 channels with 20 mA current output)

Physical characteristics

Dimensions: 42 x 116 x 130 mm (1.65 x 4.57 x 5.12 in)

Weight: 257 g (0.57 lb)

MTBF

Time: 1,874,152 hrs

Standard: Telcordia SR332

65M-5801-CT-T

Serial

No. of Ports: 8 (4 Channels/Group), Terminal Block

Serial Standards: RS-232, RS-422, RS-485-2w

Baud Rate: 300, 1200, 1800, 2400, 4800, 9600, 19200, 28800, 38400, 57600, 115200 bps

Data Bits: 7, 8

Stop Bits: 1, 2

Parity: None, Even, Odd

Flow Control: RTS/CTS, XON/XOFF

Isolation: 3k VDC (signal to system), 1k VDC (between groups)

Power Consumption

System Power: 0.143 A @ 12 VDC

Field Power: 0.11 A @ 24 VDC

Physical characteristics

Dimensions: 42 x 116 x 130 mm (1.65 x 4.57 x 5.12 in)

Weight: 259 g (0.57 lb)

MTBF

Time: 2,310,512 hrs

Standard: Telcordia SR332

65M-BMPW01-CT-T

Physical characteristics

Slots: 1 (for Power module)

Dimensions: 43 x 177 x 45.5 mm (1.69 x 6.97 x 1.79 in)

Weight: 162 g (0.36 lb)

MTBF

Time: 1,130,092,735 hrs

Standard: Telcordia SR332

65M-BMPW02-CT-T

Physical characteristics

Slots: 2 (for power module)

Dimensions: 86 x 177 x 45.5 mm (3.39 x 6.97 x 1.79 in)

Weight: 320 g (0.71 lb)

MTBF

Time: 1,382,748,219 hrs

Standard: Telcordia SR332

65M-BMCM01-CT-T

Physical characteristics

Slots: 1 (for switch module)

Dimensions: 43 x 177 x 45.5 mm (1.69 x 6.97 x 1.79 in)

Weight: 169 g (0.37 lb)

MTBF

Time: 1,856,744,727 hrs

Standard: Telcordia SR332

65M-BMCM02-CT-T

Physical characteristics

Slots: 2 (for switch module)

Dimensions: 86 x 177 x 45.5 mm (3.39 x 6.97 x 1.79 in)

Weight: 330 g (0.73 lb)

MTBF

Time: 1,856,744,727 hrs

Standard: Telcordia SR332

65M-BMEXP01-CT-T

Physical characteristics

Slots: 1 (for Expansion module)

Dimensions: 43 x 177 x 45.5 mm (1.69 x 6.97 x 1.79 in)

Weight: 173 g (0.38 lb)

MTBF

Time: 1,856,744,727 hrs

Standard: Telcordia SR332

65M-BMEXP02-CT-T

Physical characteristics

Slots: 2 (for Expansion module)

Dimensions: 86 x 177 x 45.5 mm (3.39 x 6.97 x 1.79 in)

Weight: 322 g (0.71 lb)

MTBF

Time: 1,856,744,727 hrs

Standard: Telcordia SR332

65M-BMCPU01-CT-T

Physical characteristics

Slots: 1 (for CPU module)

Dimensions: 43 x 177 x 45.5 mm (1.69 x 6.97 x 1.79 in)

Weight: 170 g (0.37 lb)

MTBF

Time: 5,032,783,357 hrs

Standard: Telcordia SR332

65M-BMCPU02-CT-T

Physical characteristics

Slots: 2 (for CPU module)

Dimensions: 86 x 177 x 45.5 mm (3.39 x 6.97 x 1.79 in)

Weight: 325 g (0.72 lb)

MTBF

Time: 3,554,206,267 hrs

Standard: Telcordia SR332

65M-BMIO02-CT-T

Power Consumption

System Power: 0.093 A @ 12 VDC

Physical characteristics

Slots: 2 (for IO module)

Dimensions: 86 x 177 x 45.5 mm (3.39 x 6.97 x 1.79 in)

Weight: 205 g (0.45 lb)

MTBF

Time: 6,140,939 hrs

Standard: Telcordia SR332

65M-BMIO04-CT-T

Power Consumption

System Power: 0.117 A @ 12 VDC

Physical characteristics

Slots: 4 (for IO module)

Dimensions: 172 x 177 x 45.5 mm (6.77 x 6.97 x 1.79 in)

Weight: 395 g (0.87 lb)

MTBF

Time: 6,124,471 hrs

Standard: Telcordia SR332

65M-TB-1900-CT-T

Physical characteristics

ID: D1

Dimensions: 42.3 x 102.38 x 80.8 mm (1.67 x 4.03 x 3.18 in)

Weight: 164 g (0.36 lb)

65M-TB-2901-CT-T

Physical characteristics

ID: D2

Dimensions: 42.3 x 102.38 x 80.8 mm (1.67 x 4.03 x 3.18 in)

Weight: 164 g (0.36 lb)

65M-TB-3600-CT-T

Physical characteristics

ID: A1

Dimensions: 42.3 x 102.38 x 80.8 mm (1.67 x 4.03 x 3.18 in)

Weight: 164 g (0.36 lb)

65M-TB-3610-CT-T

Physical characteristics

ID: A2

Dimensions: 42.3 x 102.38 x 80.8 mm (1.67 x 4.03 x 3.18 in)

Weight: 164 g (0.36 lb)

65M-TB-3800H-CT-T

Physical characteristics

ID: A3

Dimensions: 42.3 x 102.38 x 80.8 mm (1.67 x 4.03 x 3.18 in)

Weight: 164 g (0.36 lb)

65M-TB-4820-CT-T

Physical characteristics

ID: A5

Dimensions: 42.3 x 102.38 x 80.8 mm (1.67 x 4.03 x 3.18 in)

Weight: 164 g (0.36 lb)

65M-TB-5801-CT-T

Physical characteristics

ID: F1

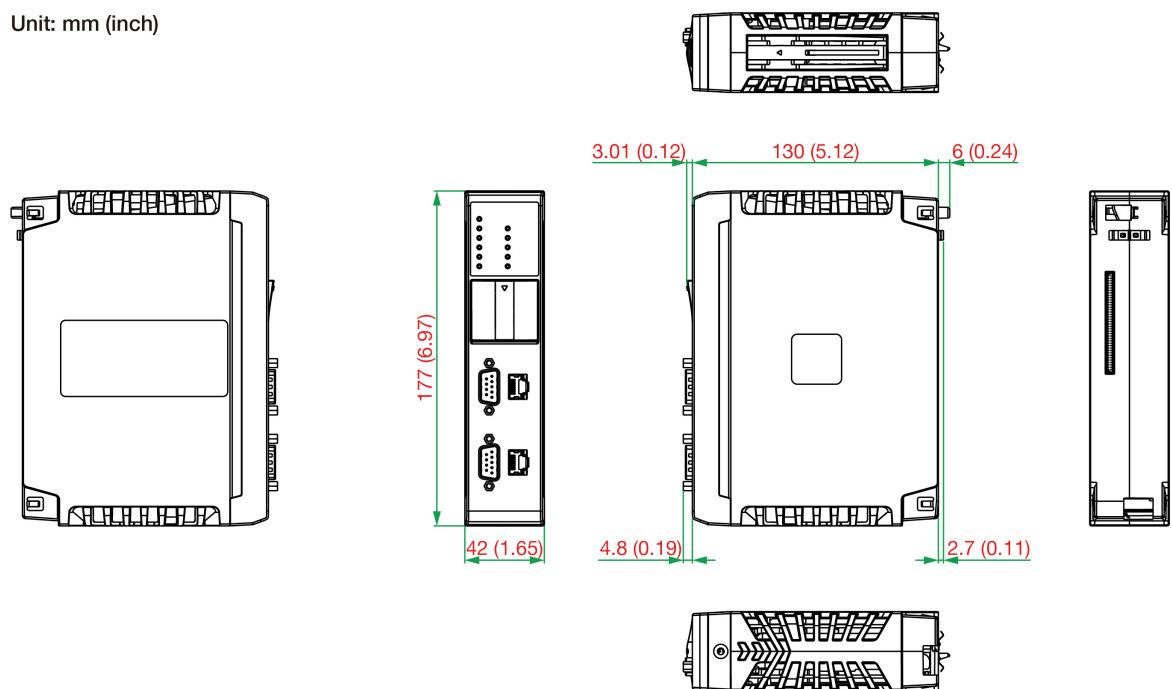
Dimensions: 42.3 x 102.38 x 80.8 mm (1.67 x 4.03 x 3.18 in)

Weight: 164 g (0.36 lb)

Physical Dimensions

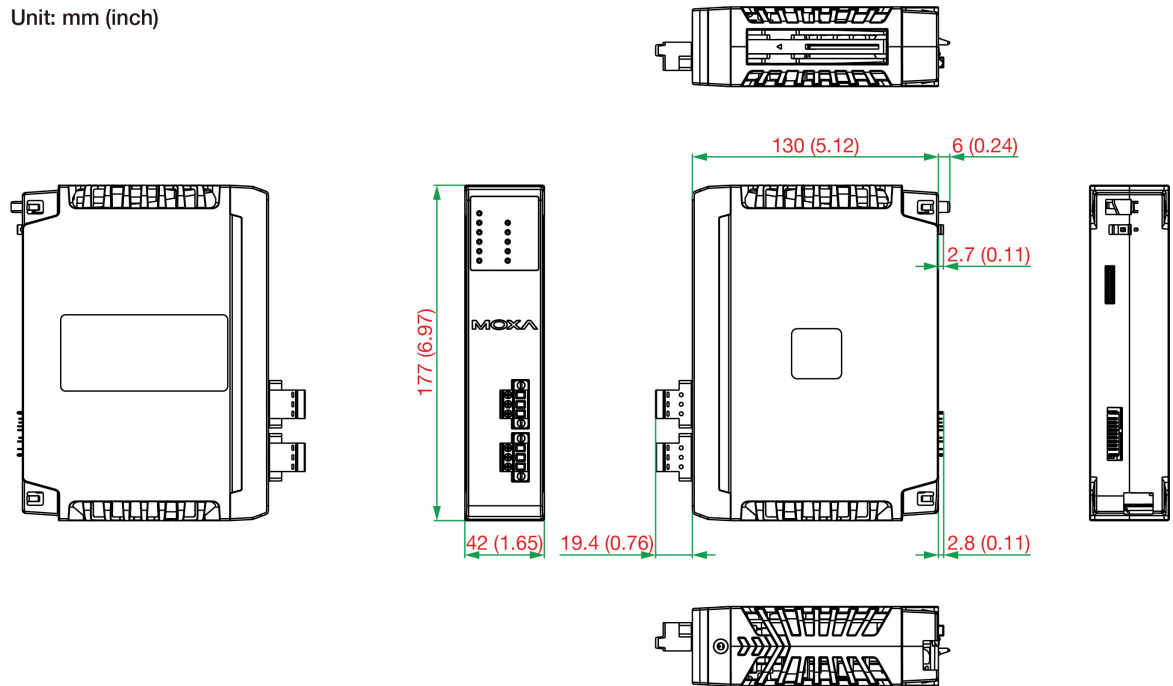
65M-CPU14-IEC-CT-T

Unit: mm (inch)



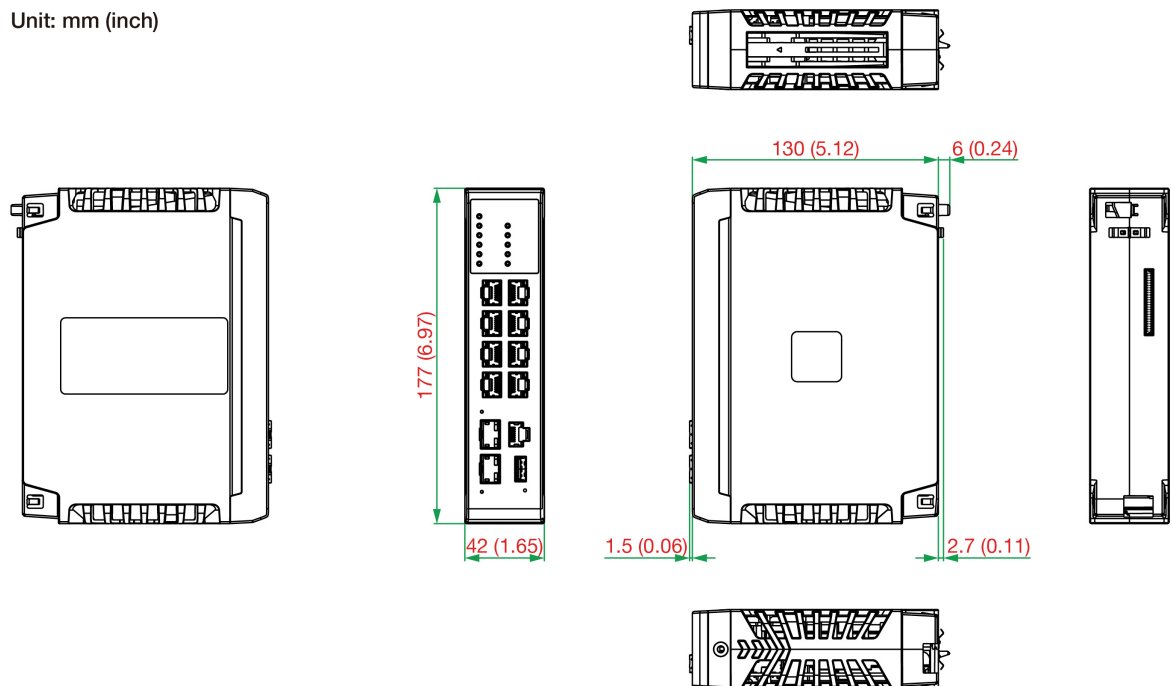
65M-PW0075-CT-T

Unit: mm (inch)



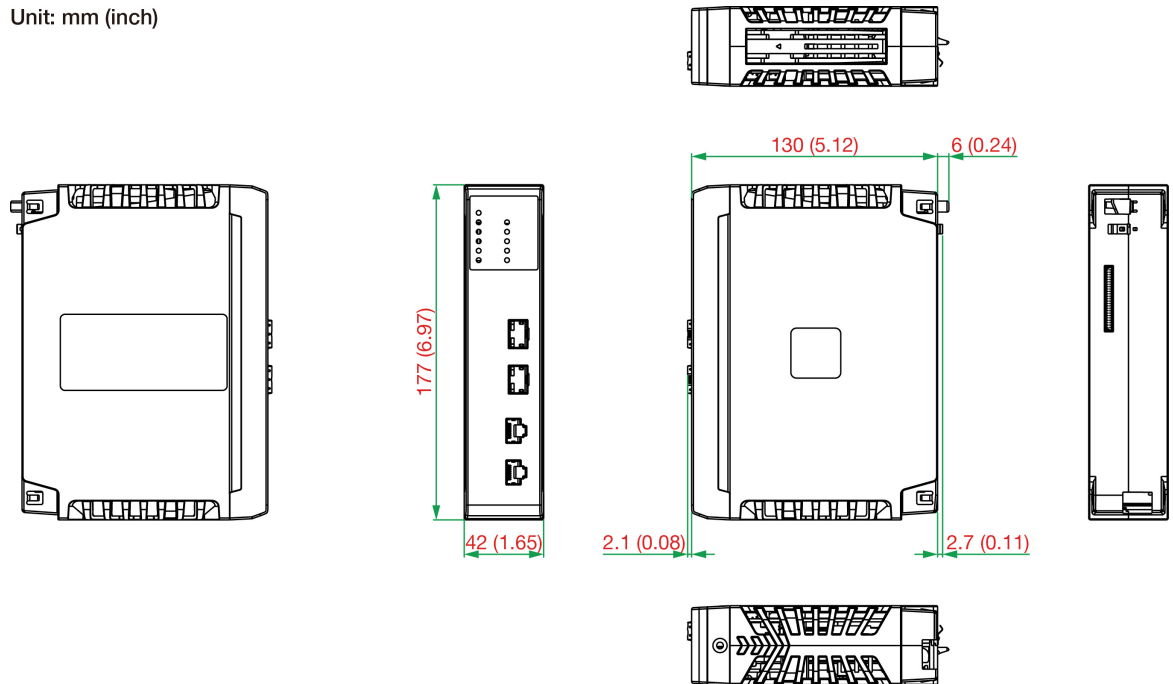
65M-5011M-CT-T

Unit: mm (inch)



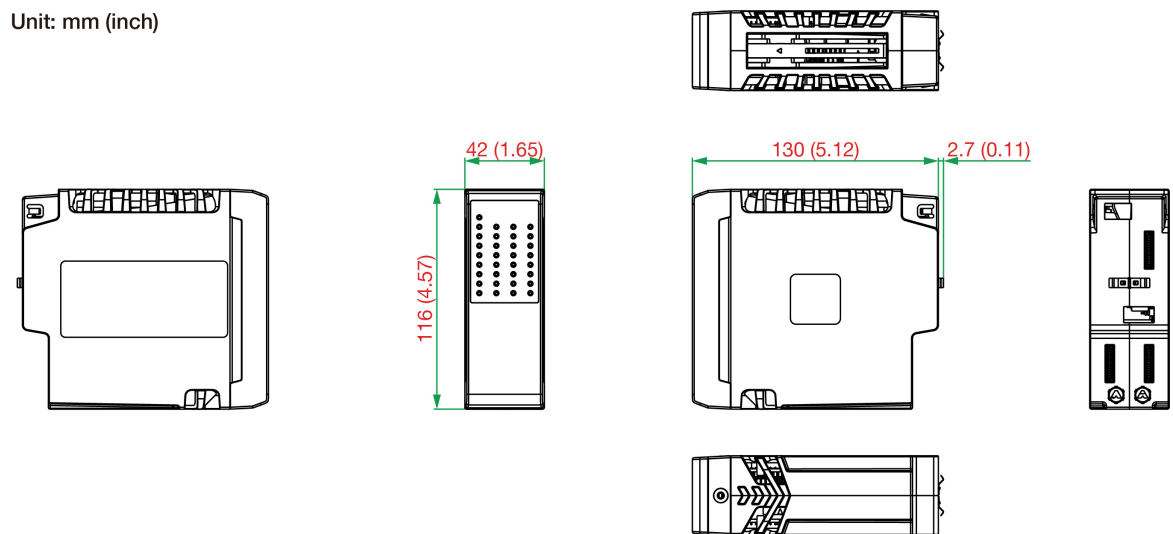
65M-5290-CT-T

Unit: mm (inch)



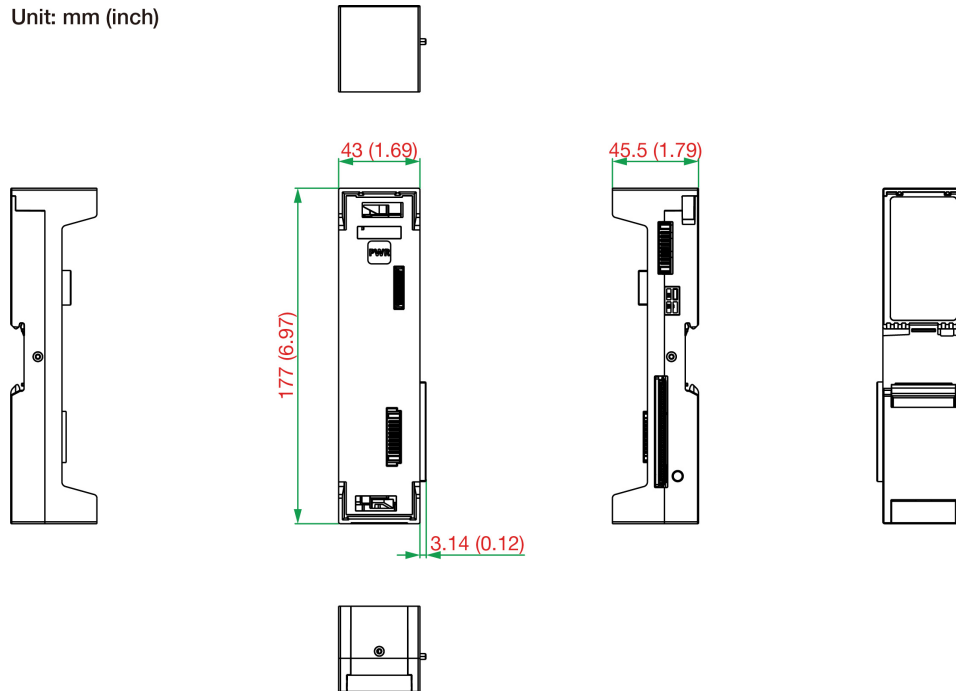
65M-1XXX/2XXX/3XXX/4XXX/5801-CT-T (IO Module)

Unit: mm (inch)



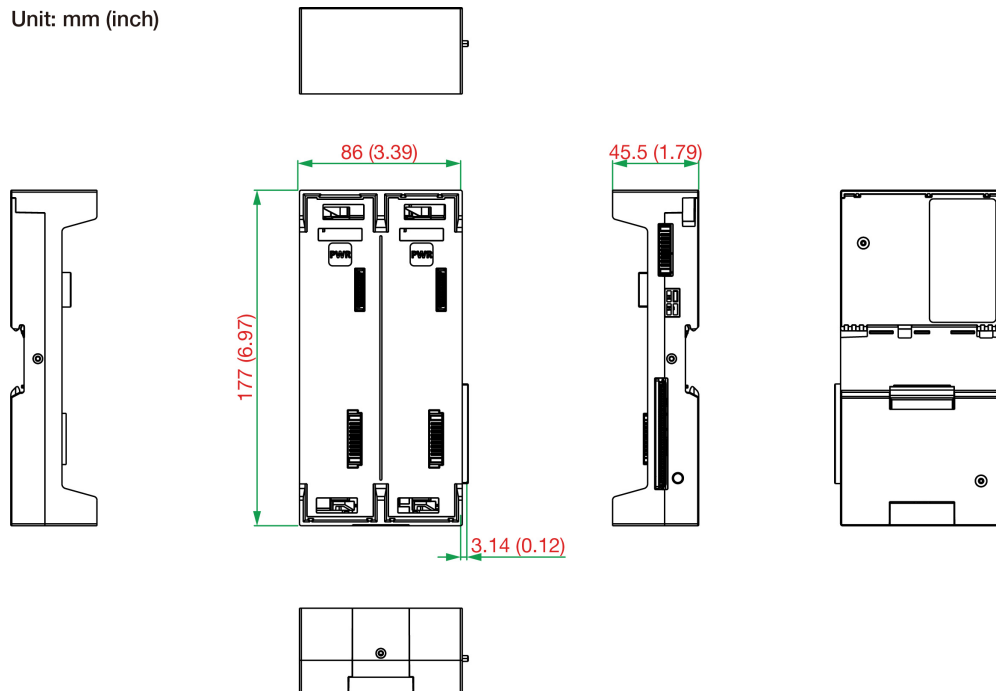
65M-BMPW01-CT-T

Unit: mm (inch)



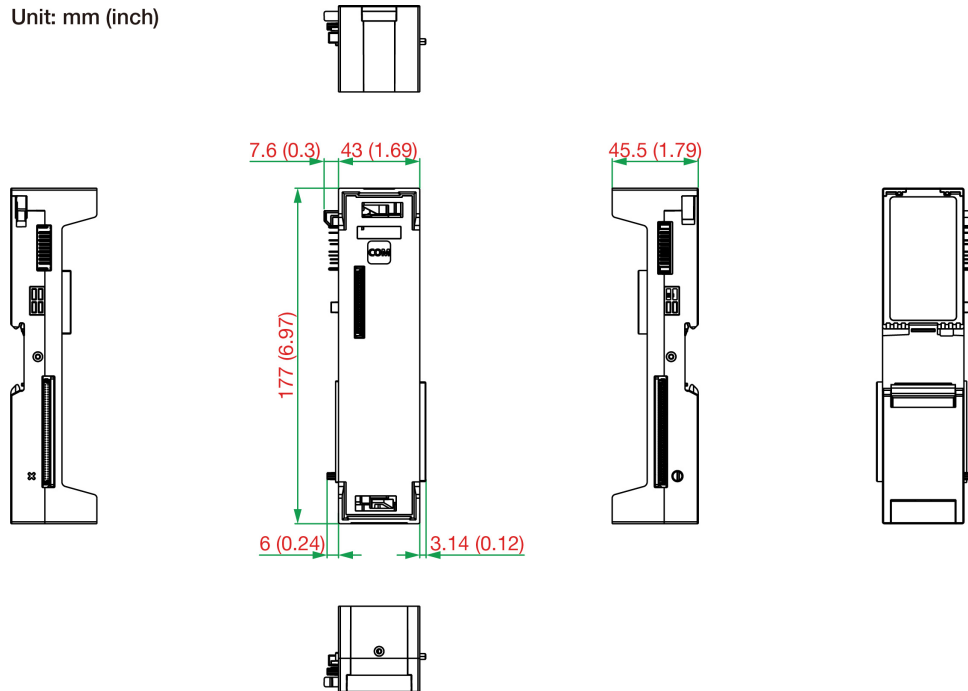
65M-BMPW02-CT-T

Unit: mm (inch)



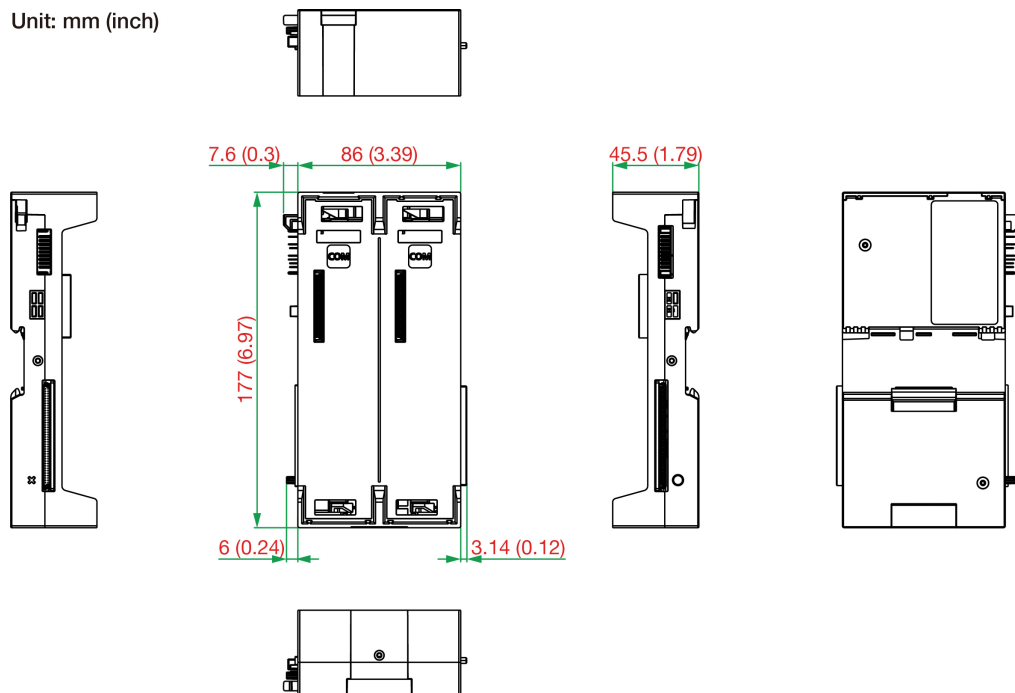
65M-BMCM01-CT-T

Unit: mm (inch)



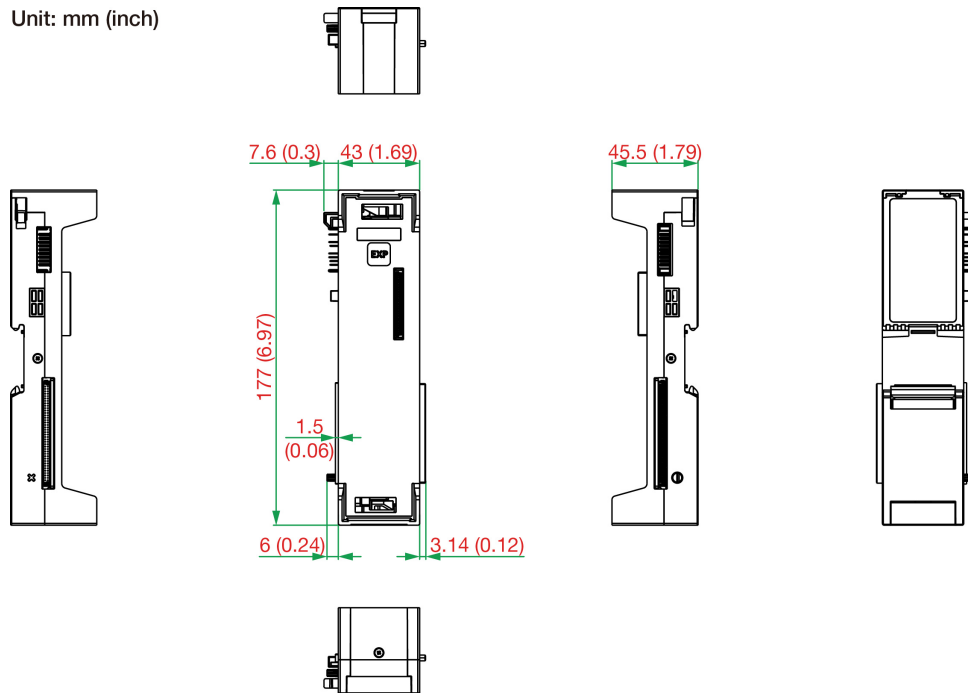
65M-BMCM02-CT-T

Unit: mm (inch)



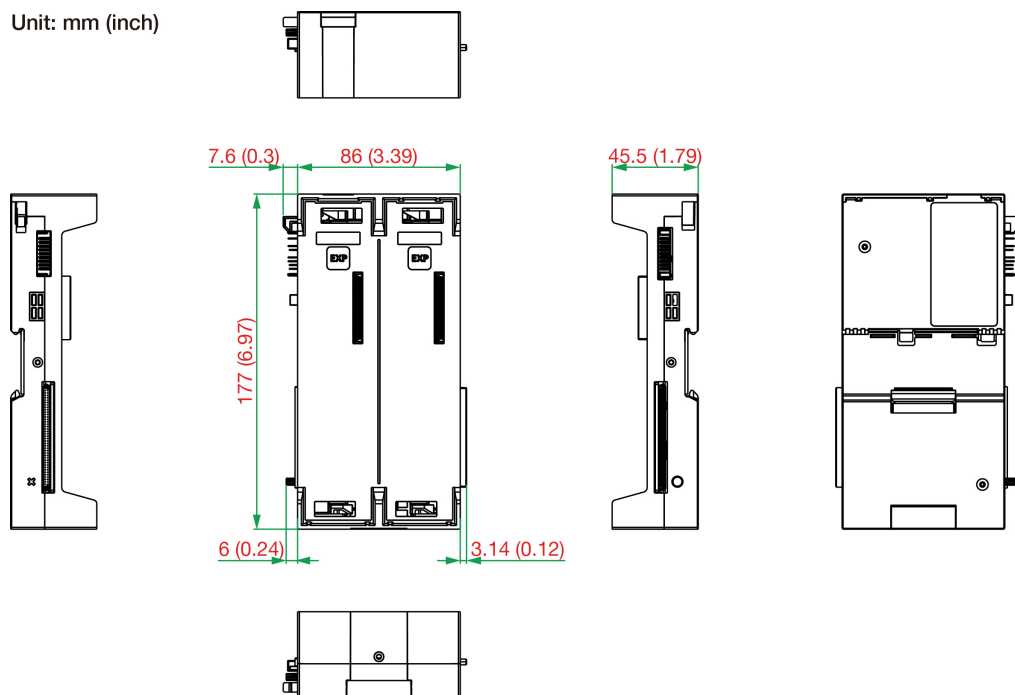
65M-BMEXP01-CT-T

Unit: mm (inch)



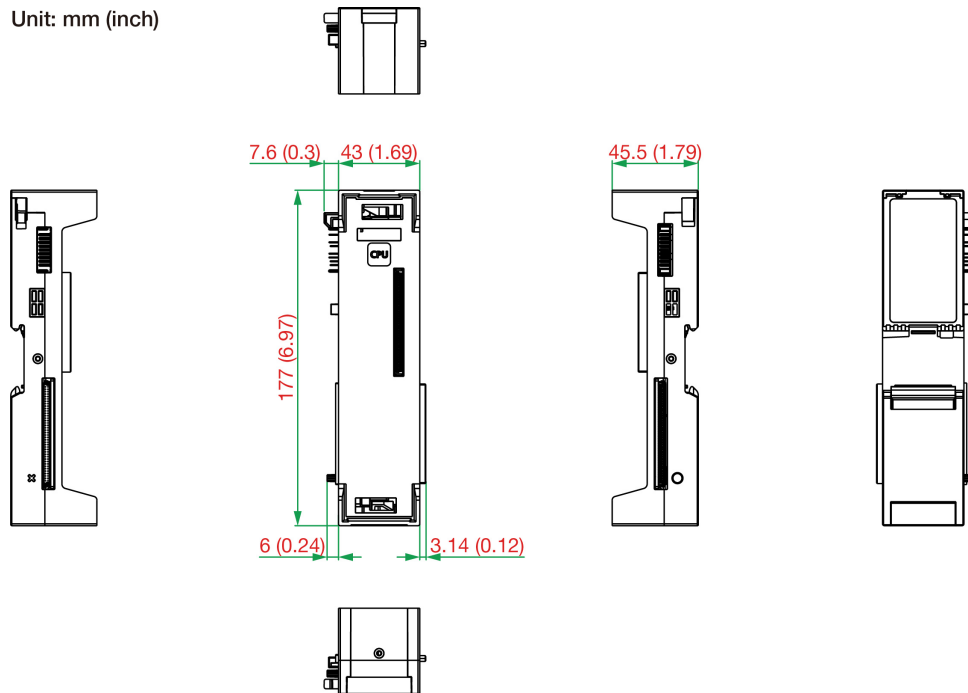
65M-BMEXP02-CT-T

Unit: mm (inch)



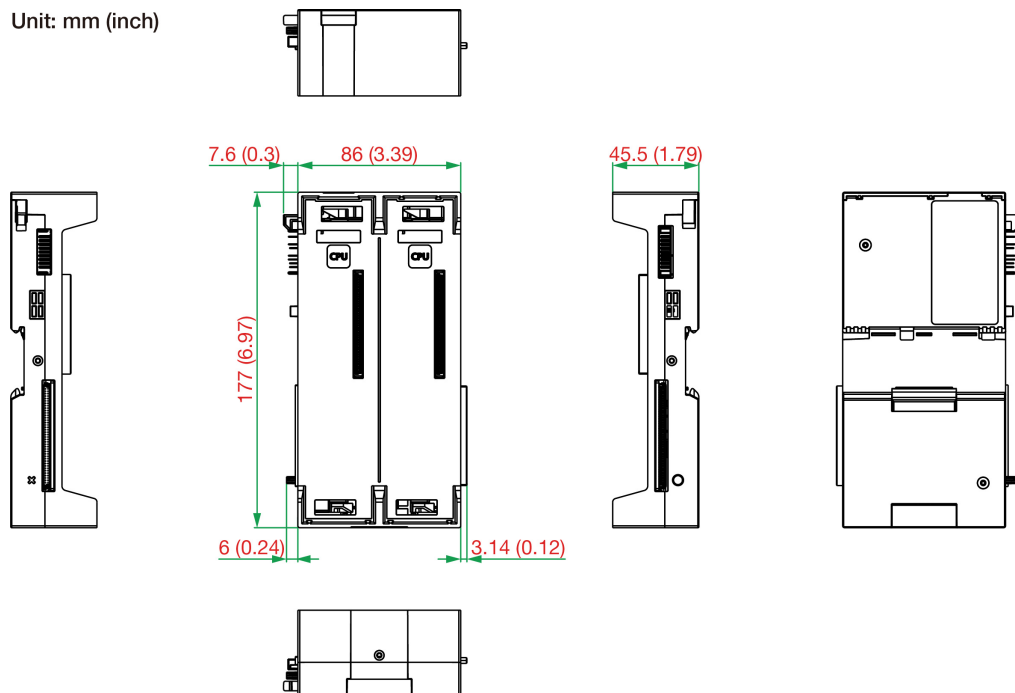
65M-BMCPU01-CT-T

Unit: mm (inch)



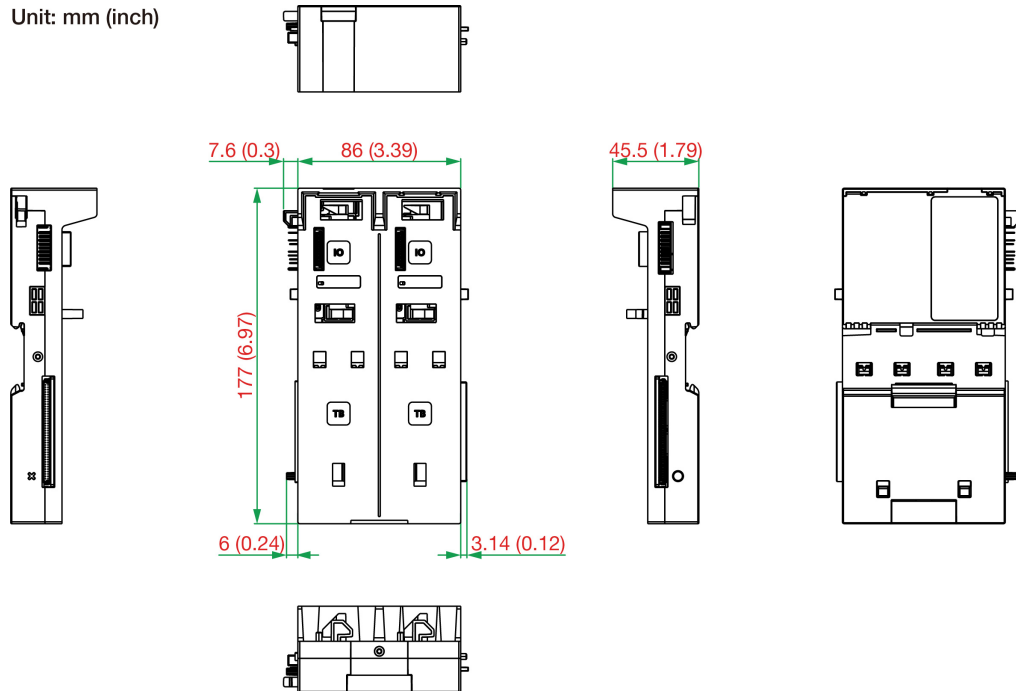
65M-BMCPU02-CT-T

Unit: mm (inch)



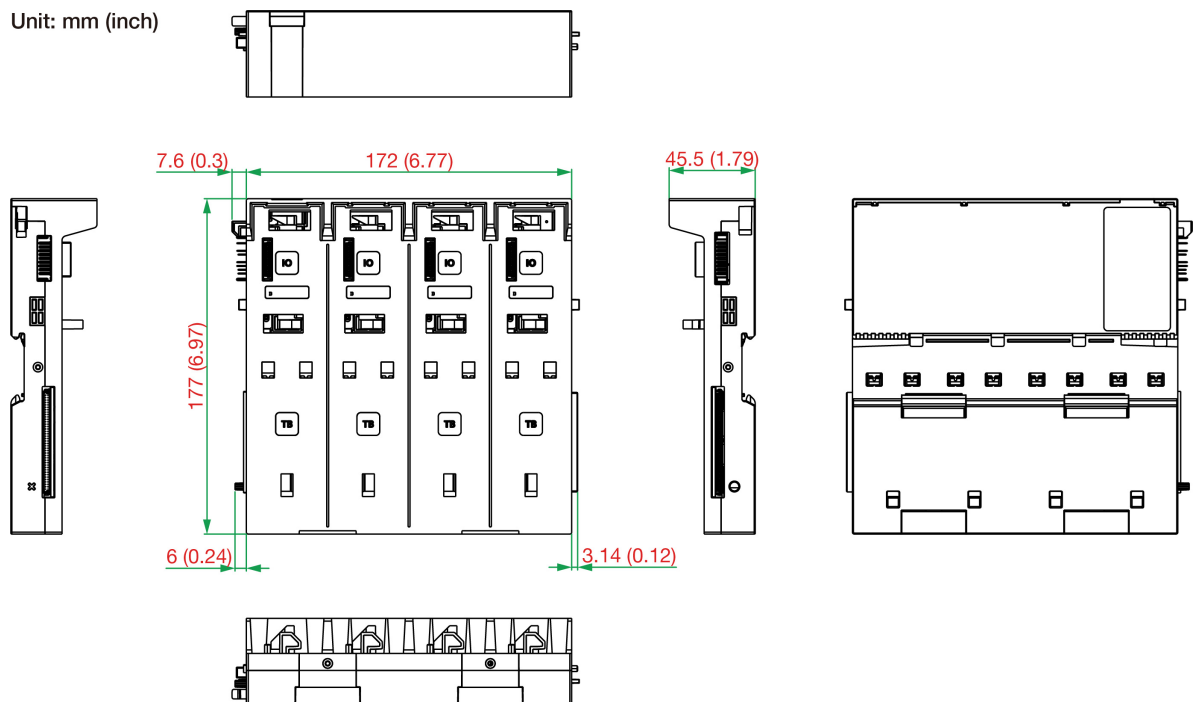
65M-BMIO02-CT-T

Unit: mm (inch)



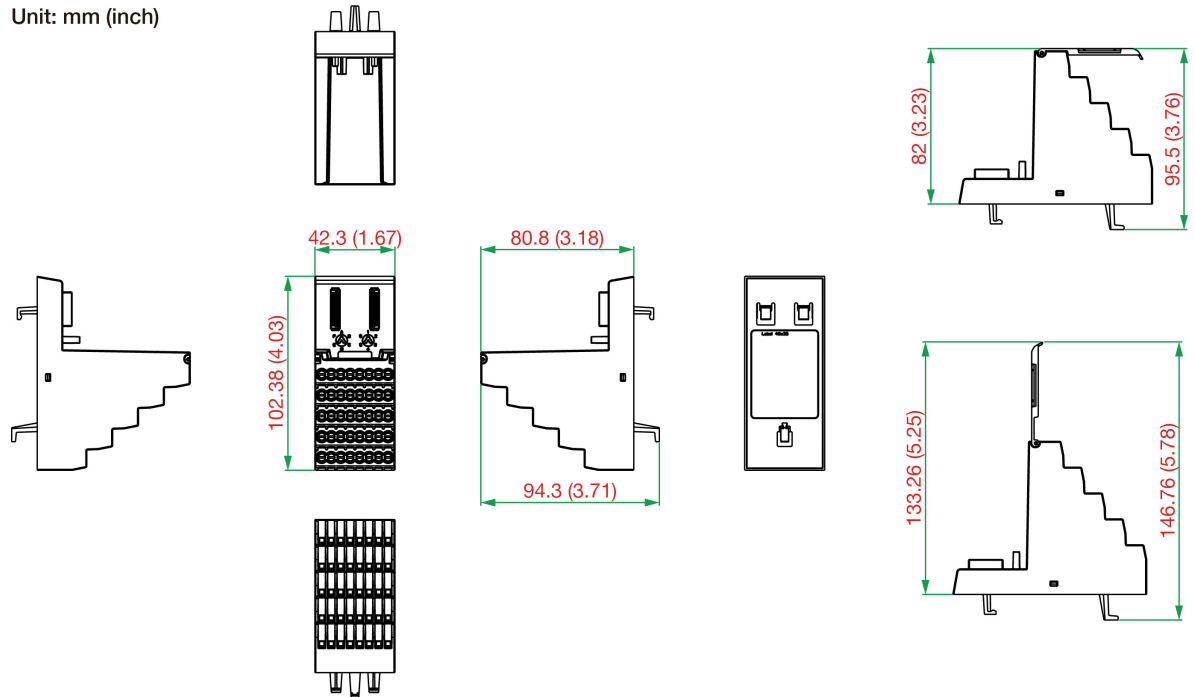
65M-BMIO04-CT-T

Unit: mm (inch)



65M-TB-1XXX/2XXX/3XXX/4XXX/5801-CT-T

Unit: mm (inch)



LED Definition

65M-CPU14-IEC-CT-T

Front View

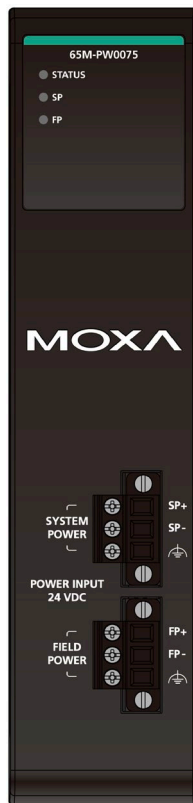


LED Description

Labeling	Indication	Qty	Color	Behavior	Description
STATUS	System status	1	Green	On	Normal
				Blinking at 5 Hz	Firmware upgrade in Progress
				Blinking at 0.5 Hz	Booting up
				Double Blinking	Module locating
			Red	On	System failure
				Blinking at 0.5 Hz	Service failure
				Double Blinking	Press reset button for 15 seconds, the STATUS will start to RED double blinking, release the reset button to start the reset to default.
ACT	Active	1	N/A	N/A	Reserved
PROG	Program	1	Green	On	Program is running
			Red	On	Runtime failure
			Off		Program has stopped
SD	SD card	1	Green	Blinking at 0.5 Hz	SD card is reading
P1/P2	Serial	1 for each	Green	Blinking at 0.5 Hz	Tx
			Amber	Blinking at 0.5 Hz	Rx
LAN1/ LAN2	Ethernet	1 for each	Green	On	Connected on 1000M
				Blinking	Data is transmitting
			Amber	On	Connected on 10/100M
				Blinking	Data is transmitting
			Off		Disconnected

65M-PW0075-CT-T

LED Indicators

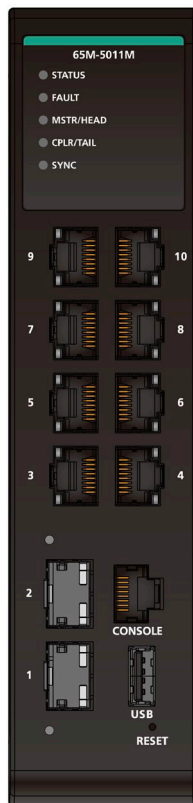


LED Description

Labeling	Indication	Qty	Color	Behavior	Description
STATUS	System status	1	Green	On	Normal
				Blinking at 5 Hz	Firmware upgrade in progress
				Blinking at 0.5 Hz	Booting up
				Double Blinking	Module located
			Red	On	System failure
				Blinking at 5 Hz	Lost the connection to CPU
SP	System Power	1	Green	Blinking at 0.5 Hz	Diagnostic error
				On	Normal
FP	Field Power	1	Green	Blinking at 5 Hz	Abnormal
				On	Normal

65M-5011M-CT-T

Front view



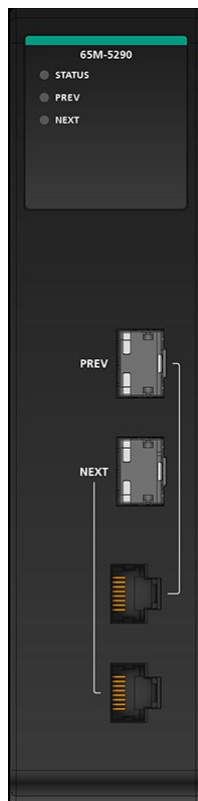
LED Definition

Labeling	Indication	Qty	Color	Behavior	Description
STATUS	System status	1	Green	On	When the system has passed a power-on self-test (POST) and is ready to run.
				Blinking at 1 Hz	1. When pressing the reset button, depress for 1 second to reboot the switch. 2. System service initialization.
				Blinking at 2 Hz	1. When pressing the reset button, depress for 5 seconds to reset to factory default. 2. While external storage is connected to the switch.
			Red	On	System failed in boot up process. Reading system info failed or EEPROM info error.
FAULT	Fault indication	1	Red	On	1. Network loop is detected when loop protection is enabled. 2. External storage Loading/Saving Fail. 3. The port is being disabled because exceeding the ingress rate limit of shut down mode. 4. Invalid Ring port connection.
				Off	When the system boots up and runs correctly or a user-configured event is not triggered.
Client/ HEAD	Client or head	1	Green	On	When the switch is Client/Head of Turbo Ring/Turbo Chain.
				Blinking at 4 Hz	1. The switch has become the Client of Turbo Ring after Turbo Ring has gone down. 2. The switch is set as Head of Turbo Chain and Turbo Chain has gone down. 3. The switch is set as the Turbo Ring's Member and the corresponding Ring port is down. 4. The switch is set as the Turbo Chain's Member/ Tail and the corresponding Head-end Chain port is down.

Labeling	Indication	Qty	Color	Behavior	Description
				Off	When the switch is not the Client/Head of this Turbo Ring/Turbo Chain.
CPRL/ TAIL	Coupling or Tail	1	Green	On	1. The switch's ring coupling or dual homing function is enabled. 2. The switch is set as the Tail of Turbo Chain.
				Blinking at 4 Hz	1. Chain and the Chain has gone down. 2. The switch is set as the Turbo Chain's Member/ Head and the corresponding Tail-end Chain port is down.
				Off	When the switch disables the coupling or tail role of Turbo Chain.
SYNC	Synchroniz ation	1	N/A	N/A	Reserved
3-10	10M/100M/ 1000M RJ45 Top LED	1 for each	Green	On	When the port is active and links on 1000Mbps.
				Blinking	When the port's data is being transmitted at 1000Mbps.
				Off	When the port is inactive or link is down.
	10M/100M/ 1000M RJ45 Bottom LED	1 for each	Amber	On	When the port is active and links on 10/100Mbps.
				Blinking	When the port's data is being transmitted at 10/100Mbps.
				Off	When the port is inactive or link is down.
1-2	100M/1000 M SFP Port	1 for each	Green	On	When the port is active and links on 1,000Mbps.
				Blinking	When the port's data is being transmitted at 1,000Mbps.
				Off	When the port is inactive or link is down.
			Amber	On	When the port is active and links on 100Mbps.
				Blinking	When the port's data is being transmitted at 100Mbps.
				Off	When the port is inactive or link is down.

65M-5290-CT-T

Front view

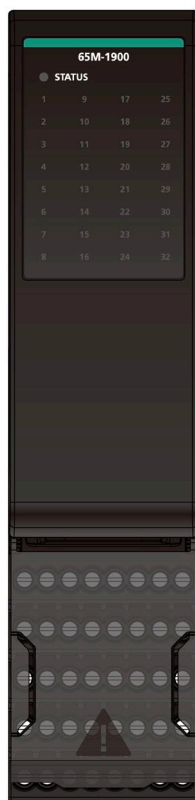


LED Definition

Labeling	Indication	Qty	Color	Behavior	Description
STATUS	Module status	1	Green	Blinking at 0.5 Hz	Module starts up
				On	Module operates normally
				Double Blinking	Locate
				Blinking at 5 Hz	Firmware upgrade in process
			Red	On	Startup failed or other component error
				Blinking at 5 Hz	Connection to CPU lost
PREV	PREV status	1	Green	Blinking at 0.5 Hz	Firmware upgrade failed
				On	• Module starts up • I/O link connection established between the client PRE and server NEXT
NEXT	NEXT status	1	Green	Blinking at 0.5 Hz	Acting as the client PREV module without an active IO link
				On	• Module Startup • IO link connection established between the client NEXT and server PREV
NEXT	NEXT status	1	Green	Blinking at 0.5 Hz	Acting as the client NEXT module without an active I/O link
				On	• Module Startup • IO link connection established between the client NEXT and server PREV

65M-1900-CT-T

Front View

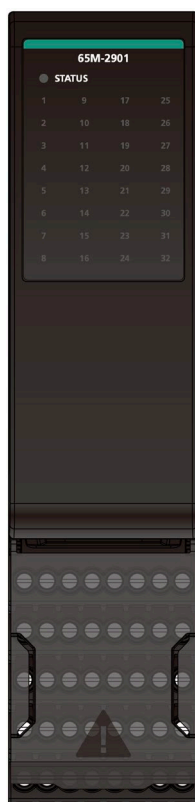


LED Definition

Labeling	Indication	Qty	Color	Behavior	Description
STATUS	System status	1	Green	On	Normal
				Blinking at 5 Hz	Firmware upgrade in progress
				Blinking at 0.5 Hz	Booting up
				Double Blinking	Module located
			Red	On	System failure
				Blinking at 5 Hz	Lost the connection to CPU
				Blinking at 0.5 Hz	Diagnostic failure
1-32	DI channels	1 for each	Double Blinking	No field power	
			Green	On	ON
			Red	On	Diagnostic error
			Off		OFF/Inactive

65M-2901-CT-T

Front View

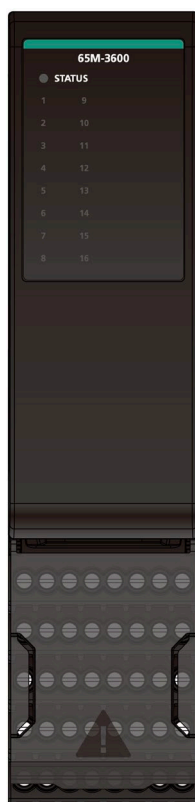


LED Definition

Labeling	Indication	Qty	Color	Behavior	Description
STATUS	System status	1	Green	On	Normal
				Blinking at 5 Hz	Firmware upgrade in progress
				Blinking at 0.5 Hz	Booting up
				Double Blinking	Module located
			Red	On	System failure
				Blinking at 5 Hz	Failsafe mode
				Blinking at 0.5 Hz	Diagnostic failure
				Double Blinking	No field power
1-32	DO channels	1 for each	Green	On	ON
			Red	On	Diagnostic error
			Off		OFF/Inactive

65M-3600-CT-T

Front view



LED Definition

Labeling	Indication	Qty	Color	Behavior	Description
STATUS	System status	1	Green	On	Normal
				Blinking at 5 Hz	Firmware upgrade in progress
				Blinking at 0.5 Hz	Booting up
				Double Blinking	Module located
			Red	On	System failure
				Blinking at 5 Hz	Lost the connection to CPU
				Blinking at 0.5 Hz	Diagnostic failure
1-16	AI channels	1 for each	Double Blinking	No field power	
			Green	On	ON
			Red	On	Diagnostic error
			Off		Inactive

65M-3610-CT-T

Front View

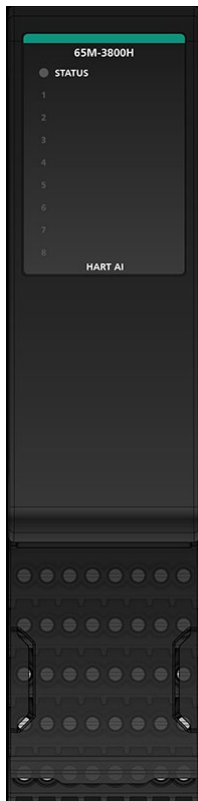


LED Definition

Labeling	Indication	Qty	Color	Behavior	Description
STATUS	System status	1	Green	On	Normal
				Blinking at 5 Hz	Firmware upgrade in progress
				Blinking at 0.5 Hz	Booting up
				Double Blinking	Module located
			Red	On	System failure
				Blinking at 5 Hz	Lost the connection to CPU
				Blinking at 0.5 Hz	Diagnostic failure
1-16	AI channels	1 for each	Double Blinking	No field power	
			Green	On	ON
			Red	On	Diagnostic error
			Off		Inactive

65M-3800H-CT-T

Front View



LED Definition

Labeling	Indication	Qty	Color	Behavior	Description
STATUS	System status	1	Green	On	Normal
				Blinking at 5 Hz	Firmware upgrade in progress
				Blinking at 0.5 Hz	Booting up
				Double Blinking	Module located
			Red	On	System failure
				Blinking at 5 Hz	Lost the connection to CPU
				Blinking at 0.5 Hz	Diagnostic failure
1-8	AI channels	1 for each	Double Blinking	No field power	
			Green	On	ON
			Red	On	Diagnostic error
			Off		Inactive

65M-4820-CT-T

Front View

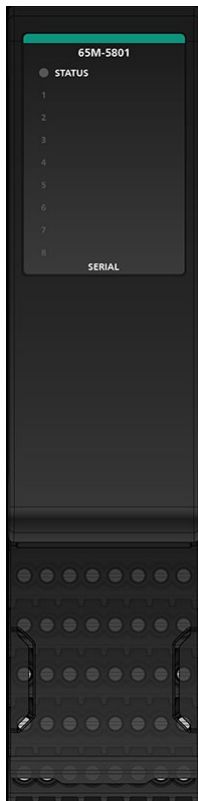


LED Definition

Labeling	Indication	Qty	Color	Behavior	Description
STATUS	System status	1	Green	On	Normal
				Blinking at 5 Hz	Firmware upgrade in progress
				Blinking at 0.5 Hz	Booting up
				Double Blinking	Module located
			Red	On	System failure
				Blinking at 5 Hz	Failsafe mode
				Blinking at 0.5 Hz	Diagnostic failure
				Double Blinking	No field power
1-8	AO channels	1 for each	Green	On	ON
			Red	On	Diagnostic error
			Off		Inactive

65M-5801-CT-T

Front View



LED Definition

Labeling	Indication	Qty	Color	Behavior	Description
STATUS	System status	1	Green	On	Normal
				Blinking at 5 Hz	Firmware upgrade in progress
				Blinking at 0.5 Hz	Booting up
				Double Blinking	Module located
			Red	On	System failure
				Blinking at 5 Hz	Failsafe mode
				Blinking at 0.5 Hz	Diagnostic failure
				Double Blinking	No field power
1-8	Serial channels	1 for each	Green	Blinking at 0.5 Hz	Tx
			Red		Rx
			Off		Inactive

I/O Pin Definitions

The terminal blocks of ioPAC 6500 Series have 40 pins. The pin definitions of each module are listed in the following.

65M-TB-1900

5	10	15	20	25	30	35	40
FCS	FCS	GND	GND	NC	NC	NC	NC
4	9	14	19	24	29	34	39
DI4	DI8	DI12	DI16	DI20	DI24	DI28	DI32
3	8	13	18	23	28	33	38
DI3	DI7	DI11	DI15	DI19	DI23	DI27	DI31
2	7	12	17	22	27	32	37
DI2	DI6	DI10	DI14	DI18	DI22	DI26	DI30
1	6	11	16	21	26	31	36
DI1	DI5	DI9	DI13	DI17	DI21	DI25	DI29

65M-TB-2901

5	10	15	20	25	30	35	40
V+	V+	V-	V-	NC	NC	NC	NC
4	9	14	19	24	29	34	39
DO4	DO8	DO12	DO16	DO20	DO24	DO28	DO32
3	8	13	18	23	28	33	38
DO3	DO7	DO11	DO15	DO19	DO23	DO27	DO31
2	7	12	17	22	27	32	37
DO2	DO6	DO10	DO14	DO18	DO22	DO26	DO30
1	6	11	16	21	26	31	36
DO1	DO5	DO9	DO13	DO17	DO21	DO25	DO29

65M-TB-3600

5	10	15	20	25	30	35	40
LS1+	LS1+	LS1-	LS1-	LS2+	LS2+	LS2-	LS2-
4	9	14	19	24	29	34	39
AI4+	AI4-	AI8+	AI8-	AI12+	AI12-	AI16+	AI16-
3	8	13	18	23	28	33	38
AI3+	AI3-	AI7+	AI7-	AI11+	AI11-	AI15+	AI15-
2	7	12	17	22	27	32	37
AI2+	AI2-	AI6+	AI6-	AI10+	AI10-	AI14+	AI14-
1	6	11	16	21	26	31	36
AI1+	AI1-	AI5+	AI5-	AI9+	AI9-	AI13+	AI13-

65M-TB-3610

5	10	15	20	25	30	35	40
NC	NC	NC	NC	NC	NC	NC	NC
4	9	14	19	24	29	34	39
AI4+	AI4-	AI8+	AI8-	AI12+	AI12-	AI16+	AI16-
3	8	13	18	23	28	33	38
AI3+	AI3-	AI7+	AI7-	AI11+	AI11-	AI15+	AI15-
2	7	12	17	22	27	32	37
AI2+	AI2-	AI6+	AI6-	AI10+	AI10-	AI14+	AI14-
1	6	11	16	21	26	31	36
AI1+	AI1-	AI5+	AI5-	AI9+	AI9-	AI13+	AI13-

65M-TB-3800H

5	10	15	20	25	30	35	40
LS+	LS+	LS-	LS-	NC	NC	NC	NC
4	9	14	19	24	29	34	39
AI4+	AI4-	AI8+	AI8-	NC	NC	NC	NC
3	8	13	18	23	28	33	38
AI3+	AI3-	AI7+	AI7-	NC	NC	NC	NC
2	7	12	17	22	27	32	37
AI2+	AI2-	AI6+	AI6-	NC	NC	NC	NC
1	6	11	16	21	26	31	36
AI1+	AI1-	AI5+	AI5-	NC	NC	NC	NC

65M-TB-4820

5	10	15	20	25	30	35	40
NC	NC	NC	NC	NC	NC	NC	NC
4	9	14	19	24	29	34	39
IO2+	IO2-	IO4+	IO4-	IO6+	IO6-	IO8+	IO8-
3	8	13	18	23	28	33	38
VO2+	VO2-	VO4+	VO4-	VO6+	VO6-	VO8+	VO8-
2	7	12	17	22	27	32	37
IO1+	IO1-	IO3+	IO3-	IO5+	IO5-	IO7+	IO7-
1	6	11	16	21	26	31	36
VO1+	VO1-	VO3+	VO3-	VO5+	VO5-	VO7+	VO7-

65M-TB-5801

RS-232

5	10	15	20	25	30	35	40
GND1	GND1	GND1	GND1	GND2	GND2	GND2	GND2
4	9	14	19	24	29	34	39
CTS1	CTS2	CTS3	CTS4	CTS5	CTS6	CTS7	CTS8
3	8	13	18	23	28	33	38
RTS1	RTS2	RTS3	RTS4	RTS5	RTS6	RTS7	RTS8
2	7	12	17	22	27	32	37
Rx1	Rx2	Rx3	Rx4	Rx5	Rx6	Rx7	Rx8
1	6	11	16	21	26	31	36
Tx1	Tx2	Tx3	Tx4	Tx5	Tx6	Tx7	Tx8

RS-422

5	10	15	20	25	30	35	40
GND1	GND1	GND1	GND1	GND2	GND2	GND2	GND2
4	9	14	19	24	29	34	39
Rx1-	Rx2-	Rx3-	Rx4-	Rx5-	Rx6-	Rx7-	Rx8-
3	8	13	18	23	28	33	38
Rx1+	Rx2+	Rx3+	Rx4+	Rx5+	Rx6+	Rx7+	Rx8+
2	7	12	17	22	27	32	37
Tx1-	Tx2-	Tx3-	Tx4-	Tx5-	Tx6-	Tx7-	Tx8-
1	6	11	16	21	26	31	36
Tx1+	Tx2+	Tx3+	Tx4+	Tx5+	Tx6+	Tx7+	Tx8+

RS-485-2w

5	10	15	20	25	30	35	40
GND1	GND1	GND1	GND1	GND2	GND2	GND2	GND2
4	9	14	19	24	29	34	39
D1-	D2-	D3-	D4-	D5-	D6-	D7-	D8-
3	8	13	18	23	28	33	38
D1+	D2+	D3+	D4+	D5+	D6+	D7+	D8+
2	7	12	17	22	27	32	37
NC	NC	NC	NC	NC	NC	NC	NC
1	6	11	16	21	26	31	36
NC	NC	NC	NC	NC	NC	NC	NC

3. Hardware Installation

In this chapter, we describe how to install the ioPAC 6500 Series devices.

Mounting the Unit

In this section, we describe how to mount the devices and how to dismount the device.



NOTE

ioPAC 6500 Series supports the following modules, collecting all the modules you need before installing the system.

- CPU module
- Power module
- Backplane module for CPU
- Backplane module for power
- Communication (switch) module (optional, based on the application)
- IO module (optional, based on the application)
- Backplane module for communication (switch) (optional, based on the application)
- Backplane module for IO (optional, based on the application)
- Terminal block (TB) module for IO (optional, based on the application)
- Backplane module for expansion
- Expansion (optional, based on the application)

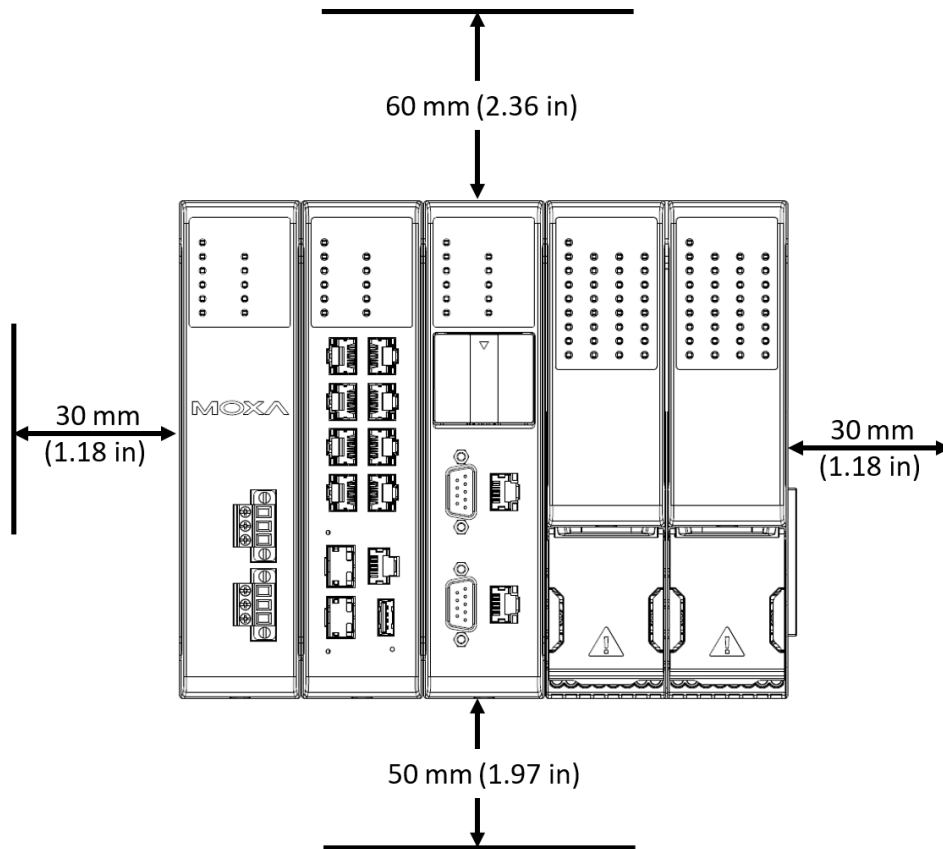


NOTE

The ioPAC 6500 Series needs to be installed by the order: **Power Module > communication(switch) Module (optional) > CPU Module > Expansion Module (optional) > IO Module (optional)**

Horizontal Installation

Before mounting the device onto the DIN rail, make sure that there is enough space around the device so that heat generated from the system can be dissipated. The suggested space dimension is shown below.



CAUTION

DO NOT install the device upright, as the fanless heat dissipation design will not perform as intended.

Installing the System on the DIN Rail

Follow the steps to mount the modules onto the DIN rail.

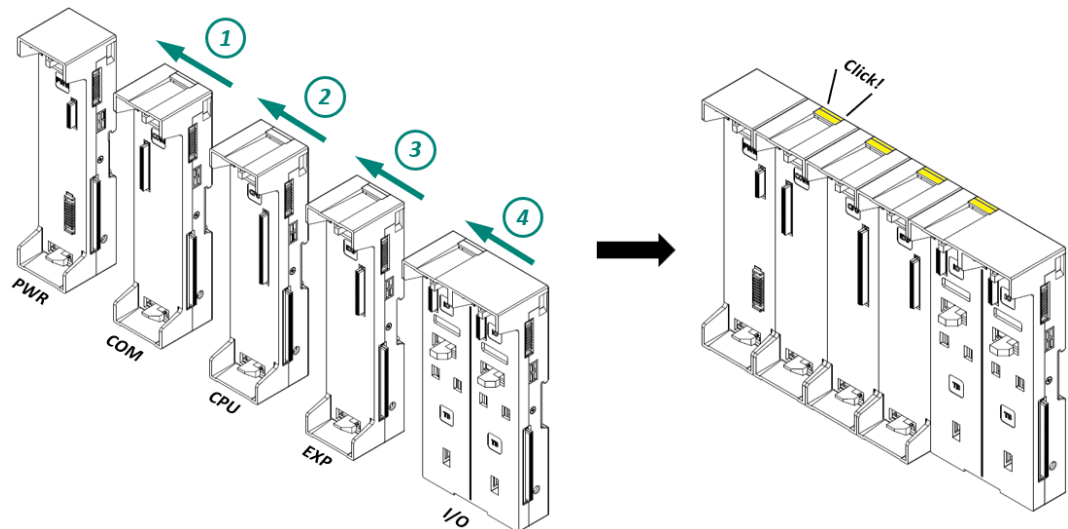


NOTE

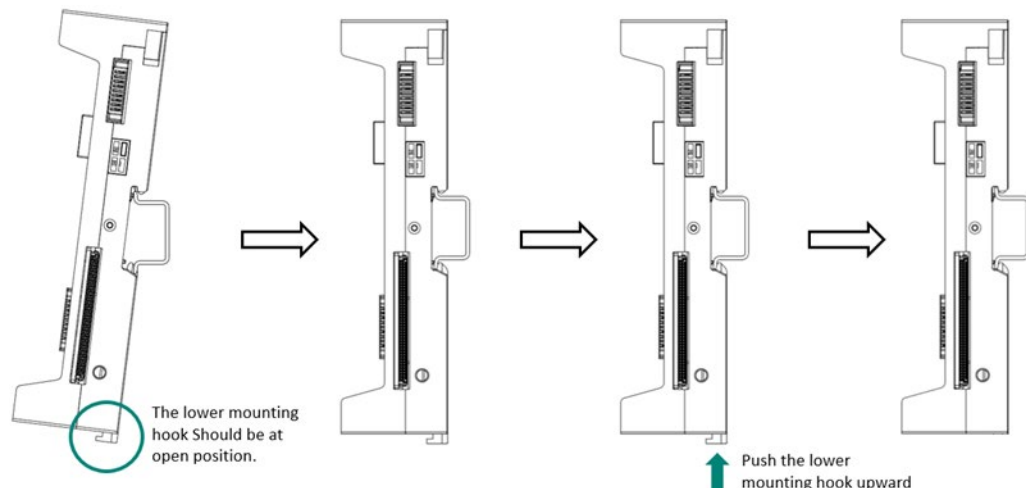
Use a DIN rail with a thickness of 1.5 mm and made of stainless steel to ensure a safe installation.

The demonstrated configuration includes one power module, one communication module (Switch), one CPU module, one expansion module, and two IO modules.

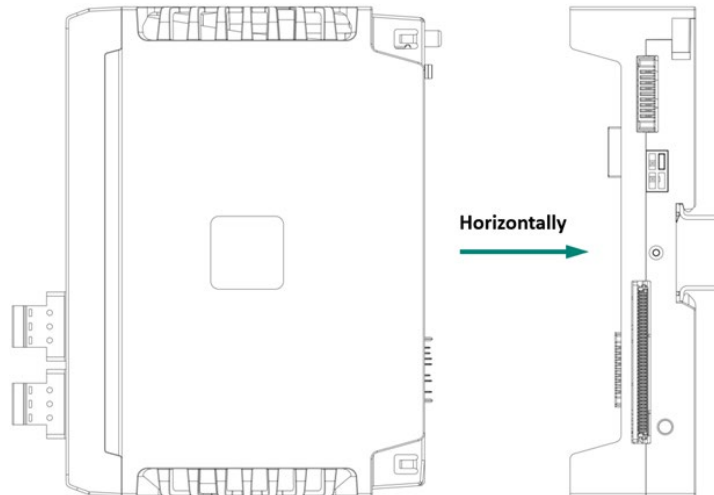
Step 1: Assemble all the backplane modules you need all at once before mounting them onto the DIN-rail. Follow the order: Power Module > Communication Module (Switch) > CPU Module > Expansion Module > IO Module. When hearing a "click" from the top clip, meaning the backplane modules are connected.



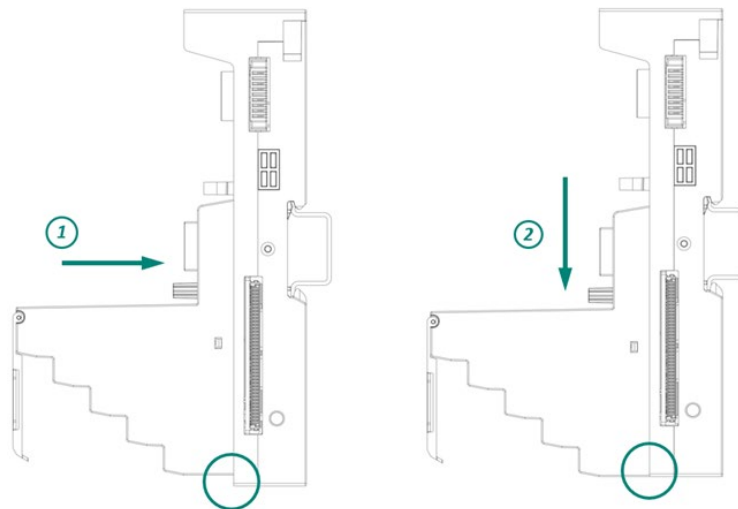
Step 2: Mount the upper mounting hook of all assembled backplanes onto the DIN rail while making sure the lower mounting hook of it is at an open position as shown below (side view). Push the assembled backplane towards the DIN rail, then push the lower mounting hook upward until latch so that all the backplane modules are fixed in position.



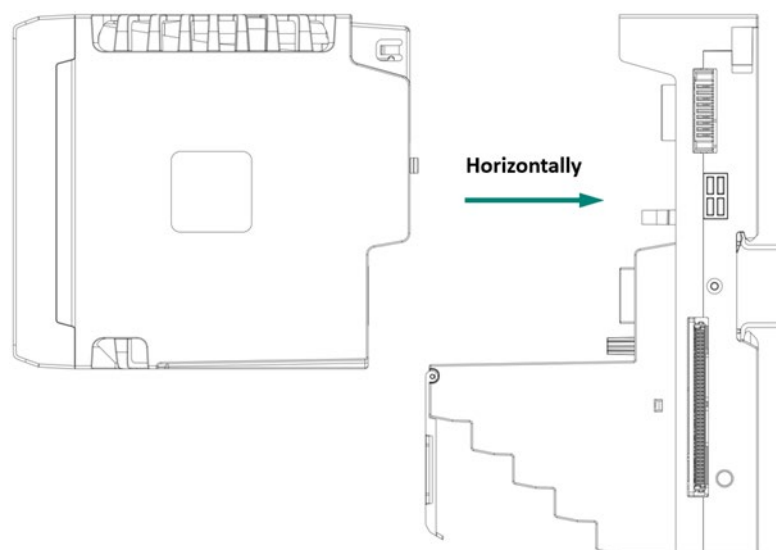
Step 3: Hold the Power module with two hands and install onto the power backplane module vertically. As with the CPU module, also the expansion module and communication module (if applicable).



Step 4: Place the terminal block module on the I/O backplane module, then pull down the TB module to fix the position.



Step 5: Hold the I/O module and install it onto the I/O backplane module horizontally. Note that there is a poka-yoke design to make sure the I/O module is installed on the correct terminal block.



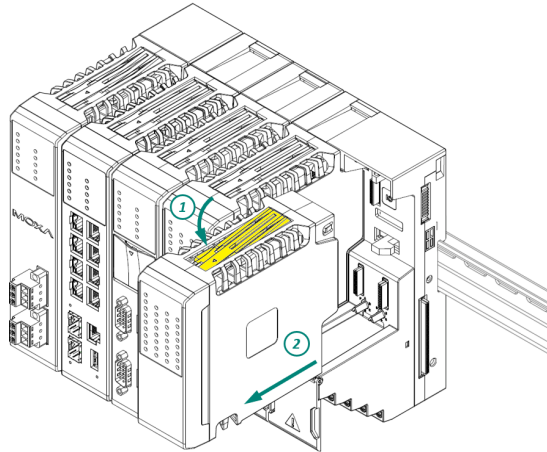
Unmounting the System from a DIN Rail

Follow the steps to demount the modules from the DIN rail.

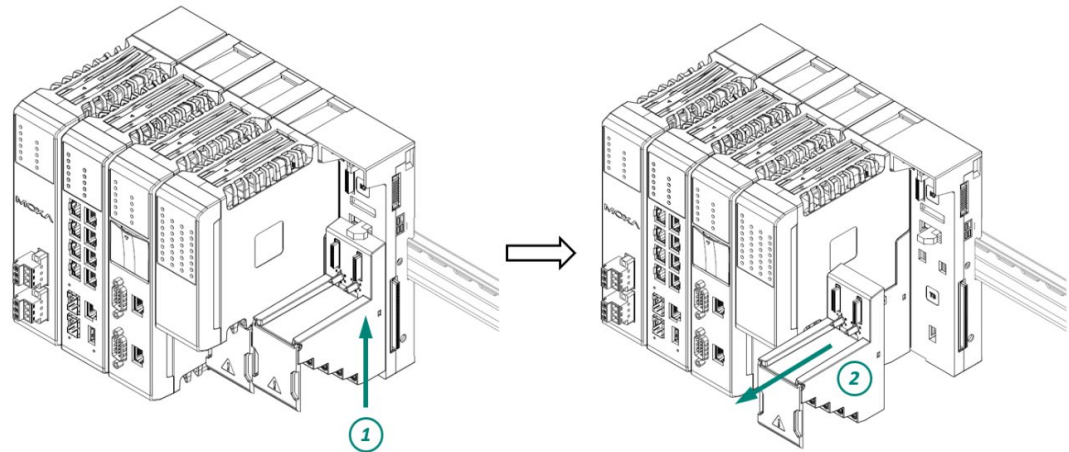
The demonstrated configuration includes 1 power module, 1 communication module (switch), 1 CPU module, and 2 IO modules.

Step 1: Turn off the power to shut down the system.

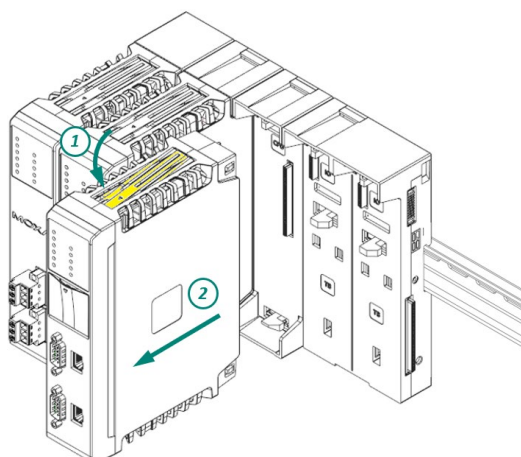
Step 2: Press the release tab on top of the IO module, then remove the I/O module from the backplane as shown below.



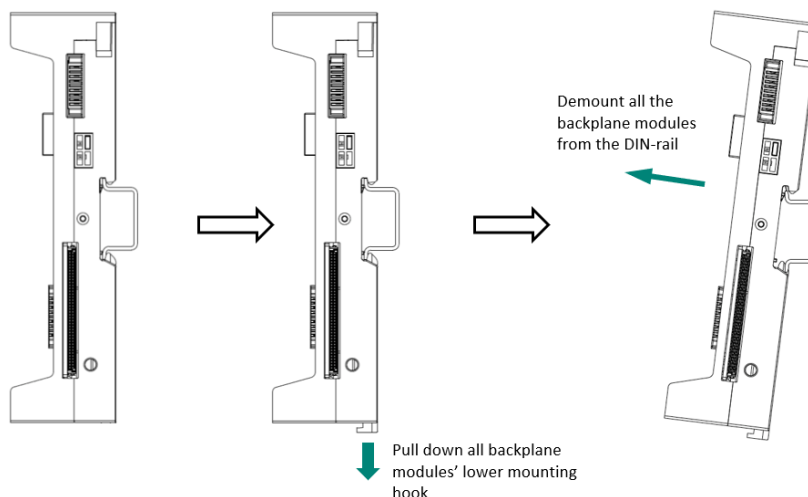
Step 3: Pull up the terminal block module, then remove it from the backplane.



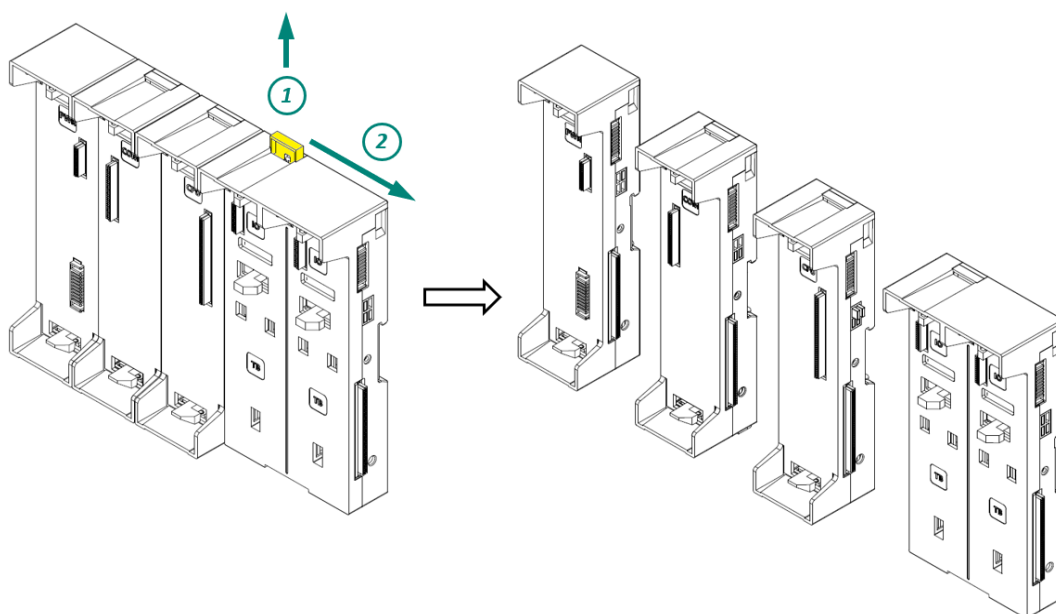
Step 4: Press the release tab on top of the CPU module, then remove the CPU module from the backplane horizontally. Remove the module with two hands to prevent dropping. Repeat the same procedure for removing the switch and power module as well.



Step 5: Pull down all backplane modules' lower mounting hook as shown below, then demount all the backplane modules from the DIN rail.



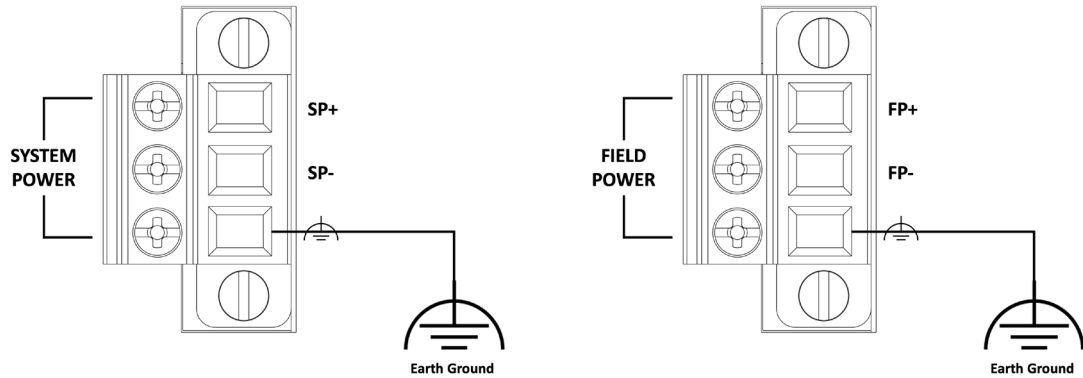
Step 6: Pull up the top clip (yellow part) of the IO backplane module to disassemble. Repeat the procedure for the CPU backplane and switch the backplane module.



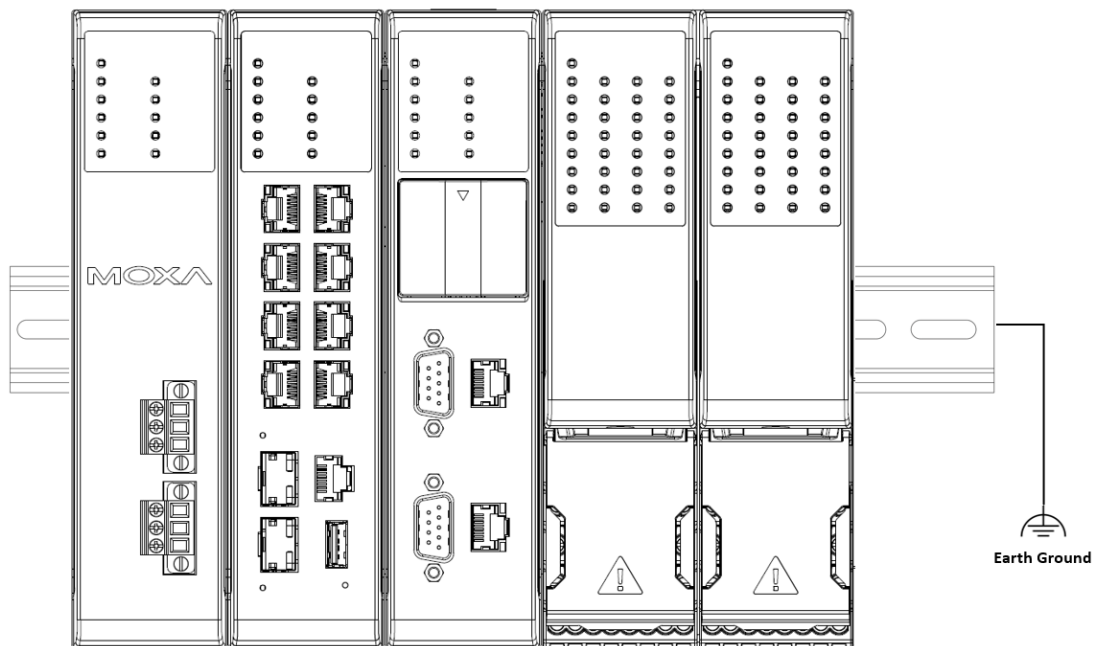
Grounding the System

Ensure that you properly ground the system. There are three places that should be grounded as shown below. Use the different power supplies for system and field power to ensure the system and I/Os are isolated.

The first and second grounding points are the earth ground pin of the system, and field power connector.



The third grounding point is on the back side of each backplane module. The grounding spring will be connected to the DIN rail directly when successfully mounted.



Wiring System and Field Power

Wire range: 12 to 18 AWG (ferrule diameter: 2.0 to 1.0 mm)

Wire strip length: 12 to 13 mm

Unit: mm (in.)

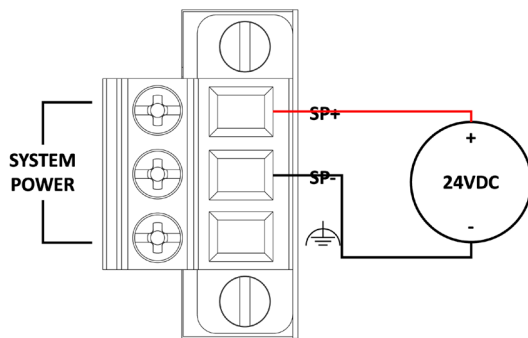


NOTE

We recommend using different power supplies for system power and field power to ensure the system and I/Os are isolated.

System Power

The system requires a 24-VDC system power input. The system powers this system via an internal bus, which is on the backplane module.

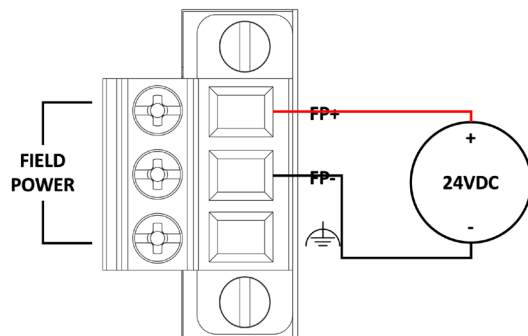


NOTE

The suggested tightening torque: 5.0 kgf-cm.

Field Power

The ioPAC 6500 provides a field power input of 24 VDC that powers up the IO circuit inside the I/O module through the internal bus.

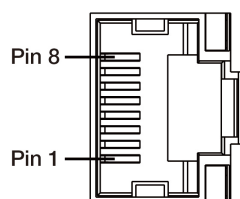


NOTE

The suggested tightening torque: 5.0 kgf-cm.

Wiring Ethernet Ports

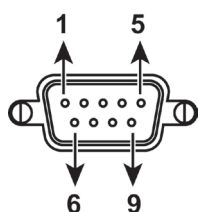
The maximum cable length is 100 m (350 feet), but the actual limit for your application could be longer or shorter depending on the amount of electrical noise in the environment. To minimize the amount of noise, Ethernet cables should not run parallel to power cables or other types of cables that generate electrical noise. The following diagram and table show the pin assignments for the RJ45 Ethernet ports:



Pin	Media Direct Interface Signal
1	TRD(0)+
2	TRD(0)-
3	TRD(1)+
4	TRD(2)+
5	TRD(1)-
6	TRD(2)-
7	TRD(3)+
8	TRD(3)-

Wiring Serial Port(s)

The ioPAC 6500 is equipped with two 3-in-1 serial ports that support RS-232/422/485, making it more convenient to connect field serial devices.



Pin	RS-232	RS-422	2-wire RS-485
1	DCD	TxD-(A)	-
2	RXD	TxD+(B)	-
3	TXD	RxD+(B)	Data+(B)
4	DTR	RxD-(A)	Data-(A)
5	GND	GND	GND
6	DSR	-	-
7	RTS	-	-
8	CTS	-	-
9	RI	-	-

Wiring the Fiber Port(s)

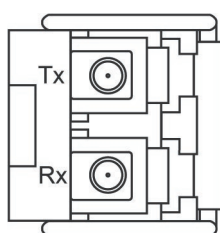
100/1000BaseSFP (mini-GBIC) Fiber Port

The Gigabit Ethernet fiber ports on the switch are 100/1000BaseSFP fiber ports, which must use 100/1000M mini-GBIC fiber transceivers to work properly.

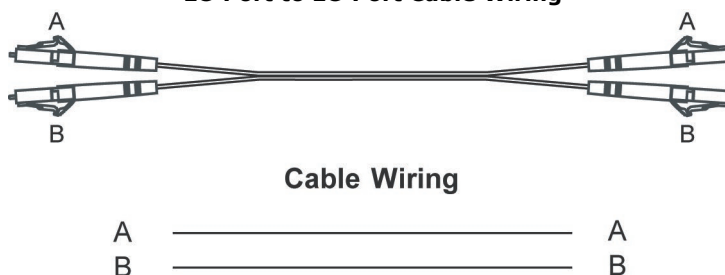
The concept behind the LC port and cable is straightforward. Suppose you are connecting devices I and II. Contrary to electrical signals, optical signals do not require a circuit to transmit data. Consequently, one of the optical lines is used to transmit data from device I to device II, and the other optical line is used to transmitting data from device II to device I for full-duplex transmission.

Remember to connect the Tx (transmit) port of device I to the Rx (receive) port of device II, and the Rx (receive) port of device I to the Tx (transmit) port of device II. If you make your own cable, we suggest labeling the two sides of the same line with the same letter (A-to-A and B-to-B, as shown below, or A1-to-A2 and B1-to-B2).

LC-Port Pinouts



LC-Port to LC-Port Cable Wiring

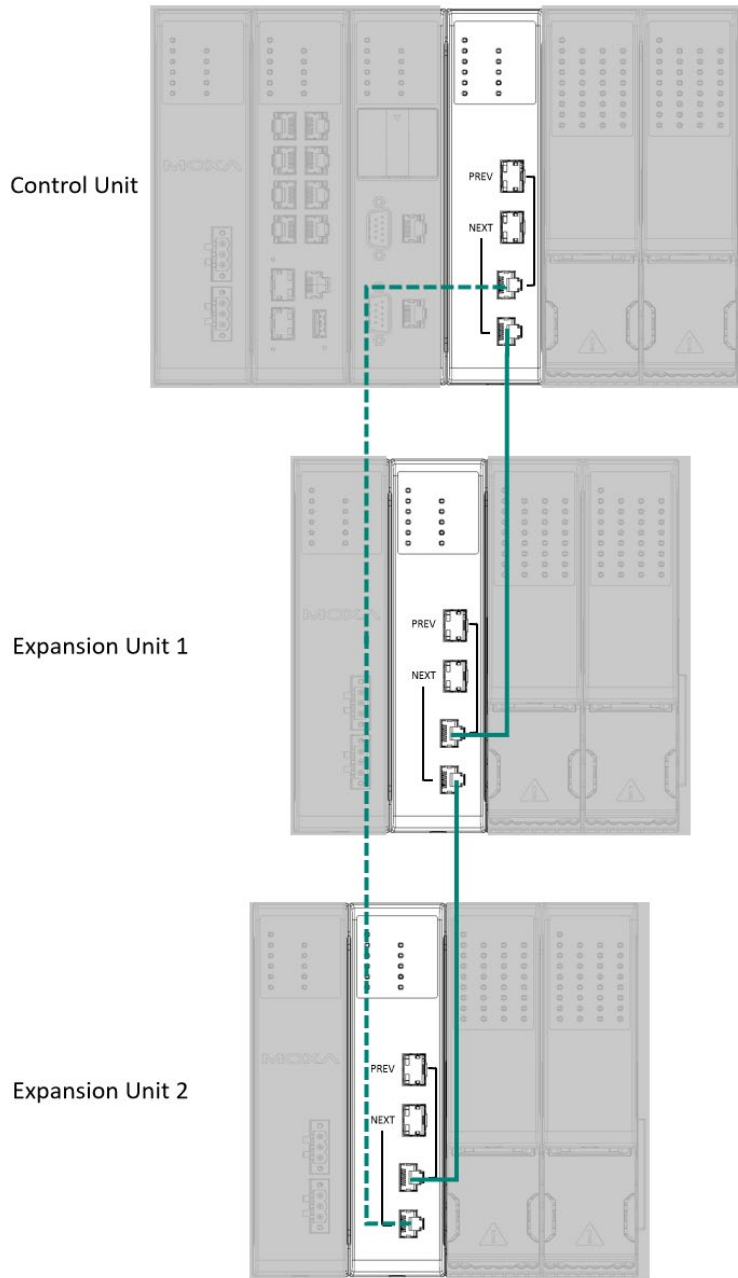


Connecting Expansion Module

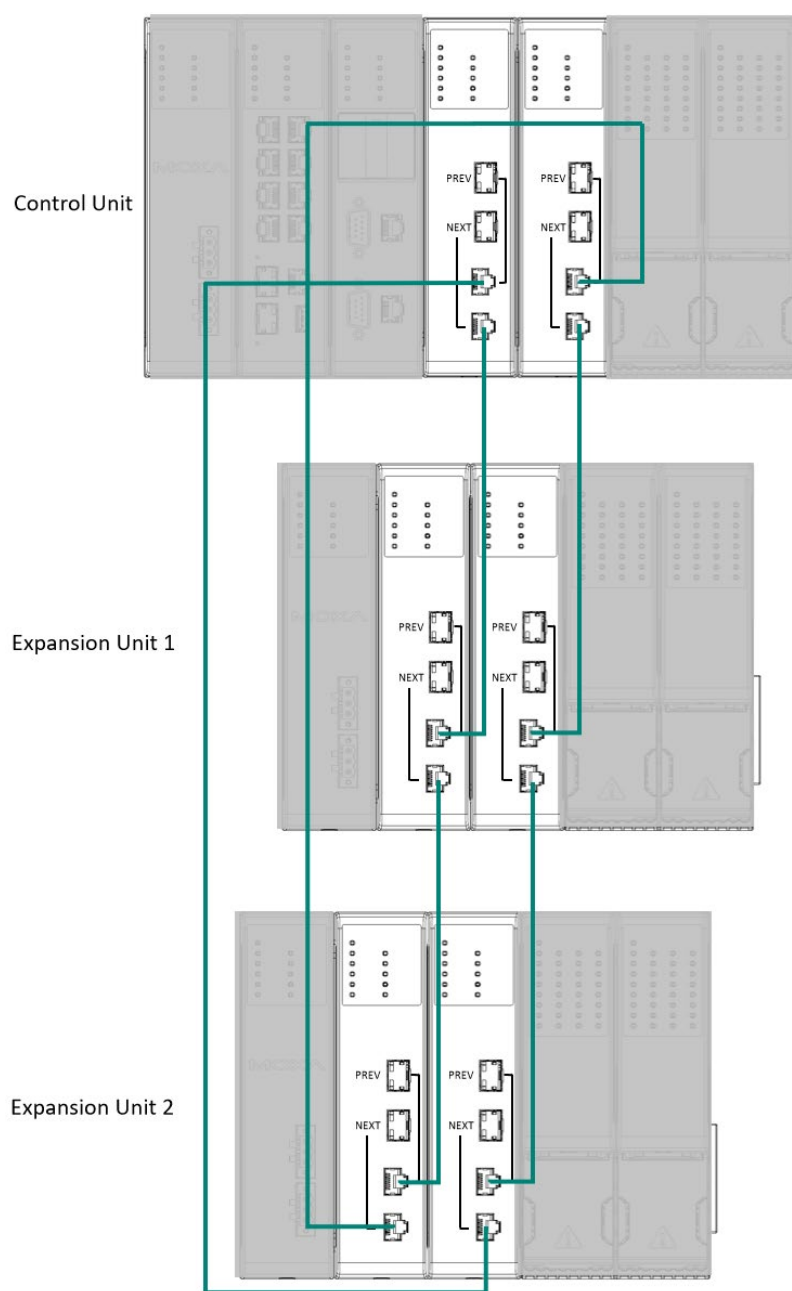
The ioPAC 6500 supports expansion modules, ensuring the expandability of the system. The connecting method shown below ensures redundancy. However, if no expansion unit is required, do not install expansion modules on the control unit.

1 Expansion module per Unit Ring Topology — Redundancy for single cable failure. Please be noted, data will be lost during expansion module hot swapping.

Daisy-chain: Without the dashed line.



2 Expansion modules per Unit Ring Topology — Redundancy for single-cable or single-module failure. We recommend employing this structure for critical applications, as it provides higher level of communication reliability between Control unit and Expansion Units.



ATTENTION

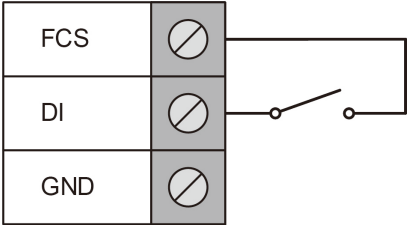
This is a Class 1 Laser/LED product. To avoid causing serious damage to your eyes, do not stare directly into the laser beam.

Wiring I/O Channels

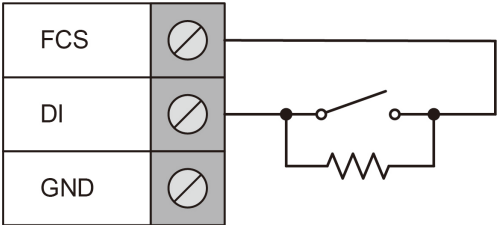
The ioPAC 6500 supports general DI, DO, AI, AO channels, which can be used to collect the data in the field site.

65M-1900-CT-T

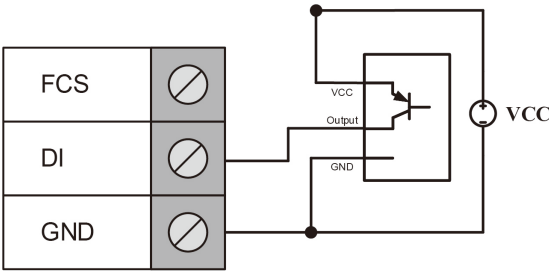
Dry Contact



Dry Contact (with Wire Break Diagnostic)

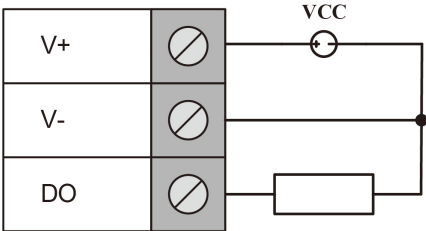


Wet Contact

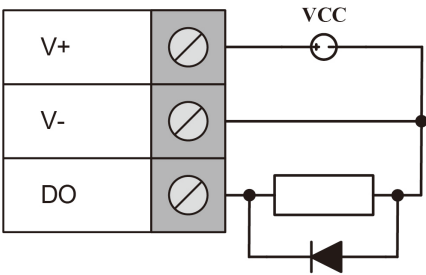


65M-2901-CT-T

Resistive Load



Inductive Load



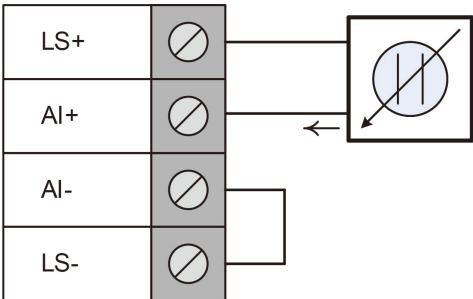
65M-3600-CT-T



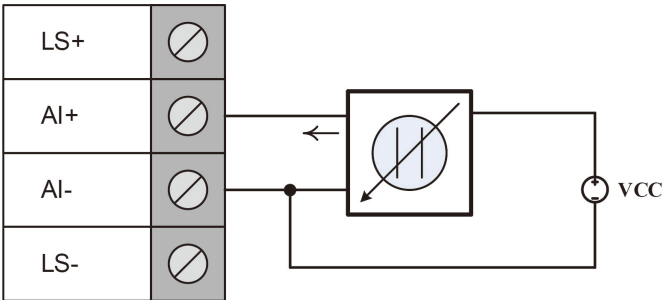
NOTE

LS1 should be wired with AI1-AI8 and LS2 should be wired with AI9-AI16.

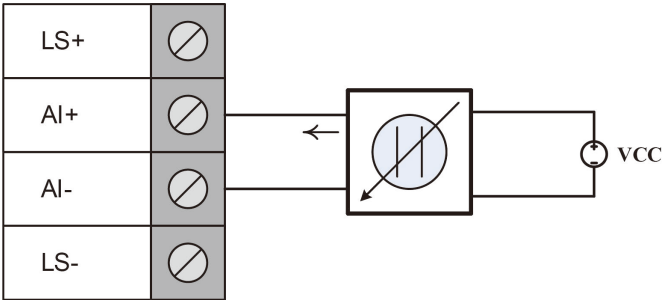
2-Wire Current Sensor



3-Wire Current Sensor

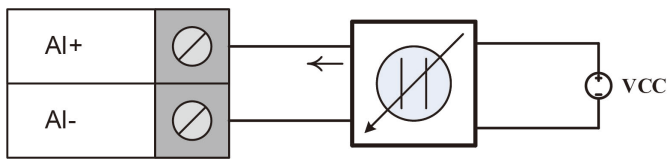


4-Wire Current Sensor



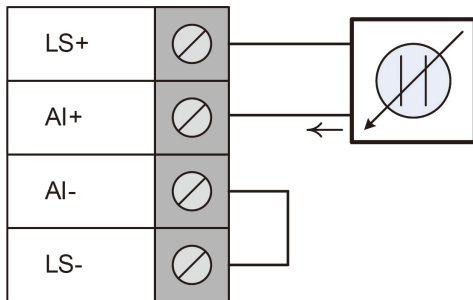
65M-3610-CT-T

4-Wire Voltage Sensor

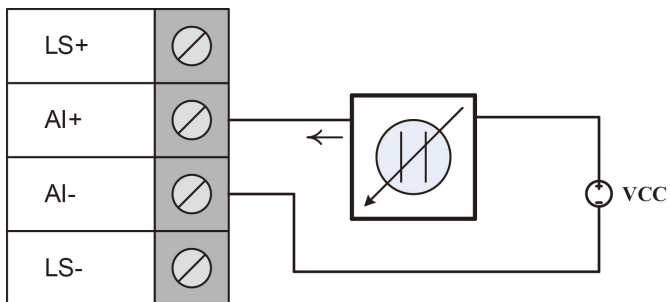


65M-3800H-CT-T

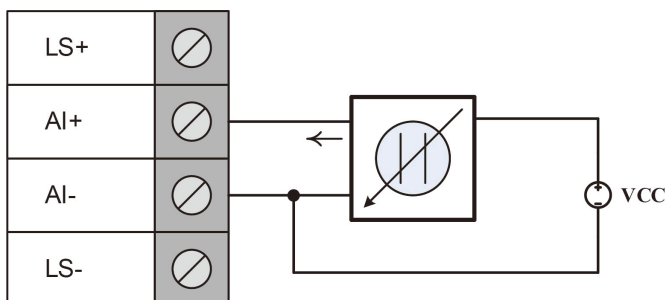
2-wire Current Sensor (Internal Loop Power)



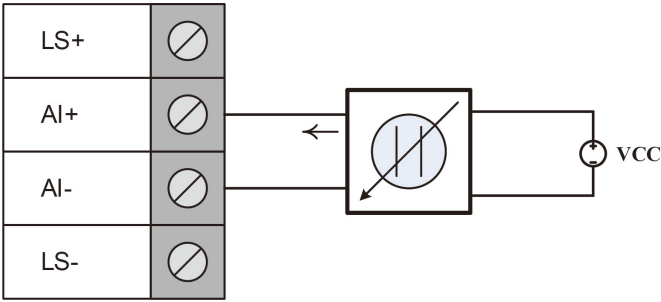
2-wire Current Sensor (External Loop Power)



3-wire Current Sensor

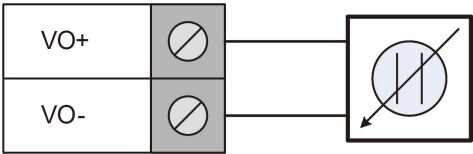


4-wire Current Sensor

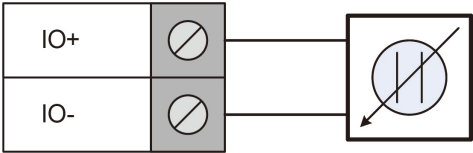


65M-4820-CT-T

Voltage Output

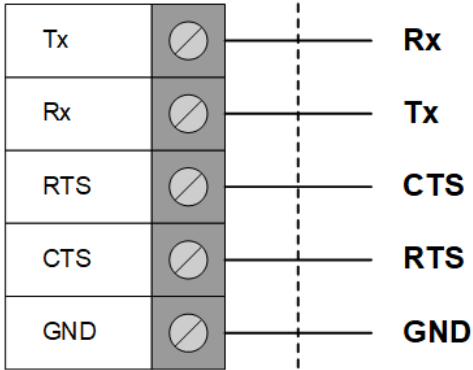


Current Output

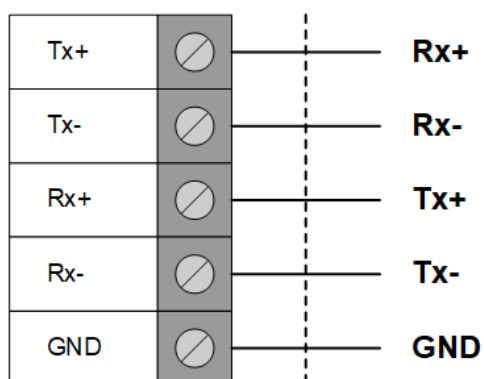


65M-5801-CT-T

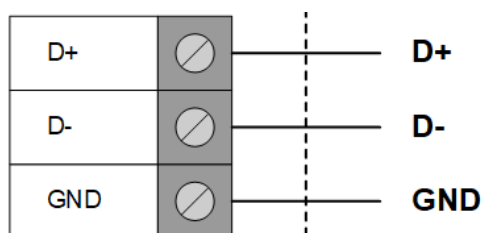
RS-232



RS-422

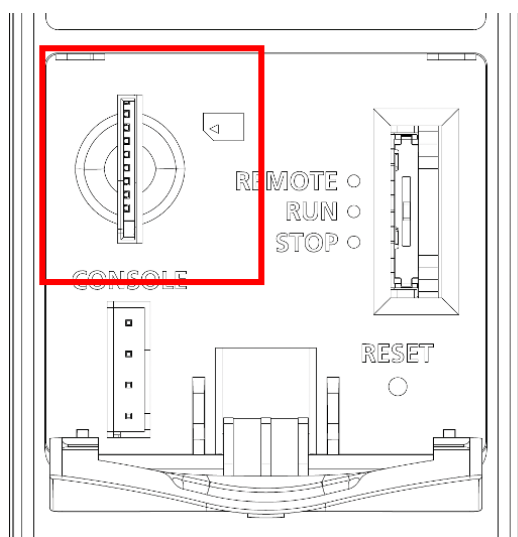


RS-485-2w



Inserting the microSD™ Card

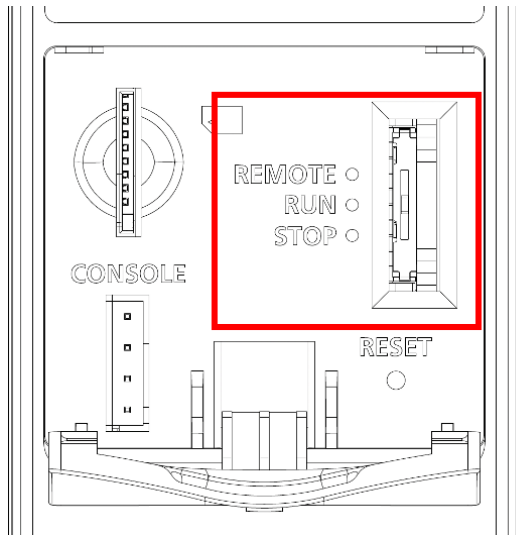
The ioPAC 6500 CPU module offers a microSD slot. This function is currently reserved. Open the cover on the CPU module, you can see the microSD slot inside.



Powering on the Unit

When all the installation and wiring are complete, you can turn on the power to boot up the system. After turning on the system power supply, it will take 90 seconds for the operating system to boot up. The green Ready LED will illuminate continuously until the operating system is ready.

Mode Switch



Open the cover on the CPU module, you can see the mode switch inside. The ioPAC 6500 CPU module offers a mode switch for you to change the system status.

Remote: the device is allowed to download the program and change the device setting remotely. The authorized user with secure access is required.

Run: The device is actively running the program. It rejects any attempt to interrupt the device running, either locally or over the network. The device information is set to read only.

Stop: The device will not execute the program in any condition. The authorized user is allowed to download the program and change the device setting.

The table shows which action can be performed in each mode.

	STOP	RUN	REMOTE – Run	REMOTE - STOP
IDE				
Configuration Download	Yes	No	Yes	Yes
Online Change	Yes	No	Yes	Yes
Firmware Upgrade	Yes	No	No	Yes
Warm / Cold Reboot	Yes	No	Yes	Yes
Force Output	Yes	Yes	Yes	Yes
Reset Warm, Reset Cold, Reset Origin	Yes	No	No	Yes
STOP COMMAND	No	No	Yes	No
Factory Default/ Device Decommission	Yes	No	No	Yes
Backup	Yes	Yes	Yes	Yes
Restore	Yes	No	Yes	Yes
Security Hot Plug	Yes	Yes	No	No
Web				
System Settings	Yes	View/Export only	Yes	Yes
Maintenance	Yes	View/Export only	Yes	Yes
Diagnostic	Yes	View/Export only	Yes	Yes
Certificate	Yes	View/Export only	Yes	Yes
Security	Yes	View/Export only	Yes	Yes

Reset Button: Reset Origin Device

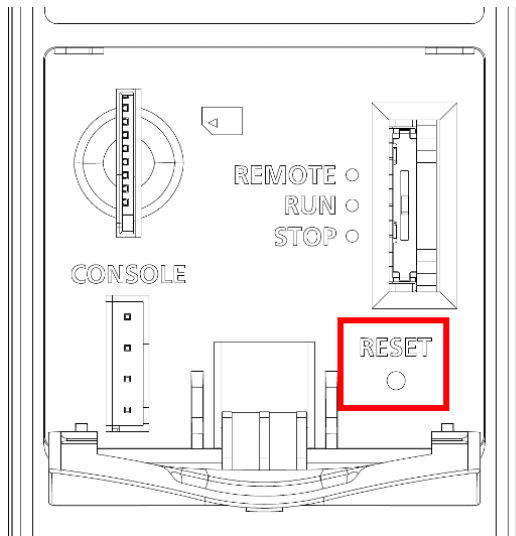
Open the cover on the CPU module; you can see the reset button inside. Follow the steps to perform **Reset Origin Device**, which will reset the whole system to its original status.

1. Keep pressing the reset button for **15 seconds**; the STATUS LED starts double blinking RED.
2. Releasing the reset button when the STATUS LED is double blinking RED, the ioPAC 6500 system will start to reset the system to its original status.



NOTE

Except for the system logs, all other data and settings of the system will be reset once Reset Origin Device is performed successfully.



4. Software Configuration

In this chapter, we introduce the web interface and serial console of the ioPAC 6500 CPU module.

Connecting the Web Interface

The Web Console is already embedded in the ioPAC 6500 system. Use the web console to check the device status, configure network settings, or update the firmware of the device. Follow the steps below to connect to the web interface.

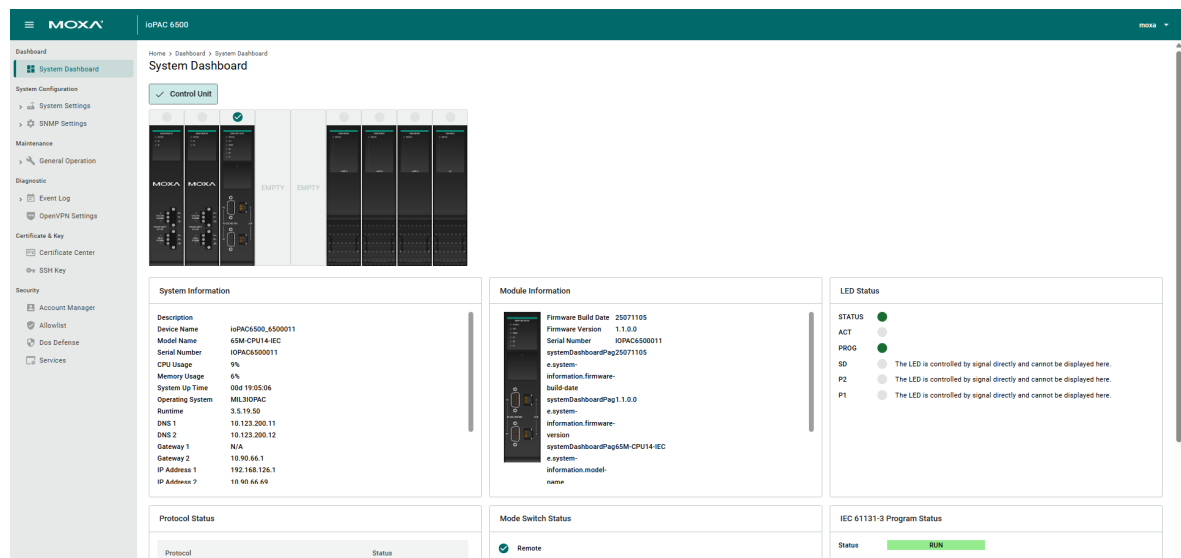
1. Connect the system to your PC through an Ethernet cable.
2. Power on the unit.
3. Open a web browser (Chrome is recommended) on your PC and type the default IP address shown on the model label of the unit.



INFORMATION

Type in the IP address (if the IP address is not set by default). If the IP address is not available, use the IINxpress utility to search for the device, or load the factory default settings by holding down the RESET button to access the device through the default IP address.

When you log into the system successfully, you will see the product page is composed of three parts.



1. **Title panel:** Provides the log out function. The login account will be shown at the top right corner.
2. **Menu panel:** Provides the access monitor the device status to configure functions or services.
3. **Information panel:** The device information associated with the functions selected in the menu panel.



NOTE

For security reasons, select Logout when no longer accessing this device. DO NOT leave the web interface unattended.

Dashboard

System Dashboard

System Dashboard is the first page when you log in the device. The dashboard provides information about the module information, panel status, service status, protocol status, and IEC 61131-3 program status.

On the top of the system dashboard, the system combination will be displayed. Select the Control Unit, Expansion Unit 1, etc. to check the system combination of each unit.



On the bottom of the system dashboard, the information will be displayed.

System Information

The system information will be displayed here. For example, device name, system status, Ethernet status, time status, etc.

Module Information

The information of the selected module will be displayed here. For example, model name, firmware version, serial number, etc.



NOTE

For detailed information on the switch module, check in the built-in web of the switch module.

LED Status

The LED status of all modules will be displayed here. For the LED definition, refer to the LED definition section.



NOTE

For the LED status of the switch module, check in the built-in web of switch module.

Mode Switch Status

The mode switch status will be displayed here. There are three statuses of mode switch.

Remote: The device is allowed to download the program and change the device setting remotely. An authorized user with secure access is required.

Run: The device is actively running the program. It rejects any attempt to download the program or change the device settings. The device information is set to read only.

Stop: The device will not execute the program in any condition. The authorized user is allowed to download the program and change the device setting.

Protocol Status

The status of all protocol services will be displayed here. There are three statuses.

Run: the service is running.

Stop: the service is stopped.

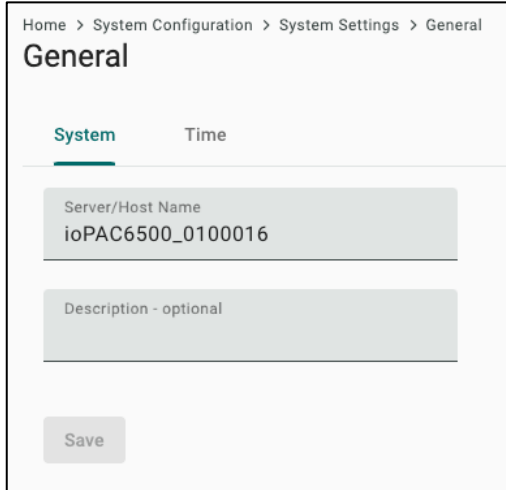
Disable: the service is currently disabled.

IEC 61131-3 Program Status

The IEC engine status will be displayed here. **RUN** and **STOP** are two statuses for you to identify if the engine is running or not.

System Configuration

System Settings—General



The screenshot shows a web interface for system configuration. At the top, a breadcrumb trail reads: Home > System Configuration > System Settings > General. Below this, the title 'General' is displayed. There are two tabs: 'System' (which is selected and underlined) and 'Time'. Under the 'System' tab, there are two input fields. The first is labeled 'Server/Host Name' and contains the text 'ioPAC6500_0100016'. The second is labeled 'Description - optional' and is currently empty. At the bottom left of the form area is a 'Save' button.

Go to **System Settings > General > System** to specify a new device name and enter a description for the device.

Device Name: Set enter a name to identify the whole ioPAC 6500 system. The maximum length is 64 characteristics, alphanumeric, and special characteristics are allowed.

Description: Extra information for you to better identify the device.

Go to **System Settings > General > Time** to set up the time of the device.

Home > System Configuration > System Settings > General

General

System

Time

Current date and time: May 24, 2024 15:07:28

Time Zone

(GMT+08:00)Taipei

Daylight Saving Time

☐

Enable

☒

Disable

DNP3 Sync Time: Off

Sync Mode

☐

Manual

☒

Auto

Time Server

pool.ntp.org

NTP Authentication

☐

NTP Authentication

Save

The current data and time will be displayed here.



NOTE

The current date and time are based on the system setting.

Time Zone: Specify the time zone where the devices is located.

Daylight Saving Time

☒

Enable

☐

Disable

Start

Month

4

Week

5

Day

0

Hour

0

End

Month

11

Week

1

Day

0

Hour

0

Offset

+01:00

Daylight Saving Time: Enable and enter the daylight-saving time of the device.



NOTE

0 to 6 in Day represents Sunday to Saturday, respectively.

The screenshot shows the 'Sync Mode' configuration interface. At the top, there are two radio buttons: 'Manual' (selected) and 'Auto'. Below this is a section titled 'Sync with browser' with a refresh icon. Inside this section, there is a 'Date' field showing '5/27/2024' with a calendar icon. Below the date are three fields for 'Hour' (13), 'Minute' (30), and 'Second' (9), separated by colons.

Sync Mode: How to sync up the device time. In **Auto** mode, the device will sync with the time server you specified automatically. In **Manual** mode, select  Sync with browser icon to sync with the browser, or input a specific time.

The screenshot shows the 'Create Key' screen. It has three input fields: 'Key ID' with the value '1', 'Hash Type' with the value 'MD5', and 'Password' with masked characters '....'. Below the password field is a character count '4 / 20'. At the bottom are 'Cancel' and 'Save' buttons.

The screenshot shows the 'NTP Authentication' screen. At the top, there is a toggle switch for 'NTP Authentication' which is turned on. Below it is a 'Choose a key' dropdown menu showing '1'. The main section is titled 'NTP Authentication Keys' and contains a table with columns 'Key', 'Hash Type', and 'Password'. There is a 'Delete' button and a 'Create' button at the top right of the table. At the bottom is a 'Save' button.

	Key	Hash Type	Password
☐	1	md5	*****

NTP Authentication: The device supports NTP Authentication for a secured connection between NTP servers. If you want to use the NTP authentication, follow the steps to enable the NTP authentication.

1. Select **Create**, enter the key ID and password in the pop out window, and then **Save** to close the window.
2. Choose the created key, then **Save** to enable the NTP Authentication.

System Settings—IP Address

The screenshot displays the Moxa ioPAC 6500 web interface. The top header shows the Moxa logo and the device model 'ioPAC 6500'. The left sidebar contains a navigation menu with categories: Dashboard, System Configuration, Maintenance, Diagnostic, Certificate & Key, and Security. The 'System Configuration' section is expanded, showing 'System Settings' and 'IP Address'. The main content area is titled 'IP Address' and shows the configuration for 'LAN mode' set to 'Dual IP'. Below this, the 'Port Enable/Disable' section shows checkboxes for 'LAN 1' and 'LAN 2', both of which are checked. The 'LAN 1' section is expanded, showing the 'IP Configuration' options: 'DHCP: Obtain an IP address automatically.' (unselected) and 'Static: Specify the IP address.' (selected). The 'Static' configuration shows the 'IPv4 Address' as '192 . 168 . 126 . 1', the 'Subnet Mask' as '255 . 255 . 255 . 0', and the 'Gateway - optional' field is empty.

Go to **System Settings > IP Address** to set up the device IP.

LAN mode: The device supports **Dual IP** mode currently.

Port Enable/Disable: Enable or disable port by selecting LAN1 or LAN2

LAN1/LAN2: Set up the IP for LAN1 or LAN2. The device supports **DHCP** or **Static** mode.

DNS Server: Need to input the DNS server.

DNS Server

Preferred DNS Server - optional

10 . 123 . 200 . 11

Alternate DNS Server - optional

.

SAVE

System Settings—Switch Information

MOXA

ioPAC 6500

moxa

Dashboard

System Dashboard

System Configuration

System Settings

General

IP Address

Switch Information

Home > System Configuration > System Settings > Switch Information

Switch Information

Name	IP	Link
moxa	10.123.26.10	Open

Go to **System Settings > Switch Information** to check the switch information. If any switch module is installed in the system, the IP information will be displayed here. For the switch module setup, select [Open](#) and set up in the web of the switch module.

SNMP Settings

SNMP Agent: The SNMP agent continuously gathers information about the device. When an SNMP manager sends a request, the agent responds with the requested data. **Versions: v1v2c, v3only, v1v2cv3.**

MOXA

ioPAC 6500

moxa

Dashboard

System Dashboard

System Configuration

System Settings

SNMP Settings

SNMP Agent

SNMP Trap

Maintenance

General Operation

Dagnostic

Event Log

OpenVPN Settings

Certificate & Key

Certificate Center

SSH Key

Home > System Configuration > SNMP Settings > SNMP Agent

SNMP Agent

General

SNMPv3 Account

SNMPv3 Account Protection

SNMP Agent

Enable

Version

v3only

Contact

0 / 30

Location

0 / 30

Minimum Authentication/Privacy Password Length

8

8 - 64

SNMPv3 Account and Account Protection

Click “Create” to configure the SNMPv3 Account and you could decide whether to disable the SNMPv3 Account if authentication failed.

The screenshot shows the 'SNMP Agent' configuration page with the 'SNMPv3 Account Protection' tab selected. The 'General' tab is also visible. The 'SNMPv3 Account' tab shows a table with columns: Account Name, Active, Authority, Authentication Type, and Privacy Type. A '+ Create' button is highlighted in red. The 'SNMPv3 Account Protection' tab has the following settings:

- ☐ Disable SNMPv3 account if authentication failed
- Max. Authentication Failures: 5 (range 1 - 10)
- ☐ Enable timeout for authentication failure
- Each Authentication Failure Timeout (min): 10 (range 1 - 1440)
- Account Disabled Time Interval (min): 10 (range 1 - 60)
- Save button

SNMP Trap: The agent proactively sends a notification to the server without waiting for a request, should a critical event occur.

The screenshot shows the Moxa ioPAC 6500 System Dashboard. The left sidebar contains the following menu items: Dashboard, System Dashboard, System Configuration, System Settings, SNMP Settings, SNMP Agent, and SNMP Trap. The main content area shows the 'SNMP Trap' configuration page with the 'General' tab selected. The 'Trap service' is enabled, indicated by a toggle switch.

Click “Create” to configure the Trap Server.

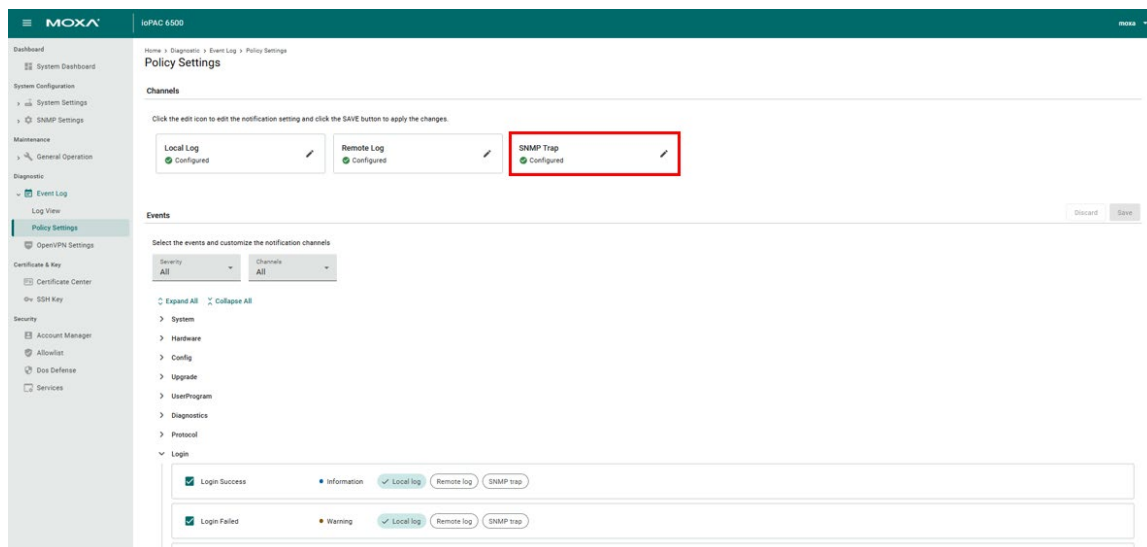
The screenshot shows the 'SNMP Trap' configuration page with the 'SNMP Trap Server' tab selected. The 'General' tab is also visible. The 'SNMP Trap Server' tab shows a table with columns: Server IP or Domain Name, Port, Trap Version, Community String, Account Name, Authentication Type, and Privacy Type. A '+ Create' button is highlighted in red. The 'Create Trap Server' dialog is open, showing the following settings:

- General Settings**
- Server IP or Domain Name: 0.0.0.0
- Port: 162
- Trap Method**
- Trap Version: Disable
- Cancel and Save buttons



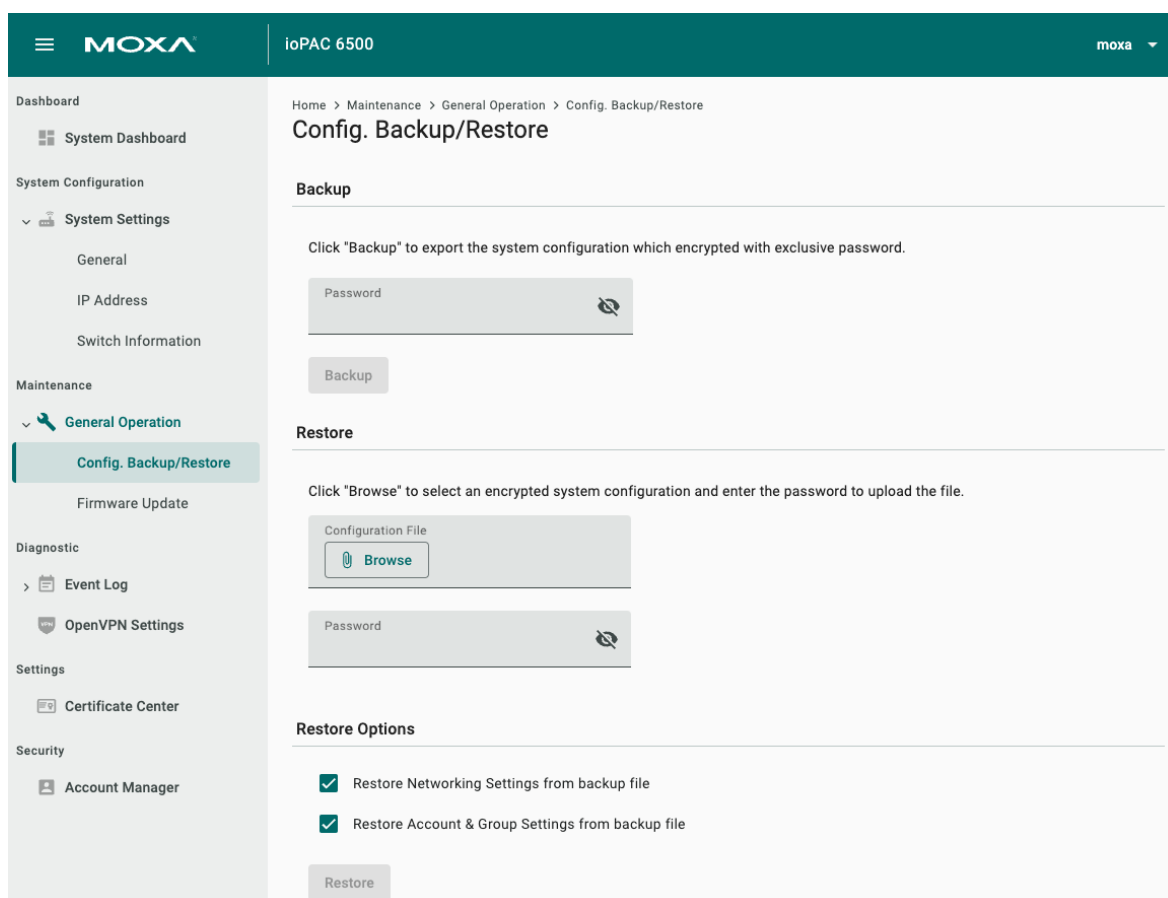
NOTE

Events could also be sent via SNMP Trap. See **Event Log - Policy Settings**.



Maintenance

General Operation—Config. Backup/Restore



Go to **General Operation > Config. Backup/Restore** to back up the system settings to the encrypted configuration file or restore the system settings from an encrypted configuration file.

Backup: Input a password first, then select **Backup** to save the configuration file which is encrypted with the password specified by you. The maximum length of password is 40 characteristics, alphanumeric, and special characteristics are allowed.

Restore: Restore the system with an encrypted configuration file. Select **Browse** to choose the file and input the password. You can choose to restore the networking, account, and group setting from the backup file by selecting the checkbox or not. Once all the information is ready, select the **Restore** to restore the system.

General Operation—Firmware Update

Slot	Type	Model Name	Current Version	Update Version	Progress(%)	Note
[1]	Backplane	65M-BMPW01	1.0.0.0	Not Supported		
1	Power	65M-PW0075	1.0.0.2			
[2,3]	Backplane	65M-BMCM02	1.0.0.0	Not Supported		
2	Switch	65M-S011M	1.0.0.0	Not Supported		
3						
[4]	Backplane	65M-BMCPU01	1.0.0.0	Not Supported		
4	CPU	65M-CPU14-IEC	1.0.0.29			
[5,6,7,8]	Backplane	65M-BMI004	1.0.0.3			
5	DI	65M-1900	1.0.0.4			
6	DO	65M-2901	1.0.0.2			

Go to **General Operation > Firmware Update** to update the firmware to the system. The page provides three steps to guide you in updating the firmware.

- Select Firmware File:** Select **Browse** to choose the firmware file that needs to be updated to the system. Select the release note to check the details.
- Select Module on List:** Select the modules that need to be updated on the **Module List**. Use the module filter to speed up the module selection. Module information will be displayed in the module list.
 - **Slot:** It shows the slot that the module is installed in. The slot number is calculated based on the current system combination. The number 1 shows the leftmost module of each unit. The slot of the backplane module will be displayed with a number in square brackets, e.g., [1].
 - **Type:** It shows the module type. E.g. CPU, DI, Backplane, etc.
 - **Model Name:** The model name of the module will be displayed here.
 - **Current Version:** Current firmware version of the module will be displayed here.
 - **Update Version:** The firmware version included in this firmware file will be displayed here.



NOTE

Update the switch module's firmware on the web page of the switch module.

- **Progress(%):** The progress of the update will be here
 - **Note:** Any other information that cannot be categorized will be displayed here.
- Update:** Select **Update** to start the system firmware update. Choose **Update Firmware One by One** to update the firmware module by module.

Diagnostic

Event Log—Log View

The screenshot shows the MOXA ioPAC 6500 web interface. The left sidebar contains navigation menus for Dashboard, System Configuration, Maintenance, Diagnostic, and Settings. The 'Diagnostic' menu is expanded, showing 'Event Log' and 'Log View'. The 'Log View' page displays a table of log entries. At the top of the table, there is a search bar with a date range selector and a 'Search' button. Below the search bar, there are links for 'Export', 'Clear', and 'Refresh'. The table has the following columns: ID, Severity, Category, Event Name, Source, Message, and Timestamp. The table contains 10 log entries. At the bottom of the table, there is a pagination control showing 'Items per page: 10' and '1 - 10 of 266'.

ID	Severity	Category	Event Name	Source	Message	Timestamp
1	Warning	Account	Account Password Expiration Warning	NA	EVID=101010,EVTYP=Account,DVID=ioPAC...	2024-05-27T10:59:50.142+08:00
2	Information	Protocol	Modbus Disable	Host 192.168.126.1	EVID=007402,EVTYP=Protocol,DVID=ioPA...	2024-05-27T11:00:14.151+08:00
3	Information	Certificate&Key	Certificate & Private Key Generate Success	NA	EVID=104000,EVTYP=Certificate&Key,DVID...	2024-05-27T11:00:39.872+08:00
4	Information	Certificate&Key	HTTPS Certificate & Key Set Success	NA	EVID=104008,EVTYP=Certificate&Key,DVID...	2024-05-27T11:00:39.945+08:00
5	Information	Config	Configuration Change Success	NA	EVID=003000,EVTYP=Config,DVID=ioPAC6...	2024-05-27T11:00:39.968+08:00
6	Information	Certificate&Key	Certificate & Private Key Generate Success	NA	EVID=104000,EVTYP=Certificate&Key,DVID...	2024-05-27T11:00:40.861+08:00
7	Information	Certificate&Key	MQTT Certificate & Key Set Success	NA	EVID=104044,EVTYP=Certificate&Key,DVID...	2024-05-27T11:00:40.912+08:00
8	Information	Config	Configuration Change Success	NA	EVID=003000,EVTYP=Config,DVID=ioPAC6...	2024-05-27T11:00:40.934+08:00
9	Information	Certificate&Key	Certificate & Private Key Generate Success	NA	EVID=104000,EVTYP=Certificate&Key,DVID...	2024-05-27T11:00:41.431+08:00
10	Information	Certificate&Key	OPCUA Certificate & Key Set Success	NA	EVID=104048,EVTYP=Certificate&Key,DVID...	2024-05-27T11:00:41.454+08:00

Go to **Event Log > Log View** to check all logs generated by the system. The following information of the logs will be displayed in the table.

- **ID:** The orders of the logs in the list
- **Severity:** The severity of the event; three severities (alert, warning, information).
- **Category:** The category from which the log is generated. Check the categories in the Policy Settings page.
- **Event Name:** Event name shows why the log was generated.
- **Source:** If the log is generated by an external source, the information will be displayed here.
- **Message:** The message included in the log.
- **Timestamp:** When the log is generated.

Export, **Clear**, and **Refresh** the log list based on the requirement.

Event Log—Policy Settings

MOXA ioPAC 6500

Dashboard > System Dashboard

System Configuration > System Settings > General > IP Address > Switch Information > SNMP Settings

Maintenance > General Operation

Diagnostic > Event Log > Log View > **Policy Settings**

OpenVPN Settings

Certificate & Key > Certificate Center > SSH Key

Security > Account Manager > Allowlist > Dos Defense > Services

Home > Diagnostic > Event Log > Policy Settings

Policy Settings

Channels

Click the edit icon to edit the notification setting and click the SAVE button to apply the changes.

Local Log	Remote Log	SNMP Trap
✓ Configured	✓ Configured	✓ Configured

Events

Select the events and customize the notification channels

Severity: All Channels: All

Expand All Collapse All

System

Event	Severity	Local log	Remote log	SNMP trap
✓ PWR On	Information	✓	✓	✓
✓ PWR Off	Warning	✓	Remote log	SNMP trap
✓ PWR Fail	Error	✓	Remote log	SNMP trap
✓ CPU Usage Over Threshold	Warning	✓	Remote log	SNMP trap
✓ CPU Usage Under Threshold	Warning	✓	Remote log	SNMP trap

Go to **Event Log > Policy Settings** to check the policy settings of the log.

The log will be stored locally as the default. The modification can be done in the **Channels**.

Local Log: Select the  to change the settings. **Event Log Overwrite Policy** and **Log Capacity Warning** can be configured.

Local Log Settings

Event Log Overwrite Policy

☒ Overwrite the oldest Event Log

☐ Stop Recording Event Log

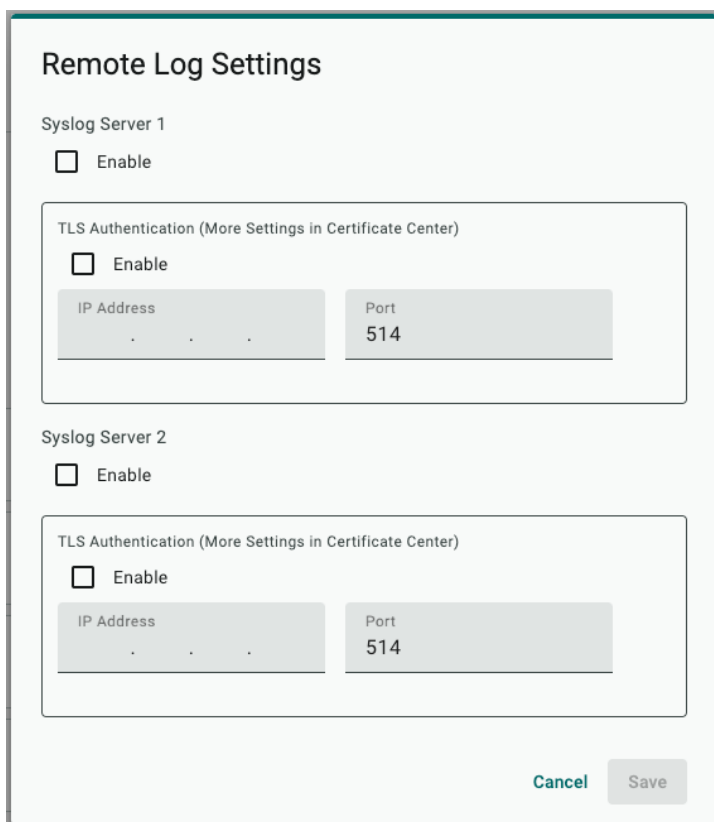
☒ Log Capacity Warning

Capacity Threshold (%)

80

Cancel Save

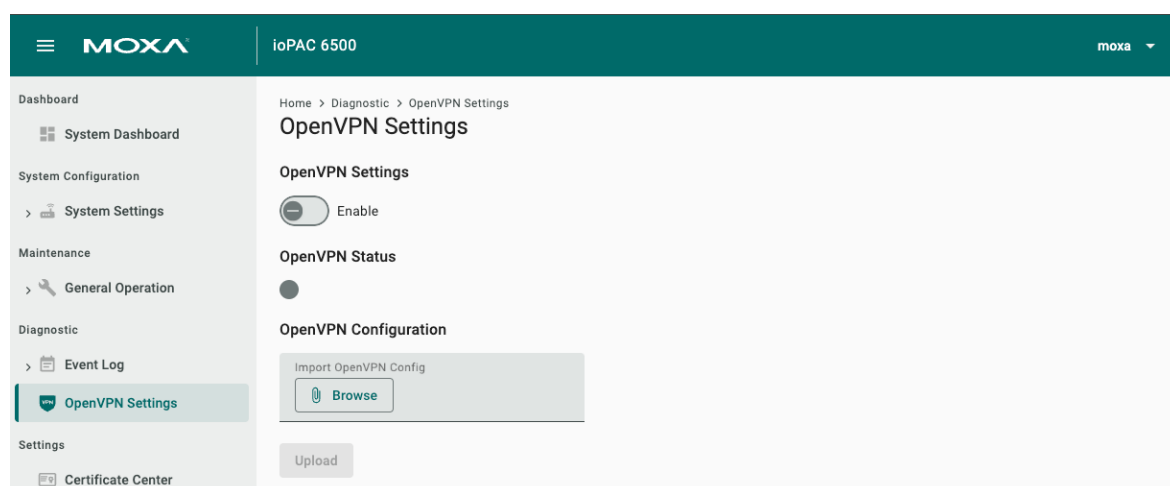
Remote Log: Select the  to change the settings. The system supports two syslog servers and can deliver the log to two syslog servers simultaneously. Enable the server and key in the IP to activate the syslog server. The system supports TLS authentication. Remember to complete the settings in the **Certificate Center**.



The image shows a 'Remote Log Settings' window. It contains two sections for 'Syslog Server 1' and 'Syslog Server 2'. Each section has an 'Enable' checkbox, a 'TLS Authentication (More Settings in Certificate Center)' checkbox, an 'IP Address' input field, and a 'Port' input field (set to 514). At the bottom right are 'Cancel' and 'Save' buttons.

The logs supported by systems are listed in the **Events** section. The events are enabled and stored locally in default. Change the logs based on the application.

OpenVPN Settings



The image shows the 'OpenVPN Settings' page in the Moxa ioPAC 6500 web interface. The left sidebar contains a navigation menu with 'OpenVPN Settings' highlighted. The main content area shows the 'OpenVPN Settings' title, an 'Enable' toggle switch, 'OpenVPN Status' (a grey circle), and 'OpenVPN Configuration' section with an 'Import OpenVPN Config' button and a 'Browse' button. At the bottom is an 'Upload' button.

Go to **OpenVPN Settings** to configure the OpenVPN settings. Follow the steps to enable the OpenVPN

1. Import the OpenVPN config file. The file is generated in an OpenVPN server.
2. Enable the OpenVPN.
3. If connected successfully, the status will become Green.

Certificate

Certificate Center

Home > Settings > Certificate Center

Certificate Center

My Certificates Trusted Root CA

Create Certificate Signing RequestImport Signed CertificateCreate Self Signed Certificate

Search

File Name	Issued To	Issued By	Valid From	Valid Until	Status	Used By	Download	
240603024259_60148.crt	/C=CT/ST=State/L=City/O=Moxa/OU=ioPAC/CN=10.123.26.9/emailAddress=moxa@moxa.com	/C=CT/ST=State/L=City/O=Moxa/OU=ioPAC/CN=10.123.26.9/emailAddress=moxa@moxa.com	2024-6-3	2029-6-2	valid	MQTT	Download	
240603024300_92820.crt	/C=CT/ST=State/L=City/O=Moxa/OU=ioPAC/CN=10.123.26.9/emailAddress=moxa@moxa.com	/C=CT/ST=State/L=City/O=Moxa/OU=ioPAC/CN=10.123.26.9/emailAddress=moxa@moxa.com	2024-6-3	2029-6-2	valid	GPC UA	Download	
240605061009_27352.crt	/C=CT/ST=State/L=City/O=Moxa/OU=ioPAC/CN=10.123.26.9/emailAddress=moxa@moxa.com	/C=CT/ST=State/L=City/O=Moxa/OU=ioPAC/CN=10.123.26.9/emailAddress=moxa@moxa.com	2024-6-5	2029-6-4	valid		Download	
240603024258_90065.crt	/C=CT/ST=State/L=City/O=Moxa/OU=ioPAC/CN=10.123.26.9/emailAddress=moxa@moxa.com	/C=CT/ST=State/L=City/O=Moxa/OU=ioPAC/CN=10.123.26.9/emailAddress=moxa@moxa.com	2024-6-3	2029-6-2	valid	HTTPS	Download	

- Go to **Certificate Center > My Certificates** to check the search, view the status, and download the system certificates.
- Create Certificate Signing Request:** This function will generate a .csr file based on current system status. Use the .csr file to obtain a signed certificate from Root CA.
- Import Signed Certificate:** The signed Certificate generated by Root CA in the previous step should be imported here.
- Create Self-signed Certificate:** If the Root CA is not available, the system also provides the self-signed certificate for you to download.

Home > Settings > Certificate Center

Certificate Center

My Certificates Trusted Root CA

Import Certificate

Search

File Name	Issued To	Issued By	Valid From	Valid Until	Status	Used By	Download
No data to display.							

Go to **Certificate Center > Trusted Root CA** to import the certificate of the Trusted Root CA.

Protocol Mapping Table		
Protocol	My Certificates	Trusted Root CA
HTTPS	Certificate 240603024258_90065.crt(18... ▼	CA ▼
MQTT	Certificate 240603024259_60148.crt(5C... ▼	CA ▼
SYSLOG TLS	Certificate ▼	CA ▼
OPC UA 01	Certificate 240603024300_92820.crt(76... ▼	CA ▼
OPC UA 02	Certificate ▼	CA ▼
OPC UA 03	Certificate ▼	CA ▼
OPC UA 04	Certificate ▼	CA ▼
LDAPS	Certificate ▼	CA ▼
RadSec	Certificate ▼	CA ▼

Save

Go to **Certificate Center > Protocol Mapping Table** to link the saved My Certificates and Trusted Root CA to a protocol. Note that not all protocols need My Certificate and Trusted Root CA.

- Only My Certificate: HTTPS, MQTT
- Only Trusted Root CA: OPC UA 2/3/4, LDAPS, RadSec

Security

Account Manager

Home > Security > Account Manager

Account Manager

Password Policy Settings

Login Sessions Settings

Authentication, Authorization, and Accounting Settings

Minimum password length

8

8 - 64

☐

At least one numeric(0-9)

☒

At least one uppercase letter(A-Z)

☒

At least one lowercase letter(a-z)

☐

At least one special character(~!@#\$%^&*~|;,:.<>[]{}))

☐

Enforce password history: 6 unique passwords must be entered before the old passwords can be re-used

☒

Must not contain the username

User Welcome Message

This device is for company business use only. This system may be monitored as permitted by law. Unauthorized use may result in criminal prosecution, termination or other action.

177 / 512

User Login Failed Message

Login failed

12 / 512

Save

Go to **Account Manager > Password Policy Settings** to set up the password policy of the device. The length, letter combination, and uniqueness of the password can be set up. Besides the password policy, change the welcome and login-failed message on this page.

Home > Security > Account Manager

Account Manager

Password Policy Settings

Login Sessions Settings

Authentication, Authorization, and Accounting Settings

Maximum number of Login Users for HTTP+HTTPS

5

1 - 10

Auto Logout Time (unit: minute(s))

1440

1 - 1440

Save

Go to **Account Manager > Login Session Settings** to set up the login sessions. The maximum connection and logout time.

Home > Security > Account Manager

Account Manager

Password Policy Settings Login Sessions Settings **Authentication, Authorization, and Accounting Settings**

Authentication Mode
Local Only ▼

Save

Go to **Account Manager > Authentication, Authorization and Accounting Settings** to set up the AAA settings. Several authentication modes are available.

- **Local Only:** Use the accounts that have been set up in the system.
- **RADIUS Only:** Link to the RADIUS server to verify the login account.
- **TACACS+ Only:** Link to the TACACS+ server to verify the login account.
- **LDAP Only:** Link to the LDAP server to verify the login account.
- **RADIUS Then Local:** Link to the RADIUS server to verify the login account first. If a timeout happens, use the accounts set up in the system as an alternative.
- **TACACS+ Then Local:** Link to the TACACS+ server to verify the login account first. If a timeout happens, use the accounts set up in the system as an alternative.
- **LDAP Then Local:** Link to the LDAP server to verify the login account first. If a timeout happens, use the accounts set up in the system as an alternative.

RADIUS Settings

Home > Security > Account Manager

Account Manager

Password Policy Settings Login Sessions Settings **Authentication, Authorization, and Accounting Settings**

Authentication Mode
RADIUS Only

RADIUS Server Settings

☐ Secure

RADIUS Server
0.0.0.0

RADIUS Key
0 / 128

port
1812
1 - 65535

Authentication Type
CHAP

Timeout (sec)
3
1 - 10

Group Mapping

Filter-ID	Group	
filter_id-map-to-gid0	Viewer	⋮
filter_id-map-to-gid1	Operator	⋮
filter_id-map-to-gid2	Engineer	⋮
filter_id-map-to-gid3	Installer	⋮
filter_id-map-to-gid4	Secure_Admin	⋮
filter_id-map-to-gid5	Secure_Auditor	⋮
filter_id-map-to-gid6	Account_Manager	⋮
filter_id-map-to-gid7	Admin	⋮

Save

The ioPAC 6500 supports RADIUS. Here are detailed descriptions of the RADIUS server settings:

- **Secure:** Enabling the system to communicate encrypted data with the RADIUS server. The certificate will be specified in the Certificate Center.
- **RADIUS Server:** Input the IP of the RADIUS server here.
- **RADIUS Key:** Input the key of the RADIUS server here.
- **Port:** The port that communicates with the RADIUS server.
- **Authentication Type:** The authentication type used in the RADIUS server. The ioPAC 6500 supports PAP, CHAP, MSCHAP, and EAP-MD5, offering a total of four authentication types.
- **Timeout:** How long the ioPAC 6500 will wait for the response from the RADIUS server.
- **Group Mapping:** It listed the Filter-ID and Group mapping in the ioPAC 6500 system. The current groups will be displayed here. The table shows the authority of each default group of users.



NOTE

1. The ioPAC 6500 system supports a maximum of 16 groups, eight are default and another eight are user-defined.
2. The group's modification should be done in IINxpress.

Group	Monitor and Diagnostic	Operational Activities	Configuration	IEC Code	System Log	Security Configuration and Secure Log	Upgrade and Rollback	Account Management
Viewer	R	R		R	R			
Operator	R	R/W		R/W	R			
Engineer	R/W	R/W	R/W	R/W	R			
Installer	R/W	R	R/W	R/W	R	R	R/W	
Secure Admin	R/W	R	R/W	R	R/W	R/W	R/W	R/W
Secure Auditor	R	R	R		R	R		R
Account Manager	R					R/W		R/W
Admin	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W

TACACS+ Settings

Home > Security > Account Manager

Account Manager

Password Policy Settings Login Sessions Settings **Authentication, Authorization, and Accounting Settings**

Authentication Mode
TACACS+ Only

TACACS+ Server Settings

TACACS+ Server
0.0.0.0

Shared Secret
0 / 128

port
49
1 - 65535

Authentication Type
CHAP

Timeout (sec)
3
1 - 10

Group Mapping

Priv-lvl	Group	
0	Viewer	⋮
1	Operator	⋮
2	Engineer	⋮
3	Installer	⋮
4	Secure_Admin	⋮
5	Secure_Auditor	⋮
6	Account_Manager	⋮
7	Admin	⋮

Save

The ioPAC 6500 supports TACACS+. Here are detailed descriptions of the TACACS+ server settings:

- **TACACS+ Server:** Input the IP of TACACS+ server here.
- **Shared Secret:** Input the key of TACACS+ server here.
- **Port:** The port used to communicate with the TACACS+ server.
- **Authentication Type:** The authentication type used in the TACACS+ server. The ioPAC 6500 supports PAP, CHAP, ASCII, three authentication types in total.
- **Timeout:** How long the ioPAC 6500 will wait for the response from the TACACS+ server.
- **Group Mapping:** The privilege level and group mapping in the ioPAC 6500 system. The current groups will be displayed here. The authority of each default group of users is the same as RADIUS.



NOTE

1. The ioPAC 6500 system supports a maximum of 16 groups; eight are default and another eight are user-defined.
2. The group modification should be done in IINxpress.

LDAP Settings

Home > Security > Account Manager

Account Manager

Password Policy Settings Login Sessions Settings Authentication, Authorization, and Accounting Settings

Authentication Mode
LDAP Only

LDAP Server Settings

☐ Secure

LDAP Server
0.0.0.0

Search Base DN
0 / 256

Search Filter
0 / 128

Bind DN
0 / 256

Bind Password
0 / 64

port
389
1 - 65535

Authentication Type
by Group Attribute

Timeout (sec)
3
1 - 10

Group Attribute

Group Mapping

Group Attribute	Group	
group_attr-value-map-to-gid0	Viewer	⋮
group_attr-value-map-to-gid1	Operator	⋮
group_attr-value-map-to-gid2	Engineer	⋮
group_attr-value-map-to-gid3	Installer	⋮
group_attr-value-map-to-gid4	Secure_Admin	⋮
group_attr-value-map-to-gid5	Secure_Auditor	⋮
group_attr-value-map-to-gid6	Account_Manager	⋮
group_attr-value-map-to-gid7	Admin	⋮

Save

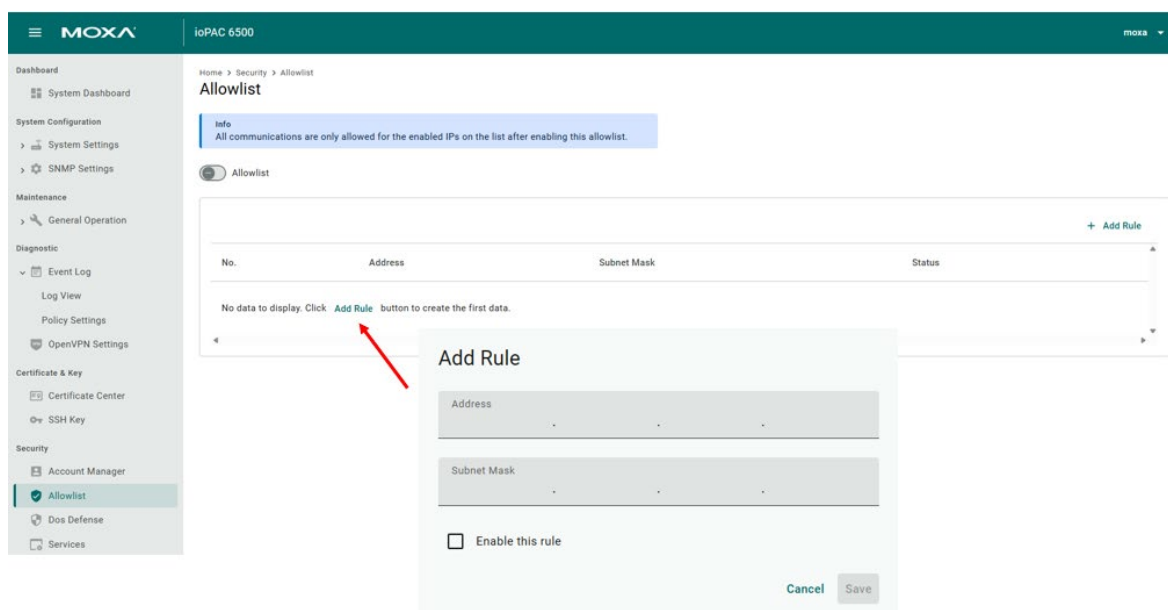
The ioPAC 6500 supports LDAP. Here are the detailed descriptions of the LDAP server settings:

- **Secure:** Enabling the system to communicate encrypted data with the LDAP server. The certificate will be specified in the Certificate Center.
- **LDAP Server:** Input the IP of LDAP server here.
- **Search Base DN:** The LDAP DN (Distinguished name) that serves as a starting point for the search for users over all child nodes.
- **Search Filter:** The LDAP search filter used for the search for users
- **Bind DN:** Enter the Distinguished Name of the user to search in the LDAP directory.

- **Port:** The port used to communicate with the LDAP server.
- **Authentication Type:** The authentication type used in the server. The ioPAC 6500 supports Group Attributes and DN, two authentication types.
- **Timeout:** How long the ioPAC 6500 will wait for the response from the LDAP server.
- **Group Mapping:** Listing the Group Attributes and Group mapping in the ioPAC 6500 system. The systems consist of eight groups. The authority of each group of users is the same as RADIUS.

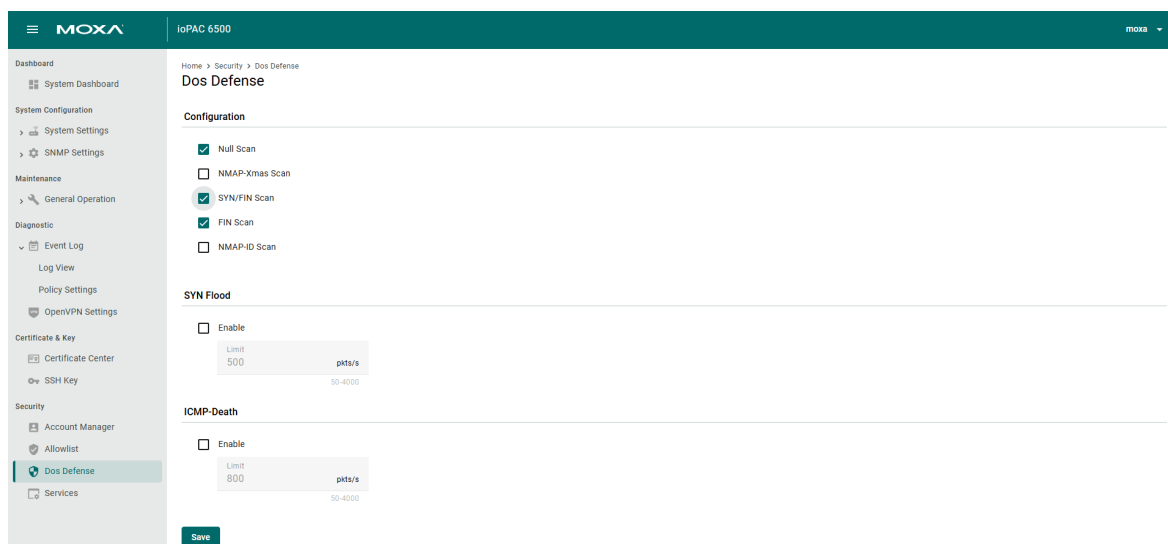
Allowlist

All communications are only allowed for the enabled IPs on the list after enabling this allowlist. Select **Add Rule** to edit the IP and subnet mask.



DoS Defense

This section configures protections against **Denial-of-Service attacks**, which are attempts to make a device or network service unavailable by overwhelming it with traffic.



Configuration

Items	Description
Null Scan	TCP scan with no flags set; used in stealth attacks to probe for open ports
NMAP-Xmas Scan	TCP scan with FIN, URG, PSH flags; used to bypass simple detection methods
SYN/FIN Scan	Sends TCP packets with both SYN and FIN flags set; non-standard combination
FIN Scan	Sends TCP packets with only the FIN flag; used for stealth port scanning
NMAP-ID Scan	Detects IP ID-based scans used in host discovery and fingerprinting

SYN Flood

When enabled, it activates protection against SYN flood attacks. The packet limit can be set from 50 to 4000.

ICMP-Death

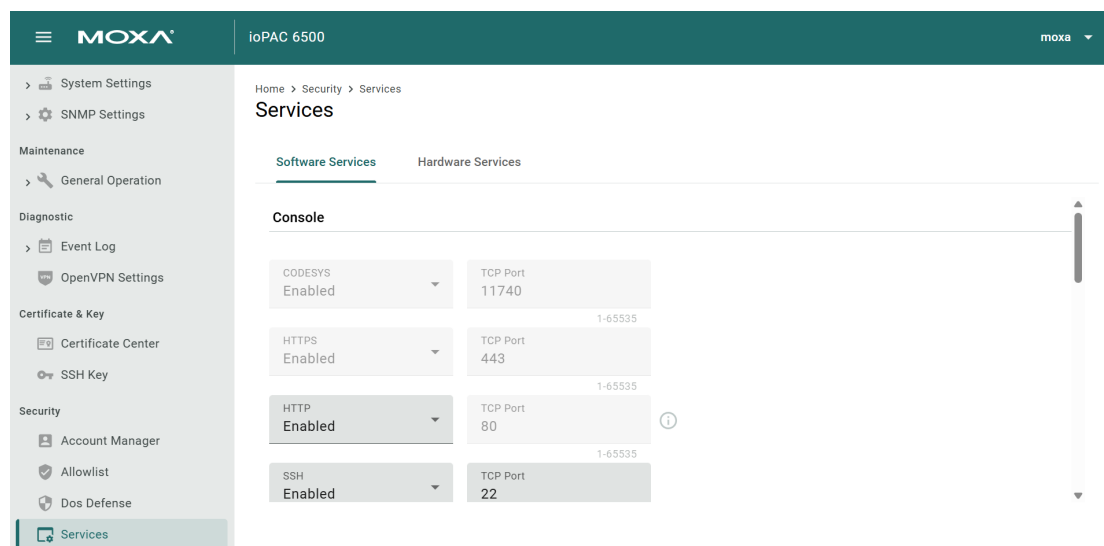
When enabled, it activates protection against ICMP flood attacks. The packet limit can be set from 50 to 4000.

Services

This section allows you to supervise and configure the software and hardware services, including the service and its corresponding port.

Software services: Console, System, Industrial Data.

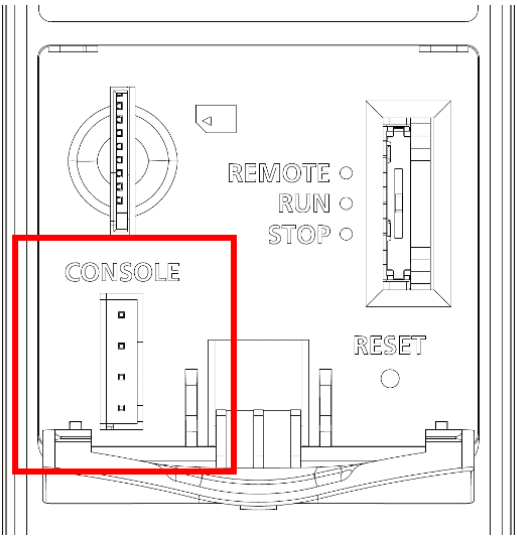
Hardware services: CPU module.



Logging in by Console Port

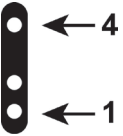
The ioPAC 6500 Series offers a serial console port, allowing you to reboot and reset to default. Followed the steps to use the console port.

Step 1: Open the cover on the CPU module to see the console port inside.



Step 2: Connect the 4-pin serial console cable to the console port. The following diagram shows the 4-pin serial connector and pin connections.

Pin Assignment for the Serial Console Port

	<table><tr><th>Pin</th><th>Definition</th></tr><tr><td>1</td><td>TxD</td></tr><tr><td>2</td><td>RxD</td></tr><tr><td>3</td><td>NC</td></tr><tr><td>4</td><td>GND</td></tr></table>	Pin	Definition	1	TxD	2	RxD	3	NC	4	GND
Pin	Definition										
1	TxD										
2	RxD										
3	NC										
4	GND										

Serial Console Default Settings

Parameter	Value
Baudrate	115200 bps
Parity	None
Data bits	8
Stop bits	1
Flow Control	None



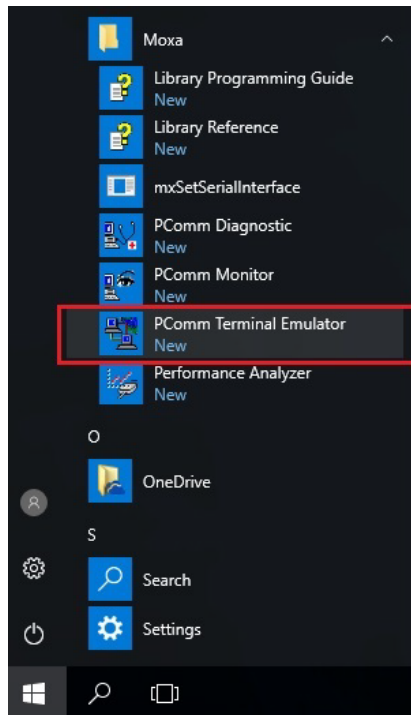
NOTE

Contact the sales representative in your region for the console cable.

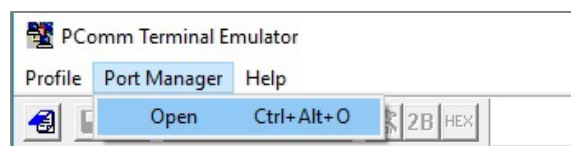
We recommend you use PComm Terminal Emulator for serial communication. Download the software free from Moxa's website.

After installing PComm Terminal Emulator, access the Moxa switch's console:

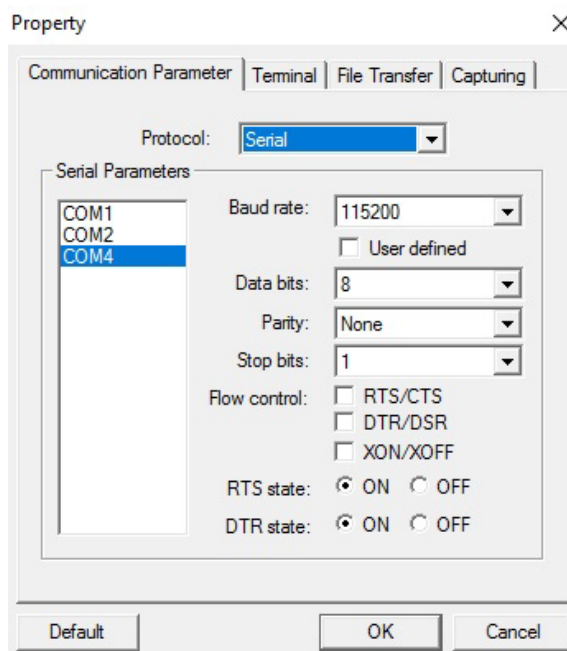
1. From the Windows desktop, select **Start > Moxa > PComm Terminal Emulator**.



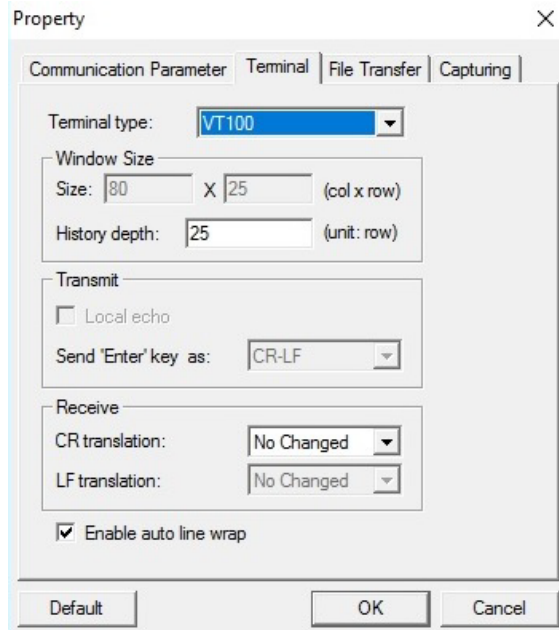
2. Select **Open** under the **Port Manager** menu to open a new connection.



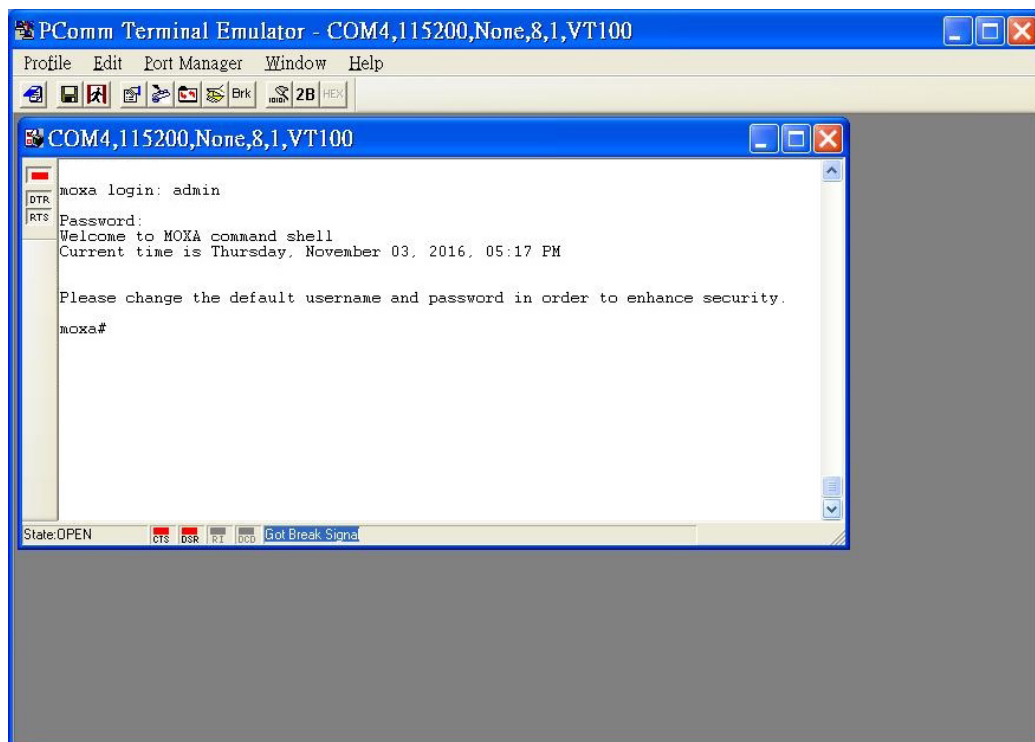
3. The **Property** window will open. On the **Communication Parameter** tab for **Ports**, select the COM port that is being used for the console connection. Set the other fields: **115200** for **Baud Rate**, **8** for **Data Bits**, **None** for **Parity**, and **1** for **Stop Bits**.



- On the **Terminal** tab, select **VT100** for **Terminal Type**, and then select **OK** to continue.



- The console will prompt you to log in. The default login name is **admin**, and the default password is **moxa**. This password will be required to access any of the consoles (web, serial, Telnet).



- After successfully connecting to the switch by serial console, start configuring the switch's parameters by using command line instructions. Refer to the **Moxa Command-line Interface Manual** for details.



NOTE

By default, the password assigned to the Moxa switch is **moxa**. Be sure to change the default password after you first log in to help keep your system secure.

5. IINxpress

In this chapter, we introduce how to configure the ioPAC 6500 by IINxpress. IINxpress is a Moxa utility, which is the integrated development environment (IDE) software for the Moxa ioPAC 6500 Series. IINxpress provides easy access to all status information, ready-to-run service settings, and IEC 61131-3 programming ability. IINxpress requires a paid license, but it can be upgraded for free when future basic functions are available.



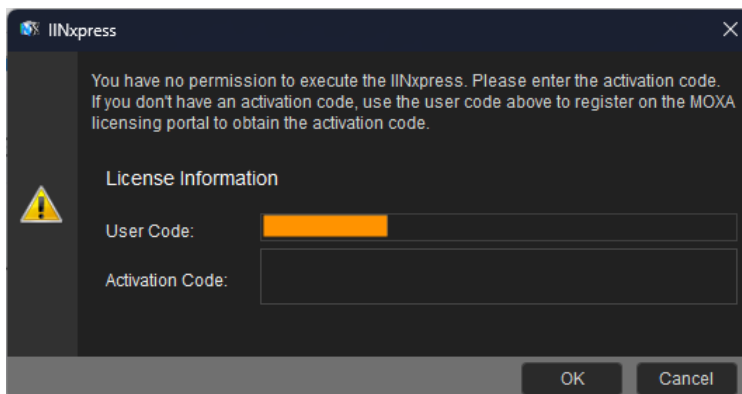
NOTE

Avoid installing IINxpress on ARM-based CPUs. To ensure a smooth user experience, the recommended specifications are: x86-64 CPU (i5 or above), 8 GB RAM or higher, and make sure enough storage is reserved for installation and the project; project file size varies depending on the application.

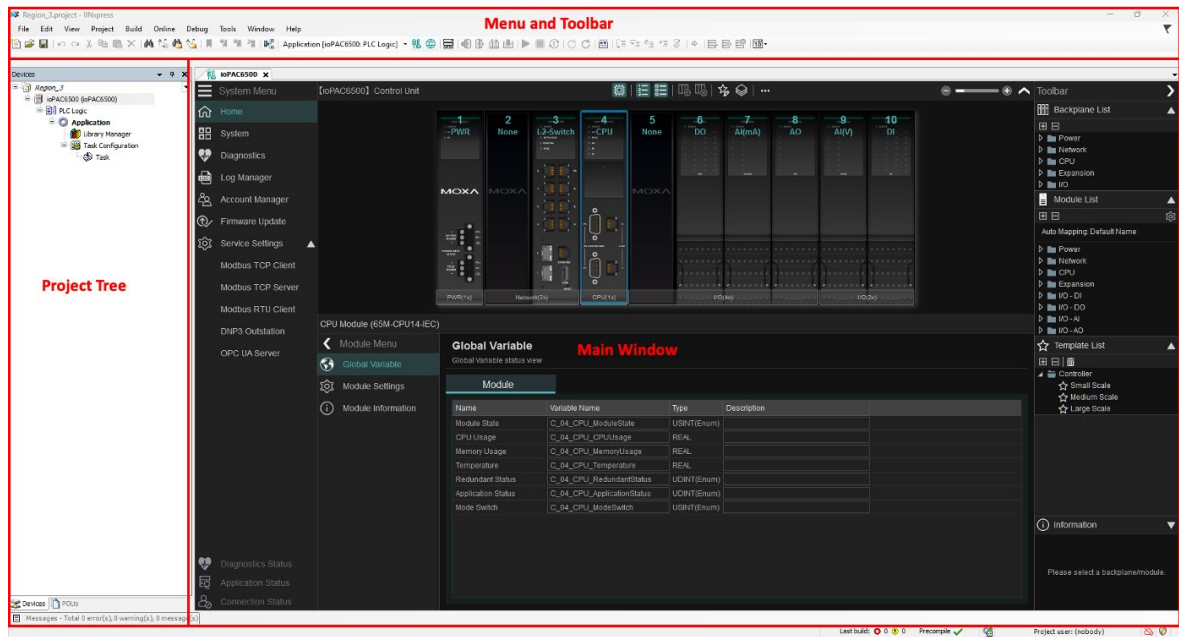


NOTE

Download the IINxpress software from Moxa's official website (<https://www.moxa.com/>) to do the installation. Once the installation is completed, the following window will appear to ask you to activate the IINxpress. The window will display a 21-digit encrypted user code. Use this code to register on the Moxa Licensing Portal (<https://license.moxa.com/>) and get an activation code. Then, activate IINxpress.



When IINxpress is launched successfully, you see the following windows. The IINxpress user interface can be divided into three blocks.



Menu and Toolbar: The settings related to the device can be found here.

Project Tree: The functions of the projects will be listed here hierarchical.

Main window: The detailed parameters of each function will be displayed here, switch between each function by the tab.

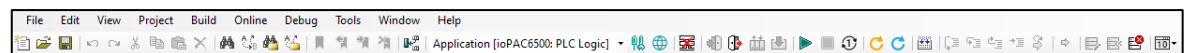


NOTE

When logging in for the first time into IINxpress, follow the instructions in the **Build New Project** section to create a new project.

Menu and Toolbar

IINxpress' menu and toolbar provide the functions for you to develop the program. We will now discuss functions related to the device's configuration and program execution.



New Project: Built a new project. Refer to the **Build New Project** section for details.

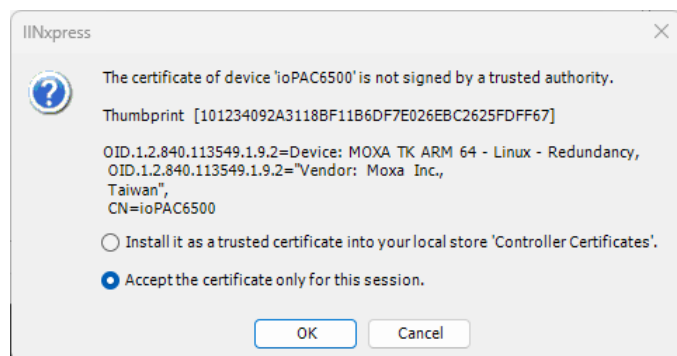
Open project: Opens an existing project.

Device helper: Provides the device scan, mapping functions, and performs some basic settings.

Open ioPAC 6500 Configuration: Opens the ioPAC 6500 configuration page where you configure all the device settings. Refer to the **ioPAC 6500 Configuration** section for details.

Open ioPAC 6500 Web page: Opens the ioPAC 6500 webpage where you configure IT-related device settings.

 **Connect device:** Used to connect the ioPAC 6500 devices. When connecting the device for the first time, IINxpress will show the warning message about the certificate. Choose the preference option to **accept the certificate once** or **put the certificate into a local store**. The log-on window will show. Key in the username and password to log into the device. After a successful connection, monitor the real-time device status on the ioPAC 6500 Configuration page.



 **Login application:** When you log in the application, you can control the device to run and stop the program remotely. Note: The mode switch should be switched to "REMOTE" to allow the control from the remote side.

 **Logout application:** Logs out the application to close the remote control session.

 **Online change:** You can use this command to initiate an online change on the current application. When this is done, CODESYS re-downloads only the changed parts of an application that is already running on the PLC.

 **Download:** Downloads the compiled program to the device.

 **Run:** Runs the program remotely.

 **Stop:** Stops the program remotely.

 **Single cycle:** Asks the device to run one cycle.

 **Reset warm:** Resets the program with warm-start condition.

 **Reset cold:** Resets the program with cold-start condition.

 **Generate code:** Compiles the code on completing the program.

 **Step over:** The command executes the statement where the program is currently located and stops before the next statement in the POU. For details, check **Help**.

 **Step into:** The command executes the statement where the program is currently located and stops before the next statement. For details, check **Help**.

 **Step out:** The command executes the program until the next return and stops afterwards. For details, check **Help**.

 **Run to cursor:** The command executes a program until a specified position as marked by the cursor. For details, check **Help**.

 **Set next statement:** The command determines which statement is executed next. For details, check **Help**.

 **Show next statement:** The command displays the program statement that is processed in the next step. For details, check **Help**.

 **Write values:** This command sets a predefined value to a variable on the controller once. For details, check **Help**.

 **Force values:** The command sets a permanent predefined value to a variable on the controller. For details, check **Help**.

 **Unforce values:** This command resets the forcing of all variables. The variables receive their current values from the PLC. For details, check **Help**.

 **Display mode:** The value in the project is displayed in Binary, Decimal, and Hexadecimal.

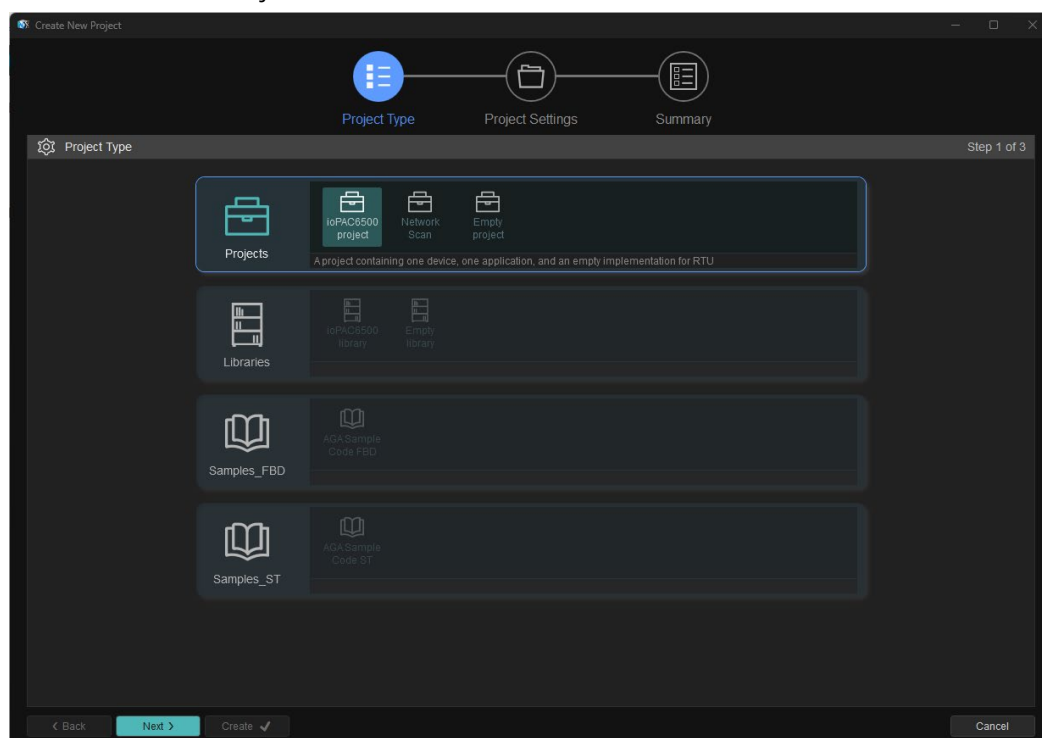
Build New Project

Selecting the New project button allows you to select from three ways to create a new project.

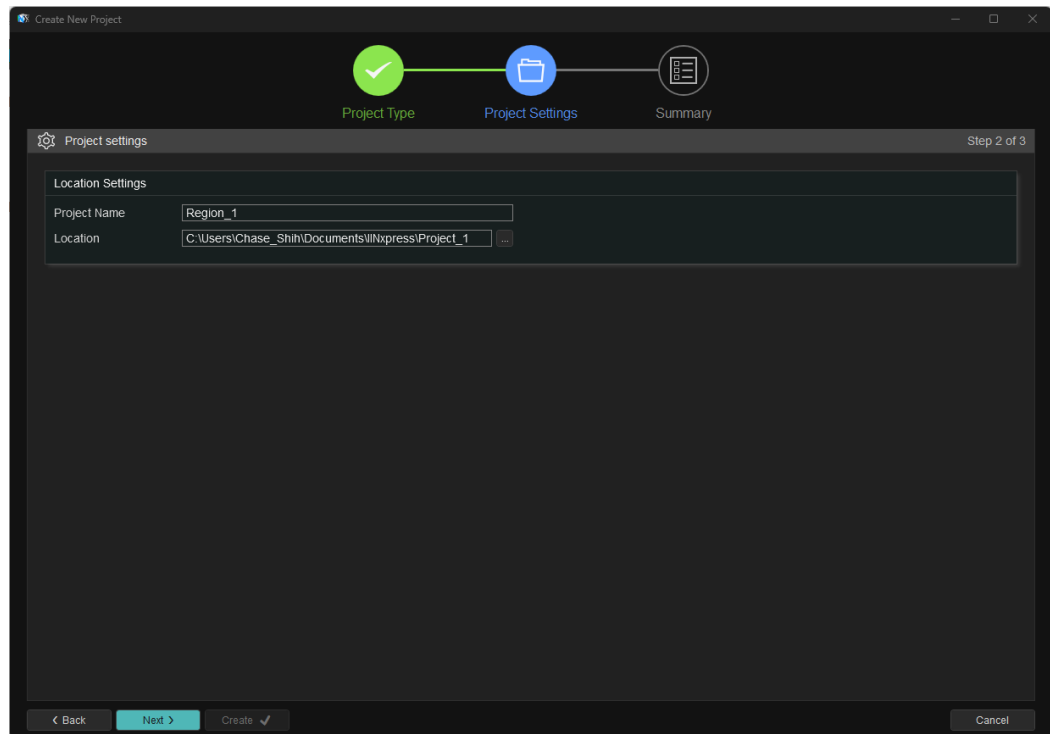
ioPAC 6500 Project

If there are no ioPAC 6500 devices on hand, we suggest using this option to start a project.

Step 1: Choose ioAPC 6500 Project icon and select **Next**.



Step 2: Specific a project name and assign a location. Customize a location by selecting .



Create New Project

Project Type Project Settings Summary

Project settings Step 2 of 3

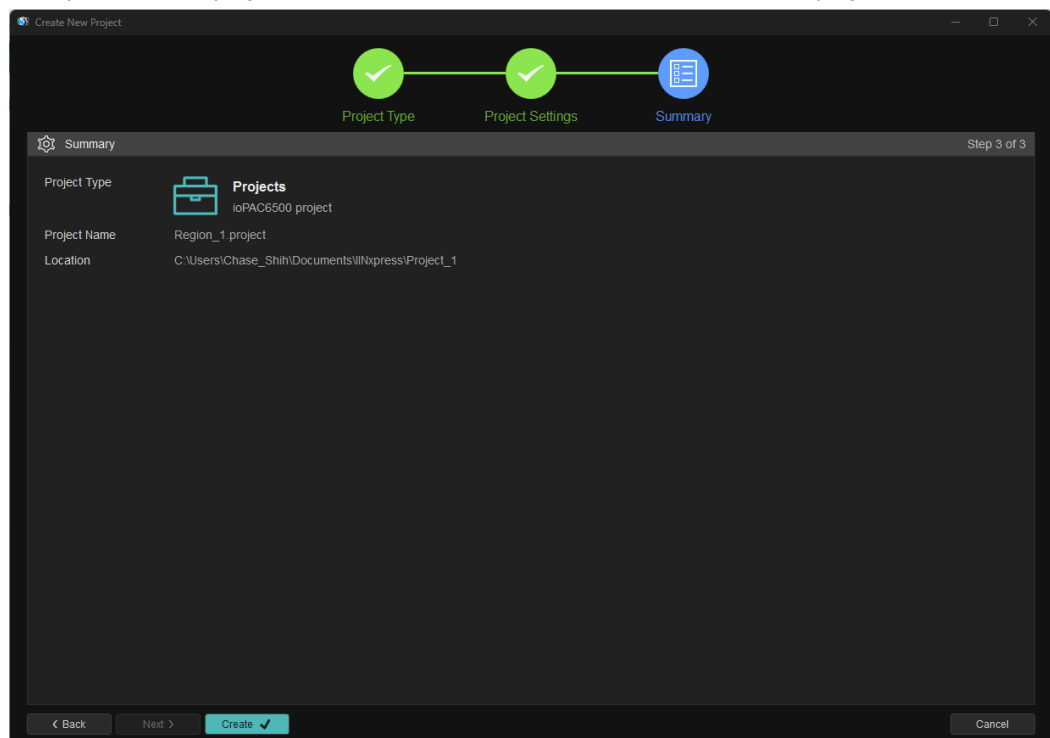
Location Settings

Project Name Region_1

Location C:\Users\Chase_Shih\Documents\iNexpress\Project_1

< Back Next > Create ✓ Cancel

Step 3: Finally, review the project information, and then select **Create** to create a project.



Create New Project

Project Type Project Settings Summary

Summary Step 3 of 3

Project Type Projects
ioPAC6500 project

Project Name Region_1 project

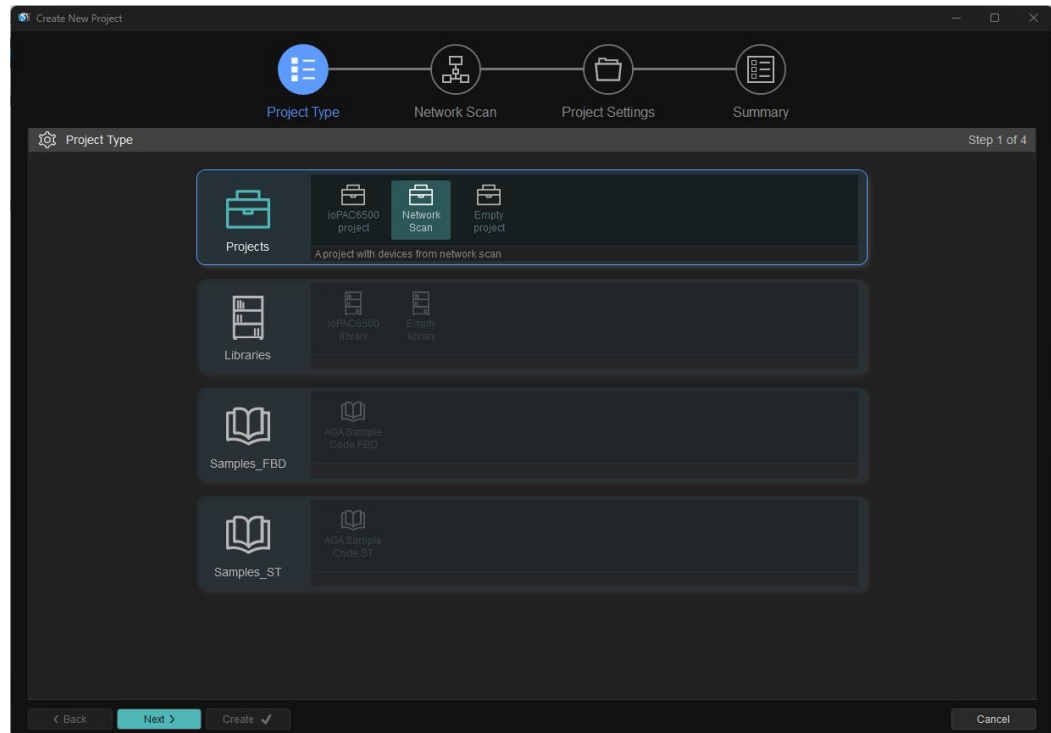
Location C:\Users\Chase_Shih\Documents\iNexpress\Project_1

< Back Next > Create ✓ Cancel

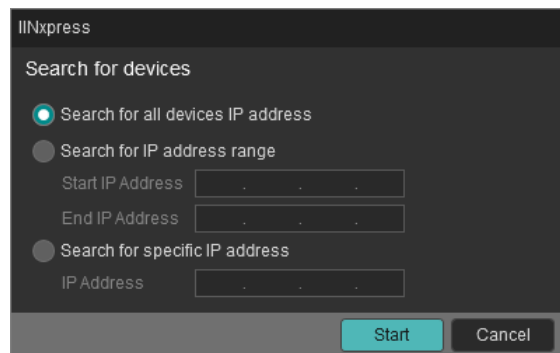
Network Scan

When powering up the device and connecting it to the Ethernet, use the scan function to find the device.

Step 1: Choose Network Scan icon and select **Scan Network**.



Step 2: Choose one from Scan all network, scan an IP range, and appoint a specific IP.



Step 3: The scanned device(s) will be displayed in the table. Choose the device, input the **Username** and **Password**, then select **Next**.

Step 2 of 4

Scan Network... ☐ Certificate validation confirmation is enabled

Device List

Mass Configuration Login Helper

	Model Name	Device Name	LAN1 Information	LAN2 Information	User Name	Password	Status
☒	ioPAC6500	ioPAC6500_0100016	00:90:E8:12:00:02 10.90.30.17	00:A0:C9:12:00:01 192.168.126.254			

< Back Next > Create Cancel

Step 4: Input the project information. Set up the mapping of the global variable in this step. When the setup is completed, select **Next**.

Step 3 of 4

Project Name: Region2

Location: C:\Users\Chase_Shih\Documents\Winpress\Project_2

Global Variable Auto Mapping Settings

☐ None

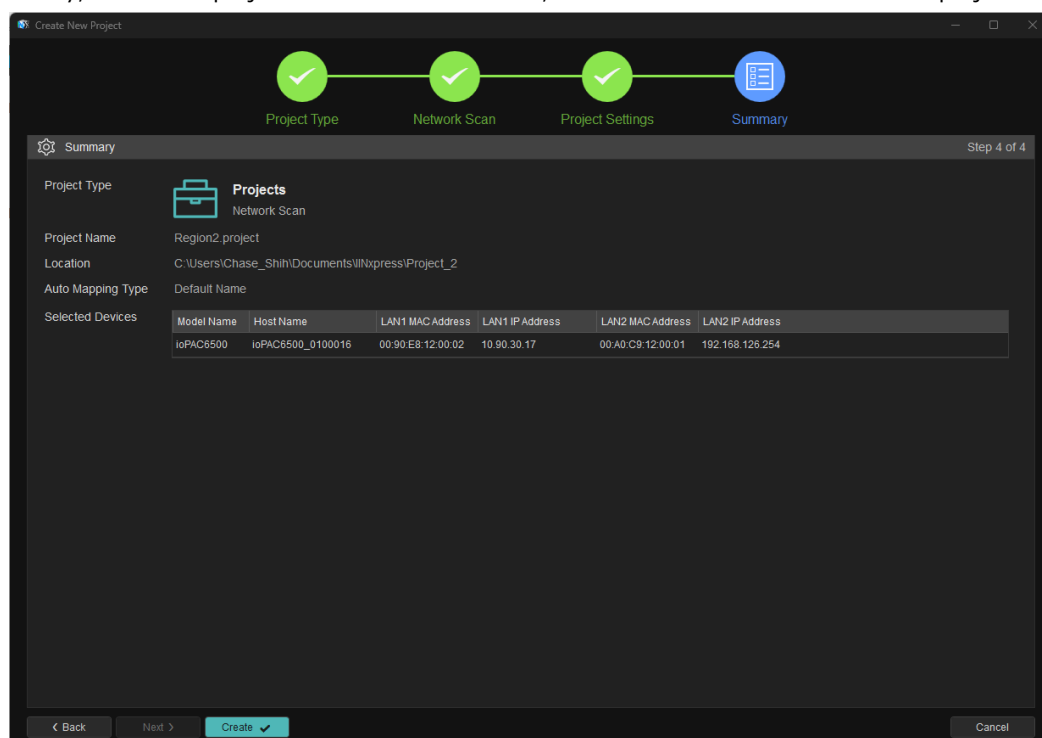
☒ Default Name

☐ Customized Prefix Name

M1_Dt_Value

< Back Next > Create Cancel

Step 5: Finally, review the project and device information, and then select **Create** to create a project.



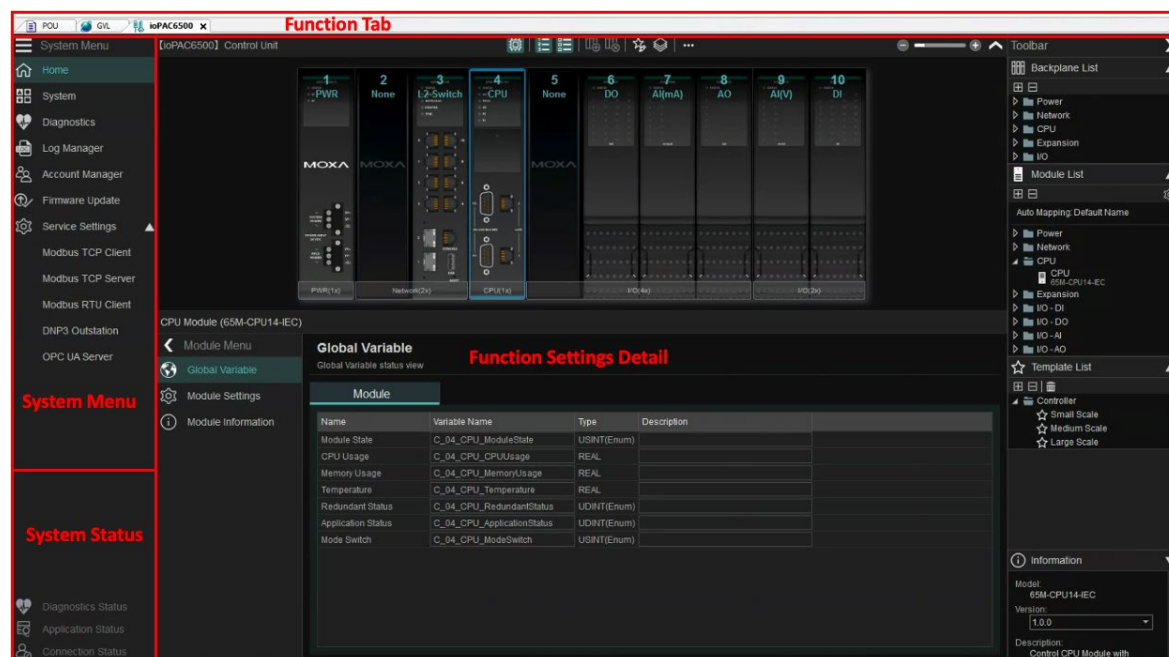
Empty Project

The process to open an empty project is the same as opening an ioPAC 6500 project. The only difference is there will be no pre-loaded ioPAC 6500 in the project file.

ioPAC 6500 Configuration

The ioPAC 6500 Configuration is one of the most important parts of IINxpress. Double-click the ioPAC 6500 (ioPAC 6500) in the project tree or the icon on the toolbar to open it.

The ioPAC 6500 configuration page can be categorized into the following parts.



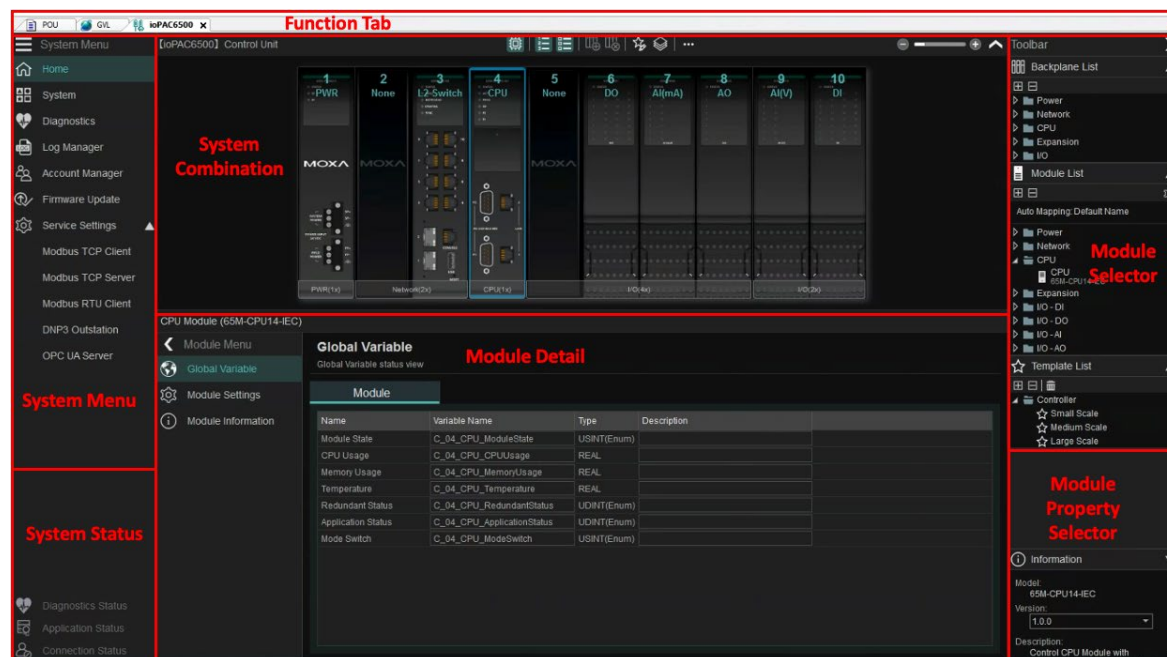
System Menu: The function related to the devices are listed here.

System Status: The diagnostic status (error or not), application status (run or stop), and connection status (which connection is established) are displayed here.

Function Settings Detail: The settings detail of each function is displayed here once the function was selected in the system menu.

Home

On the home page, the function settings detail window is categorized into the following parts.



System Combination

The module list of the system will be displayed here. There are some operations can be done in the system combination window.

1. Left select on the module: The module details will be displayed in the module detail window.
2. Right select on the module: You can remove and remap the variables supported by the module and import/export the module configuration.
3. Drag and drop the module: The module can be moved to the empty slot or be deleted.
4. For frequently used system combinations, select **Save as Template** (🌟) to save the combination in the Template List.
5. Add/Remove expansion unit:

Select **Add Expansion** (🔧) to add an expansion unit. The ioPAC 6500 Series supports up to four expansion units.

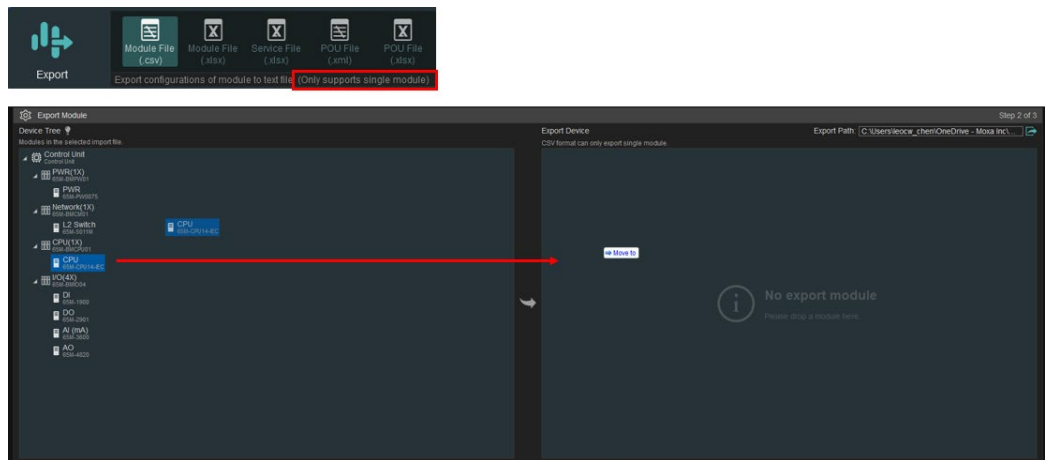
Select **Remove Expansion** (🔧) to remove the expansion unit.

6. Mass configuration:

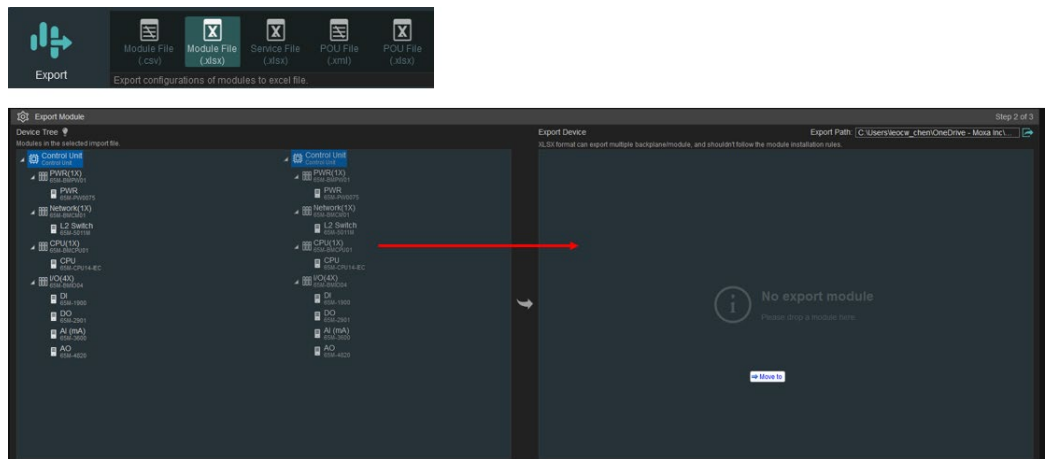
Select **Mass Configuration** () to export/import configuration.

➤ Export Configuration:

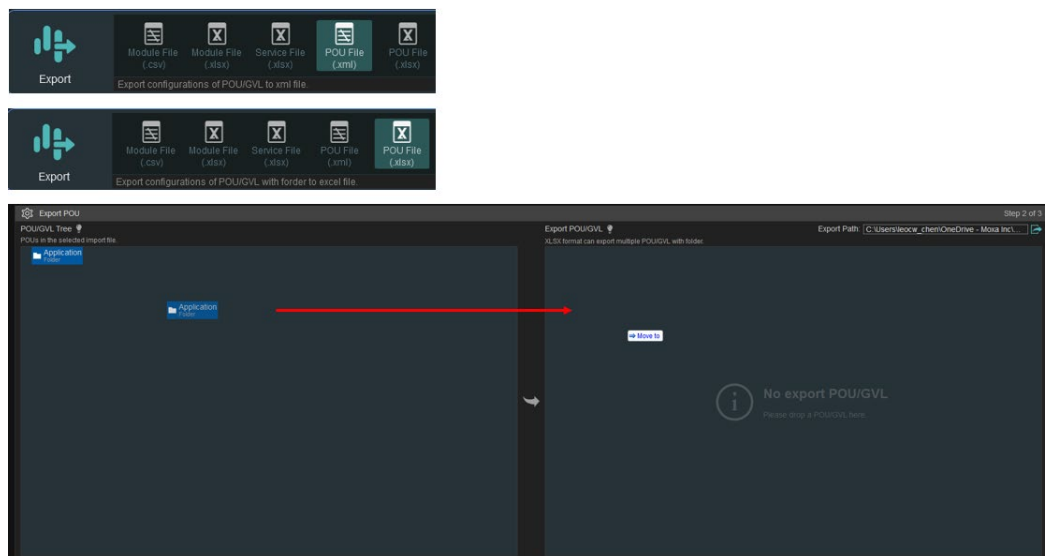
- ❑ Export module file (csv.)—supports only single module



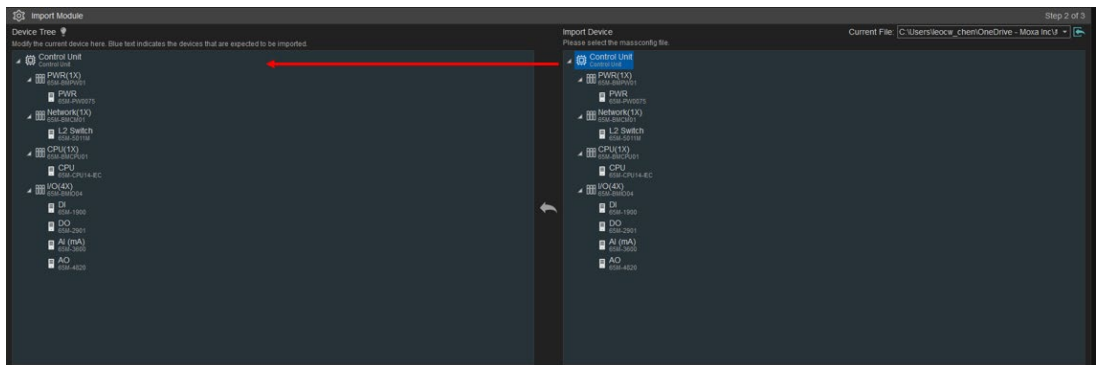
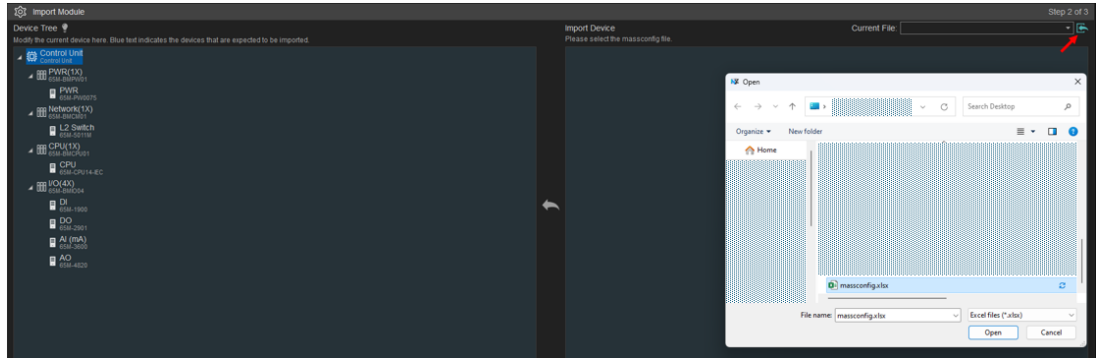
- ❑ Export module file (xlsx.)—supports multiple modules



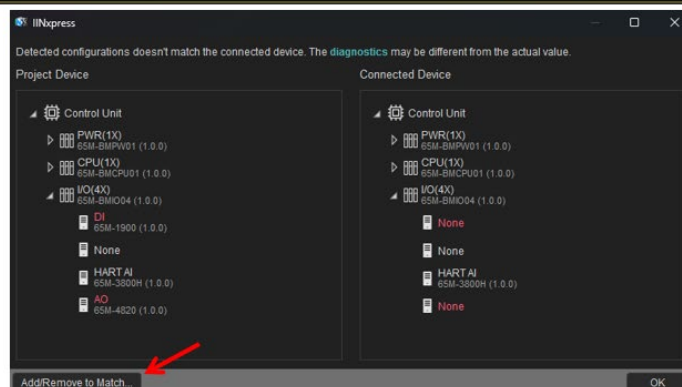
- ❑ Export Service file—see details in Service Settings
- ❑ Export POU file (xml. or xlsx.)—POU and GVL



- **Import Configuration:** Reverse the process of exporting. Choose the file that's meant to be imported, drag and drop the configuration from right to left.



- When connecting device, please ensure there is no topology or configuration mismatch between projects and devices. If a mismatch occurs, please address it promptly (See top left yellow exclamation mark)

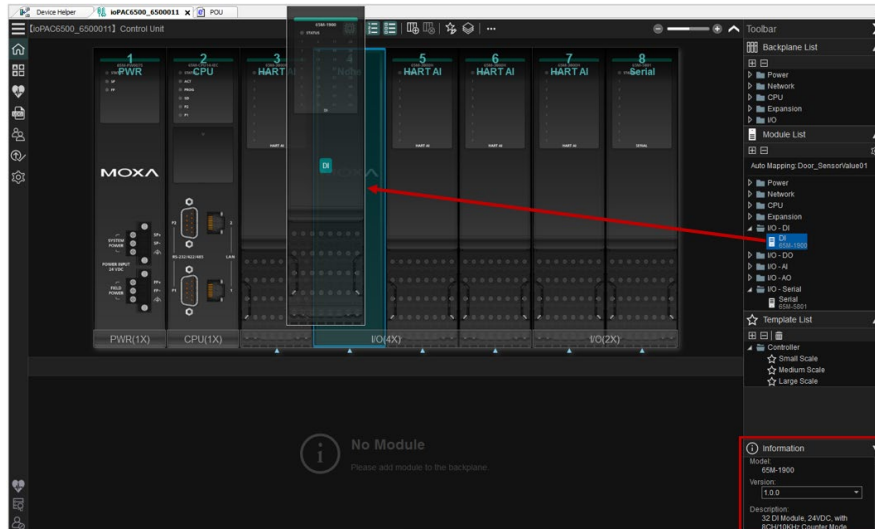


Module Detail

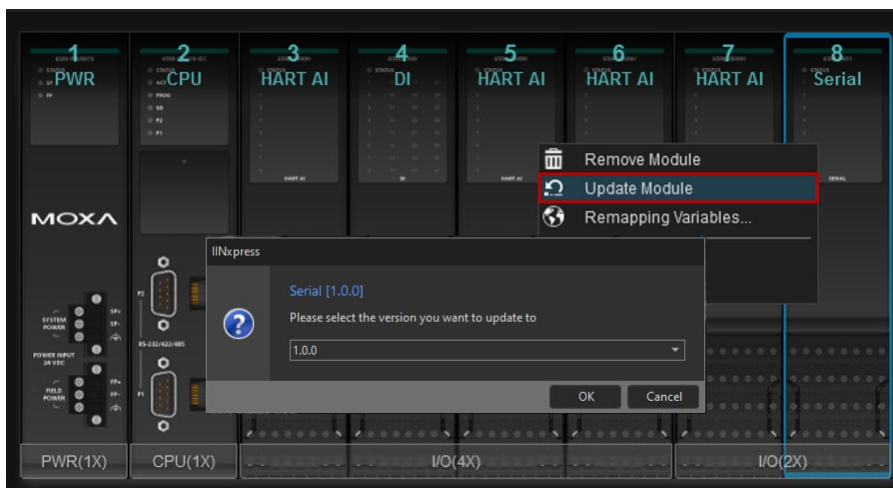
The selected module details will be displayed here. The details can be grouped into three sections: **Global Variables**, **Module Settings**, **Module Information**.

General information and settings for all modules:

- Before dragging and dropping the module into the desired slot, be sure to check the firmware version on the bottom right to avoid any incompatible issues.



- Right-select on the module to update module firmware when deemed necessary.



NOTE

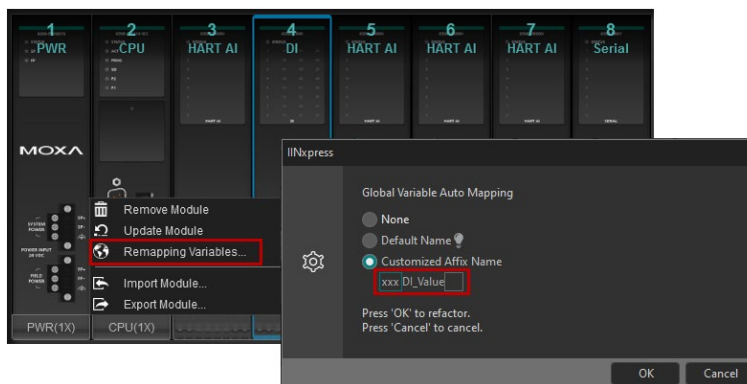
Be aware that an old project (configuration) must be updated to be compatible with hardware preloaded with newer firmware to enable the use of new functions (if applicable).

Global Variables: The Global Variables supported by the module will be displayed here. The module and channel will be listed as global variables, which can be used in POU. When the device is connected, the value of variables can also be monitored as well.

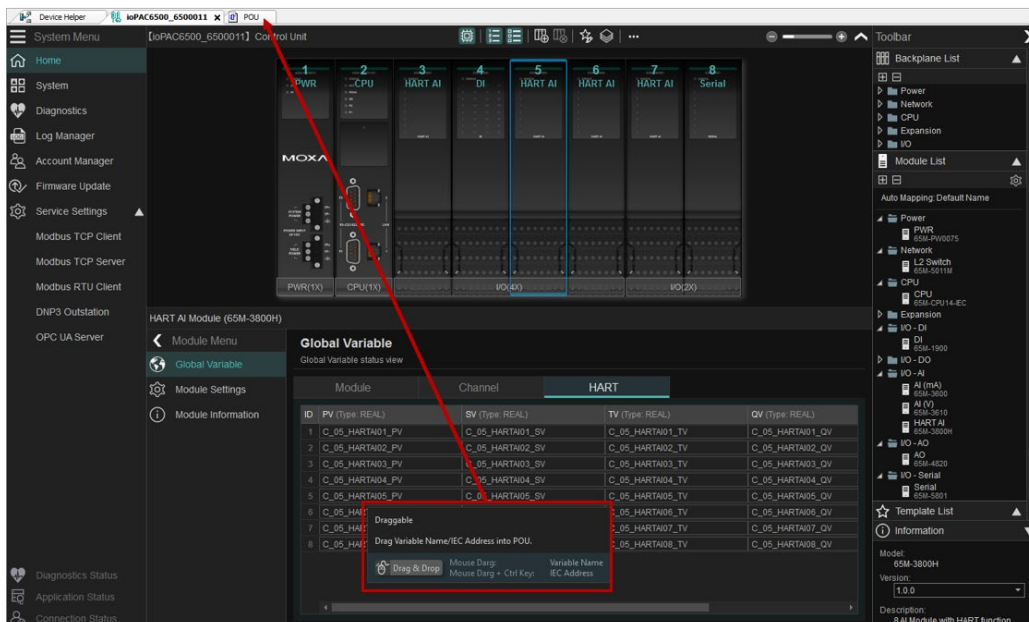
- Double-click the default name to rename the Global Variable based on the application's context, which can be useful when later called in the POU.

ID	Value (Type: BOOL)	Diagnostic Error (Type: BOOL)	Wirebreak (Type: BOOL)	Description
1	C_04_DI01_Value	C_04_DI01_DiagnosticError	C_04_DI01_Wirebreak	
2	C_04_DI02_Value	C_04_DI02_DiagnosticError	C_04_DI02_Wirebreak	
3	C_04_DI03_Value	C_04_DI03_DiagnosticError	C_04_DI03_Wirebreak	
4	C_04_DI04_Value	C_04_DI04_DiagnosticError	C_04_DI04_Wirebreak	
5	C_04_DI05_Value	C_04_DI05_DiagnosticError	C_04_DI05_Wirebreak	
6	C_04_DI06_Value	C_04_DI06_DiagnosticError	C_04_DI06_Wirebreak	
7	C_04_DI07_Value	C_04_DI07_DiagnosticError	C_04_DI07_Wirebreak	
8	C_04_DI08_Value	C_04_DI08_DiagnosticError	C_04_DI08_Wirebreak	
9	C_04_DI09_Value	C_04_DI09_DiagnosticError	C_04_DI09_Wirebreak	
10	C_04_DI10_Value	C_04_DI10_DiagnosticError	C_04_DI10_Wirebreak	
11	C_04_DI11_Value	C_04_DI11_DiagnosticError	C_04_DI11_Wirebreak	
12	C_04_DI12_Value	C_04_DI12_DiagnosticError	C_04_DI12_Wirebreak	

- Right-select on the module and select "Remapping Variables" to customize in a batch the affix naming of the Global Variables.



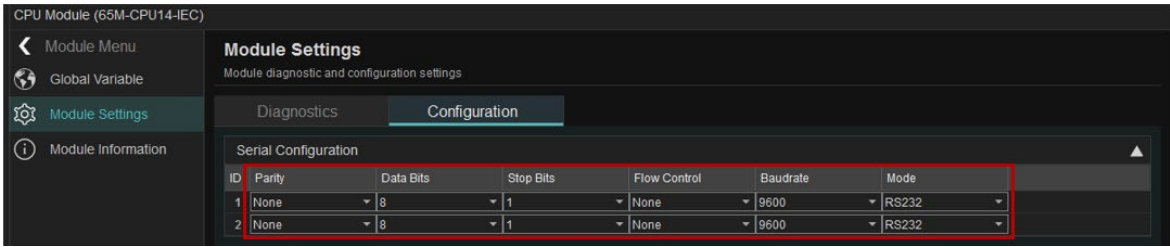
- After renaming the Global Variables, they can simply be dragged and dropped into the POU.



Module Settings: The diagnostic variable and module configuration will be displayed here. See below for more detailed module information.

65M-CPU14-IEC CPU module:

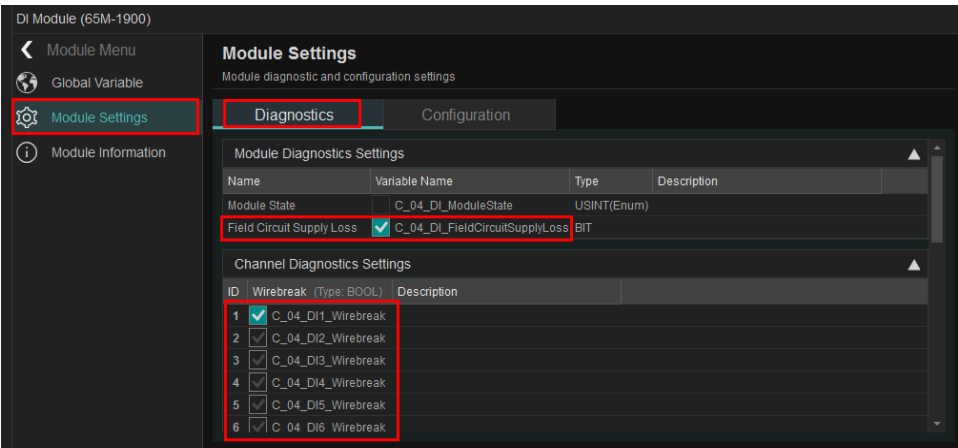
Configuration: There are two serial ports on the CPU module with DB9 interfaces. The parameters for serial communication can be configured as shown below.



65M-1900 DI module Settings:

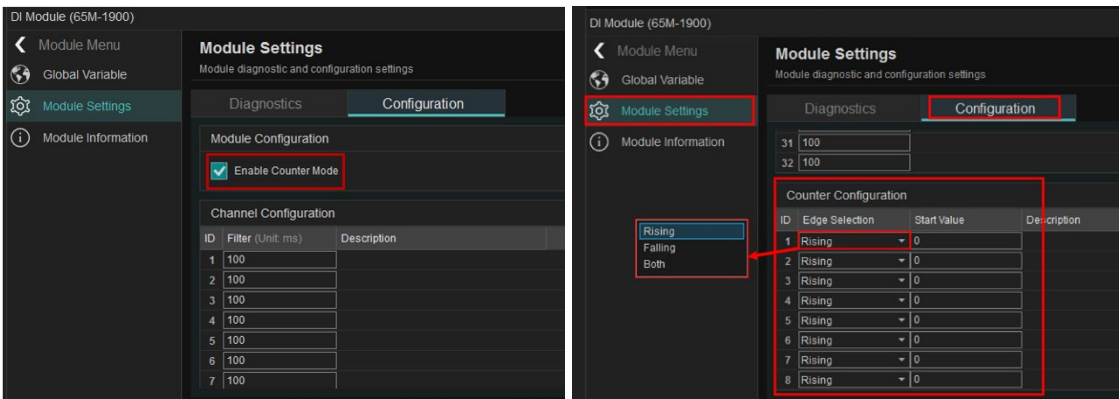
Enable/Disable Diagnostics:

- Field Circuit Supply Loss: To detect if field power supplying for DI contacts fails.
- Wirebreak: To detect if the wiring between the DI contact to the channel is broken.

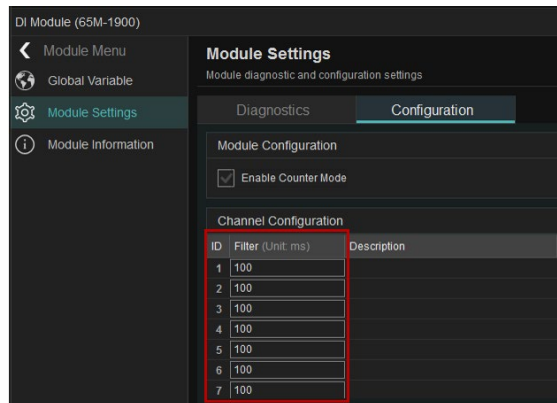


Configuration:

- Enable counter mode: Only Channel 1 to 8 can be configured in counter mode, while the triggering condition can be defined as rising, falling, or both.



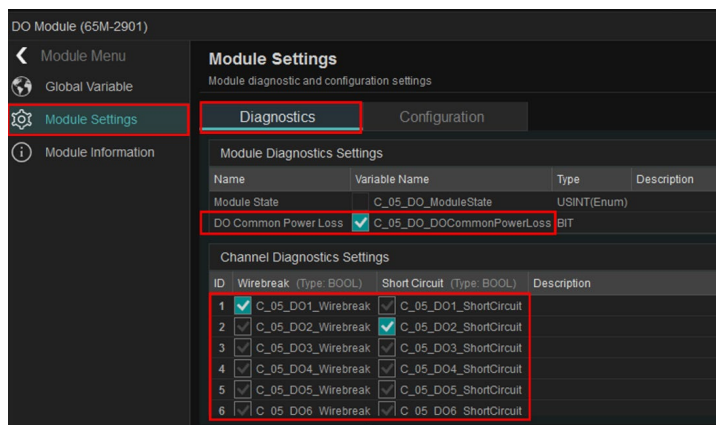
- **Filter:** The filter can be set to ignore the spurious signals by waiting for a certain period before registering a valid state change.



65M-2900 DO module Settings:

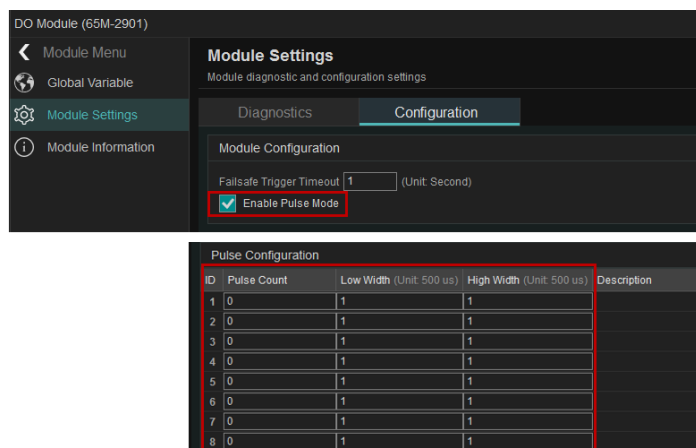
Enable/Disable Diagnostics:

- **DO Common Power Loss:** To detect if external power supplying for DO contacts fails.
- **Wirebreak:** To detect if the wiring between the DO unit to the channel is broken.
- **Short Circuit:** To detect if there is a short circuit on the DO channel.



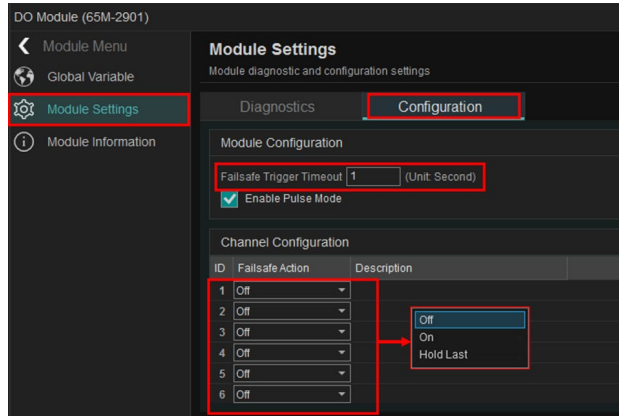
Configuration:

- **Enable Pulse Mode:** Only Channel 1 to 8 can be configured in Pulse mode. Scroll down in configuration, set the following parameters for counter mode.
- **Pulse Count:** Set the number of counts to output after the start.
- **Low Width:** Set the time of the low state in the pulse.
- **High Width:** Set the time of the high state in the pulse.



Failsafe configuration:

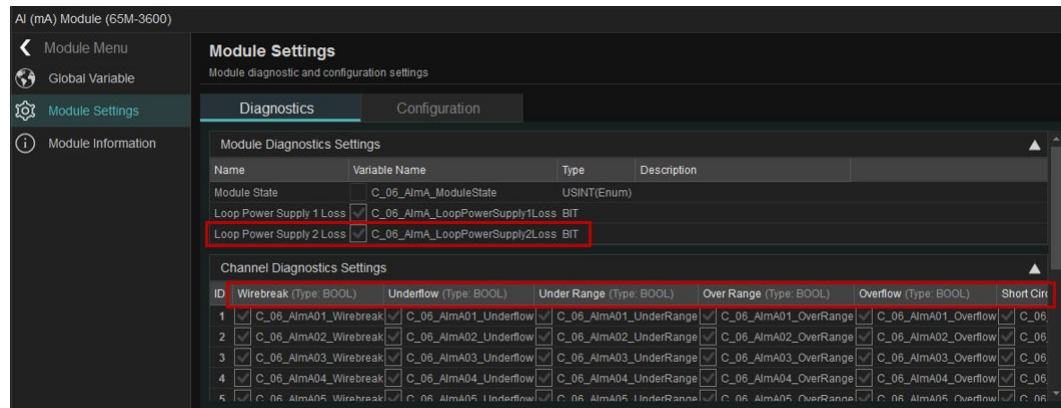
- Failsafe Trigger Timeout: Set timeout failsafe will be triggered after DO module communication loss.
- Failsafe Action: Set the action of each DO channel after DO module communication loss. The action of the DO channel can be OFF/ON/Hold Last.



65M-3600 AI (mA) module Settings:

Enable/Disable AI (mA) diagnostics:

- Loop Power Supply Loss: To detect if field power supplying for AI fails.
- Wirebreak: To detect if the wiring between the sensor to the channel is broken, which means the current value is smaller than the wirebreak threshold.
- Underflow: To detect if the current value is smaller than the underflow threshold.
- Under Range: To detect if the current value is below the range of the AI (mA) channel.
- Over Range: To detect if the current value is over the range of the AI (mA) channel.
- Overflow: To detect if the current value is larger than the overflow threshold.
- Short Circuit: To detect if there is a short circuit on the AI (mA) channel, which means the current value is larger than the short-circuit threshold.



Configuration:

- Range: 0 to 20 (mA), 4 to 20 (mA)
- The Diagnostics threshold for Wirebreak, Underflow, Over Range and Short Circuit can be adjusted.

ID	Range	Wirebreak Threshold (Unit: mA)	Underflow Threshold (Unit: mA)	Overflow Threshold (Unit: mA)	Short Circuit Threshold (Unit: mA)	Description
1	4 - 20 mA	0.80	2.40	21.60	23.20	
2	4 - 20 mA	0.80	2.40	21.60	23.20	
3	0 - 20 mA	0.80	2.40	21.60	23.20	
4	4 - 20 mA	0.80	2.40	21.60	23.20	
5	4 - 20 mA	0.80	2.40	21.60	23.20	
6	4 - 20 mA	0.80	2.40	21.60	23.20	
7	4 - 20 mA	0.80	2.40	21.60	23.20	
8	4 - 20 mA	0.80	2.40	21.60	23.20	
9	4 - 20 mA	0.80	2.40	21.60	23.20	
10	4 - 20 mA	0.80	2.40	21.60	23.20	

65M-3610 AI (V) module Settings:

Enable/Disable AI (V) diagnostics:

- Wirebreak: To detect if the wiring between the sensor to the channel is broken, which means the voltage value is smaller than the wirebreak threshold.
- Underflow: To detect if the voltage value is smaller than the underflow threshold.
- Under Range: To detect if the voltage value is below the range of the AI (V) channel.
- Over Range: To detect if the voltage value is over the range of the AI (V) channel.
- Overflow: To detect if the voltage value is larger than the overflow threshold.

ID	Wirebreak (Type: BOOL)	Underflow (Type: BOOL)	Under Range (Type: BOOL)	Over Range (Type: BOOL)	Overflow (Type: BOOL)	Description
1	☒ C_07_AI01_Wirebreak	☒ C_07_AI01_Underflow	☒ C_07_AI01_UnderRange	☒ C_07_AI01_OverRange	☒ C_07_AI01_Overflow	
2	☒ C_07_AI02_Wirebreak	☒ C_07_AI02_Underflow	☒ C_07_AI02_UnderRange	☒ C_07_AI02_OverRange	☒ C_07_AI02_Overflow	
3	☒ C_07_AI03_Wirebreak	☒ C_07_AI03_Underflow	☒ C_07_AI03_UnderRange	☒ C_07_AI03_OverRange	☒ C_07_AI03_Overflow	
4	☒ C_07_AI04_Wirebreak	☒ C_07_AI04_Underflow	☒ C_07_AI04_UnderRange	☒ C_07_AI04_OverRange	☒ C_07_AI04_Overflow	
5	☒ C_07_AI05_Wirebreak	☒ C_07_AI05_Underflow	☒ C_07_AI05_UnderRange	☒ C_07_AI05_OverRange	☒ C_07_AI05_Overflow	
6	☒ C_07_AI06_Wirebreak	☒ C_07_AI06_Underflow	☒ C_07_AI06_UnderRange	☒ C_07_AI06_OverRange	☒ C_07_AI06_Overflow	
7	☒ C_07_AI07_Wirebreak	☒ C_07_AI07_Underflow	☒ C_07_AI07_UnderRange	☒ C_07_AI07_OverRange	☒ C_07_AI07_Overflow	

Configuration:

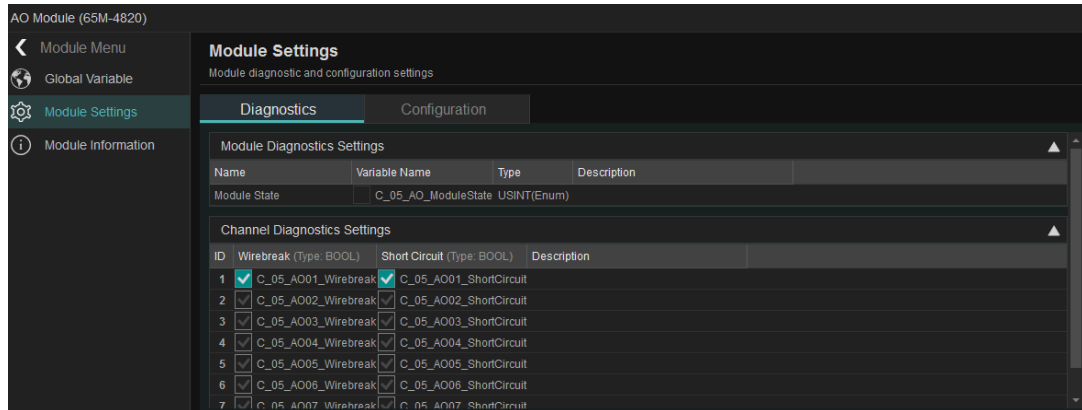
- Range: 1 to 5 (V), 0 to 10 (V)
- The Diagnostics threshold for Wirebreak, Underflow, and Overflow can be adjusted.

ID	Range	Wirebreak Threshold (Unit: V)	Underflow Threshold (Unit: V)	Overflow Threshold (Unit: V)	Description
1	0 - 10 VDC	-2.00	-1.00	11.00	
2	0 - 10 VDC	-2.00	-1.00	11.00	
3	1 - 5 VDC	-2.00	-1.00	11.00	
4	0 - 10 VDC	-2.00	-1.00	11.00	
5	0 - 10 VDC	-2.00	-1.00	11.00	
6	0 - 10 VDC	-2.00	-1.00	11.00	
7	0 - 10 VDC	-2.00	-1.00	11.00	
8	0 - 10 VDC	-2.00	-1.00	11.00	
9	0 - 10 VDC	-2.00	-1.00	11.00	
10	0 - 10 VDC	-2.00	-1.00	11.00	

65M-4820 AO module Settings:

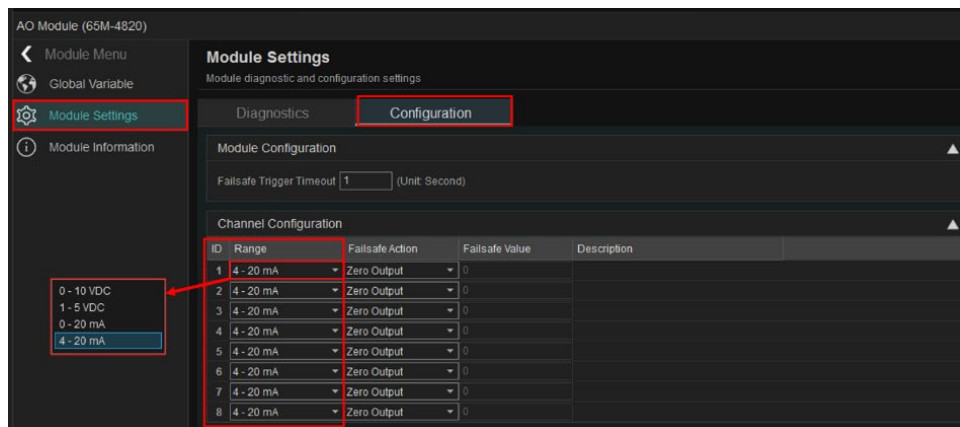
Enable/Disable AO diagnostics:

- Wirebreak: To detect if the wiring between the AO unit to the channel is broken.
- Short Circuit: To detect if there is a short circuit on the AO channel.



Configuration:

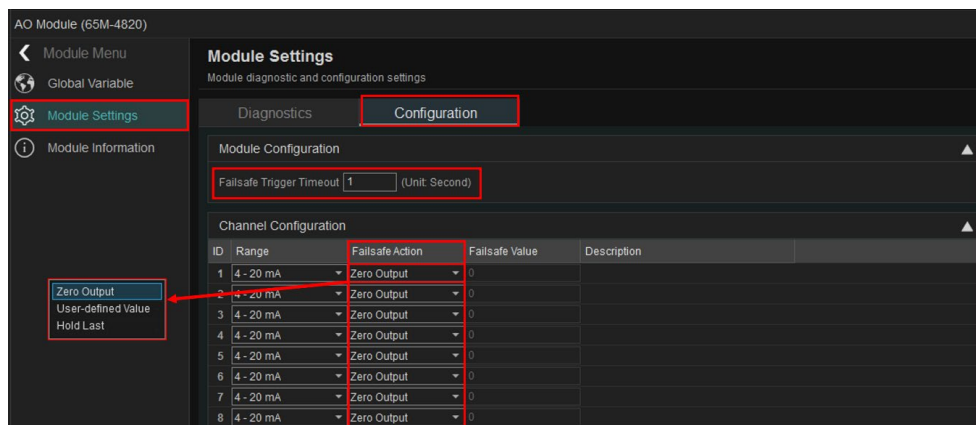
- Configure the Range of the AO channel. Choose 0 to 0 VDC / 1 to 5 VDC / 0 to 20 mA / 4 to 20 mA.



- Set the parameters for Failsafe.

Failsafe Trigger Timeout: Set timeout failsafe will be triggered after AO module communication loss.

Failsafe Action: Set the action of each AO channel after AO module communication loss. The action of the AO channel can be Zero Output / User-defined Value / Hold Last.



65M-3800H HART AI (mA) module Settings:

Global Variable:

PV, SV, TV, QV Setting—After configuring PV, SV, TV, and QV via PACTware, these data will also be sent to IINxpress (ioPAC 6500 IDE Utility Software) and can be accessed in the POU. Make sure the HART is enabled.



NOTE

For detailed PACTware configuration guidance, refer to "ioPAC 6500 Series HART Module Configuration Manual—PACTware"

The screenshot shows two software windows. The top window is PACTware, displaying the HART AI Module (65M-3800H) configuration. The bottom window is IINxpress, displaying the Global Variable status view for the HART module. A red box highlights the 'Global Variable' section in IINxpress, which contains a table of variables and their values.

ID	PV (Type: REAL)	SV (Type: REAL)	TV (Type: REAL)	QV (Type: REAL)
1	C_03_HARTAI01_PV	0.00	C_03_HARTAI01_TV	0.00
2	C_03_HARTAI02_PV	0.00	C_03_HARTAI02_TV	0.00
3	C_03_HARTAI03_PV	0.00	C_03_HARTAI03_TV	0.00
4	C_03_HARTAI04_PV	0.00	C_03_HARTAI04_TV	0.00
5	C_03_HARTAI05_PV	0.00	C_03_HARTAI05_TV	0.00
6	C_03_HARTAI06_PV	0.00	C_03_HARTAI06_TV	0.00
7	C_03_HARTAI07_PV	0.00	C_03_HARTAI07_TV	0.00
8	C_03_HARTAI08_PV	0.00	C_03_HARTAI08_TV	0.00

Enable/Disable AI (mA) diagnostics:

- Loop Power Supply Loss: To detect if field power supplying for AI fails.
- Wirebreak: To detect if the wiring between the sensor to the channel is broken, which means the current value is smaller than the wirebreak threshold.
- Underflow: To detect if the current value is smaller than the underflow threshold.
- Under Range: To detect if the current value is below the range of the AI (mA) channel.
- Over Range: To detect if the current value is over the range of the AI (mA) channel.
- Overflow: To detect if the current value is larger than the overflow threshold.
- Short Circuit: To detect if there is a short circuit on the AI (mA) channel, which means the current value is larger than the short-circuit threshold.

The screenshot shows the 'Module Settings' window for the HART AI Module (65M-3800H). The 'Diagnostics' tab is selected, showing 'Module Diagnostics Settings' and 'Channel Diagnostics Settings'.

Name	Variable Name	Type	Description
Module State	C_03_HARTAI_ModuleState	USINT(Enum)	
Loop Power Supply Loss	C_03_HARTAI_LoopPowerSupplyLoss	BIT	

ID	Wirebreak (Type: BOOL)	Underflow (Type: BOOL)	Under Range (Type: BOOL)	Over Range (Type: BOOL)	Overflow (Type: BOOL)	Short Circuit (Type: BOOL)
1	C_03_HARTAI01_Wirebreak	C_03_HARTAI01_Underflow	C_03_HARTAI01_UnderRange	C_03_HARTAI01_OverRange	C_03_HARTAI01_Overflow	C_03_HARTAI01_ShortCircuit
2	C_03_HARTAI02_Wirebreak	C_03_HARTAI02_Underflow	C_03_HARTAI02_UnderRange	C_03_HARTAI02_OverRange	C_03_HARTAI02_Overflow	C_03_HARTAI02_ShortCircuit
3	C_03_HARTAI03_Wirebreak	C_03_HARTAI03_Underflow	C_03_HARTAI03_UnderRange	C_03_HARTAI03_OverRange	C_03_HARTAI03_Overflow	C_03_HARTAI03_ShortCircuit
4	C_03_HARTAI04_Wirebreak	C_03_HARTAI04_Underflow	C_03_HARTAI04_UnderRange	C_03_HARTAI04_OverRange	C_03_HARTAI04_Overflow	C_03_HARTAI04_ShortCircuit
5	C_03_HARTAI05_Wirebreak	C_03_HARTAI05_Underflow	C_03_HARTAI05_UnderRange	C_03_HARTAI05_OverRange	C_03_HARTAI05_Overflow	C_03_HARTAI05_ShortCircuit
6	C_03_HARTAI06_Wirebreak	C_03_HARTAI06_Underflow	C_03_HARTAI06_UnderRange	C_03_HARTAI06_OverRange	C_03_HARTAI06_Overflow	C_03_HARTAI06_ShortCircuit
7	C_03_HARTAI07_Wirebreak	C_03_HARTAI07_Underflow	C_03_HARTAI07_UnderRange	C_03_HARTAI07_OverRange	C_03_HARTAI07_Overflow	C_03_HARTAI07_ShortCircuit

Configuration:

- Channel Enable/Disable (Default Enabled): The disabled channel will be skipped when polling.
- HART Enable/Disable (Default Disabled): The disabled channel is used as a regular 4-20 (mA) AI. Check "enable" box if HART field device is used.
- The range is set to be 4-20 (mA) and can't be adjusted.
- The threshold for Wirebreak, Underflow, Overflow, and Short Circuit can be adjusted.

HART AI Module (65M-3800H)

Module Settings
Module diagnostic and configuration settings

Diagnostics Configuration

ID	Channel Enable	HART Enable	Range	Wirebreak Threshold (Unit: mA)	Underflow Threshold (Unit: mA)	Overflow Threshold (Unit: mA)	Short C
1	☒	☐	4 - 20 mA	0.80	2.40	21.60	23.20
2	☒	☐	4 - 20 mA	0.80	2.40	21.60	23.20
3	☒	☐	4 - 20 mA	0.80	2.40	21.60	23.20
4	☒	☐	4 - 20 mA	0.80	2.40	21.60	23.20
5	☒	☐	4 - 20 mA	0.80	2.40	21.60	23.20
6	☒	☐	4 - 20 mA	0.80	2.40	21.60	23.20
7	☒	☐	4 - 20 mA	0.80	2.40	21.60	23.20
8	☒	☐	4 - 20 mA	0.80	2.40	21.60	23.20

65M-5801 Serial module Settings:

Configuration:

- Interface, Baud rate, Parity, Data bits, Stop bits and Flow control can be adjusted in configuration.

Serial Module (65M-5801)

Module Settings
Module diagnostic and configuration settings

Diagnostics Configuration

ID	Interface	Baudrate	Parity	Data Bits	Stop Bits	Flow Control
1	RS232	28800	None	8	1	None
2	RS422	28800	None	8	1	None
3	RS485 2-wire	28800	None	8	1	None
4	RS485 2-wire	28800	None	8	1	None
5	RS485 2-wire	28800	None	8	1	None
6	RS485 2-wire	28800	None	8	1	None
7	RS485 2-wire	28800	None	8	1	None
8	RS485 2-wire	28800	None	8	1	None

Module Information: The module information (e.g., firmware version, module serial number, LED status, serial status, mode switch, etc.) will be displayed here. IINxpress shows product specifications here for reference. **Connect the device** to access information.



NOTE

All the information and settings of the switch module can be completed in the web interface of the switch module. Select the link in the module detail page, and the web interface of the switch module will open in the default browser.

Module Selector

The available modules are listed here. Drag and drop the selected module to the system combination window for the system setup. Follow the steps to set up the system combination.

1. Choose the backplane module: The ioPAC 6500 is fully modular design. Drag and drop the needed backplane module in designated order.
2. Choose the other modules: Drag and drop other modules to the designated slot. The module can only be placed on the corresponding backplane. The restricted sign will appear when you drag a module to an unsupported backplane, reminding you not to place it in the slot.

IINxpress also supports the template list. Drag and drop the whole system combination and make some minor changes to meet your application's requirements. IINxpress provides small, medium, and large scale as template. You can also reuse a system combination that you saved previously.

Module Property Selector

When you select an available module, you will see its properties displayed here. Choose the property version here to match the combination you need.

System

All the system information, settings, and configuration can be found on the system page.

System Information

System identification (model name, serial number, device name), device information (system uptime, CPU/memory usage), runtime/OS version, network information, and time can be found here. All the information is read-only.

System Menu

Home

System

Diagnostics

Log Manager

Account Manager

Firmware Update

Service Settings

Modbus TCP Client

Modbus TCP Server

Modbus RTU Client

DNP3 Outstation

OPC UA Server

Diagnostics OK

Stop

moxa

System

System, service status and configuration

System Information

Services Status

Reset/Restart

Backup/Restore

ioPAC6500

Model Name

65M-CPU14-IEC

Serial Number

IMOXA0100016

Device Name

ioPAC6500_0100016

Description

Device Information

System Up Time

05d 23:19:48

CPU Usage

11%

Memory Usage

17%

Version

Runtime

3.5.19.50

Operating System

MIL3IOPAC

Network

IP Address 1

10.90.30.17

Subnet Mask 1

255.255.252.0

LAN MAC 1

00:90:a8:12:00:02

Gateway 1

10.90.28.1

IP Address 2

192.168.126.254

Subnet Mask 2

255.255.255.0

LAN MAC 2

00:a0:c9:12:00:01

Gateway 2

DNS 1

10.123.200.11

DNS 2

Time

Current Time

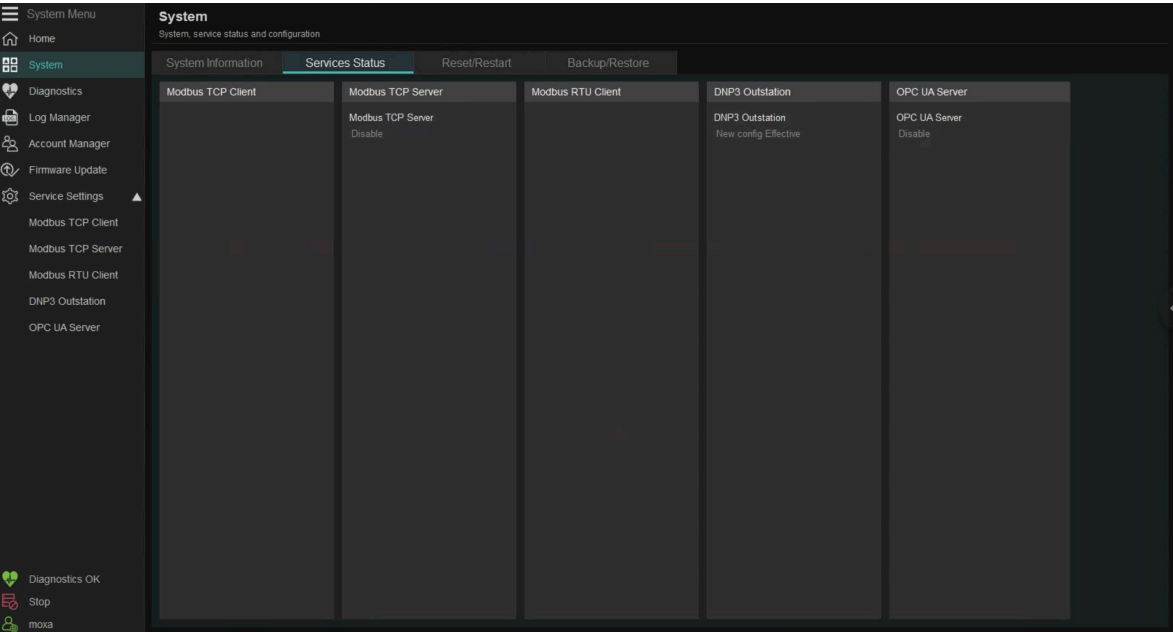
2024/07/24 18:42:25

Time Zone

(GMT+08:00)Taipei

Service Status

It shows the status of all supported services, which include the Modbus TCP/RTU Server/Client, DNP3 outstation, OPC UA, etc.



Reset/Restart

There are several reset/restart types supported by ioPAC 6500, and all of them are listed on the page. Select an action first, then select Run. A pop-up warning message will appear. Follow the instructions to complete the reset/restart process.



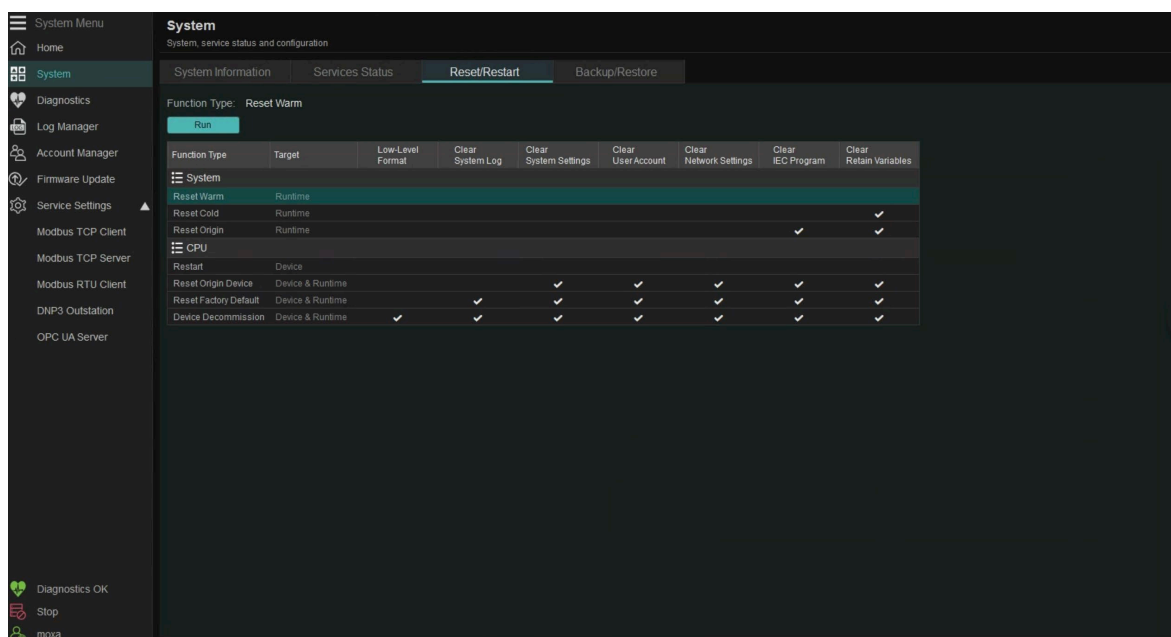
NOTE

Resetting or restarting the system will clear different system information. Make sure to read the table before performing the rest/restart process.



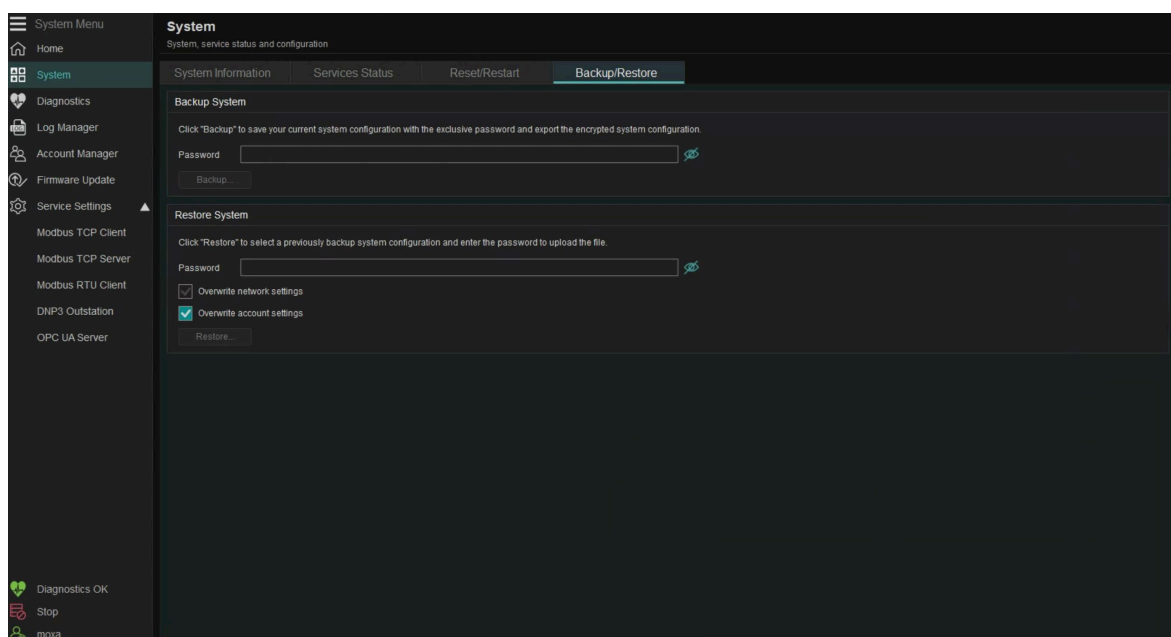
NOTE

Push the reset button to complete the **Reset Factory Default** and **Device Decommission**. Follow the instructions to complete the process.



Backup/Restore

Back up and restore the system configuration on this page.



Follow these steps to back up the system configuration.

1. Key in the password.
2. Select the **Backup** button and choose where you want to save the configuration file. The password length is required to be between 8 and 63 characteristics.

Follow these steps to restore the system configuration.

1. Key in the password
2. Choose to overwrite the network and account settings or not.
 - Overwrite the network settings: The restore process will overwrite the network settings. The system's Ethernet connection might be lost during the restoration.
 - Overwrite the account settings: The restore process will overwrite the account settings. The account you are using might not be available anymore.
3. Select the **Restore** button and choose the configuration file which you want to restore.

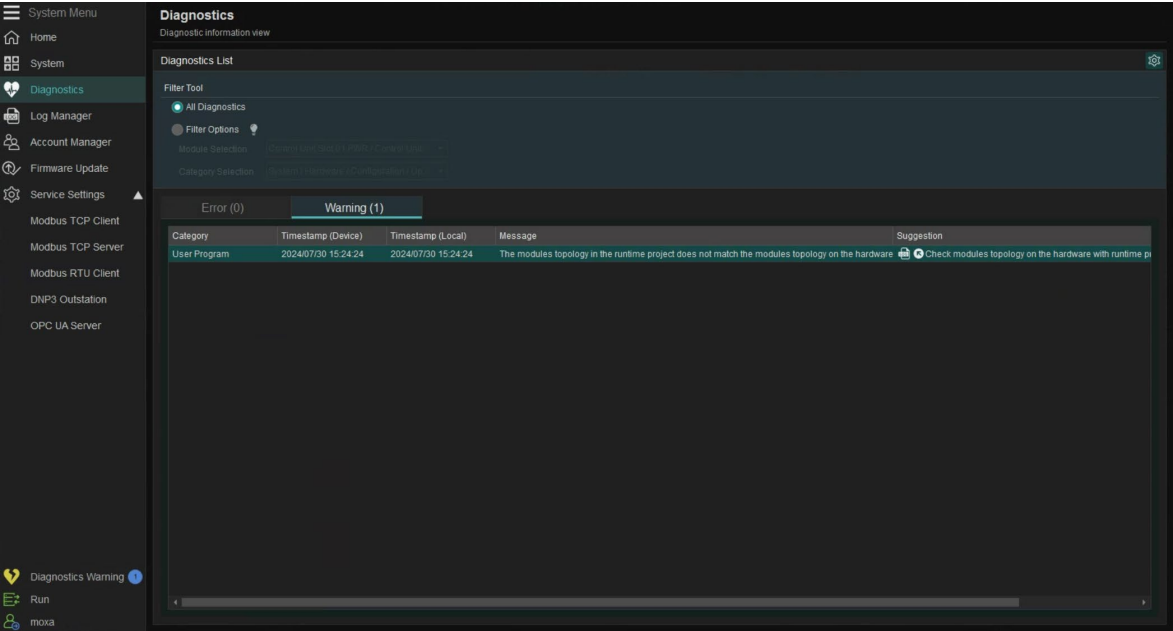
Diagnostic

The diagnostic information will be displayed on the Diagnostic page. The error and warning messages that are persistent can be found in the Error and Warning tab, respectively.



NOTE

Diagnostics will not display the error and warning messages that occur once.



Log Manager

All the logs will be stored inside the ioPAC 6500 system. Use IINXpress to retrieve the log and show in IINXpress. IINXpress can perform five actions in a log.

- **Retrieve:** Retrieves the log from the device and shows it in IINXpress.
- **Delete:** Deletes the log stored in the device.
- **Backup:** Back ups the displayed log to the file.
- **Open:** Opens the backup log file.
- **Clear:** Clears the log list in IINXpress. This action will not clear the log inside the device.

For the detailed log list, refer to the log section of the web interface.

The screenshot displays the Log Manager interface within a web application. On the left is a sidebar menu with options: System Menu, Home, System, Diagnostics, Log Manager (selected), Account Manager, Firmware Update, Service Settings, Modbus TCP Client, Modbus TCP Server, Modbus RTU Client, DNP3 Outstation, and OPC UA Server. The main panel is titled 'Log Manager' and includes a sub-header 'Retrieve log files and and system log view'. Below this are five buttons: Retrieve (highlighted in blue), Delete, Backup, Open, and Clear. A 'Log List' section contains a 'Filter Tool' with a 'Field Selection' dropdown (set to 'Selected Field...'), a 'Show Filter' checkbox (checked), and a 'Clear Filter' button. Below the filter tool is a pagination bar showing 'Page: 1', '1 - 3 of 3', and 'Items Per Page: 10'. The log list is a table with the following data:

ID	Severity	Category	Event Name	Source	Timestamp (Device)	Timestamp (Local)	Message	Suggest
1	Informational	UserProgram	Application Run Success	10.160.123.189	2024/08/05 11:12:50	2024/08/05 11:12:50	Application run successfully	Check #
2	Informational	UserProgram	Application Stop Success	10.160.123.189	2024/08/05 11:12:49	2024/08/05 11:12:49	Application stop successfully	Check #
3	Informational	Log	Event Log Clear Success	10.160.123.189	2024/08/05 11:12:00	2024/08/05 11:12:00	Clear event log successfully	Check #

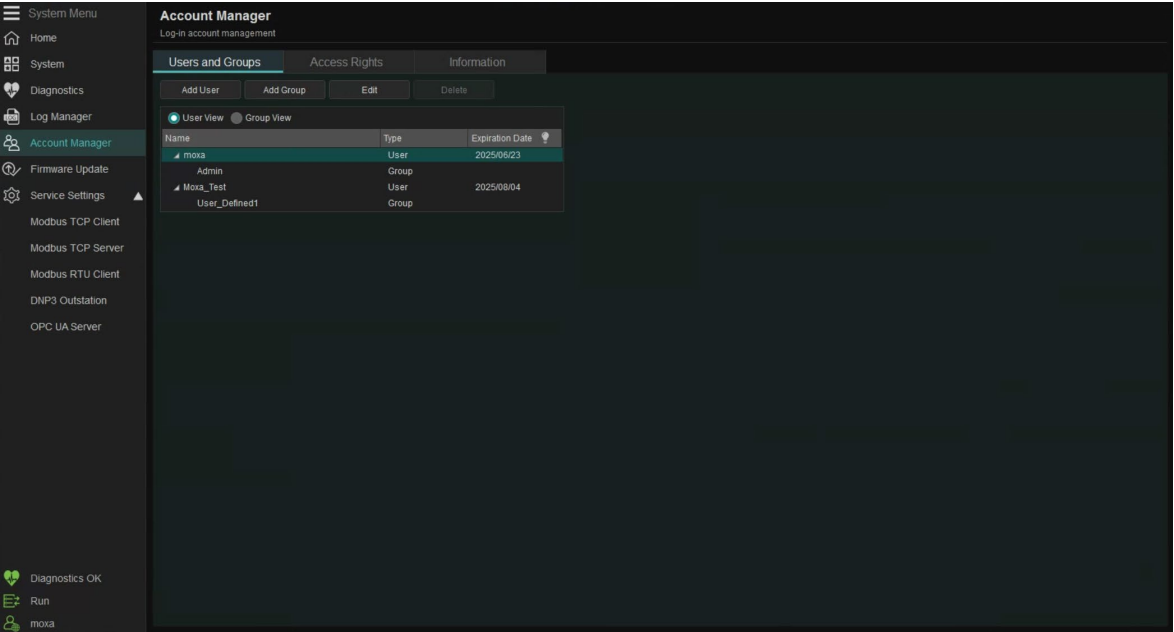
At the bottom of the interface, there is a 'Diagnostics Warning' section with a 'Run' button and a 'Data from: Device' section showing a clock icon and the timestamp '2024/08/05 11:11:18'.

Account Manager

The account and its authority can be managed on the Account Manager page. Account manager settings consist of three main parts.

Users and Groups

On this page, make changes related to the users and groups. All user accounts will be displayed on this page. Choose to show in User view and Group view. In the ioPAC 6500 system, the login property of account belongs to the user group.



Add User

When you want to create a new user account, select the **Add User** and a window will pop up. Once you confirmed all the account property and group assignments, select OK to complete the account creation.



NOTE

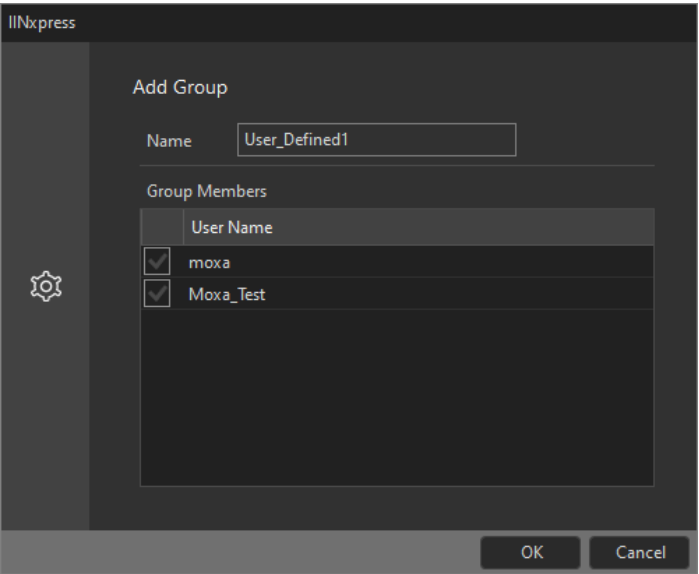
Before editing the users and groups, make sure the login account has permission to change the account settings.

	Group Name
☒	Admin
☒	Account_Manager
☒	Secure_Auditor
☒	Secure_Admin
☒	Installer
☒	Engineer
☒	Operator
☒	Manager

OK Cancel

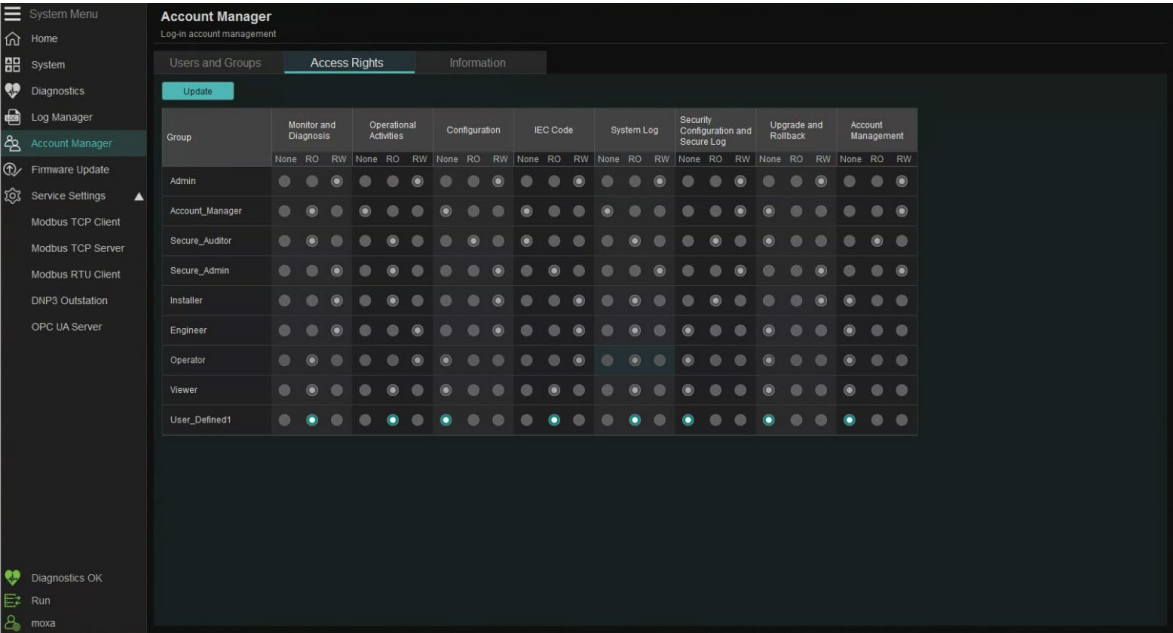
Add Group

When you want to create a new user group, select the **Add Group** and a window will pop up. Specify the group name and assign the user accounts to the group. For the group property, change in Access Rights tab.



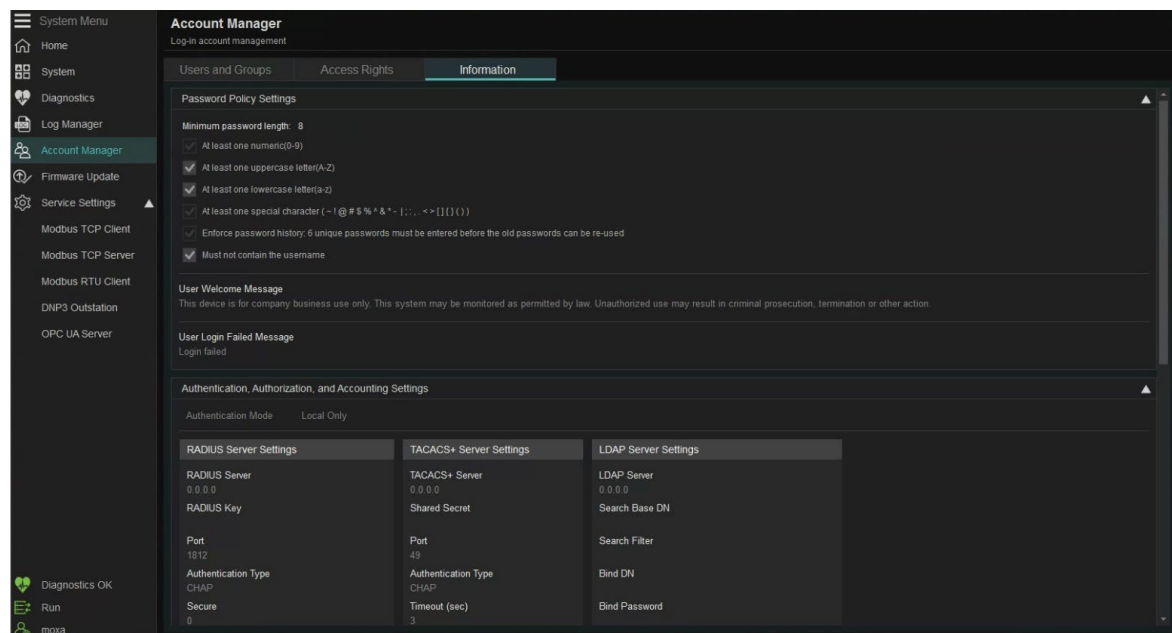
Access Rights

Change the property of the group on the Access Rights page. You cannot change the authority of the default 8 groups. You can only change the authority of the user-created group.



Information

The information will display the current password policy. It can only be modified on the system webpage. When IINxpress connects the device, the latest password policy will be loaded automatically. For the details about the password policy, refer to the Account Manager section on the webpage.



Firmware Update

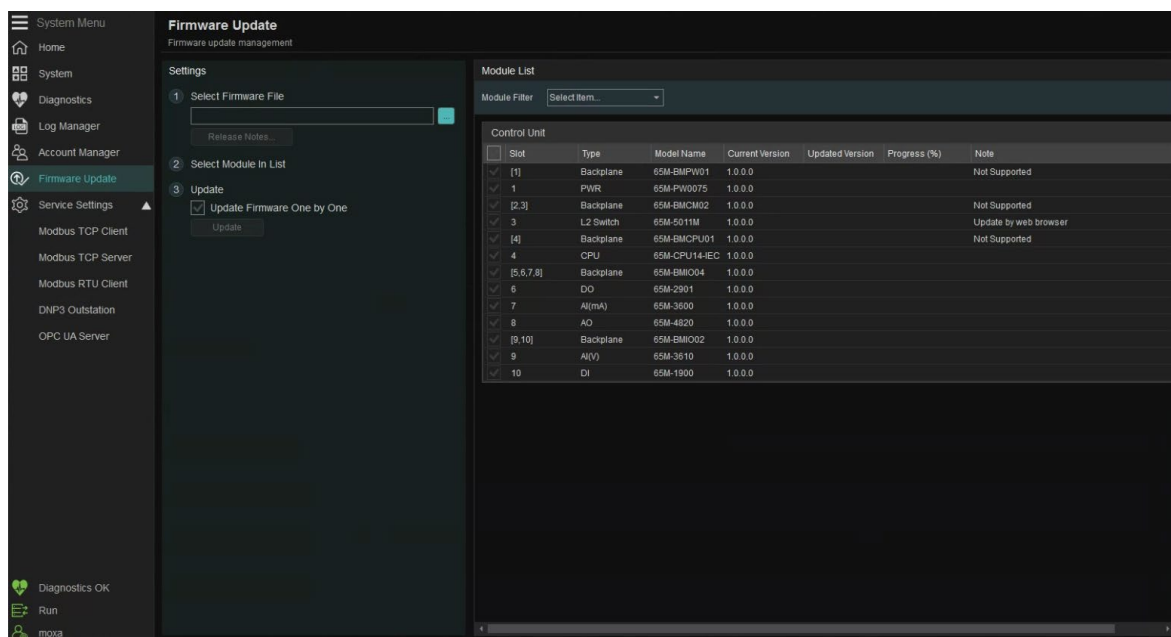
IINxpress also allows you to update the firmware to the system. Follow the following three steps to complete the firmware update.

- Select Firmware File:** Select  to choose the firmware file that needs to be updated to the system. The firmware file can be chosen from the local disk or a SFTP from a remote site. You can also select the Release Notes button to check the release details.
- Select Module on List:** Select the modules that need to be updated on the **Module List**. Use the module filter to speed up the module selection. The module list will display module information.
 - **Slot:** Shows the slot where the module is installed. The system combination determines the slot number. The number 1 shows the left-most module of each unit. The slot of the backplane module will be displayed with a number in square brackets, e.g., [1].
 - **Type:** It shows the module type. E.g., CPU, DI, backplane, etc.
 - **Model Name:** The model name of the module will be displayed here.
 - **Current Version:** The current firmware version of the module will be displayed here.
 - **Update Version:** The firmware version included in this firmware file will be displayed here.
 - **Progress(%):** The updated progress will be here.
 - **Note:** Any other information that cannot be categorized will be displayed here.
- Update:** Select **Update** to start the system firmware update. Choose **Update Firmware One by One** to update the firmware module by module.



NOTE

Update the switch module's firmware on the web page of the switch module.

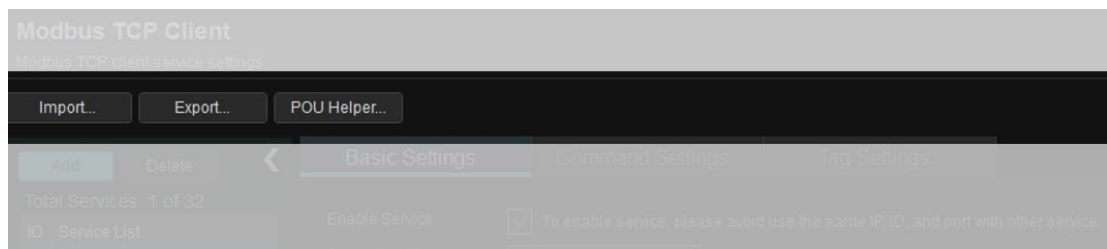


Service Settings

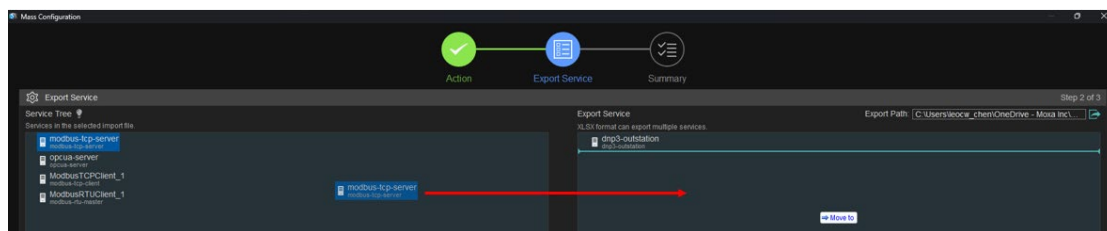
The ioPAC 6500 system provides a protocol service to lower your programming effort. Use the protocol service to collect data from other devices and use the collected data in the program or deliver to the upper-level system.

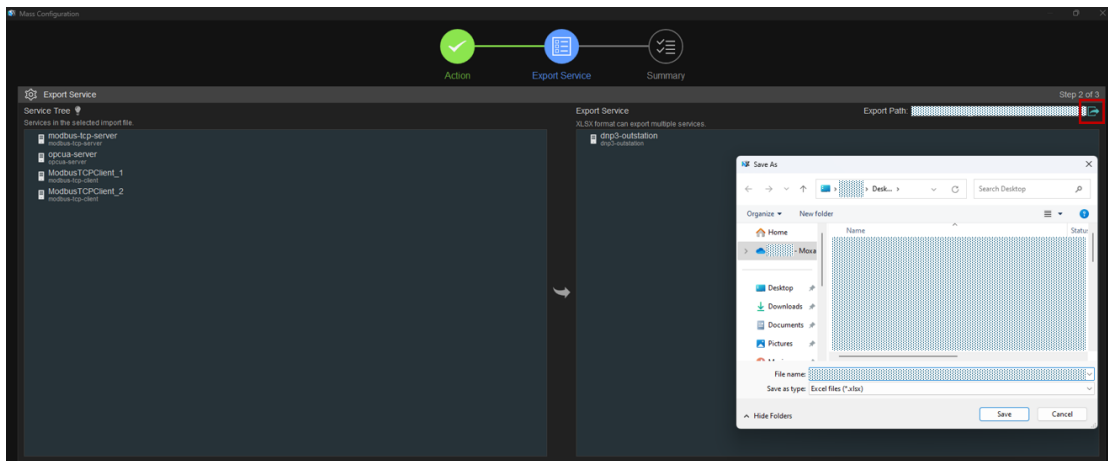
General Information for All Services

Import, Export, and POU Helper: They can be seen in each of the service pages, prompting easier mass configuration and better service management.

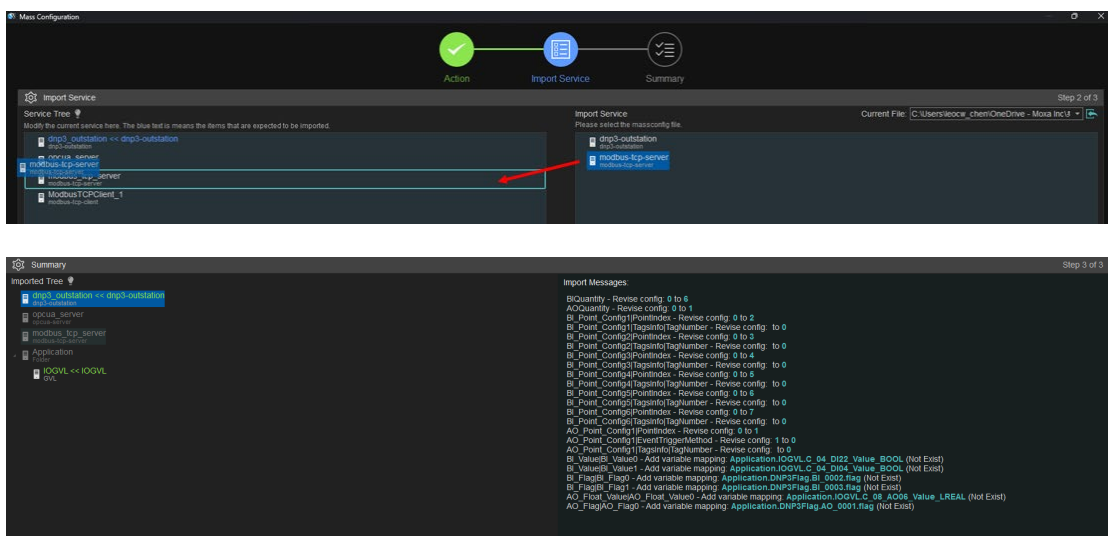


Export: Drag and drop the service from Service Tree to Export Service. The configuration will be stored as .xlsx file.





Import: Select the desired .xlsx file. Drag and drop from import service to service tree. Blue text indicates the services that are expected to be imported

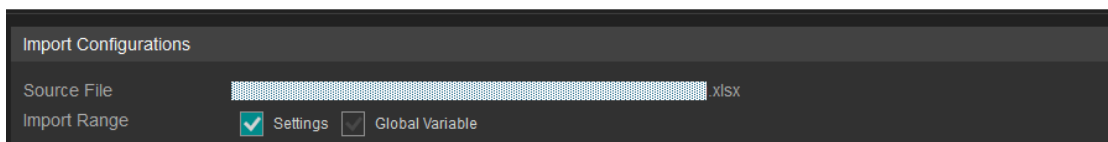


NOTE

When importing the service configuration, the system checks the following:

1. When a new variable is specified, the system checks whether the variable name already exists. If a duplicate is found, the variable cannot be created, and the importing operation will be blocked.
2. When an existing variable is specified, the system checks whether it is an I/O variable. If so, the system will attempt to generate the corresponding IOGVL. If the generation fails, the importing operation will also be blocked.

Uncheck the "Global Variable" in import Configurations, if variables importing is not needed.



POU Helper: POU Helper shows detailed information on how sources and variables are mapped, as the data exchange between service and I/O points are carried out via POU. Select **Load** to get the status. Select **Clear** to delete everything.

Service with I/O

DNP3 Flag

The data exchange between Service and I/O points must be carried out through POU.
In this table all data exchange variables generated automatically by the system are displayed. (Including all Services)

Load

Repair

Clear

Variables

Suggestion	Variable	Source	Source Type	Reference	Count	
	C_04_DI22_Value_BOOL	C_04_DI22_Value	BOOL	dnp3-outstation	1	
	C_04_DI04_Value_BOOL	C_04_DI04_Value	BOOL	dnp3-outstation	1	
	C_05_DO10_Value_BOOL	C_05_DO10_Value	BOOL	ModbusTCPClient_1	2	

NOTE

If “Remove”, “Rename” or “Recreate” appears in the suggestion, revisit the configuration within your application or select **Repair**.

Service with I/O

DNP3 Flag

The data exchange between Service and I/O points must be carried out through POU.
In this table all data exchange variables generated automatically by the system are displayed. (Including all Services)

Load

Repair

Clear

Variables

Suggestion	Variable	Source	Source Type	Reference	Count	
Remove	C_01_PWR_SystemPowerFail_...	C_01_PWR_SystemPowerFail	BOOL		0	
	C_04_DI22_Value_BOOL	C_04_DI22_Value	BOOL	dnp3-outstation	1	
	C_04_DI04_Value_BOOL	C_04_DI04_Value	BOOL	dnp3-outstation	1	

Service with I/O

DNP3 Flag

The data exchange between Service and I/O points must be carried out through POU.
In this table all data exchange variables generated automatically by the system are displayed. (Including all Services)

Load

Repair

Clear

Variables

Suggestion	Variable	Source	Source Type	Reference	Count	
Rename	C_05_DO01_ValueA_BOOL	C_05_DO01_Test	BOOL		0	

Service with I/O

DNP3 Flag

The data exchange between Service and I/O points must be carried out through POU.
In this table all data exchange variables generated automatically by the system are displayed. (Including all Services)

Load

Repair

Clear

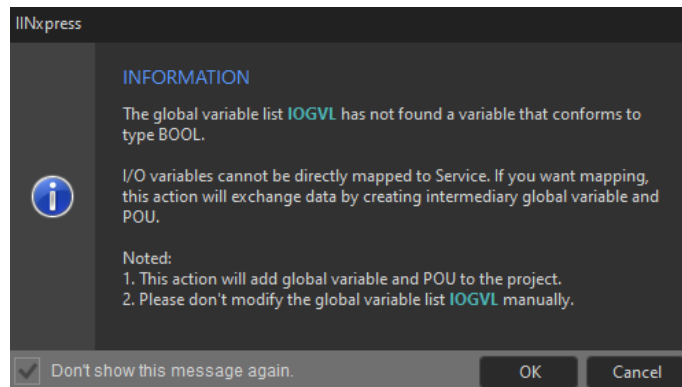
Variables

Suggestion	Variable	Source	Source Type	Reference	Count	
Recreate	C_04_DI22_Value_BOOL	C_04_DI22_Value	BOOL		0	
Recreate	C_04_DI04_Value_BOOL	C_04_DI04_Value	BOOL		0	
Recreate	C_05_DO16_Value_BOOL	C_05_DO16_Value	BOOL		0	



NOTE

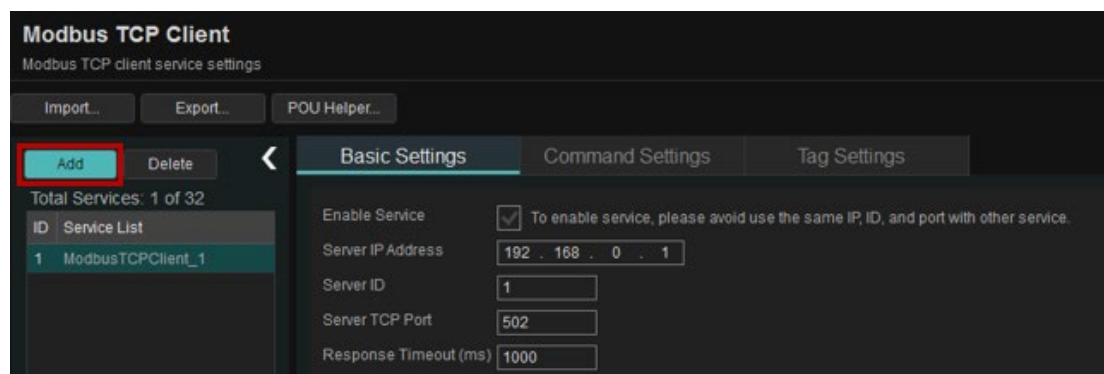
When mapping the variables, a message tells you that a variable was automatically created. Select OK to proceed.



Modbus TCP Client

Modbus TCP Client can collect data from up to 32 Modbus TCP servers. To add a Modbus TCP client, click the Add button and a new Modbus client profile will be added to the Service List. All properties of the Modbus TCP client are categorized into **Basic Settings**, **Command Settings**, and **Tag Settings**.

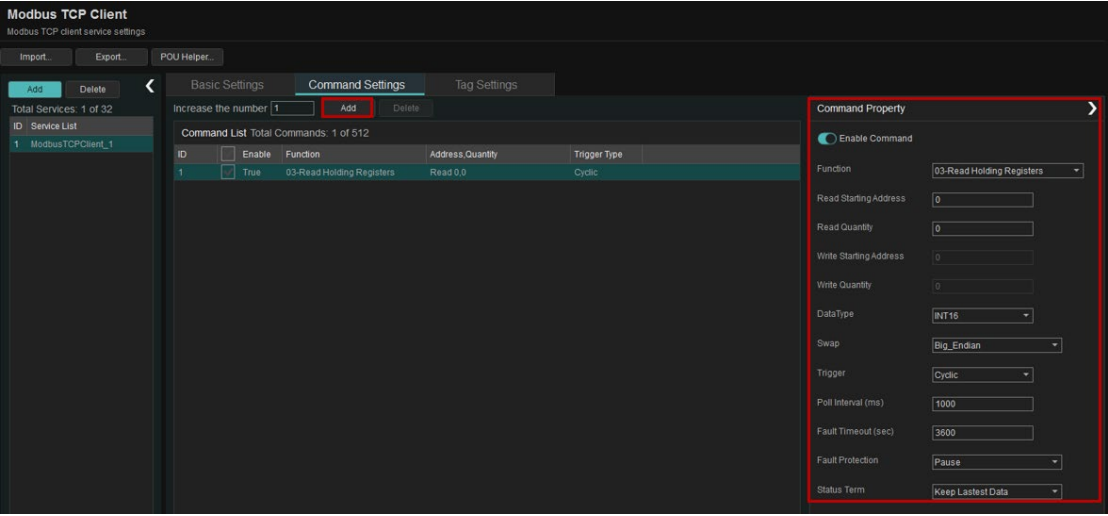
Basic Settings: Enable the service, set up the Server IP Address, Server ID, Server port, and response timeout on this page.



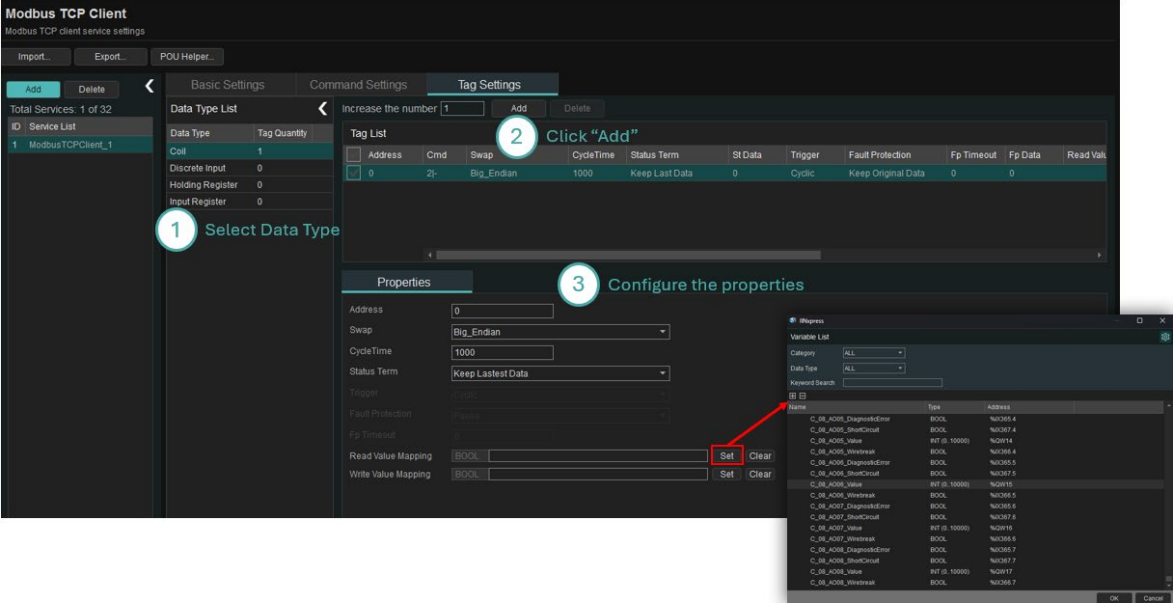
NOTE

Double-click the Name (ModbusTCPClient_1) on the Service list to rename.

Command Settings: Create command profiles to read from or write to Modbus TCP Server devices. Select **Add** and configure the command property on the right-hand side, e.g., Function Code, Start Address, Read Quantity, etc.



Tag Settings: The data array created on the Command Settings page will automatically appear on the Tag Settings page. Select **Set** to map the variables. Alternatively, follow the steps below to create tags manually.



Modbus TCP Server

Modbus TCP Server services can provide data to other Modbus TCP Client systems. All properties of the Modbus TCP Client are categorized into **Basic Settings**, **Function Settings**, **Variable Mapping**, and **Tag Summary**.

Basic Settings: Enable Service, Listen Port, Keep Alive Time and Server ID can be configured here.

The screenshot shows the 'Modbus TCP Server' window with the 'Basic Settings' tab selected. It includes buttons for 'Import...', 'Export...', and 'POU Helper...'. The settings are as follows:

Setting	Value
Enable Service	☒
Listen Port	502
Keep Alive Time (min)	1
Server ID	1

Function Settings: The ioPAC 6500 supports the function types: Coil, Discrete Input, Holding Register, and Input Register. Set up the tag quantity in the Function Settings based on the application. Follow the steps below to configure the functions.

The screenshot shows the 'Modbus TCP Server' window with the 'Function Settings' tab selected. It includes buttons for 'Import...', 'Export...', and 'POU Helper...'. The 'Data Type' section on the left has 'Coil' selected (1 section). The 'Section List' table shows 1 of 512 sections. The 'Function Property' section on the right shows 'Start Address' as 0 and 'Quantity' as 1. Numbered callouts indicate: 1. Select Data Type, 2. Click 'Add', and 3. Configure the start address and Quantity.

Function Type	Sections
Coil	1
Discrete Input	0
Holding Register	0
Input Register	0

ID	Start Address	Quantity
1	0	1

Variable Mapping: The tag quantity defined in Function Settings will appear here automatically. Sort the variables in the Variable List, then drag and drop them into the array to complete data mapping.

The screenshot shows the 'Modbus TCP Server' window with the 'Variable Mapping' tab selected. It includes buttons for 'Import...', 'Export...', and 'POU Helper...'. The 'Data Type' section on the left has 'Coil' selected (1 section). The 'Variable Mapping' table shows a list of variables. The 'Variable List' on the right shows a list of variables. Numbered callouts indicate: 1. Select the address that's meant to be mapped, 2. Select the variable, and 3. Drag the variable and drop it in the red box area.

Tag Name	Address	Data Type	Global Variable
Coil_Cmd01	000000	ARRAY [0..9] OF BOOL	
Coil[1]	000000	BOOL	Application.IOGVL_C_05_DO16_Val
Coil[4]	000003	BOOL	
Coil[5]	000004	BOOL	
Coil[6]	000005	BOOL	
Coil[7]	000006	BOOL	
Coil[8]	000007	BOOL	
Coil[9]	000008	BOOL	
Coil[10]	000009	BOOL	

Name	Type	Address
C_05_DO16_Diagno...	BOOL	%IX169.7
C_05_DO16_ShortCl...	BOOL	%IX177.7
C_05_DO16_Value	BOOL	%QX13.7
C_05_DO16...	BOOL	%IX178.0
C_05_DO17_ShortCl...	BOOL	%QX14.0
C_05_DO17_Value	BOOL	%QX174.0
C_05_DO17_Wirebr...	BOOL	%IX174.0
C_05_DO18_Diagno...	BOOL	%IX170.1

Tag Summary: Overview of all tags

Modbus TCP Server

Modbus TCP server service settings

Import...Export...POU Helper...

Basic SettingsFunction SettingsVariable MappingTag Summary

Data Type

Function Type	Sections
Coil	1
Discrete Input	0
Holding Register	0
Input Register	0

RefreshShow in new tab

Tag Summary

Address	Name	Data Type	Global Variable
000000	Cmd000_Coil[1]	Bool	Application.IOGVLC_05_DO16_Value_BOOL
000001	Cmd000_Coil[2]	Bool	Application.IOGVLC_05_DO18_Value_BOOL
000002	Cmd000_Coil[3]	Bool	
000003	Cmd000_Coil[4]	Bool	
000004	Cmd000_Coil[5]	Bool	
000005	Cmd000_Coil[6]	Bool	
000006	Cmd000_Coil[7]	Bool	
000007	Cmd000_Coil[8]	Bool	
000008	Cmd000_Coil[9]	Bool	
000009	Cmd000_Coil[10]	Bool	

Modbus RTU Client

The ioPAC 6500 system also supports the Modbus RTU client service. The only difference between Modbus TCP and RTU client service is the COM Port settings, which can be found on the basic setting page.

Basic Settings: Select **Add**, Enable Service, COM Port, Server ID, and Response Timeout can be configured here.

Modbus RTU Client

Modbus RTU client service settings

Import...Export...POU Helper...

AddDelete<Basic SettingsCommand SettingsTag Settings

Total Services: 1 of 31

ID	Service List
1	ModbusRTUClient_1

Enable Service☒To enable service, please avoid use the same ID, and port with other service.

COM Port

Server ID

1

Response Timeout (ms)

1000

Command Settings: Create command profiles to read from or write to Modbus RTU Server devices. Select **Add** and configure the command property on the right-hand side, e.g., Function Code, Start Address, Read Quantity, etc.

Modbus RTU Client

Modbus RTU client service settings

Import...Export...POU Helper...

AddDelete<Basic SettingsCommand SettingsTag Settings

Total Services: 1 of 31

ID	Service List
1	ModbusRTUClient_1

Increase the number

1

AddDelete

Command List Total Commands: 1 of 512

ID	Enable	Function	Address.Quantity	Trigger Type
1	☒	03-Read Holding Registers	Read 0.0	Cyclic

Command Property

☒Enable Command

Function

03-Read Holding Registers

Read Starting Address

0

Read Quantity

0

Write Starting Address

0

Write Quantity

0

DataType

INT16

Swap

Big_Endian

Trigger

Cyclic

Poll Interval (ms)

1000

Fault Timeout (sec)

3600

Fault Protection

Pause

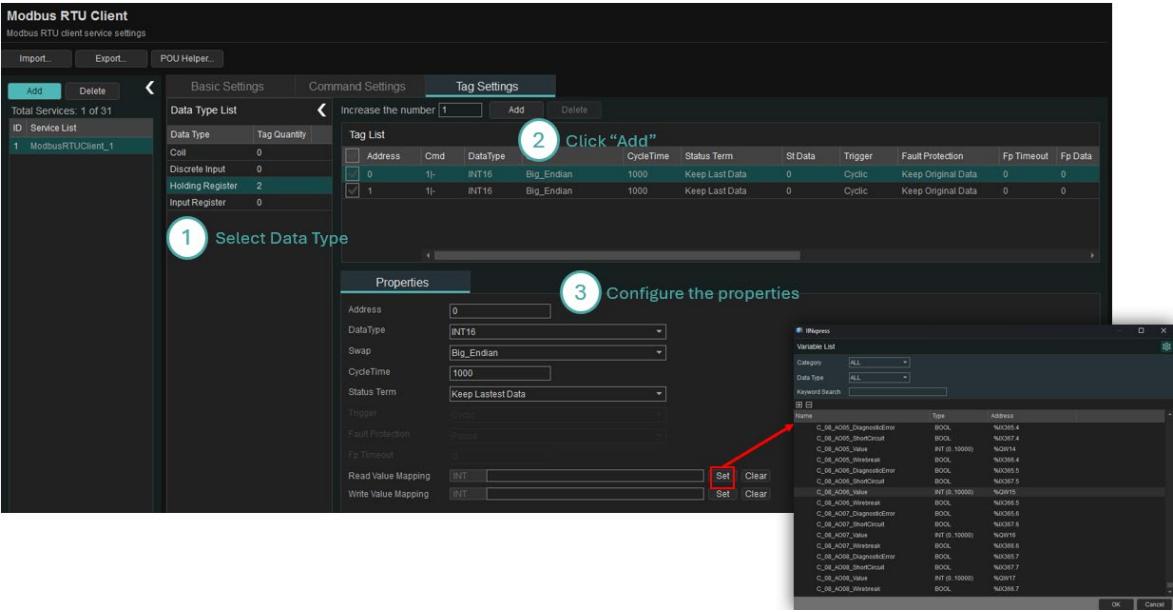
Status Term

Keep Lastest Data

ioPAC 6500 Series User Manual

125

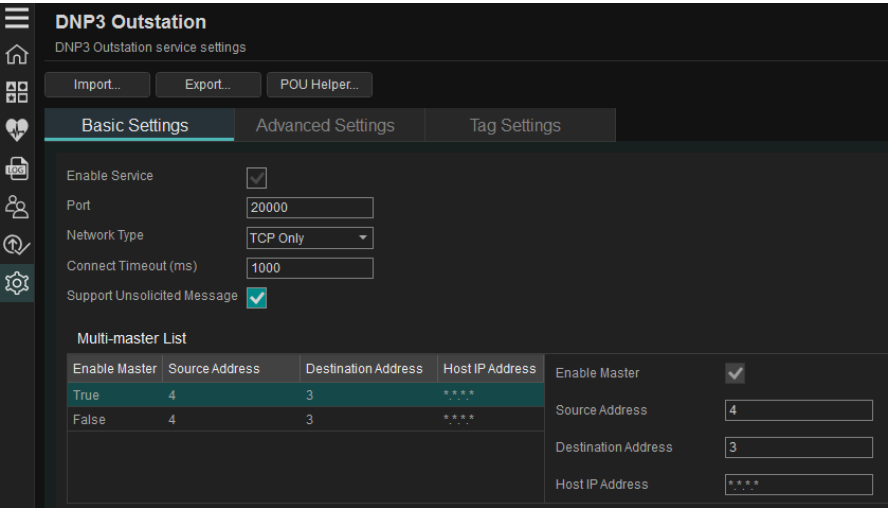
Tag Settings: The data array created on the Command Settings page will automatically appear on the Tag Settings page. Select **Set** to map the variables. Alternatively, follow the steps below to create tags manually.



DNP3 Outstation

DNP3 Outstation services can be used to provide data to other systems via DNP3 protocol. All properties of the DNP3 Outstation are categorized into **Basic Settings**, **Advanced Settings**, and **Tag Settings**.

Basic Settings: The basic settings page provides the essential functions, such as port, Network Type, etc., for you to set up. Multi-master can be enabled on this page as well. The ioPAC 6500 Series supports up to 2 clients. When the DNP 3 Outstation service is enabled, the first client is set to enabled.



Advanced settings

Security settings: These settings configure DNP3 Secure Authentication (SA) to protect communication between master and outstation from spoofing, tampering, or replay attacks.

Authenticated User List: This list defines who may operate or view. Please type the authentication update key before checking the "Enable User" box.

DNP3 Outstation : DNP3 Outstation service settings

Import... Export... POU Helper...

Basic Settings **Advanced Settings** Tag Settings

Security Settings

Enable Secure Authentication ☒

Authenticated Response Timeout (ms)

Support Aggressive Mode ☒

Max Session Key Change Count

Session Key Change Interval (ms)

Event Class of Authentication

MAC Algorithm

Authenticated User List

Enable User	User Name	User Number	User Role
False	default01	1	Role Operator
False	default02	2	Role Operator
False	default03	3	Role Operator
False	default04	4	Role Operator

Enable User ☒

User Name

User Number

User Role

Authentication Update Key

(16 or 32 hex octets) Total hexadecimal digits(Must be 32 or 64 hexadecimal digits) : 0

Item	Description
Enable Secure Authentication	Enables DNP3 Secure Authentication. Required to authenticate control commands or data exchanges.
Authenticated Response Timeout (ms)	Time (in milliseconds) the outstation waits for a "challenge" response from the client. If exceeded, the request is rejected.
Support Aggressive Mode	When enabled, the outstation proactively initiates challenge.
Max Session Key Change Count	The number of authenticated operations before a new session key must be generated. Enhances security by limiting key reuse.
Session Key Change Interval (ms)	Minimum time interval (in milliseconds) between session key changes. Prevents overly frequent updates.
Event Class of Authentication	Defines the class of authentication events.
MAC Algorithm	Specifies the Message Authentication Code (MAC) algorithm. 3 options are available: SHA1_Oct10, SHA256_Oct16 and AES_GMAC.

Unsolicited and event settings:

Unsolicited and Event Settings	
Unsolicited Confirm Timeout (ms)	10000
Unsolicited Response Retry	5
Unsolicited Class 1 Max Delay (ms)	1000
Unsolicited Class 2 Max Delay (ms)	1000
Unsolicited Class 3 Max Delay (ms)	1000
Unsolicited Class 1 Max Events	5
Unsolicited Class 2 Max Events	5
Unsolicited Class 3 Max Events	5
Event Buffer Overflow	Drop Oldest
BI Event Buffer Size	100
BO Event Buffer Size	100
Counter Event Buffer Size	30
Frozen Counter Event Buffer Size	30
AI Event Buffer Size	30
AO Event Buffer Size	100

Item	Description
Unsolicited Confirm Timeout (ms)	Timeout for waiting for an application layer confirmation (ACK) from the client after the outstation sends an unsolicited message.
Unsolicited Response Retry	Number of retries if the unsolicited message is not confirmed.
Unsolicited Class (X) Max Delay (ms)	Maximum delay allowed before the outstation sends an unsolicited message if any events are waiting in each class.
Unsolicited Class (X) Max Events	Limits how many events of each class are bundled into a single unsolicited response.
Event Buffer Overflow	What would be dropped if buffer overflows? Two options are available: Drop Oldest or Drop Latest.
BI Event Buffer Size	Number of Binary Input events stored
BO Event Buffer Size	Number of Binary Output events stored
Counter Event Buffer Size	Number of Counter events (e.g., pulse count changes) stored
Frozen Counter Buffer Size	Number of frozen counters (e.g., snapshots) values stored
AI Event Buffer Size	Number of Analog Input changes stored
AO Event Buffer Size	Number of Analog Output feedback or confirmation events stored

Data Link Layer Settings:

Data Link Layer Settings	
Enable Data Link Layer	☒
Data Link Layer Confirm Timeout (ms)	10000
Data Link Layer Confirm Max Retry	5

Item	Description
Enable Data Link Layer	Enables data link layer functions
Data Link Layer Confirm Timeout (ms)	Time to wait for data link acknowledgment before retrying
Data Link Layer Confirm Max Retry	Number of times the outstation will retry a message if the link-layer acknowledgment isn't received

Other Settings:

Other Settings	
Application Confirm Timeout (ms)	10000
Keepalive Period (ms)	30000
Enable Time Sync	☒
Time Sync Period (ms)	1800000
Select Control Timeout (ms)	5000

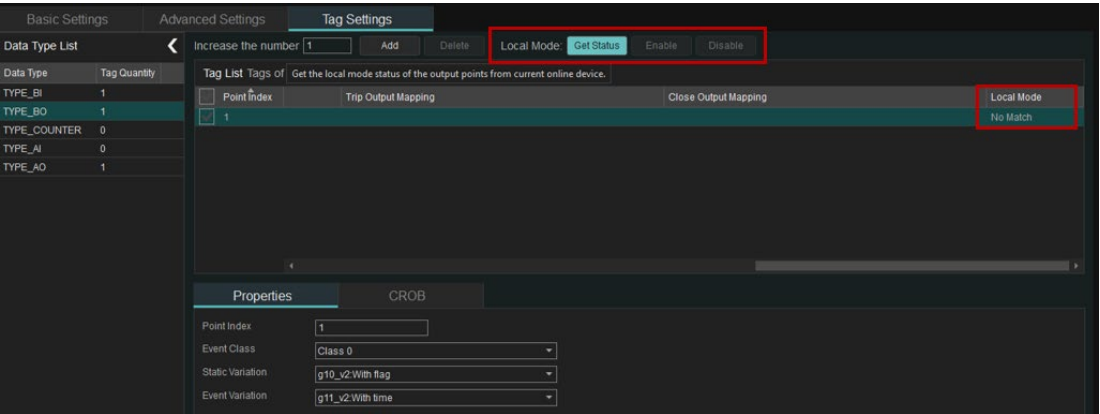
Item	Description
Application Confirm Timeout	The time the outstation waits for an application-layer confirmation (APPL-CONFIRM) after sending a message that requires one.
Keepalive Period	Interval at which the outstation sends an idle test message. If no activity has occurred, to keep the session alive.
Enable Time Sync	Whether the outstation allows the client to synchronize its internal clock.
Time Sync Period	How often does the outstation expect a time sync.
Select Control Timeout	Time allowed between the Select and Operate commands in a Select-Before-Operate (SBO) control.

Tag settings: Follow the steps below to configure Tags

The screenshot shows the 'DNP3 Outstation' configuration window, specifically the 'Tag Settings' tab. The interface includes a 'Data Type List' on the left, a 'Tag List' in the center, and a 'Properties' panel at the bottom. Three numbered callouts indicate the configuration steps:

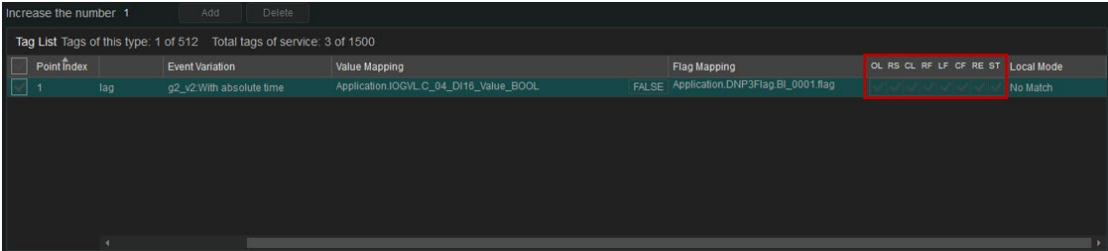
- 1 Select Data Type:** Points to the 'Data Type List' on the left, which shows various data types like TYPE_BI, TYPE_BO, etc.
- 2 Click "Add":** Points to the 'Add' button in the 'Tag List' section, which is used to add new tags.
- 3 Configure the properties:** Points to the 'Properties' panel at the bottom, where specific tag attributes like Point Index, Event Class, and Value Mapping are configured.

Local Mode: The DNP3 Outstation service in ioPAC 6500 system supports Local Mode. It prevents all output categories, including TYPE_BO and TYPE_AO, from being remotely controlled when the ioPAC 6500 is connected locally, ensuring the safety of field site personnel. To enable/disable the Local Mode, steps are as follows: Download Application (Connect the device) > Select **Get Status > Select Point > Enable/Disable Local Mode**.



Flag: Log in to application to see the flag status.

OL	RS	CL	RF	LF	CF	RE	ST
Online	Restart	Comm Lost	Remote Forced	Local Forced	Chatter Filter	Reserved	State

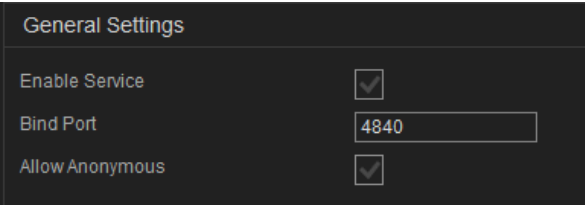


OPC UA Server

OPC UA Server services can be used to provide data to other systems via the OPC UA protocol. All properties of the OPC UA are categorized into **Basic Settings**, **Tag Settings**, and **Variable Mapping**.

Basic Settings: The Basic Function Settings page provides the essential functions setup, including General Settings, Session Settings, and Subscription Settings.

General Settings:



Session Settings:

Session Settings	
Max Session	2
Min Lifetime (ms)	10000
Max Lifetime (ms)	3600000

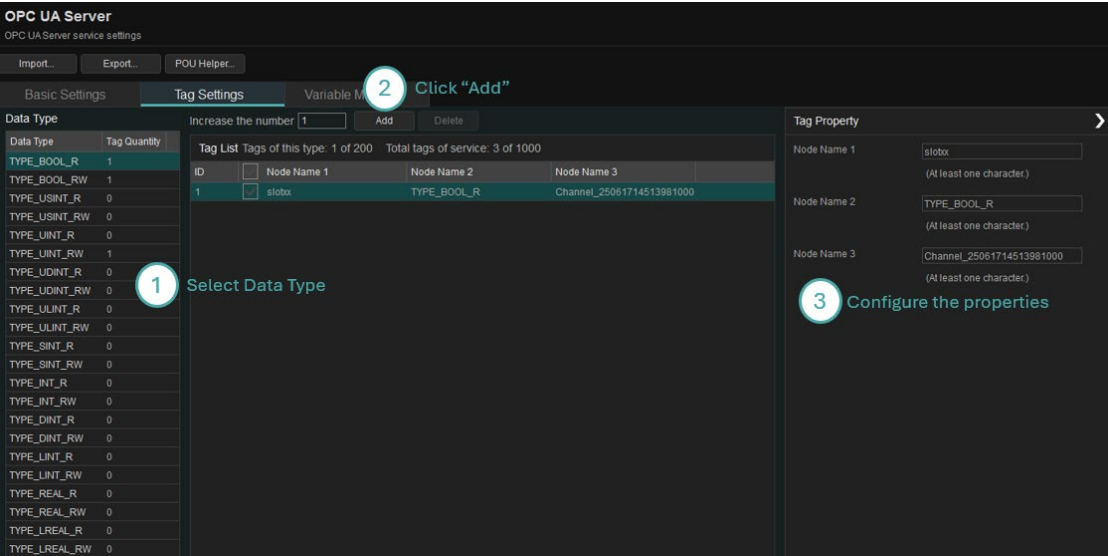
Items	Description
Max Session	Maximum number of concurrent client sessions allowed
Min Lifetime (ms)	Minimum time (in milliseconds) a session is held before being eligible for termination.
Max Lifetime (ms)	Maximum duration a session can stay active without being renewed by the client.

Subscription Settings:

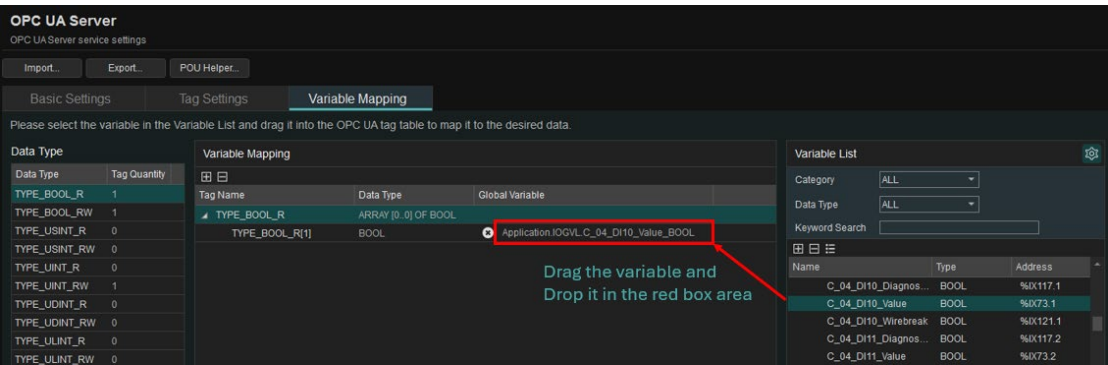
Subscription Settings	
Number of Subscriptions	10
Max number of notifications per publish	10
Min Publish Interval (ms)	500
Max Publish Interval (ms)	50000
Number of Monitored Items	1000
Min Sampling Interval (ms)	200
Max Sampling Interval (ms)	50000
Max size of monitored item's queue	1
Min number of subscription lifetime (ms)	1000
Max number of subscription lifetime (ms)	100000

Items	Description
Number of Subscriptions	Maximum number of concurrent OPC UA subscriptions the server will allow.
Max number of notifications per publish	Limits how many data change events are sent in a single publish response.
Min Publish Interval (ms)	Minimum interval for sending published responses.
Max Publish Interval (ms)	Maximum interval for sending published responses.
Number of Monitored Items	Max number of variables (tags) that can be monitored across all subscriptions.
Min Sampling Interval (ms)	Fastest rate at which a monitored item is sampled.
Max Sampling Interval (ms)	The slowest rate at which a monitored item is sampled.
Max size of monitored item's queue	The number of historical values stored in the queue per monitored item.
Min number of subscription lifetime (ms)	Minimum amount of time a subscription remains valid without interaction.
Max number of subscription lifetime (ms)	Maximum allowable time a subscription can exist before it's deleted.

Tag Settings: The ioPAC 6500 supports multiple data types to suit various applications. Each type allows up to 200 tags, with a total limit of 2,000 tags. Up to three names can be assigned to each tag for identification purposes. Follow the steps below to configure tags.



Variable Mapping: The tag quantity defined in Tag Settings will appear here automatically. Sort the variables in the Variable List, then drag and drop them into the array to complete data mapping. Follow the step below to map variables.



System Status

In the ioPAC 6500 Configuration page, the system status is at the left-bottom corner. The Diagnostic Status, Application Status, and Connection Status will be displayed here. Log in the system and all status will be displayed here.

Diagnostic Status: Diagnostic Status: Warnings and errors will trigger an alert here, reminding you to check the status. Select the icon and open the Diagnostic page to review the status.

Application Status: Shows the system is in run or stop mode.

Connection Status: Shows which accounts are logged into the system.



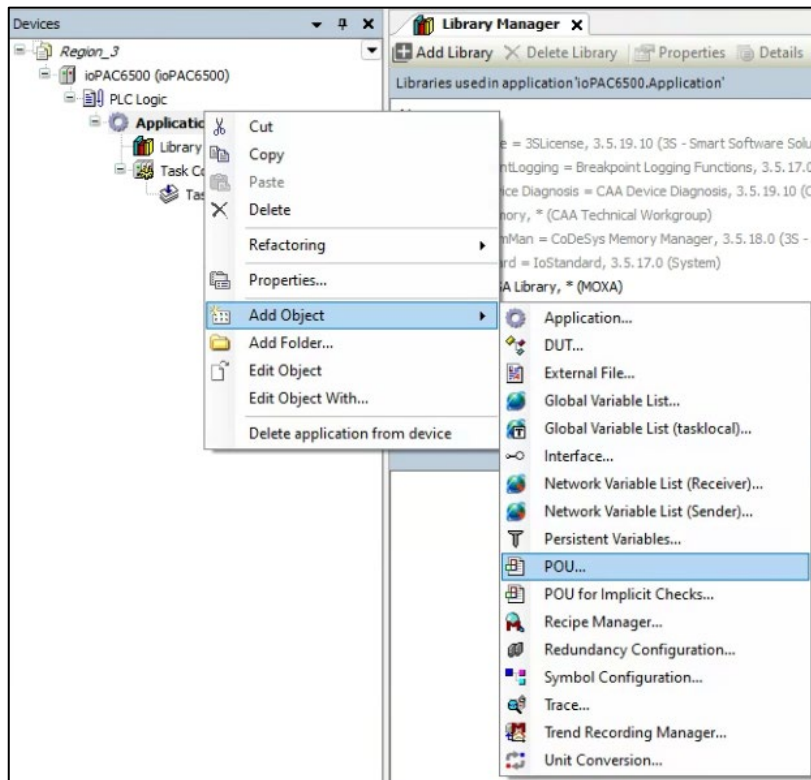
Library Manager

Double-click the Library Manger in the project tree, and the Library Manager page will show in the main window. The libraries supported by IINxpress can be found here. Besides the standard library, Moxa also provides the AGA3, 5, 8 libraries for oil-and-gas applications.

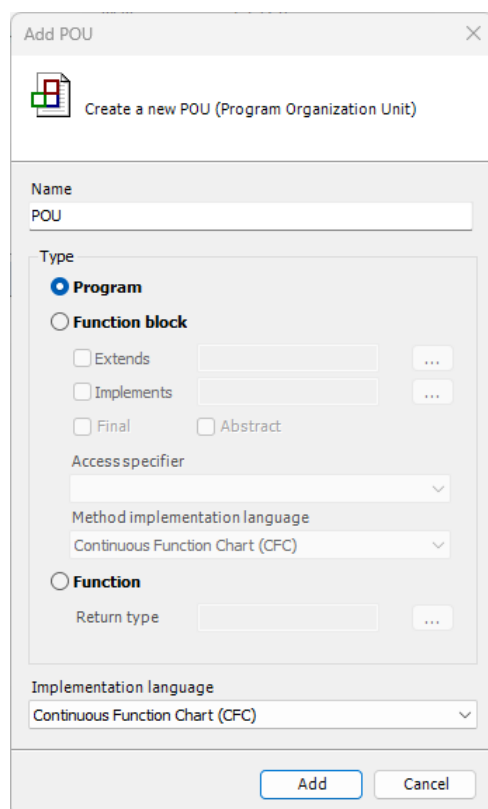
Libraries used in application 'ioPAC6500.Application'		
Name	Namespace	Effective Version
3SLicense = 3SLicense, 3.5.19.10 (3S - Smart Software Solutions GmbH)	_3S_LICENSE	3.5.19.10
BreakpointLogging = Breakpoint Logging Functions, 3.5.17.0 (3S - Smart Software Solutions GmbH)	BPLog	3.5.17.0
CAA Device Diagnosis = CAA Device Diagnosis, 3.5.19.10 (CAA Technical Workgroup)	DED	3.5.19.10
CAA Memory, * (CAA Technical Workgroup)	MEM	3.5.17.0
CDS_MemMan = CoDeSys Memory Manager, 3.5.18.0 (3S - Smart Software Solutions GmbH)	CMM	3.5.18.0
IoStandard = IoStandard, 3.5.17.0 (System)	IoStandard	3.5.17.0
Moxa AGA Library, * (MOXA)	mx_aga	1.0.0.0
Moxa Standard Library, * (MOXA)	mx_std	1.0.0.0

POU

POU stands for Programming Organization Unit, where you can develop your application. Add the POU by the path **Application (right-select) > Add Objects > POU**.



Once opening the POU, you will see the following window. Specify the information you need, then select **Add** to create the POU.



Name: The name to identify the program.

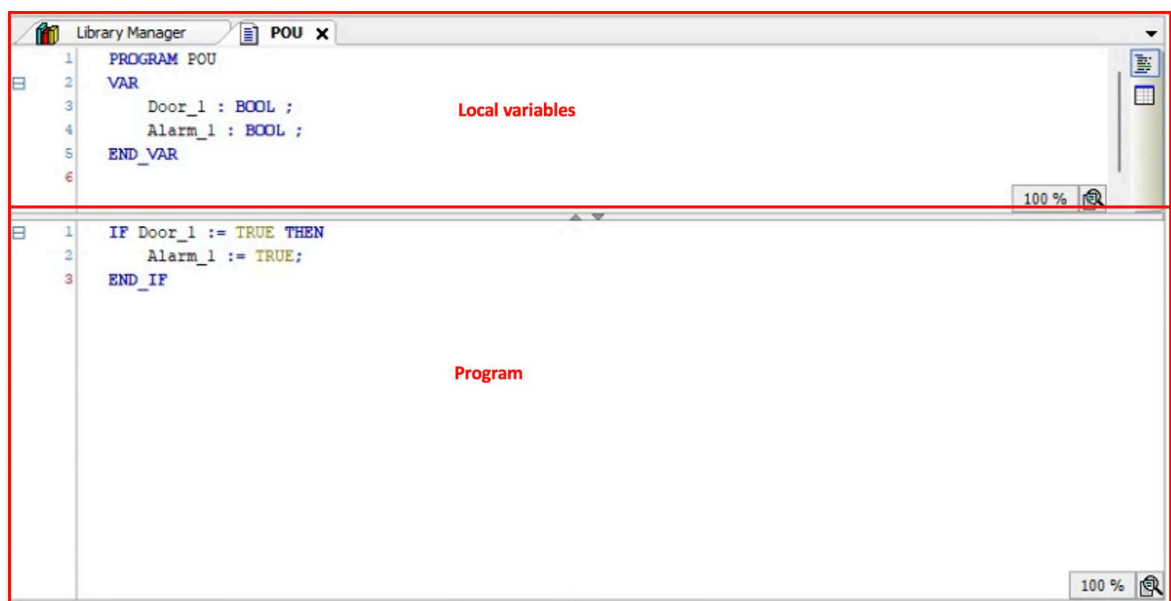
Type: You can choose from three different types.

- **Program:** These POU's contain logical control or function block calls.
- **Function Block:** These are POU's with multiple input and output parameters and can be called into other programs.
- **Function:** These are POU's with multiple input parameters and only one output parameter.

Implemented language: You can choose the familiar IEC 61131-3 language to develop the program. The following languages are supported.

- Continuous Function Chart (CFC)
- Function Block Diagram (FBD)
- Ladder Logic Diagram (LD)
- Sequential Function Chart (SFC)
- Structured Test (ST)

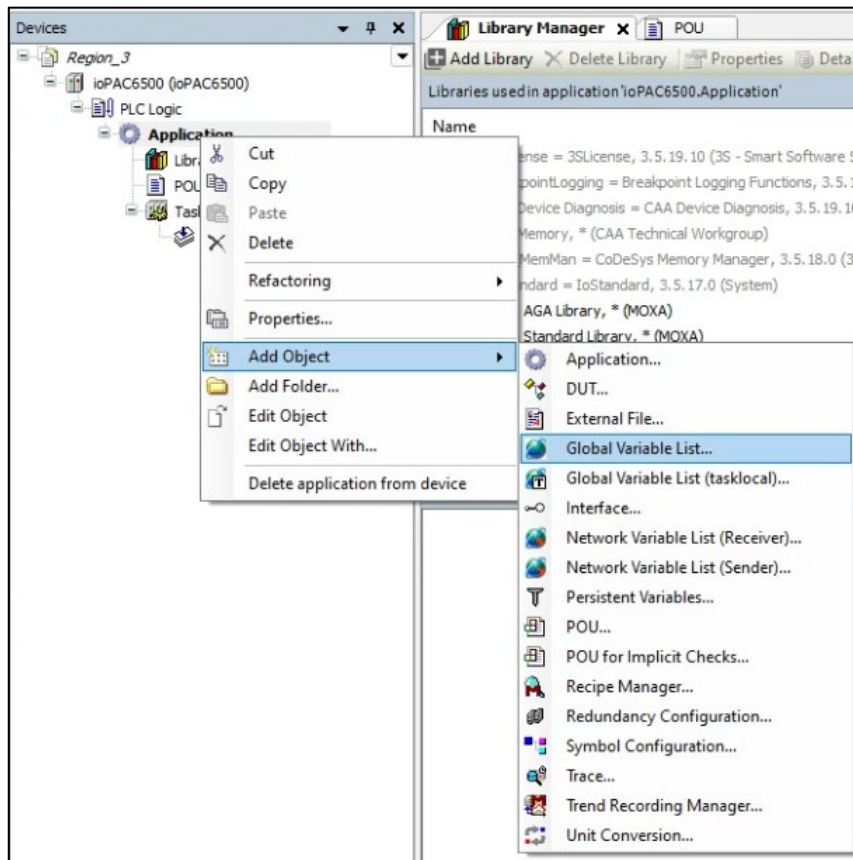
After selecting **Add**, one POU page will be created. You will see the following page.



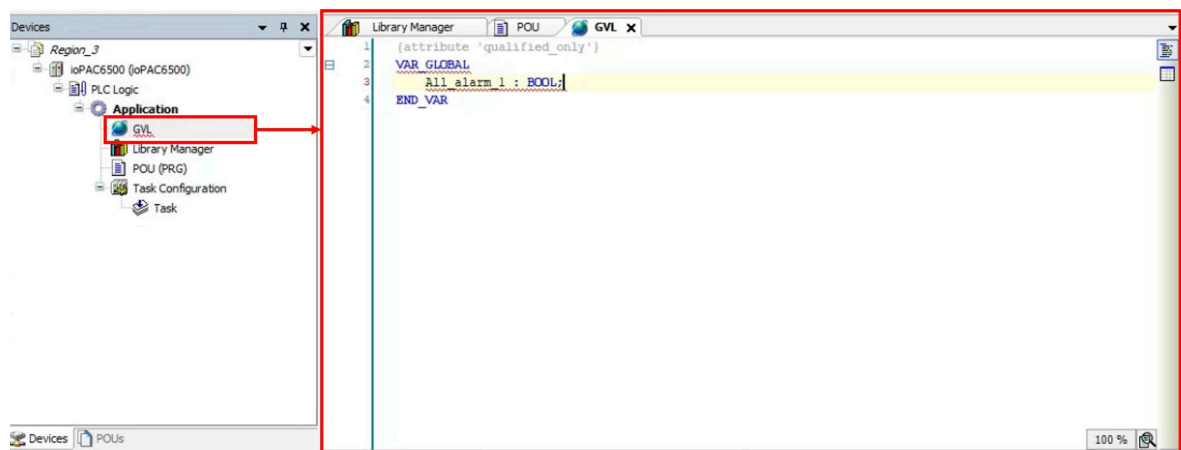
The POU window can be separated into two parts. You can define the local variable on the upper side. The lower side is where you develop your own program.

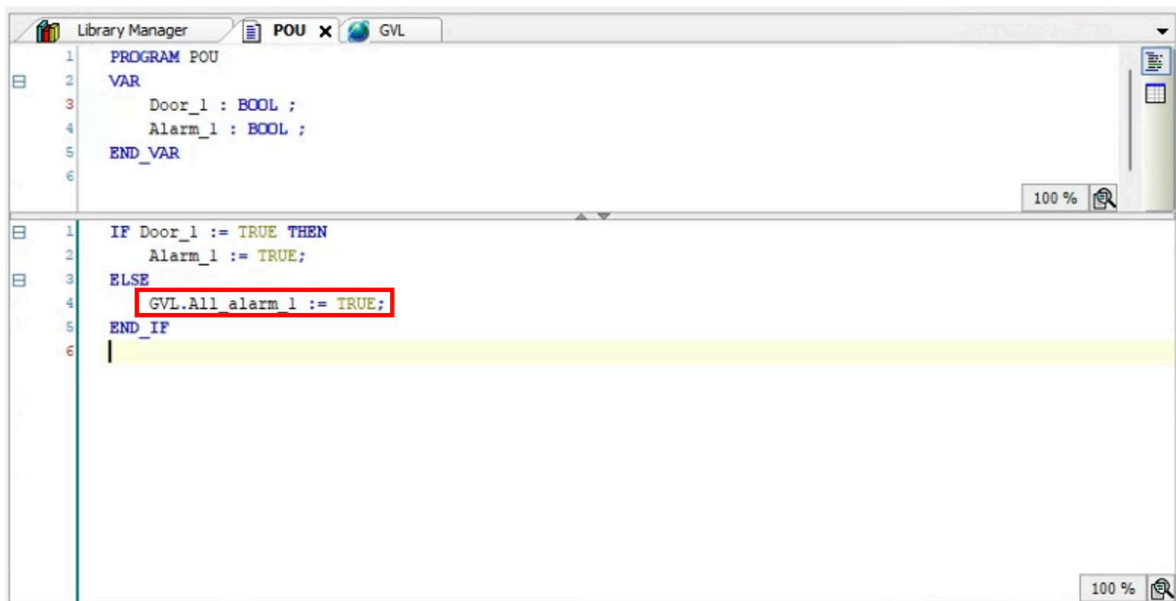
GVL

If you have the global variable demand, you can create the global variables by the path **Application (right-select) > Add Objects > GVL**.



Define the global variable in the window, and these global variables can be used in the program. Add an "GVL." prefix to distinguish the variables are local or global.





6. Switch Module Configuration

About this Chapter

In this chapter, learn how to connect your switch module with various interfaces and how to configure all settings and parameters via the user-friendly web interface.

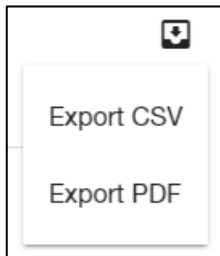
Meanings of the Symbols in the Web Interface Configurations

The Web Interface Configuration includes various symbols. Refer to the following table for the meanings of the symbols.

Symbols	Meanings
	Add
	Read detailed information
	Clear all
	Column selection
	Refresh
	Enable/Disable Auto Save When Auto Save is disabled, users need to select this icon to save the configurations.
	Export*
	Edit
	Re-authentication
	Delete
	Panel View
	Expand
	Collapse
	Hint Information
	Settings
	Data Comparison
	Menu icon
	Change mode
	Locator
	Reboot

Symbols	Meanings
	Reset to default
	Logout
	Increase
	Decrease
	Equal
	Menu
	Search
	Hide text that is typed into a text box (usually used when typing a password)
	Show text typed into a text box (usually used when providing password)

*The **Export** function helps you save the current configurations or information for the specific functions. It is on the upper part of the configuration area. Two formats are available: CSV or PDF. Select the format and save it on your local computer.



Configuration Reminders

In this section, several examples will remind you when configuring the settings for a switch module.

A: About Mandatory Parameters

Add Static Multicast Entry

VLAN ID *

Required

MAC Address *

Port *

Forbidden Port

CANCEL

CREATE

1.

The items with asterisks mean they are mandatory parameters that must be provided. In the figure above, the parameters for VLAN, Version, and Query Interval need to be provided, or it will not be created or applied.
2.

If the item is marked with red, it means this item has been skipped. Fill in the parameters or you cannot apply or create the function.
- In addition, some parameter values will be limited to a specific range. If the values exceed the range, they cannot be applied or created.

B: Configurations before Enable/Disable

In another situation, some settings can be configured first but remain disabled. Enable them, when necessary, without configuring the same settings again. This is particularly convenient and user-friendly when configuring various settings. For example, on the **DHCP Server** configuration page, configure the **DHCP** settings first, but later select to disable the **DHCP** settings in the **General** tab. When enabling the **DHCP** settings, only select **Enable** in **General** settings, so that the **DHCP** settings (either **MAC-based IP Assignment** or **Port-based IP Assignment** as shown as an example in the following figure) can be enabled at the same time.

DHCP Server

General

DHCP

MAC-based IP Assignment

Port-based IP Assignment

Lease Table

Mode

Disabled

DHCP / MAC-based IP Assignment

Port-based IP Assignment

Getting Started

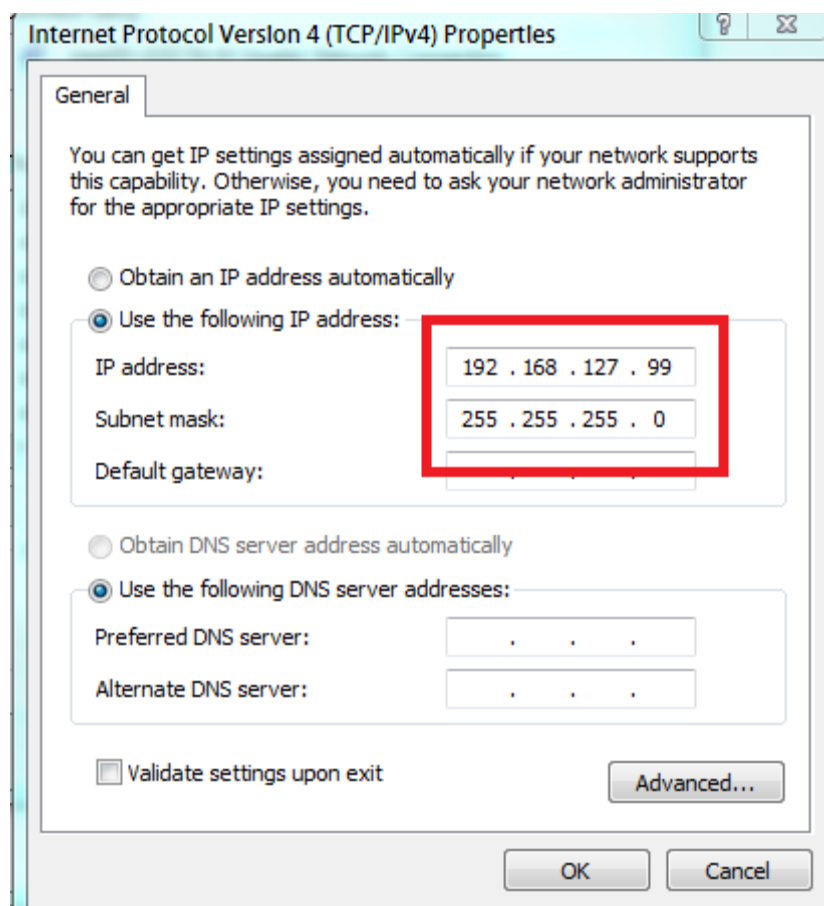
In this section, we explain how to log in a switch module for the first time. There are three ways to access the switch module's configuration settings: RS-232 console, Telnet (disabled by default) or web-based interface.

Log in by Web Interface

Directly connect the switch module to your computer with a standard network cable or install your computer at the same intranet as your switch. Then you need to configure your computer's network setting. The default IP address for the switch module is based on the slot index value:

192.168.127.101-102

For example, configure the computer's IP setting as **192.168.127.99**, and the subnet mask as 255.255.255.0.



Select **OK** when finished.

Connecting to the Switch

Open a browser, such as Google Chrome, Internet Explorer 11, or Firefox, and connect to the following IP address based on the corresponding slot index value.

1-slot Communication Module Backplane

Index Value	0
IP Address	192.168.127.101

2-slot Communication Module Backplane

Index Value	0	1
IP Address	192.168.127.101	192.168.127.102



NOTE

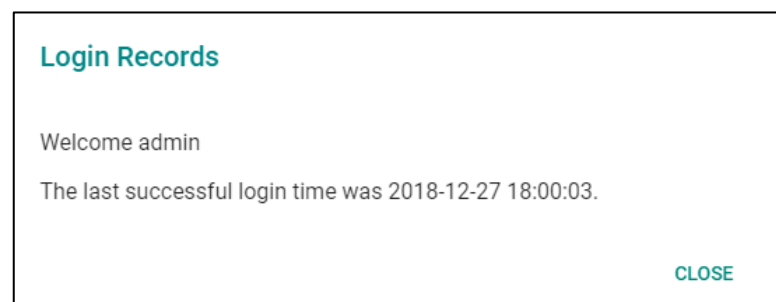
For network security consideration, all HTTP connections will be automatically redirected to HTTPS connections. The web browser will display a warning message if the device uses a certificate which isn't signed by the certification authority. You may add an exception rule for the certificate in the web browser to continue. We recommend using a certificate signed by a certification authority for security reasons. Refer to "**Security > Device Security > SSH & SSL > SSL**" for the configuration steps.

The default username and password are:

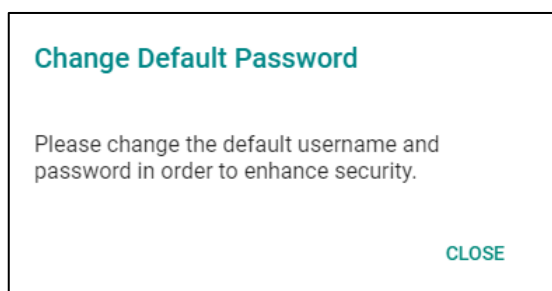
Username: **admin**

Password: **moxa**

Select **LOG IN** to continue. If you have logged in before, you will see a screen showing the previous login records. Select **CLOSE**.



Another system message will appear, reminding you to change the default password. We recommend you change your password, or a message will appear whenever you log in. Change the password in the **Account Management** section. Select **CLOSE** to continue.



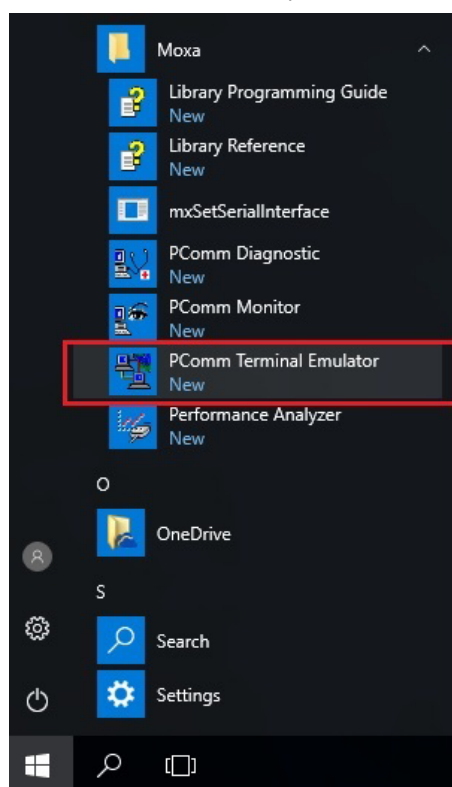
Log In by RS-232 Console

The ioPAC 6500 Layer 2 Managed Ethernet Switch Module offers a serial console port, allowing you to connect to the switch and configure the settings. Do the following steps for the serial connection and configuration.

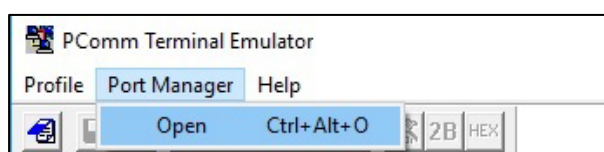
1. Prepare an RS-232 serial cable with an RJ45 interface.
2. Connect the RJ45 interface to the console port on the switch, and the other end to the computer.
3. We recommend you use **PComm Terminal Emulator** for serial communication. Download the software free from Moxa's website.

After installing PComm Terminal Emulator, open the switch module's console:

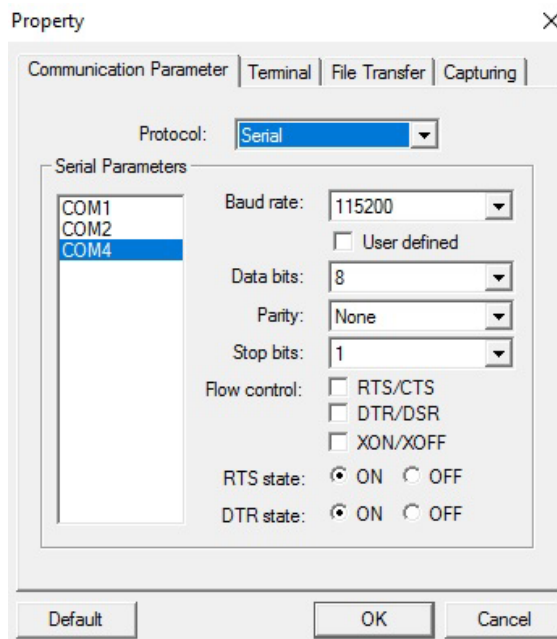
1. From the Windows desktop, select **Start > Moxa > PComm Terminal Emulator**.



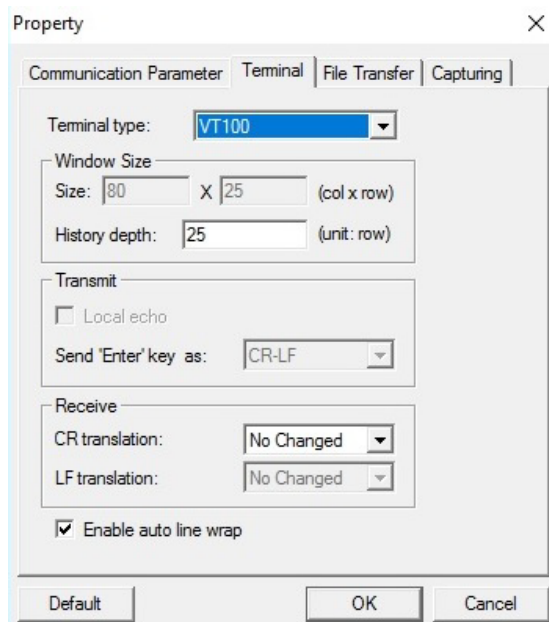
2. Select **Open** under the **Port Manager** menu to open a new connection.



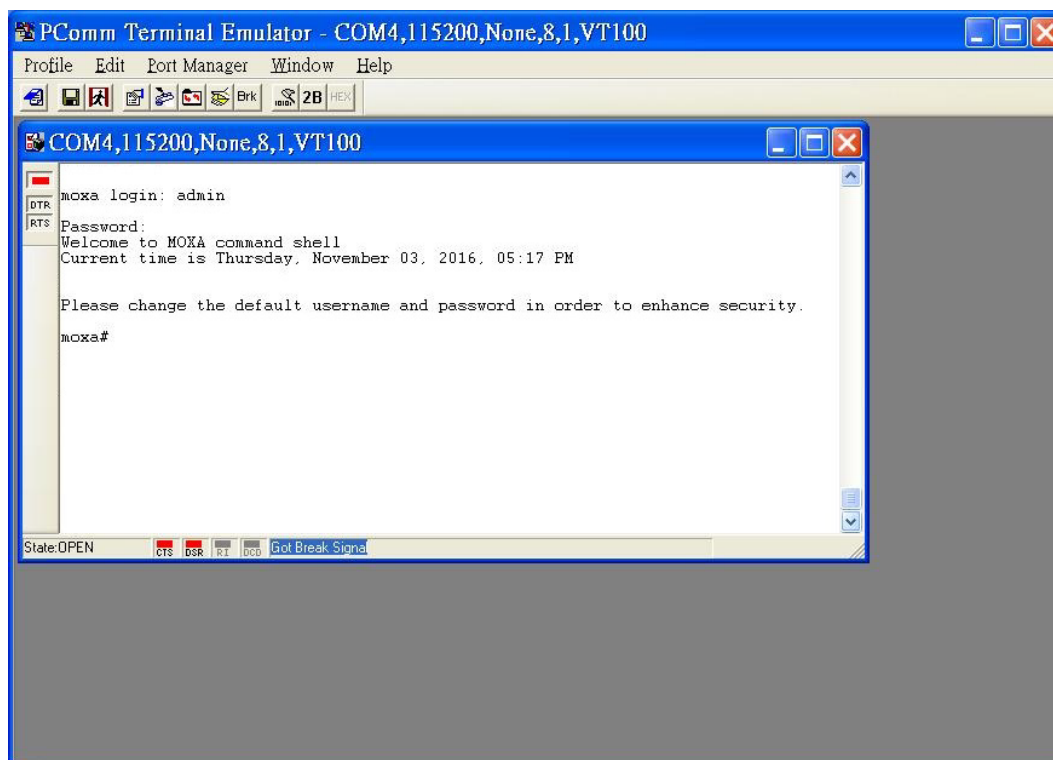
3. The **Property** window will open. On the **Communication Parameter** tab for **Ports**, select the COM port that is being used for the console connection. Set the other fields: **115200** for **Baud Rate**, **8** for **Data Bits**, **None** for **Parity**, and **1** for **Stop Bits**.



4. On the **Terminal** tab, select **VT100** for **Terminal Type**, and then select **OK** to continue.



- The console will prompt you to log in. The default login name is **admin**, and the default password is **moxa**. This password will be required to access any of the consoles (web, serial, Telnet).



- After successfully connecting to the switch by serial console, start configuring the switch parameters by using command line instructions. Refer to the **Moxa Command Line Interface Manual**.



NOTE

By default, the password assigned to the switch module is **moxa**. Be sure to change the default password after you first log in to help keep your system secure.

Log In by Telnet



NOTE

The Telnet protocol is disabled by default. Go to the **Security > Device Security > Management Interface** section to enable the telnet function first.

Opening the switch module's Telnet or web console over a network requires that the PC host and switch module are on the same logical subnet. You might need to adjust your PC host's IP address and subnet mask. By default, the switch module's IP is based on the slot index value: (192.168.127.101-102) and the switch module's subnet mask is 255.255.255.0. If the subnet mask is 255.255.0.0, you must set your PC's IP address to 192.168.xxx.xxx. If the subnet mask is 255.255.255.0, you must set your PC's IP address to 192.168.127.xxx.



NOTE

When connecting to the switch module's Telnet or web console, first connect one of the switch module's Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet port. Use either a straight-through or crossover Ethernet cable.

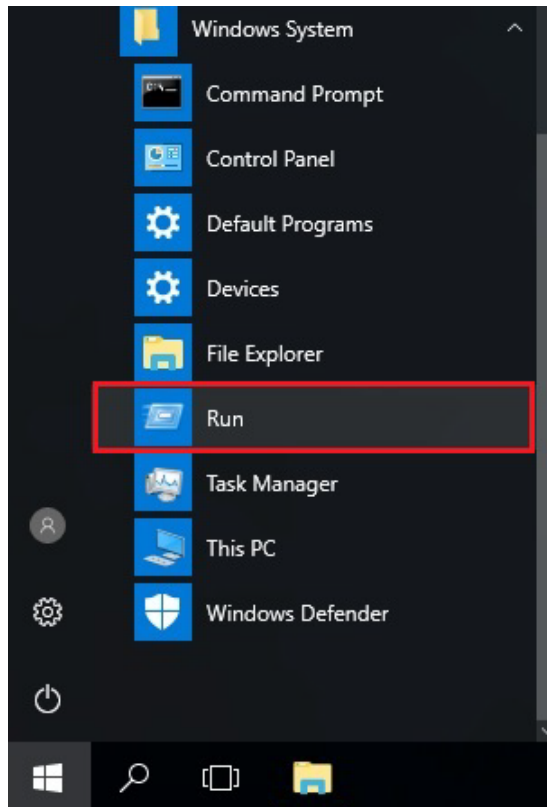


NOTE

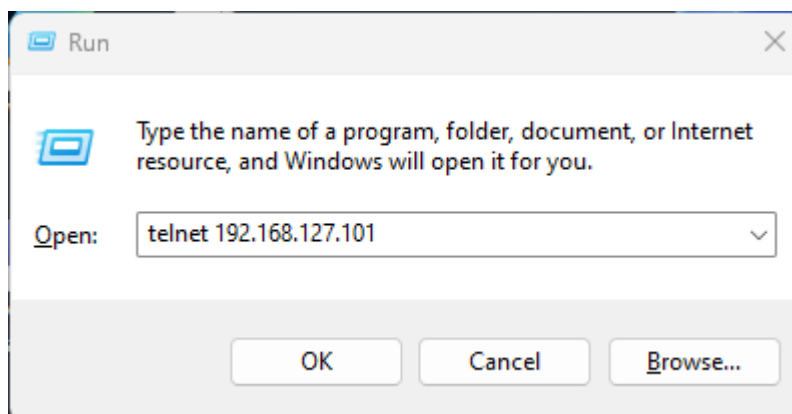
The Moxa switch's default IP address is 192.168.127.101-102 (by slot index).

After making sure that the switch module is connected to the same LAN and logical subnet as your PC, open the switch module's Telnet console:

1. Select **Start > Run** from the Windows Start menu and then Telnet to the switch module's IP address from the Windows **Run** window. You can also issue the Telnet command from a DOS prompt.



2. Next, use Telnet to connect the switch module's IP address (192.168.127.101~104) from the Windows **Run** window. You can also issue the Telnet command from a DOS prompt.



- The Telnet console will prompt you to log in. The default login name is **admin**, and the password is **moxa**. This password will be required to access any of the consoles (web, serial, Telnet).

```
moxa login: admin
Password:
Welcome to MOXA command shell
Current time is Friday, December 21, 2018, 08:51 PM

Please change the default username and password in order to enhance security.

moxa# _
```

- After successfully connecting to the switch by Telnet, start configuring the switch parameters by using command line instructions. Refer to the **Moxa Command-line Interface Manual**.



NOTE

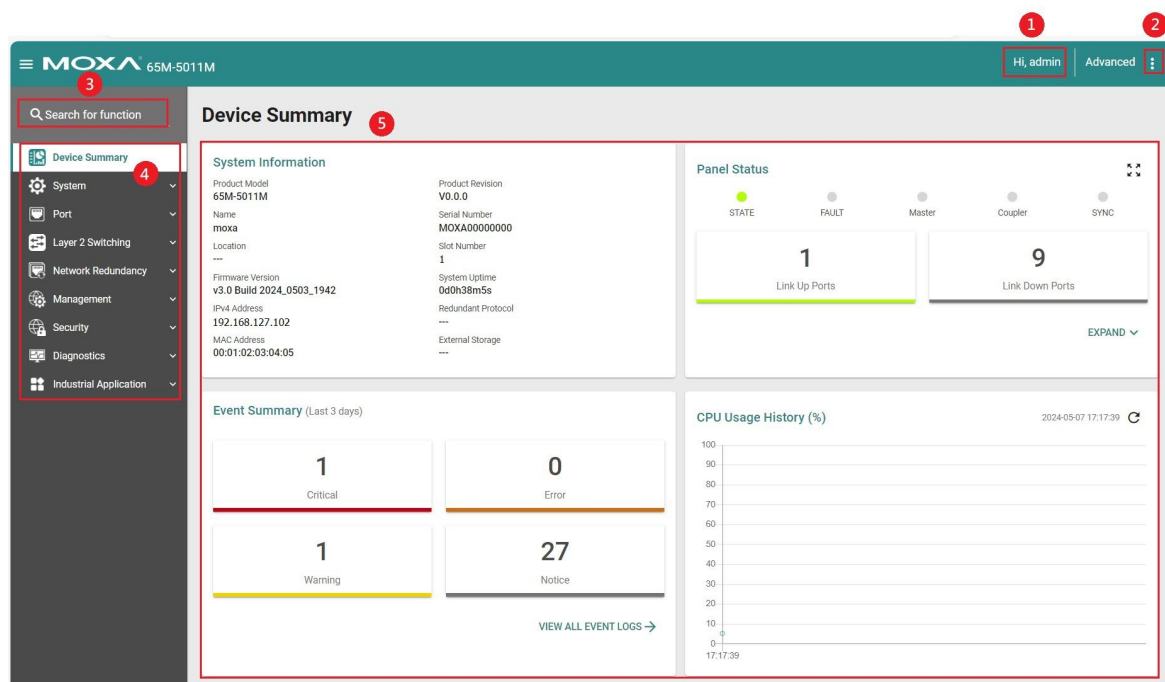
By default, the password assigned to the switch module is moxa. Be sure to change the default password after you first log in to help keep your system secure.

Web Interface Configuration

The ioPAC 6500 Layer 2 Managed Ethernet Switch Module offers a user-friendly web interface for easy configurations. It is easy to configure various settings over the web interface. All configurations for the switch module can be easily set up and done via this web interface, essentially reducing system maintenance and configuration effort.

Function Introduction

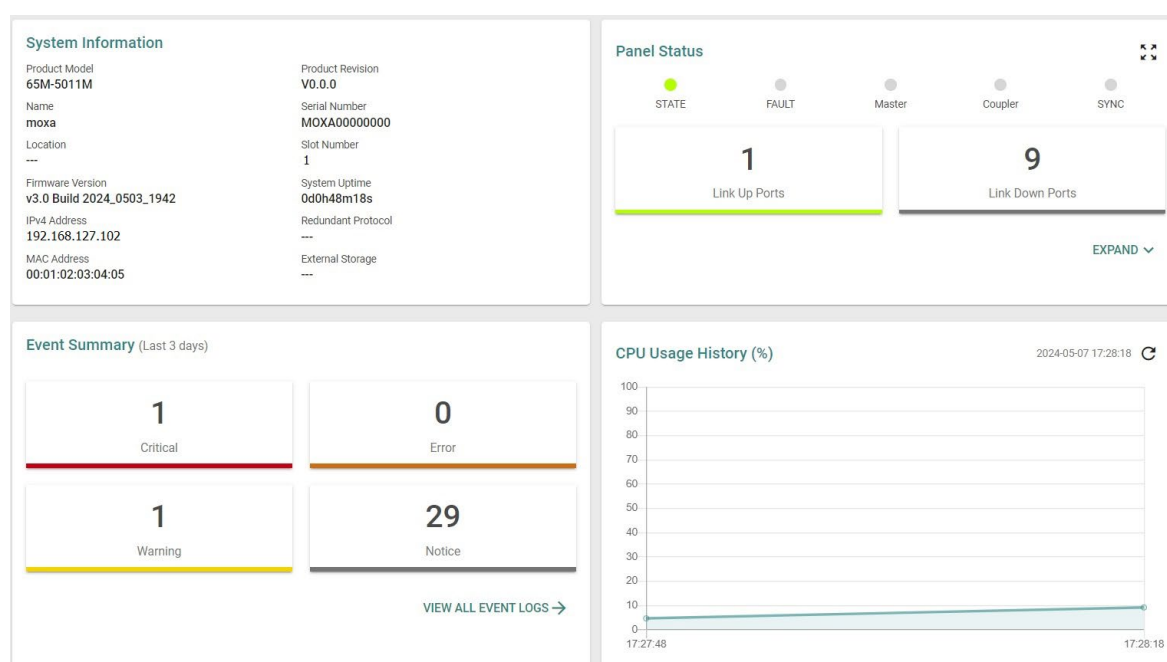
This section describes the web interface design, providing a basic visual concept for users to understand the main information or configuration menu for the web interface pages.



1. **Login Name:** It shows the role of the login name.
2. **Configuration Mode:** Two modes can be shown: **Standard Mode** and **Advanced Mode**.
 - **Standard Mode:** Some features and parameters will be hidden to make the configurations simpler (default).
 - **Advanced Mode:** More features and parameters will be shown for you to configure detailed settings.
3. **Search Bar:** Type the items you want to search for in the function menu tree.
4. **Function Menu:** Functions of the switch are shown here. Select the function you want to view or configure.
5. **Device Summary:** Important device information of the functions will be shown here.

Device Summary

After successfully connecting to the switch, the **Device Summary** will automatically appear. View the whole web interface on the screen. If you are in the middle of performing configurations, select Device Summary on the Function Menu and you can view the detailed information of the switch.



See the following sections for detailed descriptions of the specific items.

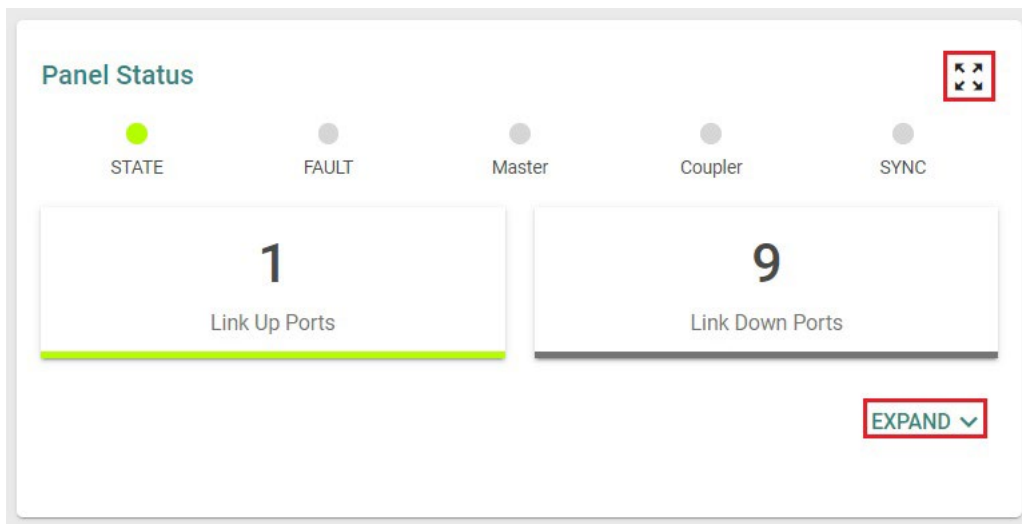
System Information

This shows the system information, including the product model name, product revision, serial number, firmware version, system uptime, etc.

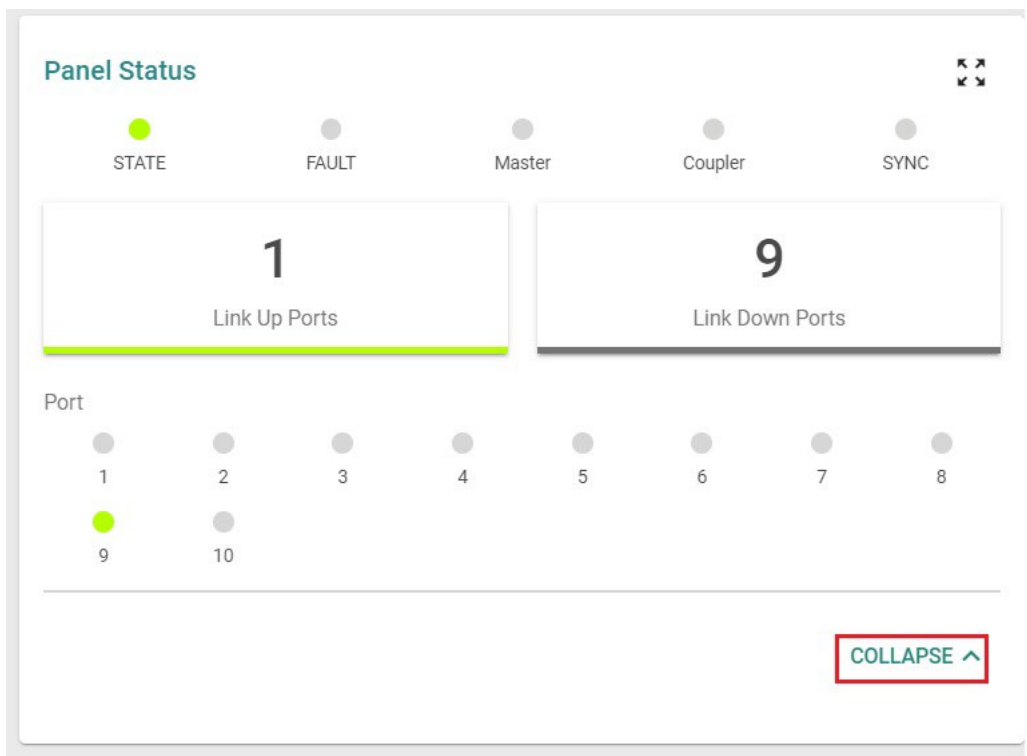
System Information	
Product Model	Product Revision
65M-5011M	V0.0.0
Name	Serial Number
moxa	MOXA00000000
Location	Slot Number
---	1
Firmware Version	System Uptime
v3.0 Build 2024_0503_1942	0d0h48m18s
IPv4 Address	Redundant Protocol
192.168.127.102	---
MAC Address	External Storage
00:01:02:03:04:05	---

Panel Status

This section illustrates the panel status. For example, the connecting ports will be shown in green, while the disconnected ports will be shown in gray. Select **EXPAND** to view more detailed information on the panel status and select **Collapse** to return.



Select **EXPAND** to view more detailed information on the panel status and select **COLLAPSE** to return.



Panel View

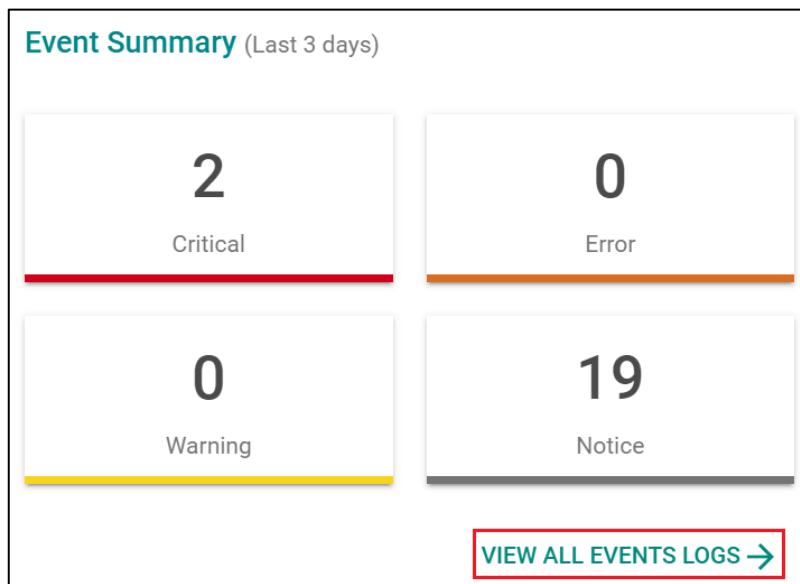
Select the icon with four arrows (↔↔) to view the device's port status. Select the close icon in the upper-right corner to return to the main page.

This appearance of the panel view figure depends on which model is being used. So, what you see might differ from the panel view shown below.



Event Summary (Last 3 Days)

This section shows the event summary for the past three days.



Select **VIEW ALL EVENTS LOGS** to go to the Event Log page, where you can view the event logs.

Event Log

[Event Log](#) [Threshold Settings](#)

Oversize-Action

Overwrite the oldest event log

APPLY

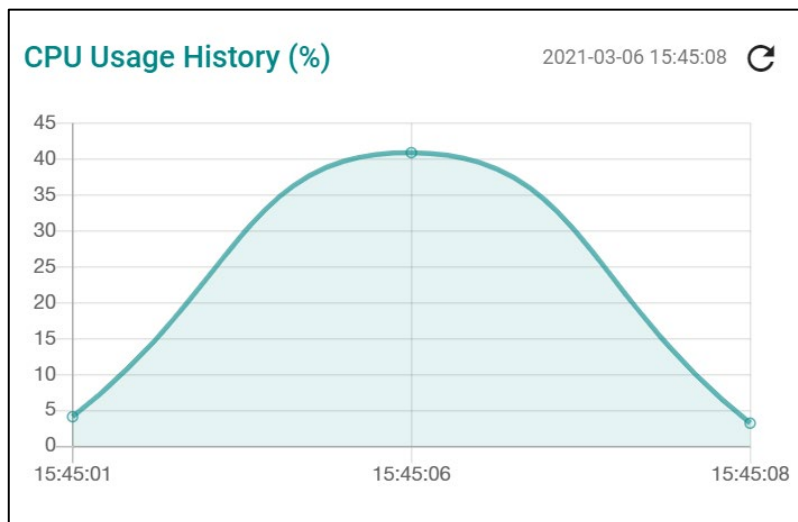
  

Index	Bootup Number	Severity	Timestamp	Uptime	Message
1	41	Notice	2019-01-22 15:58:47	0d0h27m13s	[Account:admin] logged out.
2	41	Notice	2019-01-22 15:58:01	0d0h26m26s	[Account:admin] successfully logged in via local.
3	41	Notice	2019-01-22 15:56:47	0d0h25m12s	[Account:admin] successfully logged in via local.
4	41	Notice	2019-01-22 15:56:42	0d0h25m8s	[Account:admin] logged out.
5	41	Notice	2019-01-22 15:55:25	0d0h23m50s	Configuration [Mgmt Interface] changed by admin.

For Event Log settings, refer to **Event Log** under the **Diagnosis** section.

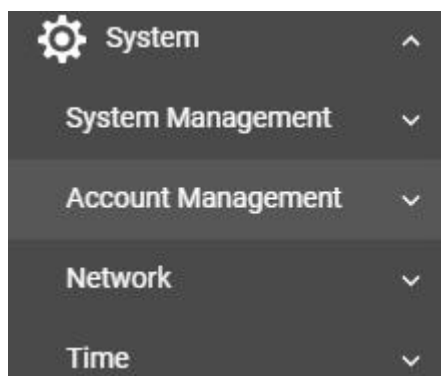
CPU Utilization History

This section shows the CPU usage. The data will be shown as a percentage over time. Select the refresh icon on the page to show the latest information.



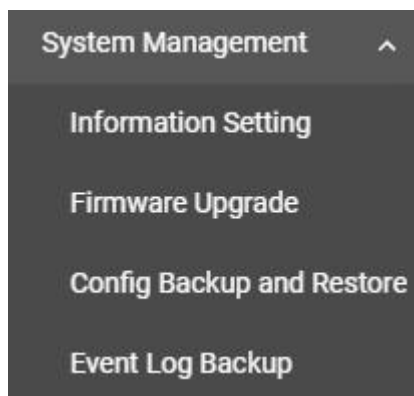
System

Select **System** on the function menu. Configure the **System Management**, **Account Management**, **Network**, and **Time** configurations.



System Management

Select **System Management**, four functions can be configured under this section: **Information Setting**, **Firmware Upgrade**, **Configure Backup and Restore**, and **Event Log Backup**.



Information Setting

Define **Information Setting** items to make it easier to identify different switches that are connected to your network.

Information Settings

Device Name

moxa

4 / 64

Location

0 / 255

Description

0 / 255

Contact Information

0 / 255

APPLY

Device Name

Setting	Description	Factory Default
1 to 64 characters	This option is useful for differentiating between the roles or applications of different units. Note that the device name cannot be empty.	moxa



NOTE

The Device Name field follows the PROFINET I/O naming rule. The name can only include the following characters, **a-z/0-9/-**.

Location

Setting	Description	Factory Default
Max. 255 characters	This option is for differentiating between the locations of different switches. Example: production line 1.	None

Description

Setting	Description	Factory Default
Max. 255 characters	This option is for recording a more detailed description of the unit.	None

Contact Information

Setting	Description	Factory Default
Max. 255 characters	Input contact information, such as email address, or telephone number when problems occur.	None

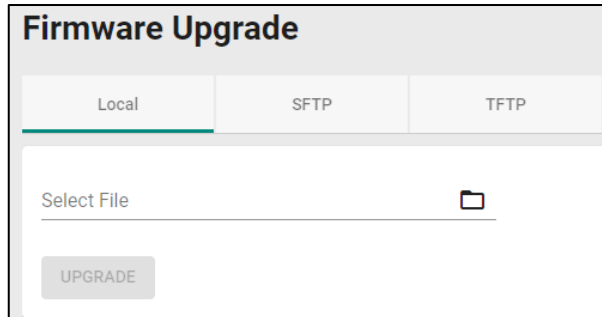
When finished, select **APPLY** to save your changes.

Firmware Upgrade

There are three ways to update your switch module's firmware: from a local *.rom file, by remote SFTP server, and remote TFTP server.

Local

Select **Local** tab.

The screenshot shows the 'Firmware Upgrade' window with the 'Local' tab selected. It features a 'Select File' text input field with a folder icon to its right. Below the input field is a grey 'UPGRADE' button.

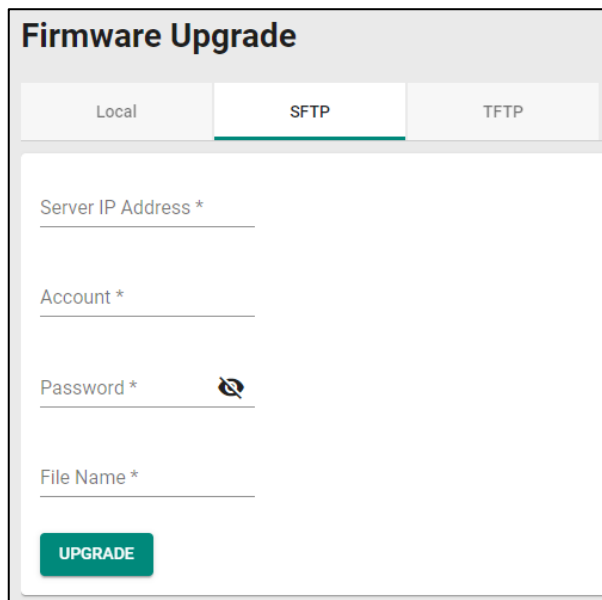
Select File

Before performing firmware upgrade, download the updated firmware (*.rom) file first from Moxa's website (www.moxa.com).

Setting	Description	Factory Default
Select the firmware file	Select the icon on the right and select the firmware file from the location where the updated firmware is located.	None
Browse for the (*.rom) file, and then select the UPGRADE button.	This option allows you to select the updated firmware file and perform the firmware upgrade.	None

SFTP

Select **SFTP** tab.

The screenshot shows the 'Firmware Upgrade' window with the 'SFTP' tab selected. It contains four text input fields: 'Server IP Address *', 'Account *', 'Password *' (with a toggle icon), and 'File Name *'. A green 'UPGRADE' button is located at the bottom left.

Server IP Address

Setting	Description	Factory Default
Input the IP address of the SFTP server.	Input the server IP address of the computer where the new firmware file (*.rom) is located.	None

Account

Setting	Description	Factory Default
Input the account of the SFTP server	The account must be authorized for the SFTP Server to have a secure connection.	None

Password

Setting	Description	Factory Default
Input the password for the SFTP server	The account must be specified to authorize the SFTP Server for secure connection.	None

File Name

Setting	Description	Factory Default
Input the filename of the firmware	Input the filename of the new firmware.	None

When finished, select **UPGRADE** to perform the firmware upgrade. The switch will reboot automatically and perform the firmware upgrade.

TFTP Server

Upgrade firmware via the TFTP server. Select **TFTP** tab first.

Firmware Upgrade

Local

SFTP

TFTP

Server IP Address *

File Name *

UPGRADE

Server IP Address

Setting	Description	Factory Default
Input the IP address of the TFTP server	Input the IP address of the TFTP server where the new firmware file (*.rom) is located.	None

File Name

Setting	Description	Factory Default
Input the filename of the firmware	Input the filename of the new firmware.	None

When finished, select **UPGRADE** to perform the firmware upgrade.

USB

Upgrade the firmware via Moxa's USB-based ABC-02 configuration tool. Connect the ABC-02 to the switch and select **USB** from the drop-down list under **Method**.

Firmware Upgrade

Method *

USB

i

Select File *

UPGRADE

Select File

Before performing the firmware upgrade, download the latest firmware (*.rom) file first from Moxa's website (www.moxa.com).

Setting	Description	Factory Default
Select the firmware file	Select the firmware file from the location where the updated firmware is located.	None
Browse for the (*.rom) file	This option allows you to select the updated firmware file and perform the firmware upgrade.	None

When finished, select **UPGRADE** to perform the firmware upgrade.



Note

If you have difficulty using the ABC-02 configuration tool, check if the **USB Function** has been enabled in the **Hardware Interface** section.

Configuration Backup and Restore

Back up the configurations of your switch module in five ways: using a local configuration file, a remote SFTP server, a remote TFTP server, or a USB tool.

Local

Select **Local** tab first.

Configuration Backup and Restore

Local

SFTP

TFTP

File Encryption

File Signature

Configuration Selection

Running Configuration

Default Configuration

Not Included

BACKUP

Select File

RESTORE

Configuration Selection

Setting	Description	Factory Default
Running Configuration	Back up the running configuration.	Running
Startup Configuration	Back up the start-up configuration.	Configuration

Default Configuration

Setting	Description	Factory Default
Not Included	Back up the configuration without default settings.	Not Included
Included	Back up the configuration with default settings.	

Select File

Setting	Description	Factory Default
Select the Backup button to back up the configuration file to a local drive.	Back up the system file to your local computer.	None
Browse for a configuration file on a local disk, and then select the RESTORE button.	Select the configuration file and perform system restoration.	None

SFTP Server

Select the **SFTP** tab first.

Configuration Backup and Restore

Local

SFTP

TFTP

File Encryption

File Signature

Server IP Address *

Account *

Password * 

File Name *

BACKUP

RESTORE

Server IP Address

Setting	Description	Factory Default
Input the IP address of the SFTP server	Input the IP address of the SFTP server where the new firmware file (*.rom) is located.	None

Account

Setting	Description	Factory Default
Input the account of the SFTP server	An account must be provided to authorize the SFTP server for a secure connection.	None

Password

Setting	Description	Factory Default
Input the passwords for the SFTP server	The password has to be specified to authorize the SFTP Server for secure connection.	None

File Name

Setting	Description	Factory Default
Input the backup/restore file name (support up to 54 characters, including the .ini file extension).	Input the filename of the configuration backup or restoration file.	None

When finished, select **BACKUP** or **RESTORE** to back up or restore the system configuration file.

TFTP Server

Select **TFTP** tab first.

Configuration Backup and Restore

Local

SFTP

TFTP

File Encryption

File Signature

Server IP Address *

File Name *

BACKUP

RESTORE

Server IP Address

Setting	Description	Factory Default
Input the IP address of the TFTP server	Input the IP address of the TFTP server.	None

File Name

Setting	Description	Factory Default
Input the backup/restore file name (supports up to 54 characters, including the .ini file extension).	Input the filename to back up or restore the system configuration file.	None

When finished, select **BACKUP** or **RESTORE** to perform the firmware upgrade.

USB

Select **USB** from the drop-down list under **Method**.

Configuration Backup and Restore

Backup

Restore

File Encryption

File Signature

Method *

USB

BACKUP

Insert Moxa's ABC-02 USB-based configuration tool into the USB port of the switch, select **BACKUP** to back up the system configuration file.



Note

If you have difficulty using the ABC-02 configuration tool, check if the **USB Function** has been enabled in the **Hardware Interface** section.

File Encryption

To encrypt the configuration file, select the **File Encryption** tab first.

Configuration Backup and Restore

LocalSFTPTFTPFile EncryptionFile Signature

Configuration File Encryption
Disabled

Password

APPLY

Enable Configuration File Encryption

Setting	Description	Factory Default
Enabled	Enable the configuration file to be encrypted.	Disabled
Disabled	Disable the feature that allows the configuration file to be encrypted.	

Password

Setting	Description	Factory Default
4 to 16 characters, numbers only.	Input the password when you encrypt the configuration file.	None

When finished, select **APPLY** to save your changes.

File Signature

Select **File Signature** tab to see additional configuration options. Enabling the file signature can ensure file integrity and authenticity.

Configuration Backup and Restore

LocalSFTPTFTPFile EncryptionFile Signature

Signed config
Disabled

APPLY

Key	Label	Algorithm	Length
Max. 1			
0 of 0			

Enable Signed Configuration

Setting	Description	Factory Default
Enabled	Enable the configuration file signature.	Disabled
Disabled	Disable the configuration file signature	

Select **APPLY** to save your changes.

Select **+** icon to add customer key.

Add Customer Key

Label *

0 / 16

Certificate *

Key *

CANCEL

CREATE

Label

Setting	Description	Factory Default
0 to 16 characters	Provide the name for the certificate and the key.	None

Certificate

Setting	Description	Factory Default
Select the import file icon to select the file from your computer	Import the certificate file.	None

Key

Setting	Description	Factory Default
Select the import file icon to select the file from your computer	Import the key file.	None

When finished, select **CREATE** to save your changes.

Event Log Backup

Three methods exist for backing up switch module's log files: using a local drive, through a remote SFTP server, or via remote TFTP.

Local

Select Local tab.

Event Log Backup

Local

SFTP

TFTP

BACKUP

Select **BACKUP** to back up the log file to a local drive.

SFTP Server

Select **SFTP** tab.

Event Log Backup

Local

SFTP

TFTP

Server IP Address *

Account *

Password * 

File Name *

BACKUP

Server IP Address

Setting	Description	Factory Default
Input the IP address of the SFTP server	Input the IP address of the SFTP server.	None

Port

Setting	Description	Factory Default
Input the port of the SFTP server, 1 to 65535	Specify the port used in the SFTP server.	None

Account

Setting	Description	Factory Default
Input the account of the SFTP server	An account must be specified to authorize the SFTP server for a secure connection.	None

Password

Setting	Description	Factory Default
Input the password for the SFTP server	The password must be entered to authorize the SFTP server for a secure connection.	None

File Name

Setting	Description	Factory Default
Input the file name for event log backup	Input the filename of the event log.	None

When finished, select **BACKUP** to back up the event log file.

TFTP Server

Select **TFTP** tab.

Event Log Backup

Local

SFTP

TFTP

Server IP Address *

File Name *

BACKUP

Server IP Address

Setting	Description	Factory Default
Input the IP address of the TFTP server	Input the IP address of the TFTP server.	None

Port

Setting	Description	Factory Default
Input the port of the TFTP server, 1 to 65535	Input the port used in the TFTP server.	None

File Name

Setting	Description	Factory Default
Input the file name for event log backup	Input the filename of the event log.	None

When finished, select **BACKUP** to back up the event log file.

Account Management

The **Account Management** feature allows you to manage the accounts of the switch. Enable different accounts with different roles to facilitate convenient management and safe access.

Account Management ^

User Account

Password Policy

Online Accounts

User Account

This section describes how to manage the existing accounts of the switch. Here, you can add, edit, and delete user accounts for the switch. Only one account, `admin`, exists by default. To enhance security, we suggest you create a new account with the user authority.

User Account



☐	Enable	Username	Authority	Email
☐ 	Enabled	admin	Admin	admin@sample.com
☐ 	Enabled	test	User	test@example.com

Max. 32

The User Account page features a search function on the upper right. Type the username you want to search for.

Search

Editing Existing Accounts

Select the account you want to edit and select the edit icon.

User Account

☐	Enable	Username	Authority	Email
☐ 	Enabled	admin	Admin	admin@sample.com
☐ 	Enabled	test	User	test@example.com

Max. 32

Configure the following settings.

Edit Account Settings

Enable *

Enabled

Username

admin

At least 4 characters5 / 32

CHANGE PASSWORD

Authority *

Admin

Email

admin@sample.com

16 / 63

CANCEL

APPLY

Enabled

Setting	Description	Factory Default
Enabled	This enables the user account.	Enabled
Disabled	This disables the user account.	

Authority

Setting	Description	Factory Default
admin	This account has read/write access for all configuration parameters.	admin
supervisor	This account has read/write access for some specific configuration parameters.	
user	This account can only view some specific configuration parameters.	

Email

Setting	Description	Factory Default
Input an email address	Input an email address for the account if required.	None

When finished, select **APPLY** to save your changes.

To change the password for the user, select **CHANGE PASSWORD**.

Edit Account Password

Username

admin

At least 4 characters5 / 32

New Password *

At least 4 characters0 / 63

Confirm Password *

At least 4 characters0 / 63

BACK

APPLY

New Password

Setting	Description	Factory Default
4 to 63 characters	Enter the password to use for this account.	None

Confirm Password

Setting	Description	Factory Default
4 to 63 characters	Reenter the password to confirm it.	None

When finished, select **APPLY** to save your changes.



NOTE

Refer to **Appendix B** for detailed descriptions for read/write access privileges for the admin, supervisor, and user authority levels.

Creating a New Account

Create a new account by selecting the + icon on the Configuration page.

User Account

+

☐	Enable	Username	Authority	Email
☐	Enabled	admin	Admin	admin@sample.com
☐	Enabled	test	User	test@example.com

Max. 32

Configure the following settings.

Create New Account

Enable *

Enabled

Username *

At least 4 characters 0 / 32

Authority *

New Password *

At least 4 characters 0 / 63

Confirm Password *

At least 4 characters 0 / 63

Email

0 / 63

CANCEL

CREATE

Enabled

Setting	Description	Factory Default
Enabled	This enables the account.	Enabled
Disabled	This disables the account.	

Username

Setting	Description	Factory Default
Input a username, 4 to 32 characters	Input a new username for this account.	None

Authority

Setting	Description	Factory Default
admin	This account has read/write access of all configuration parameters.	None
supervisor	This account has read/write access for some specific configuration parameters.	
user	This account can only view some specific configuration parameters.	

To enhance security, we suggest you create a new account with the user authority.

New Password

Setting	Description	Factory Default
4 to 63 characters	Input a new password for this account.	None

Confirm Password

Setting	Description	Factory Default
4 to 63 characters	Reenter the password to confirm.	None

Email

Setting	Description	Factory Default
Input an email address	Input an email address for the account if required.	None

When finished, select **CREATE** to complete.

Delete an Existing Account

To delete the existing account, simply select the account you want to delete, and then select the delete icon on the configuration page.

User Account



	Enable	Username	Authority	Email
☐	 Enabled	admin	Admin	admin@sample.com
☒	 Enabled	test	User	test@example.com

Max. 32

Select **DELETE** to delete the account.

Delete Account

Are you sure you want to delete the selected account?

CANCEL

DELETE

Password Policy

To prevent hackers from cracking weak passwords, a password policy can be set. The password policy can enforce users to create passwords with a minimum length and complexity, and it can also establish a maximum lifetime for the password to ensure it is changed periodically.

Password Policy

Minimum Length *

4

4 - 63

Password Complexity Strength Check

☐ At least one digit (0-9)

☐ At least one upper case letter (A-Z)

☐ At least one lower case letter (a-z)

☐ At least one special character ({}|~!@#\$%^&*~_.)

Password Max-life-time *

0

0 - 365

day

APPLY

Minimum Length

Setting	Description	Factory Default
Input from 4 to 63	This sets the minimum length of the password.	4

Password Complexity Strength Check

Setting	Description	Factory Default
digit, letter cases, special characters	These determine the required complexity for the password. Multiple options may be checked.	None

Password Max-life-time (day)

Setting	Description	Factory Default
Input from 0 to 365	This determines how long the password can be used before it must be changed.	0

When finished, select **Apply** to save your changes.

Online Accounts

The **Online Accounts** function allows you to view who has connected to the device. You may immediately remove the user who is currently online.

Online Accounts

Search

	Username	Authority	IP Address	Interface	Idle Time (sec.)
	admin	Admin	192.168.127.250	HTTP(S)	0
	test	User	192.168.127.250	HTTP(S)	44

Select the remove icon and select **REMOVE** to disconnect the user.

Remove online account

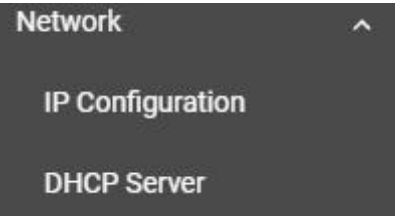
Are you sure you want to remove this online account?

CANCEL

REMOVE

Network

This section describes how to configure the switch’s network settings, including **IP Configuration** and the **DHCP Server**.



IP Configuration

You can configure the IP settings of the switch.

IP Configuration

Get IP From *

Manual

IP Address *

192.168.127.253

Subnet Mask *

24 (255.255.255.0)

Default Gateway

DNS Server IP Address1

DNS Server IP Address2

IPv6

IPv6 Global Unicast Address Prefix

IPv6 DNS Server 1

IPv6 DNS Server 2

IPv6 Global Unicast Address

IPv6 Link-Local Address

fe80::290:e8ff:fe00:56

APPLY

Get IP From

Setting	Description	Factory Default
Manual	The IP address of the switch must be set manually.	Slot Index
DHCP	The IP address of the switch will be assigned automatically by the network's DHCP server.	
Slot Index	The IP address of the switch will be assigned automatically by the slot index.	

IP Address

Setting	Description	Factory Default
Input the IP address for the switch	Specify the IP address to use for the switch.	IP address is based on the slot index value.

Subnet Mask

Setting	Description	Factory Default
Input the subnet mask for the switch	Specify the subnet mask to use for the switch.	24 (255.255.255.0)

Default Gateway

Setting	Description	Factory Default
Input the IP address for the gateway	Specify the IP address of the gateway that connects the LAN to a WAN or another network.	None

DNS Server 1

Setting	Description	Factory Default
Input the IP address of the first DNS server	Specify the IP address of the first DNS server used by your network. After specifying the DNS server's IP address, you can use the switch's URL (e.g., www.mymoxaswitch.com) to open the web console instead of entering the IP address.	None

DNS Server 2

Setting	Description	Factory Default
Input the IP address of the second DNS server	Specify the IP address of the second DNS server used by your network. The switch will use the secondary DNS server if the first DNS server cannot connect.	None

IPv6 Global Unicast Address Prefix (Prefix Length: 64 bits) Default Gateway

Setting	Description	Factory Default
Global Unicast Address Prefix	The prefix value must be formatted according to the RFC 2373 IPv6 Addressing Architecture, using 8 colon-separated 16-bit hexadecimal values. One double colon can be used in the address to show the number of zeros required to fill the undefined fields. Note: This feature is only available in Advanced Mode .	None

IPv6 DNS Server 1

Setting	Description	Factory Default
Input the IPv6 IP address of the first DNS server	Specify the IPv6 address of the first DNS server used by your network. After specifying the DNS server's IP address, you can use the switch's URL (e.g., www.mymoxaswitch.com) to open the web console instead of entering the IP address. Note: This feature is only available in Advanced Mode .	None

IPv6 DNS Server 2

Setting	Description	Factory Default
Input the IPv6 address of the second DNS server	Specify the IPv6 address of the second DNS server used by your network. The switch module will use the secondary DNS server if the first DNS server cannot connect. Note: This feature is only available in Advanced Mode .	None

IPv6 Global Unicast Address

Setting	Description	Factory Default
None	Displays the IPv6 Global Unicast address. The network portion of the Global Unicast address can be configured by specifying the Global Unicast Prefix and using an EUI-64 interface ID in the low order 64 bits of the address. The host portion of the Global Unicast address is automatically generated using the modified EUI-64 form of the interface identifier (the switch's MAC address). Note: This feature is only available in Advanced Mode .	None

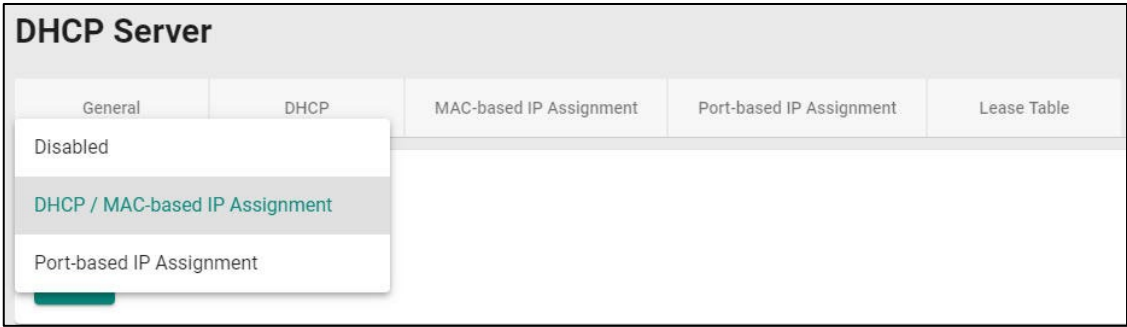
IPv6 Link-Local Address

Setting	Description	Factory Default
None	The network portion of the Link-Local address is FE80, and the host portion of the Link-Local address is automatically generated using the modified EUI-64 form of the interface identifier (the switch's MAC address). Note: This feature is only available in Advanced Mode .	None

When finished, select **APPLY** to save your changes.

DHCP Server

This section describes how to configure the DHCP server settings for switch module. First, select the **General** tab.



Then, select **DHCP/MAC-based IP Assignment** and select **APPLY**.

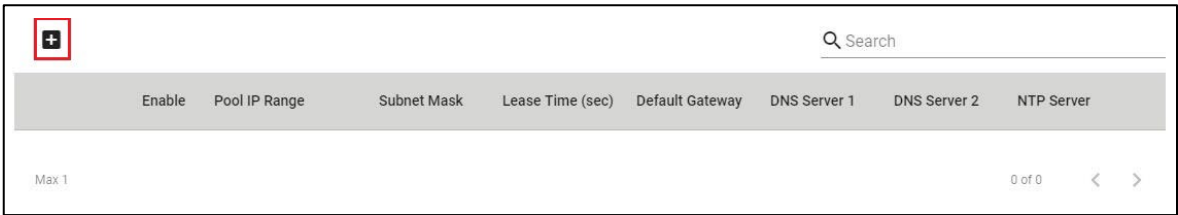


NOTE

The DHCP server will use UDP port 67 to send messages to the DHCP client.

DHCP

Select the **DHCP** tab and then select the **+** icon on the configuration page to create a new DHCP server pool.



Configure the following parameters.

Create DHCP Server Pool

Enable

Enabled

Start IP Address *

Subnet Mask *

End IP Address *

Default Gateway

Lease Time *

86400

10 - 604800 sec.

DNS Server 1

DNS Server 2

NTP Server

CANCEL

CREATE



NOTE

You can only create one IP pool. It can be connected to different network subnets with the Management IP of the switch.

Enable

Setting	Description	Factory Default
Enabled	Enables the DHCP server pool.	Disabled
Disable	Disables the DHCP server pool.	

Start IP Address

Setting	Description	Factory Default
Input the first IP address	Specify the first IP address for the pool.	None

Subnet Mask

Setting	Description	Factory Default
Select from the drop-down list	Specify the subnet mask for the pool.	None

End IP Address

Setting	Description	Factory Default
Input the last IP address	Specify the last IP address for the pool.	None

Default Gateway

Setting	Description	Factory Default
Input the IP address of the default gateway	Specify the default gateway for clients to use.	None

Lease Time (sec.)

Setting	Description	Factory Default
Input the lease time for the DHCP, from 10 to 604,800 seconds (up to 7 days)	Specify the lease time for DHCP IP assignments.	86400

DNS Server 1

Setting	Description	Factory Default
Input the IP address of the first DNS server	Specify the IP address of the first DNS server for clients to use.	None

DNS Server 2

Setting	Description	Factory Default
Input the IP address of the second DNS server	Specify the IP address of the second DNS server for clients to use.	None

NTP Server

Setting	Description	Factory Default
Input the address of the NTP server	Specify the NTP server clients will use.	None

When finished, select **CREATE**.

MAC-based IP Assignment

Assign an IP address for a specific MAC address. This can be useful if you always want the same IP address to be assigned to a specific device, even if it is reconnected or connected to a different port.

Select the **MAC-based IP Assignment** tab, and then select the + icon on the configuration page.

General

DHCP

MAC-based IP Assignment

Port-based IP Assignment

Lease Table

Search

☐	Enable	Hostname	IP Address	Subnet Mask	MAC Address	Lease Time (sec)	Default Gateway	DNS Server 1
Max 256								
						Items per page: 50	0 of 0	< >

Configure the following parameters.

Create Entry

Enable

Enabled

Hostname *

0 / 63

IP Address *

Subnet Mask *

MAC Address *

Default Gateway

Lease Time *

86400

10 - 604800 sec.

DNS Server 1

DNS Server 2

NTP Server

CANCEL

CREATE

Enable

Setting	Description	Factory Default
Enabled	Enables the MAC-based IP assignment entry.	Enabled
Disabled	Disables the MAC-based IP assignment entry.	

Hostname

Setting	Description	Factory Default
Enter a host name between 0 and 63 characters	Specify a host name to use for the DHCP client.	None

IP Address

Setting	Description	Factory Default
Input the assigned IP address	Specify the IP address to assign to the client.	None

Subnet Mask

Setting	Description	Factory Default
Select from the drop-down list	Specify the subnet mask to use for the client.	None

MAC Address

Setting	Description	Factory Default
Input the assigned MAC address	Specify the MAC address of the device you want to assign an IP address to. Make sure the MAC address is entered in the correct format. Here is an example: 28-d2-44-D3-e3-f2 or 28:d2:44:D3:e3:f2.	None

Default Gateway

Setting	Description	Factory Default
Input the IP address of the default gateway	Specify the default gateway for the client to use.	None

Lease Time (sec.)

Setting	Description	Factory Default
Input the lease time for the DHCP, from 10 to 604800.	Define how long before the IP address needs to be reassigned.	86400

DNS Server 1

Setting	Description	Factory Default
Input the IP address of the first DNS server	Specify the IP address of the first DNS server for the client to use.	None

DNS Server 2

Setting	Description	Factory Default
Input the IP address of the second DNS server	Specify the IP address of the second DNS server for the client to use.	None

NTP Server

Setting	Description	Factory Default
Input the address of the NTP server	Specify the NTP server the client will use.	None

When finished, select **CREATE**.

Port-based IP Assignment

Assign an IP to a device based on what switch port it is connected to. This can be useful if you want to always use the same IP for a device connected to a specific port, even if it is replaced with a different device.

On the **General** tab, select **Port-based IP Assignment**. Select **APPLY**.

DHCP Server

General

DHCP

MAC-based IP Assignment

Port-based IP Assignment

Lease Table

Mode

Port-based IP Assignment

APPLY

Next, select the **Port-based IP Assignment** tab, and then select the **+** icon on the configuration page.

DHCP Server

General

DHCP

MAC-based IP Assignment

Port-based IP Assignment

Lease Table

Search

☐	Port	Enable	IP Address	Subnet Mask	Lease Time (sec)	Default Gateway	DNS Server 1	DNS Server 2	NTP Server
--------------------------	------	--------	------------	-------------	------------------	-----------------	--------------	--------------	------------

12 Max0 of 0

Configure the following parameters.

Create Entry

Enable

Enabled

Port *

IP Address *

Subnet Mask *

Default Gateway

Lease Time *

86400

10 - 604800

DNS Server 1

DNS Server 2

NTP Server

CANCEL

CREATE

Enable

Setting	Description	Factory Default
Enabled	Enables the port-based IP assignment entry.	Enabled
Disabled	Disables the port-based IP assignment entry.	

Port

Setting	Description	Factory Default
Select from 1 to 28	Select which switch port the DHCP server will assign an IP address for.	None

IP Address

Setting	Description	Factory Default
Input the assigned IP address	Specify the IP address to assign to the client.	None

Subnet Mask

Setting	Description	Factory Default
Select from the drop-down list	Specify the subnet mask to use for the client.	None

Default Gateway

Setting	Description	Factory Default
Input the IP address of the default gateway	Specify the default gateway for the client to use.	None

Lease Time (sec.)

Setting	Description	Factory Default
Input the lease time for the DHCP, from 10 to 604800	Define how long before the IP address needs to be reassigned.	86400

DNS Server 1

Setting	Description	Factory Default
Input the IP address of the first DNS server	Specify the IP address of the first DNS server for the client to use.	None

DNS Server 2

Setting	Description	Factory Default
Input the IP address of the second DNS server	Specify the IP address of the second DNS server for the client to use.	None

NTP Server

Setting	Description	Factory Default
Input the address of the NTP server	Specify the NTP server the client will use.	None

When finished, select **CREATE**.

Lease Table

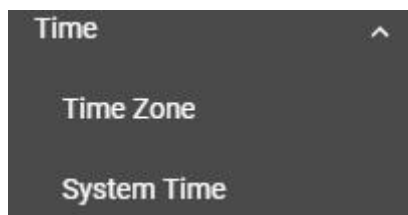
Select **Lease Table** to view detailed information for the host name, IP address, MAC address, and time left for each port.

DHCP Server				
General	DHCP	MAC-based IP Assignment	Port-based IP Assignment	Lease Table
 Search				
Hostname	IP Address	MAC Address	Time Left	
CINDY-YANG01	192.168.127.1	c8:cb:b8:02:26:5f	23 h: 57 m: 41 s	

Item	Description
Host name	The Host name of the client.
IP Address	The IP address of the client.
MAC Address	The MAC address of the client.
Time Left	The time left on the DHCP lease for the client.

Time

This section describes how to configure the **Time Zone** and **System Time** settings for the switch. The switch has a time calibration function based on information from an NTP server or a user-specified time and date, allowing functions such as automatic warning emails to include a time and date stamp.



NOTE

Update the Current Time and Current Date after the switch has been powered off for an extended period (e.g., three days). Pay particular attention to this when there is no NTP server or Internet connection available.

Time Zone

Configure the time zone for the switch.

A screenshot of the 'Time Zone' configuration page. It shows the 'Current Time' as '2018-12-27 19:35:16 UTC+00:00'. Below this, there is a 'Time Zone' dropdown menu set to 'UTC+00:00'. There is also a 'Daylight Saving' dropdown menu set to 'Disabled'. Further down, there are fields for 'Start Date *' (2000-01-01) and 'Start Time *' (12:00 AM), and 'End Date *' (2000-12-31) and 'End Time *' (11:00 PM). At the bottom, there is an 'Offset' field set to '00:00' and an 'APPLY' button.

System Uptime

Setting	Description	Factory Default
System-specified time	This shows how long the switch has been running since the last cold start.	N/A

Current Time

Setting	Description	Factory Default
User-specified time	Shows the current system time.	None

Time Zone

Setting	Description	Factory Default
Select from the drop-down list	Specify the time zone to use for the switch.	GMT (Greenwich Mean Time)

Daylight Saving Time

The Daylight Saving Time settings are used to automatically adjust the time according to regional standards.

Daylight Saving
Enabled

Start Date * 2000-01-01 Start Time * 12:00 AM

End Date * 2000-12-31 End Time * 11:00 PM

Offset
00:00

APPLY

Configure the following settings.

Daylight Saving Time

Setting	Description	Factory Default
Enabled	Enables Daylight Saving Time.	Disabled
Disabled	Disables Daylight Saving Time.	

Start Date

Setting	Description	Factory Default
User-specified date	Specify the date that Daylight Saving Time begins.	None

End Date

Setting	Description	Factory Default
User-specified date	Specify the date that Daylight Saving Time ends.	None

Offset

Setting	Description	Factory Default
User-specified hour	Specify the offset (in HH:MM format) to use during Daylight Saving Time.	None

When finished, select **APPLY** to activate the time zone settings.

System Time

This section describes how to configure the **Time**, **NTP Server**, and **NTP Authentication** settings.

Time

The section describes how to configure the system's time. Select the Time tab.

System Time

Time

NTP Server

NTP Authentication

Current Time

2018-12-27 19:37:28 UTC+00:00

Clock Source

Local

Date *

2018-12-27

Time

07:37 PM

APPLY

SYNC FROM BROWSER

Current Time

Setting	Description	Factory Default
None	This automatically shows the current time according to your default settings.	Local

Clock Source

Setting	Description	Factory Default
Select from the drop-down list	Specify whether to set the time manually (Local), from an SNTP server, or from an NTP server.	Local

Clock Source is from Local

Date

Setting	Description	Factory Default
Select the date	Select the current date.	Local

2021 MAR

< >

Su Mo Tu We Th Fr Sa

MAR

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

Time

Setting	Description	Factory Default
Input the current time	Specify the current time. Manually input the time or select Sync from Browser to set the time based on the time used by your web browser.	None

Clock Source is from SNTP

Time Server 1

Setting	Description	Factory Default
Input the address of the first SNTP time server	Specify the IP or domain address of the first SNTP server to use (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	Time.nist.gov

Time Server 2

Setting	Description	Factory Default
Input the address of the second SNTP time server	Specify the IP or domain address of the secondary SNTP server to use if the first SNTP server cannot connect.	None

Select **APPLY** to complete.

Clock Source is from NTP

If the switch is connected to an NTP server that requires authentication, refer to the **NTP Authentication** section to configure the NTP key to use.

Time Server 1

Setting	Description	Factory Default
Input the address of the first NTP time server	Specify the IP or domain address of the first NTP server to use (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	Time.nist.gov

Authentication

Setting	Description	Factory Default
Disabled	Enable or disable NTP authentication for Time Server 1.	Disabled

Time Server 2

Setting	Description	Factory Default
Input the address of the second time server	Specify the IP or domain address of the secondary NTP server to use if the first NTP server cannot connect.	None

Authentication

Setting	Description	Factory Default
Disabled	Enable or disable NTP Authentication for Time Server 2.	Disabled

Select **APPLY** to complete.

NTP Server

Select the **NTP Server** Tab to perform further configuration.

System Time

Time

NTP Server

NTP Authentication

NTP Server

Disabled

Client Authentication

Disabled

APPLY

Enable

Setting	Description	Factory Default
Enabled	Enable the NTP server.	Disabled
Disabled	Disable the NTP server.	

Client Authentication

Setting	Description	Factory Default
Enabled	Enable NTP authentication.	Disabled
Disabled	Disable NTP authentication.	

When finished, select **APPLY** to save your changes.



NOTE

The NTP server will use TCP port 123 to send messages to the NTP client.

NTP Authentication

This section describes how to configure NTP Authentication. Select the **NTP Authentication** tab, and then select the **+** icon on the page.

Key ID	Type	Key String
--------	------	------------

Configure the following settings.

Key ID *

1 - 65535

Type

MD5

Key String *

0 / 32

CANCEL CREATE

Key ID

Setting	Description	Factory Default
Input the Key ID from 1 to 10	Input the Key ID to use for NTP authentication.	None

Type

Setting	Description	Factory Default
Input the authentication type	Input the authentication type.	MD5

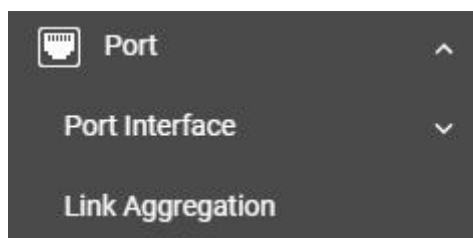
Key String

Setting	Description	Factory Default
Input the key string for authentication, from 0 to 32 characters.	Input the password to use for the authentication key.	None

When finished, select **CREATE**.

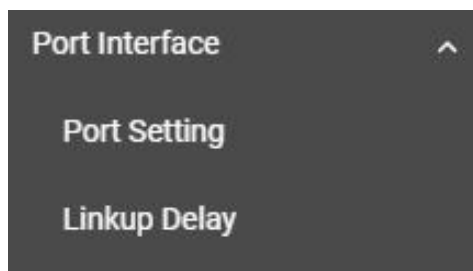
Port

This section describes how to configure the **Port Interface** and **Link Aggregation** functions for the switch.



Port Interface

Two functions are included in this section: **Port Setting** and **Linkup Delay**.



Port Setting

Under **Port Setting**, select the **Setting** tab and then select the edit icon on the port you want to configure.

Port Settings

Settings

Status

Search

Port	Admin Status	Media Type	Description	Speed/Duplex	Flow Control	MDI/MDIX
 1	Enabled	1000FX,miniGBIC		---	Disabled	---
 2	Enabled	1000FX,miniGBIC		---	Disabled	---
 3	Enabled	1000TX,RJ45		Auto	Enabled	Auto
 4	Enabled	1000TX,RJ45		Auto	Enabled	Auto
 5	Enabled	1000TX,RJ45		Auto	Enabled	Auto
 6	Enabled	1000TX,RJ45		Auto	Enabled	Auto
 7	Enabled	1000TX,RJ45		Auto	Enabled	Auto
 8	Enabled	1000TX,RJ45		Auto	Enabled	Auto
 9	Enabled	1000TX,RJ45		Auto	Enabled	Auto
 10	Enabled	1000TX,RJ45		Auto	Enabled	Auto
 SW1	Enabled	1000FX,Internal	*****	---	---	---
 SW2	Enabled	1000FX,Internal		---	---	---
 CPU1	Disabled	1000FX,Internal		---	---	---
 CPU2	Enabled	1000FX,Internal		---	---	---

Configure the following parameters.

Edit Port 1 Settings

Admin Status

Enabled

Media Type

100TX,RJ45

Description

Speed/Duplex

Auto

Flow Control

Disabled

MDI/MDIX

Auto

Copy Config to Ports

CANCEL

APPLY

Admin Status

Setting	Description	Factory Default
Enable	Allows data transmission through this port.	Enabled
Disabled	Disables data transmission through this port.	

Media Type

Setting	Description	Factory Default
Media type	Displays the media type for each module's port.	1000TX,RJ45,PTP

Description

Setting	Description	Factory Default
Max. 63 characters	Specify an alias for the port to help differentiate between different ports (e.g., PLC1).	None

Speed/Duplex

Setting	Description	Factory Default
Auto	Allows the port to use the IEEE 802.3u protocol to negotiate with connected devices. The port and connected devices will determine the best speed for that connection.	Auto
10M Half	Choose a fixed speed option if the connected Ethernet device has trouble auto-negotiating line speed.	
10M Full		
100M Half		
100M Full		

Flow Control

This setting enables or disables flow control for the port when the port's speed is set to Auto. The result will be determined by the Auto process between the switch and connected devices.

Setting	Description	Factory Default
Enable	Enables flow control for this port when the port's speed is set to Auto.	Disabled
Disable	Disables flow control for this port when the port's speed is set to Auto.	

MDI/MDIX

Setting	Description	Factory Default
Auto	Allows the port to auto-detect the port type of the connected Ethernet device and changes the port type accordingly.	Auto
MDI	Choose MDI or MDIX if the connected Ethernet device has trouble auto-detecting the port type.	
MDIX		

Copy Config to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Allows you to copy the configuration to other port(s).	None

When finished, select **APPLY** to save your changes.

Port Status

To view the status of the ports, select the **Status** tab.

Port Settings							
Settings		Status					
	Port	Admin Status	Media Type	Description	Speed/Duplex	Flow Control	MDI/MDIX
	1	Enabled	1000FX,miniGBIC		---	Disabled	---
	2	Enabled	1000FX,miniGBIC		---	Disabled	---
	3	Enabled	1000TX,RJ45		Auto	Enabled	Auto
	4	Enabled	1000TX,RJ45		Auto	Enabled	Auto
	5	Enabled	1000TX,RJ45		Auto	Enabled	Auto
	6	Enabled	1000TX,RJ45		Auto	Enabled	Auto
	7	Enabled	1000TX,RJ45		Auto	Enabled	Auto
	8	Enabled	1000TX,RJ45		Auto	Enabled	Auto
	9	Enabled	1000TX,RJ45		Auto	Enabled	Auto
	10	Enabled	1000TX,RJ45		Auto	Enabled	Auto
	SW1	Enabled	1000FX,Internal	*****	---	---	---
	SW2	Enabled	1000FX,Internal		---	---	---
	CPU1	Disabled	1000FX,Internal		---	---	---
	CPU2	Enabled	1000FX,Internal		---	---	---

Linkup Delay

Linkup Delay Overview

Linkup delay is used to prevent a port alternating between link up and link down. It is also sometimes called link flap prevention. This feature is useful when the link connection is unstable. An unstable connection might be caused by a faulty cable, faulty fiber transceiver, duplex mismatch, etc. This feature helps administrators to mitigate the risk of an unstable network, particularly when the topology changes frequently.

Linkup Delay Settings

This section describes how to configure the linkup delay for the ports. Select the **Linkup Delay** menu. The default setting disables linkup delay for all ports.



NOTE

Only ports 1 to 10 support Linkup Delay Setting. SW1, SW2, CPU1, CPU2 are internal communication ports. This function cannot be edited in these ports.

Linkup Delay

Linkup Delay

Disabled

APPLY

Enable

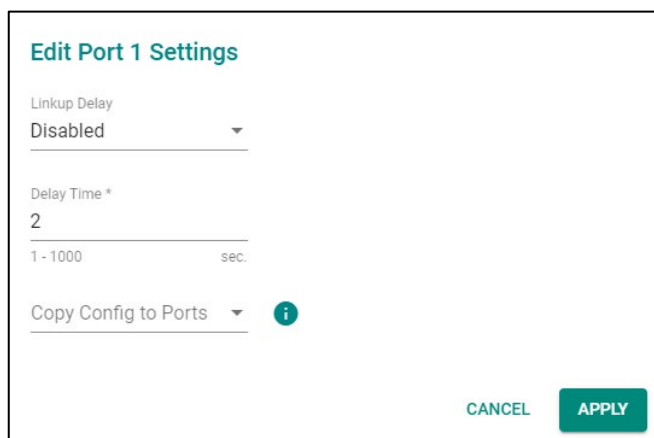
Setting	Description	Factory Default
Enable	Enables linkup delay.	Disabled
Disabled	Disables linkup delay.	

When finished, select **APPLY** to save your changes.

To configure the linkup delay for a port, select the edit icon on the port you want to configure.

	Port	Enable	Delay Time	Remaining Time
	1	Disabled	2	0
	2	Disabled	2	0
	3	Disabled	2	0
	4	Disabled	2	0
	5	Disabled	2	0
	6	Disabled	2	0
	7	Disabled	2	0
	8	Disabled	2	0
	9	Disabled	2	0
	10	Disabled	2	0
	SW1	---	---	---
	SW2	---	---	---
	CPU1	---	---	---
	CPU2	---	---	---

Some parameters need to be configured.



Linkup Delay

Setting	Description	Factory Default
Enable	Enables linkup delay for the port.	Disabled
Disable	Disables linkup delay for the port.	

Delay Time (sec.)

Setting	Description	Factory Default
1 to 1000	Specify the linkup delay time from 1 to 1000 seconds.	2

Copy Config to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Allows you to copy the configurations to other port(s).	None

When finished, select **APPLY** to save your changes.

Link Aggregation

Link Aggregation (Port Channel) Overview

Link Aggregation helps balance, optimize, and facilitate the switch's throughput. This method can combine multiple network communications in parallel to maximize data throughput, increasing data communication efficiency for each port. In addition, it also acts as a useful method for network redundancy when a link fails. In general, Link Aggregation supports combining multiple physical switch ports into a single, efficient bandwidth data communication route. This can improve network load sharing and increase network reliability.

Static Trunk

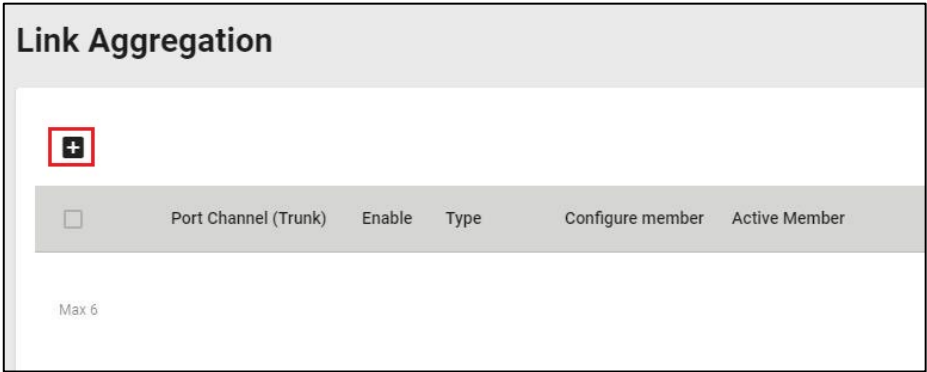
For some networking applications, a situation can arise where traffic from multiple ports is required to be filtered through one port. For example, if there are 30 UHD IP surveillance cameras deployed and connected in a ring, the traffic can reach up to 1 Gbps, causing a surge in traffic that can increase network loading by up to 50%. Hence, the uplink port needs to use the static trunk function to provide more bandwidth and redundancy protection.

LACP

The Link Aggregation Control Protocol (LACP) allows a network device to negotiate an automatic bundling of several ports by sending LACP packets to the peer, a directly connected device that also uses LACP.

Link Aggregation Settings

This section describes how to configure link aggregation for each port. Select **Link Aggregation** on the menu and then select the + icon on the configuration page.



To create a link aggregation group, configure the following parameters.

Create Link Aggregation

LA Group Status
Enabled

Type *

Config Member Port * i

CANCEL CREATE

LA Group Status

Setting	Description	Factory Default
Enable	Enable link aggregation grouping.	None
Disable	Disable link aggregation grouping.	

Type

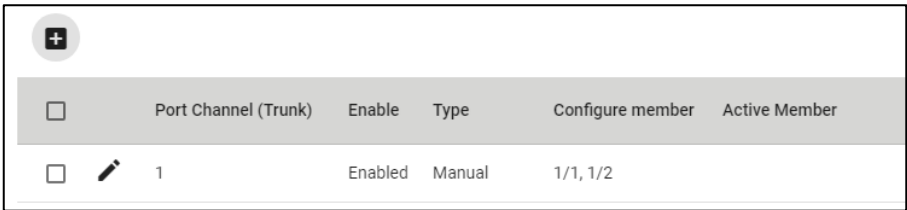
Setting	Description	Factory Default
Manual	Configure the link aggregation type manually.	None
LACP	Configure the link aggregation type by LACP.	

Config Member Port

Setting	Description	Factory Default
Select from the ports	Select the ports you want to create for link aggregation grouping.	None

When finished, select **CREATE** to continue.

View the current Link Aggregation or Port Channel (Trunk) status on the configuration page. Edit or delete by selecting the edit or delete icon on the page.



Editing Port Setting for Link Aggregation

To edit each port's setting for Link Aggregation, select the edit icon on the port name. You can also check the port and then select the edit icon for editing the port settings for Link Aggregation.



NOTE

Only port 1 to 10 support Link Aggregation setting. SW1, SW2, CPU1, CPU2 are internal communication ports. This function cannot be edited in these ports.

 Search						
☐	Port Channel (Trunk)	Enable	Type	Algorithm	Configure member	Active Member
☐	 1	Enabled	LACP	SMAC + DMAC	1/2	

Edit the following port settings.

Edit Port Channel 1 Settings

LA Group Status
Enabled

Type *
Manual

Config Member Port *
1



CANCEL APPLY

LA Group Status

Setting	Description	Factory Default
Enable	Enable link aggregation grouping.	None
Disable	Disable link aggregation grouping.	

Type

Setting	Description	Factory Default
Manual	Configure link aggregation manually.	None
LACP	Configure link aggregation by LACP.	

Config Member Port

Setting	Description	Factory Default
Select from the ports	Select the ports you want to create link aggregation grouping for.	None

When finished, select **APPLY** to save your changes.

Deleting the Port for Link Aggregation

To delete the port for Link Aggregation, check the port and then select the delete icon.

	Search					
☒	Port Channel (Trunk)	Enable	Type	Algorithm	Configure member	Active Member
☒	 1	Enabled	LACP	SMAC + DMAC	1/2	

Select **DELETE** to finish. Note that some features, such as RSTP and VLAN, will be set to default values once you delete the Link Aggregation setting.

Delete Link Aggregation

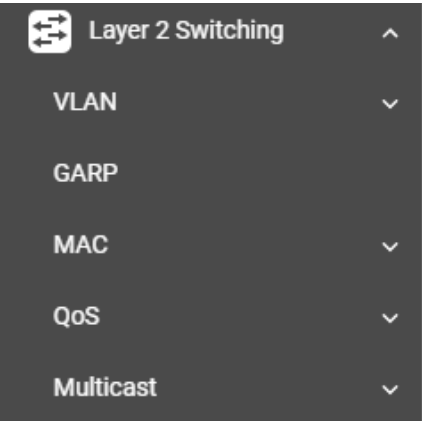
Warning:
Some features (like RSTP, VLAN...etc.) related to selected Link Aggregation will be set to default values.

Are you sure you want to delete the selected Link Aggregation?

CANCELDELETE

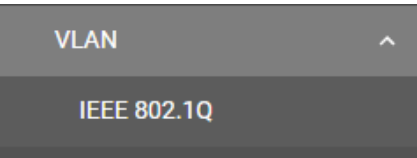
Layer 2 Switching

This section describes how to configure various parameters, such as **VLAN**, **GARP**, **MAC**, **QoS**, and **Multicast**, for switch module. Select **Layer 2 Switching** on the function menu.



VLAN

This section includes **IEEE802.1Q** configurations.



IEEE 802.1Q Overview

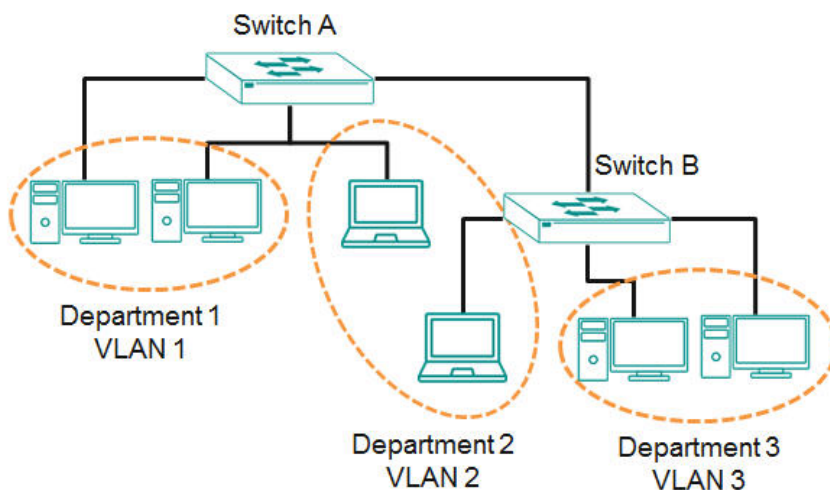
The IEEE 802.1Q is a network communication protocol that falls under the IEEE 802.1 standard regulation, allowing various segments to use a physical network at the same time to block broadcast packets by different segmentations. It specifies the VLAN tagging for Ethernet frames on switches that can control the path process.

How A VLAN Works

What is a VLAN?

A VLAN is a group of devices that can be located anywhere on a network, but which communicate as if they are on the same physical segment. With VLANs, you can segment your network without being restricted by physical connections—a limitation of traditional network design. With VLANs you can segment your network into:

- **Departmental groups**—You could have one VLAN for the marketing department, another for the finance department, and another for the product development department.
- **Hierarchical groups**—You could have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups**—You could have one VLAN for email users and another for multimedia users.



Benefits of VLANs

The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides you with three other benefits:

- **VLANs ease the relocation of devices on networks:** With traditional networks, network administrators spend much of their time dealing with changes. If you move to a different subnetwork, the addresses of each host must be updated manually. With a VLAN setup, if a host originally on the Marketing VLAN is moved to a port on another part of the network, and retains its original subnet membership, you only need to specify that the new port is on the Marketing VLAN. You do not need to do any recalling.
- **VLANs provide extra security:** Devices within each VLAN can only communicate with other devices on the same VLAN. If a device on the Marketing VLAN needs to communicate with devices on the Finance VLAN, the traffic must pass through a routing device or Layer 3 switch.
- **VLANs help control traffic:** With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices, regardless of whether they need it. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other.

VLANs and the Switch Module

Your switch module includes support for VLANs using IEEE Std 802.1Q-2005. This standard allows traffic from multiple VLANs to be carried across one physical link. The IEEE Std 802.1Q-2005 standard allows each port on your switch module to be placed:

- On a single VLAN defined in the switch
- On several VLANs simultaneously using 802.1Q tagging

The standard requires that you define the 802.1Q VLAN ID for each VLAN on your switch module before the switch can use it to forward traffic:

Managing a VLAN

A new or initialized switch module contains a single VLAN—the Default VLAN. This VLAN has the following definition:

- Management VLAN ID 1 can be changed
- 802.1Q VLAN default ID 1 cannot be deleted

All the ports are initially placed on this VLAN, and it is the only VLAN that allows you to access the management software of the switch module over the network.

Communication Between VLANs

If devices connected to a VLAN need to communicate with devices on a different VLAN, a router or Layer 3 switching device with connections to both VLANs needs to be installed. Communication between VLANs can only take place if they are all connected to a routing or Layer 3 switching device.

VLANs: Tagged and Untagged Membership

Switch module supports 802.1Q VLAN tagging, a system that allows traffic for multiple VLANs to be carried on a single physical link (backbone, trunk). When setting up VLANs you need to understand when to use untagged or tagged membership of VLANs. Simply put, if a port is on a single VLAN it can be an untagged member, but if the port needs to be a member of multiple VLANs, a tagged membership must be defined.

A typical host (e.g., clients) will be an untagged member of one VLAN, defined as an **access port** in a switch module, while an inter-switch connection will be a tagged member of all VLANs, defined as a **trunk port** in a switch module.

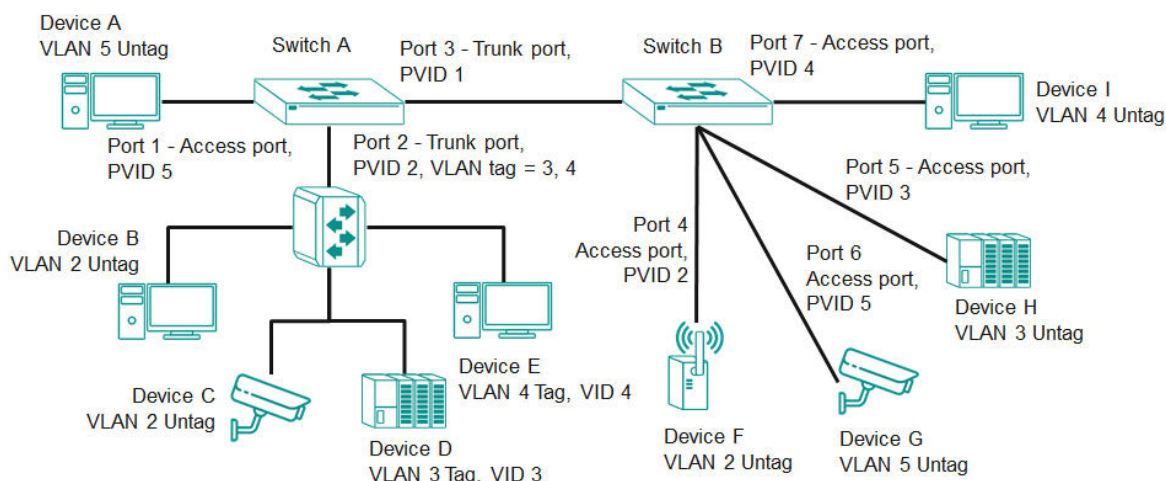
The IEEE Std 802.1Q-2005 defines how VLANs operate within an open packet-switched network. An 802.1Q compliant packet carries additional information that allows a switch to determine which VLAN the port belongs to. A frame is called a tagged frame if it carries additional information.

To carry multiple VLANs across a single physical link (backbone, trunk). Each packet must be tagged with a VLAN identifier so that the switches can identify which packets belong to which VLAN. To communicate between VLANs, a router must be used.

Switch module supports three types of VLAN port settings:

- **Access Port:** The port connects to a single device that is not tagged. You must define the default port PVID that assigns which VLAN the device belongs to. Once the ingress packet of this access port egresses to another trunk port (the port needs all packets to carry tag information), the switch will insert this PVID into this packet so the next 802.1Q VLAN switch can recognize it.
- **Trunk Port:** The port connects to a LAN that comprises untagged devices and tagged devices. In general, the traffic of the trunk port must have a tag. You can also assign a PVID to a trunk port. The untagged packet on the trunk port will be assigned the default port PVID as its VID.
- **Hybrid Port:** The port is like a trunk port, except users can explicitly assign tags to be removed from egress packets.

The following section illustrates how to use these ports to set up different applications.



In this application:

- Port 1 connects a single untagged device and assigns it to VLAN 5; it should be configured as an **access port** with PVID 5.
- Port 2 connects a LAN with two untagged devices belonging to VLAN 2. One tagged device with VID 3 and one tagged device with VID 4. It should be configured as a **hybrid port** with PVID 2 for untagged devices and Fixed VLAN (Tagged) with 3 and 4 for tagged device. Since each port can only have one unique PVID, all untagged devices on the same port must belong to the same VLAN.
- Port 3 connects with another switch. It should be configured as a **trunk port**. GVRP protocol will be used through the trunk port.
- Port 4 connects a single untagged device and assigns it to VLAN 2; it should be configured as an **access port** with PVID 2.
- Port 5 connects a single untagged device and assigns it to VLAN 3; it should be configured as an **access port** with PVID 3.
- Port 6 connects a single untagged device and assigns it to VLAN 5; it should be configured as an **access port** with PVID 5.
- Port 7 connects a single untagged device and assigns it to VLAN 4; it should be configured as an **access port** with PVID 4.

After the application is properly configured:

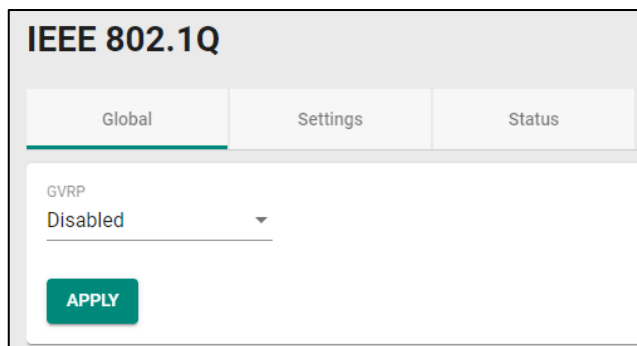
- Packets from Device A will travel through **Trunk Port 3** with tagged VID 5. Switch B will recognize its VLAN, pass it to port 6, and then remove tags received successfully by Device G, and vice versa.
- Packets from Devices B and C will travel through **Hybrid Port 2** with tagged VID 2. Switch B recognizes its VLAN, passes it to port 4, and then removes tags received successfully by Device F, and vice versa.
- Packets from Device D will travel through **Trunk Port 3** with tagged VID 3. Switch B will recognize its VLAN, pass to port 5, and then remove tags received successfully by Device H. Packets from Device H will travel through **Trunk Port 3** with PVID 3. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by Device D.
- Packets from Device E will travel through **Trunk Port 3** with tagged VID 4. Switch B will recognize its VLAN, pass it to port 7, and then remove tags received successfully by Device I. Packets from Device I will travel through **Trunk Port 3** with tagged VID 4. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by Device E.

VLAN Settings

To configure VLAN, select **VLAN** on the function menu, then select **IEEE 802.1Q**. Select **Global** tab.

GVRP (Generic VLAN Registration Protocol) is an IEEE 802.1Q standard protocol that helps specify how to define a method of tagging frames with VLAN configuration data. It essentially facilitates the management of VLAN within a larger network of data communication.

To edit the GVRP function, select the **Global** tab.



The screenshot shows the 'IEEE 802.1Q' configuration window with three tabs: 'Global', 'Settings', and 'Status'. The 'Global' tab is active. Under the 'GVRP' section, the status is 'Disabled' with a dropdown arrow. An 'APPLY' button is located at the bottom left of the configuration area.

Configure the following setting.

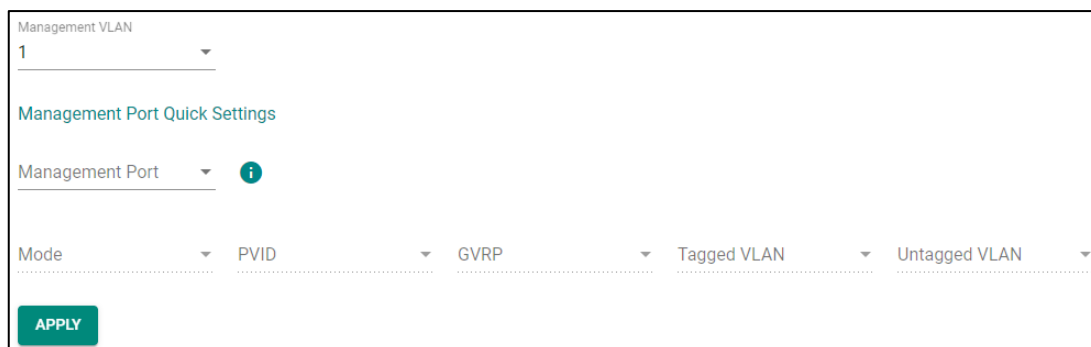
GVRP

Setting	Description	Factory Default
Disabled	Disables GVRP.	Disabled
Enabled	Enables GVRP.	

Select **APPLY** to finish.

VLAN Management Port Quick Settings

In the lower part of the configuration page, you can quickly configure the VLAN settings.



The screenshot shows the 'Management Port Quick Settings' section. At the top, 'Management VLAN' is set to '1'. Below it is the 'Management Port' dropdown with an information icon. A row of quick settings includes 'Mode', 'PVID', 'GVRP', 'Tagged VLAN', and 'Untagged VLAN', each with a dropdown arrow. An 'APPLY' button is at the bottom left.

Configure the following settings.

Management VLAN

Setting	Description	Factory Default
Select the Management VLAN from the drop-down list	Show the list of selectable VLANs.	1

Management Port

Setting	Description	Factory Default
Select the port(s) as the VLAN port(s) from the drop-down list	To select the port(s) as the VLAN port(s).	None

When finished, select **APPLY** to save your changes.

Detailed VLAN Settings

On the IEEE 802.1Q page, first select the Setting tab, and then select the edit icon.

IEEE 802.1Q

Global

Setting

Status

+

+

?

Search

	VLAN	Name	Member Port
☐ ✎ 1			1/1, 1/3, 1/4, 2/1, 2/2, 2/3, 2/4, 3/1, 3/2, 3/3, 3/4, 4/1, 4/2, 4/3, 4/4, 5/1, 5/2, 5/3, 5/4, 6/1, 6/2, 6/3, 6/4, 7/1, 7/2, 7/3, 7/4, po1

Configure the following parameters.

Create VLAN

VLAN ID *

Max. 10 VLANs

Name

0 / 32

Member Port

▼

Forbidden Port

▼

CANCEL

CREATE

VID

Setting	Description	Factory Default
Input a VLAN ID, (10 VLANs max.)	Input a VLAN ID.	None

Name

Setting	Description	Factory Default
Input a name for the VLAN, (32 characters max.)	Specify a name for the VLAN.	None

Member Port

Setting	Description	Factory Default
Select the port from the drop-down list.	Specify the ports that are the member ports for the VLAN.	None

When finished, select **CREATE**.

Forbidden Port (in Advanced Mode only)

Setting	Description	Factory Default
Select the port from the drop-down list	Specify the ports that are forbidden for the VLAN.	None

Editing the Existing VLAN Settings

To edit the exiting VLAN settings, select the edit icon of the VLAN you want to edit.

	VLAN ID	Name	Member Port
☐	1		G1, G2, G3, G4, 2, 3, 4, po1

Max. 256

Configure the following settings.

Edit VLAN 1 Settings

VLAN ID

1

Max. 10 VLANs

Name

0 / 32

Member Port

G1, G2, G3, G4, 2, 3, 4...

Forbidden Port

CANCEL

APPLY

VID		
Setting	Description	Factory Default
Show the VLAN ID	Display the VLAN ID.	None
Name		
Setting	Description	Factory Default
Show the name of the VLAN	Display the VLAN name.	None
Member Port		
Setting	Description	Factory Default
Select the port from the drop-down list	Specify the ports that are member ports for the VLAN.	None
When finished, select APPLY to save your changes.		
Forbidden Port (in Advanced Mode only)		
Setting	Description	Factory Default
Select the port from the drop-down list	Specify the ports that are forbidden for the VLAN.	None

Editing the Port Settings

To edit the port settings, in the **VLAN** tab, select the edit icon on the port you want to configure on the lower part of the page.

	Port	Mode	PVID	GVRP	Untagged VLAN	Tagged VLAN
	1/1	Access	1	Disabled	1	
	1/3	Access	1	Disabled	1	
	1/4	Access	1	Disabled	1	

Configure the following settings.

Edit Port 2 Settings

Mode
Access ▼

PVID
1 ▼

GVRP
Disabled ▼

Tagged VLAN
▼

Untagged VLAN
All Member VLAN IDs ▼

Copy Config to Ports ▼ 

CANCEL APPLY

Mode

Setting	Description	Factory Default
Access	When this port is connected to a single device, without tags.	Access
Trunk	When this port is connected to another 802.1Q VLAN aware switch.	
Hybrid	When this port is connected to another Access 802.1Q VLAN aware switch or another LAN that combines tagged and/or untagged devices.	

PVID

Setting	Description	Factory Default
1 to 4094	Sets the default VLAN ID for untagged devices connected to the port.	None

GVRP

Setting	Description	Factory Default
Enabled	Enables GVRP.	Disabled
Disabled	Disables GVRP.	

Tagged VLAN

Setting	Description	Factory Default
1 to 4094	This field will be active only when selecting the trunk or hybrid port type. Set the other VLAN ID for tagged devices that connect to the port.	None

Untagged VLAN

Setting	Description	Factory Default
VID range from 1 to 4094	This field is only active when the hybrid port type is selected. Set the other VLAN ID for tagged devices that connect to the port and tags that need to be removed in egress packets.	1

Copy Config to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configuration to other port(s).	None

When finished, select **APPLY** to save your changes.

GARP Overview

GARP stands for **Generic Attribute Registration Protocol**, which is a communication protocol defined by IEEE 802.1, offering a generic framework for bridges to register and de-register an attribute value. In a VLAN structure, two applications can be applied: **GARP VLAN Registration Protocol (GVRP)** is used to register VLAN trunking between multilayer switches, and **GARP Multicast Registration Protocol (GMRP)** to provide a constrained multicast flooding facility.

GARP Settings

Select **GARP** on the menu page and then select the edit icon on the port you want to configure.

	Port	Join Time	Leave Time	Leave All Time
	1/1	200	600	10000
	1/3	200	600	10000
	1/4	200	600	10000

Configure the following settings.

Edit Port 2 Settings

Join Time *

200

10 - 1073741810

Leave Time *

600

30 - 2147483630

Leave All Time *

10000

40 - 2147483640

Copy Config to Ports 

CANCEL APPLY

Join Time (sec.)

Setting	Description	Factory Default
10 to 499999980	Input the join time from 10 to 499999980 seconds.	200

Leave Time (sec.)

Setting	Description	Factory Default
30 to 499999980	Input the leave time from 30 to 499999980 seconds.	600

Leave All time (sec.)

Setting	Description	Factory Default
30 to 499999990	Input the leave all time.	10000

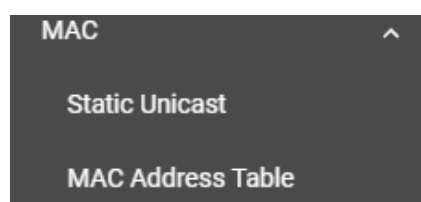
Copy Config to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configurations to other port(s).	None

When finished, select **APPLY** to save your changes.

MAC

This section explains Independent VLAN learning and describes how to configure **Static Unicast** and the **MAC Address Table**.



Independent VLAN Learning

The switch module uses the **Independent VLAN Learning (IVL)** mode.

In an **IVL Mode**, a MAC table will be created in each VLAN, which will make up many MAC tables. However, the same VID record will be selected and put in a table. A MAC table will be stored in the format of MAC + VID, the same MAC will be stored in different tables with different VIDs.

Static Unicast

Select **Static Unicast** on the function menu page and select the + icon on the configuration page.



Configure the following settings.

Add Static Unicast Entry

VLAN ID *

MAC Address *

Port *

CANCEL

CREATE

VID

Setting	Description	Factory Default
Input a VLAN ID	Input a VLAN ID.	None

MAC Address

Setting	Description	Factory Default
MAC address of the port	Input the MAC address of the port.	None

Port

Setting	Description	Factory Default
Select the port from the drop-down list	Specify the port you want to create a VLAN for.	None

When finished, select **CREATE**.

MAC Address Table

Select **MAC Address Table** and configure the following settings.

MAC Address Table

MAC Learning Mode

Independent VLAN Learning

Aging Time

300

10 - 300 sec.

APPLY

MAC Learning Mode

Information	Description	Factory Default
Independent VLAN learning	Show the current MAC Learning Mode.	Independent VLAN learning

Aging Time

Setting	Description	Factory Default
10 to 300	Input a VLAN ID.	None

When finished, select **APPLY** to save your changes.

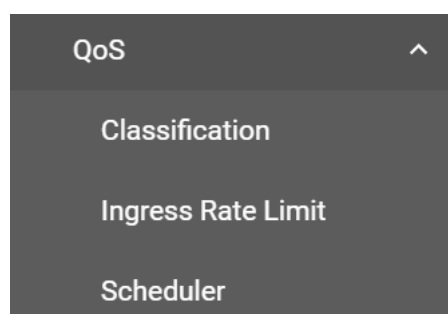
View the current MAC Address Table on the bottom part of the configuration page.

Index	VLAN	MAC Address	Type	Port
1	1	c8:cb:b8:02:26:5f	Learnt Unicast	3/4

Item Name	Description
Index	The number of the MAC address.
VLAN	The VLAN number
MAC Address	The MAC address on this device.
Type	Learnt Unicast, Learnt Multicast, Static Unicast, Static: Multicast
Port	The forwarding port of this MAC address.

QoS

This section describes how QoS works and how to configure the settings.



QoS Overview

The switch's traffic prioritization capability provides Quality of Service (QoS) to your network by making data delivery more reliable. Prioritize traffic on your network to ensure that high priority data is transmitted with minimum delay. Traffic can be controlled by a set of rules to obtain the required Quality of Service for your network. The rules define different types of traffic and specify how each type should be treated as it passes through the switch. The switch can inspect both IEEE 802.1p/1Q layer 2 CoS (Class of Service) tags, and even layer 3 DSCP (Differentiated Services Code Point) information to provide a consistent classification of the entire network. The switch's QoS capability improves the performance and determinism of industrial networks for mission-critical applications.

The Traffic Prioritization Concept

Traffic prioritization allows you to prioritize data so that time-sensitive and system-critical data can be transferred smoothly and with minimal delay over a network. The benefits of using traffic prioritization are:

- Improve network performance by controlling a wide variety of traffic and by managing congestion.
- Assign priorities to different categories of traffic. For example, set higher priorities for time-critical or mission-critical applications.
- Provide predictable throughput for multimedia applications, such as videoconferencing or voice over IP, and minimize traffic delay and jitter.
- Optimize the network utilization depending on application usage and usage needs. Hence, asset owners do not always need to expand their backbone bandwidth as the amount of traffic increases.

Traffic prioritization uses eight traffic queues to ensure that higher priority traffic can be forwarded separately from lower priority traffic, which guarantees Quality of Service (QoS) to your network.

Switch module traffic prioritization is based on two standards:

- **IEEE 802.1p**—a layer 2 QoS marking scheme
- **Differentiated Services (DiffServ)**—a layer 3 QoS marking scheme.

IEEE 802.1p Class of Service

The IEEE Std 802.1D 2005 Edition marking scheme, which is an enhancement to IEEE Std 802.1D, enables Quality of Service on the LAN. Traffic service levels are defined in the IEEE 802.1Q 4-byte tag, which is used to carry VLAN identification and IEEE 802.1p priority information. The IEEE 802.1p occupying 3 bits of the tag follows the destination MAC address and Source MAC address.

The IEEE Std 802.1D 2005 Edition priority marking scheme assigns an IEEE 802.1p priority level between 0 and 7 to each frame, which specifies the level of service that the associated packets shall be handled. The table below shows an example of how different traffic types can be mapped to the eight IEEE 802.1p priority levels.

IEEE 802.1p Priority Level	IEEE 802.1D Traffic Type
0	Best Effort
1	Background (lowest priority)
2	Reserved
3	Excellent Effort (business critical)
4	Controlled Load (streaming multimedia)
5	Video (interactive media)
6	Voice (interactive voice)
7	Network Control Reserved traffic

Even though the IEEE 802.1p standard is the most widely used prioritization scheme for LAN environments, it still has some restrictions:

- It requires an additional 4-byte tag in the frame, which is normally optional for Ethernet networks. Without this tag, the scheme cannot work.
- The tag is part of the IEEE 802.1Q header, so to implement QoS at layer 2, the entire network must implement IEEE 802.1Q VLAN tagging.
- It is only supported within a LAN and does not cross the WAN boundaries, since the IEEE 802.1Q tags will be removed when the packets pass through a router.

Differentiated Services (DiffServ) Traffic Marking

DiffServ is a Layer 3 marking scheme that uses the DiffServ Code Point (DSCP) field in the IP header to specify the packet priority. DSCP is an advanced intelligent method of traffic marking that allows you to choose how your network prioritizes different types of traffic. The DSCP field can be set from 0 to 63 to map to user-defined service levels, enabling you to regulate and categorize traffic by applications with different service levels.

The advantages of DiffServ over IEEE 802.1Q are:

- Prioritize and assign different traffic with appropriate latency, throughput, or reliability by each port.
- No extra tags are required.
- The DSCP priority tags are carried in the IP header, which can pass the WAN boundaries and through the Internet.
- DSCP is backwards compatible with IPv4 ToS (Type of Service), which allows operation with legacy devices that use IPv4 layer 3.

Traffic Prioritization

Switch module classifies traffic based on layer 2 of the OSI 7 layer model, and the switch prioritizes outbound traffic according to the priority information defined in the received packet. Incoming traffic is classified based upon the IEEE 802.1p service level field and is assigned to the applicable egress priority queue. The traffic flow through the switch is as follows:

- A packet received by the switch module may or may not have an 802.1p tag associated with it. If it does not, then it is given a default CoS value (according to the port settings in the classification section). Alternatively, the packet might be marked with a new 802.1p value, which will cause all knowledge of the previous 802.1p tag being lost.
- Each egress queue has associated 802.1p priority levels, and can be defined by users, the packet will be placed in the appropriate priority queue. When the packet reaches the head of its queue and is about to be transmitted, the device determines whether the egress port belongs to the VLAN group. If it is, then the new 802.1p tag is used in the extended 802.1D header.

Traffic Queues

The hardware of switch module has multiple traffic queues that allow packet prioritization to occur. Higher priority traffic can pass through the switch module without being delayed by lower priority traffic. As each packet arrives in the switch module, it undergoes ingress processing (which includes classification, marking/re-marking), and is then sorted into the appropriate queue. The switch then forwards packets from each queue.

Switch modules support two different queuing mechanisms:

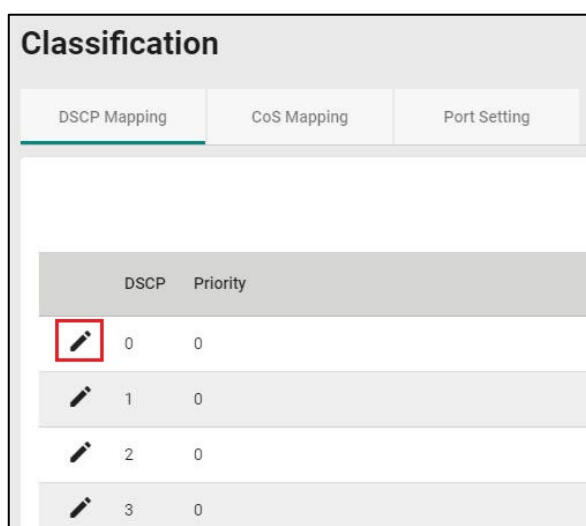
- **Weight Fair:** This method services all the traffic queues, giving priority to the higher priority queues. Under most circumstances, the Weight Fair method gives high priority precedence over low priority, but if high priority traffic does not reach the link capacity, lower priority traffic is not blocked.
- **Strict:** This method services high traffic queues first; low priority queues are delayed until no more high priority data needs to be sent. The Strict method always gives precedence to high priority over low priority.

Classification

This section includes three parameters: **DSCP Mapping**, **CoS Mapping**, and **Port Setting**. The three parameters are described below.

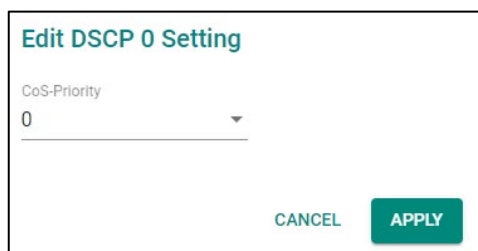
DSCP to CoS Mapping

In the **Classification** menu, select the **DSCP Mapping** tab, and then select the edit icon.



Classification		
DSCP Mapping	CoS Mapping	Port Setting
DSCP	Priority	
 0	0	
 1	0	
 2	0	
 3	0	

Configure the priority setting from the drop-down list for this port.



Edit DSCP 0 Setting

CoS-Priority
0

CANCEL APPLY

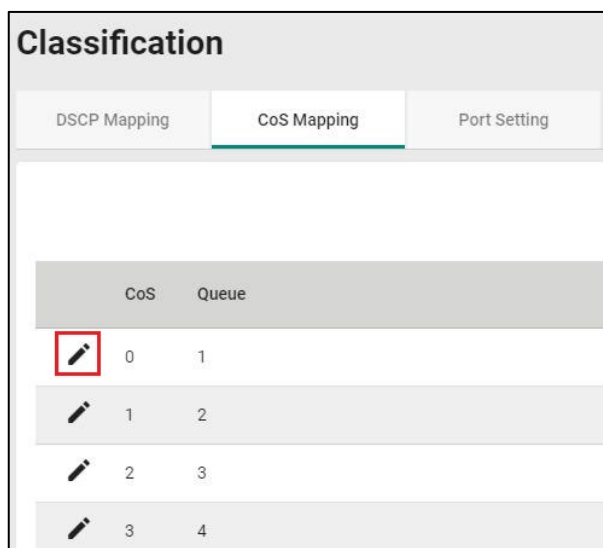
DSCP Value and Priority

Setting	Description	Factory Default
0 to 7	Different DSCP values map to one of eight different priorities from 0 to 7.	0
8 to 15		1
16 to 23		2
24 to 31		3
32 to 39		4
40 to 47		5
48 to 55		6
56 to 63		7

When finished, select **APPLY** to save your changes.

CoS to Queue Mapping

In the **Classification** menu, select the **CoS Mapping** tab, and then select the edit icon.

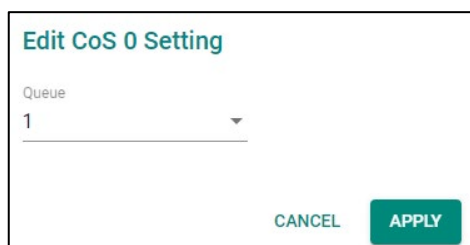


Classification

DSCP Mapping CoS Mapping Port Setting

	CoS	Queue
	0	1
	1	2
	2	3
	3	4

Configure the Queue priority setting for the port.



Edit CoS 0 Setting

Queue
1

CANCEL APPLY

Queue Priority

Setting	Description	Factory Default
0	Different 802.1p values map to one of the eight different queues from 1 (lowest priority) to 8 (highest).	1
1		2
2		3
3		4
4		5
5		6
6		7
7		8

When finished, select **APPLY** to save your changes.

Port Settings

In the **Classification** menu, select the **Port Setting** tab, and then select the edit icon.

Classification

DSCP Mapping

CoS Mapping

Port Settings

	Port	Trust Type	Priority
	G1	CoS	3
	G2	CoS	3
	G3	CoS	3
	G4	CoS	3
	1	CoS	3

Configure the following settings.

Edit Port 1 Settings

Trust Type

CoS

Untag Default Priority

3

Copy Config to Ports



CANCEL

APPLY

Trust Type

Setting	Description	Factory Default
CoS	Enables the port with CoS-based traffic classification.	CoS
DSCP	Enables the port with DSCP-based traffic classification.	

Untag Default Priority

Setting	Description	Factory Default
0 to 7	802.1p tag (CoS) can be ranged from 0 (lowest) to 7 (highest).	3



NOTE

Certain functions such as redundancy mechanisms use the highest traffic class. Therefore, assign another traffic class to application data for the 65M-5011M Series.

Copy Config to Ports

Setting	Description	Factory Default
Select from the drop-down list	Copy the settings to other ports you select.	None

When finished, select **APPLY** to save your changes.

Ingress Rate Limit

Exceed Rate Limit Threshold Port Shutdown

In general, any user shall not consume unlimited bandwidth and influence others' access. One scenario is that a malfunctioning switch or mis-configured network might cause "broadcast storms". ioPAC 6500 Layer 2 Managed Ethernet Switch Module not only prevents broadcast storms but also regulates ingress packet rates, giving administrators full control of their limited bandwidth to prevent undesirable effects caused by unpredictable faults.

Editing Port Shutdown

To edit the port shutdown configurations, select the **Port Shutdown** tab.

Ingress Rate Limit

Rate Limit Port Shutdown

Disabled

Release Interval

60

0 - 10080 min.

APPLY

Configure the following settings.

Enable

Setting	Description	Factory Default
Enable	Enable the port to be shut down.	Disabled
Disable	Disable the ability for the port to be shut down.	

Release Interval (min.)

Setting	Description	Factory Default
0 to 10080	Specify the release interval for the port to shut down. 0 means this port will be shut down until manually enabled.	60

When finished, select **APPLY** to save your changes.

Editing the Port for Port Shutdown

Edit the specific port you want to edit the port shutdown configurations for.

	Port	Port Shutdown	Threshold (Mbps)
	G1	Disabled	1000
	G2	Disabled	1000
	G3	Disabled	1000
	G4	Disabled	1000
	1	Disabled	100

Configure the following settings.

Edit Port 1 Settings

Port Shutdown
Disabled

Threshold *
100
1 - 100 Mbps

Copy Config to Ports

CANCEL APPLY

Enable

Setting	Description	Factory Default
Enable	Enable port shutdown for this port.	Disable
Disable	Disable port shutdown for this port.	

Threshold (Mbps)

Setting	Description	Factory Default
1 to 100 or 1000 for Gigabit ports	Specify the threshold for port shutdown	100 or 1000

Copy Config to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configurations to other port(s).	None

When finished, select **APPLY** to save your changes.

Scheduler

Scheduler Overview

Scheduler is an arbiter in a switch forwarding path to prioritize traffic flows by users' defined criteria. This essentially enhances data transmission efficiency and guarantees that critical packets can be transmitted earlier. Switch modules support two scheduling algorithms: Strict Priority and Weighted Round Robin.

Strict Priority

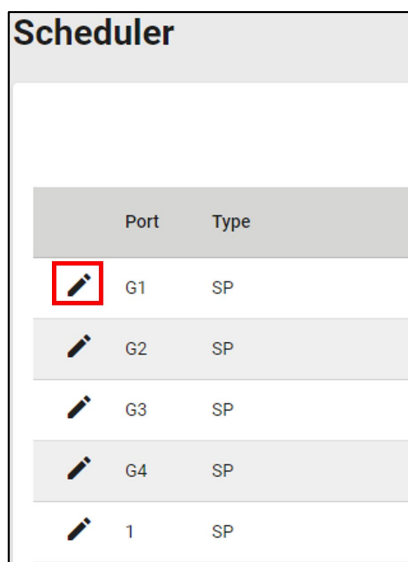
The **Strict Priority** type allows you to determine to transmit packets in the highest priority queue first, while packets with lower priority will be transmitted later. This guarantees that traffic with the highest level of priority for data transmission will go first.

Weighted Round Robin

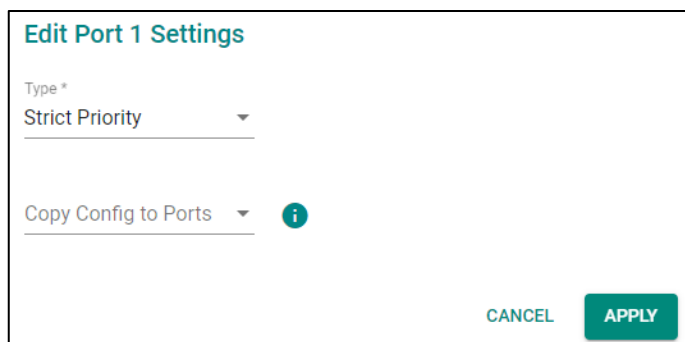
The **Weighted Round Robin** type allows you to give priority to specific packets in the higher weighted queue to ensure those packets will be sent first. Switch modules now have eight queues, and the weights from highest to lowest are 8:8:4:4:2:2:1:1.

Scheduler Settings

Select **Scheduler** in the menu and then select the edit icon on the port you want to configure.



Configure the following settings.



Type

Setting	Description	Factory Default
Strict Priority	Set scheduler algorithm as Strict Priority.	Strict Priority
Weighted Round Robin	Set the scheduler algorithm as Weighted Round Robin: The queued packet will be forwarded by its associated weight.	

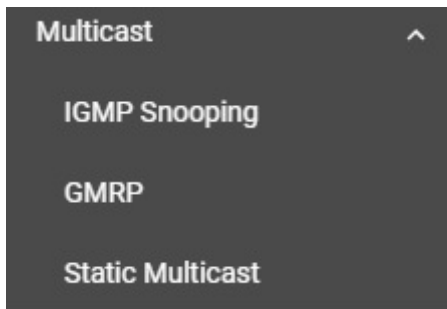
Copy Config to Ports

Setting	Description	Factory Default
Select the port from the drop-down list	Copy the same settings to other ports.	None

When finished, select **APPLY** to save your changes.

Multicast

Multicast filtering improves the performance of networks that carry multicast traffic. This section will explain the Layer 2 multicast settings, such as IGMP Snooping, GMRP, and Static Multicast.



IGMP Snooping

IGMP Snooping Overview

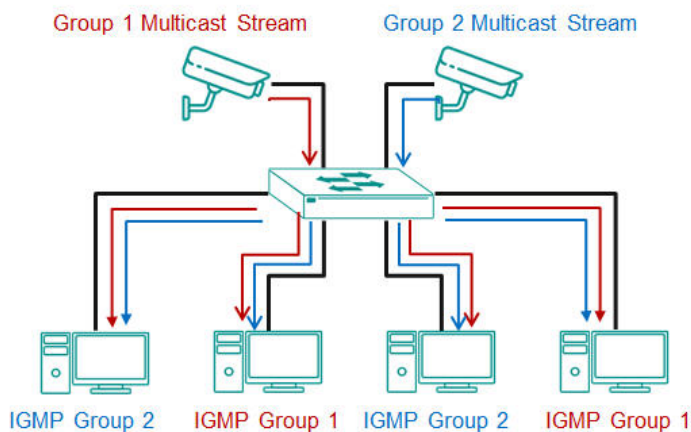
IGMP stands for **I**nternet **G**roup **M**anagement **P**rotocol, which is a network communication protocol that hosts nearby routers on networks to construct multicast group memberships.

IGMP snooping allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations, the switch maintains an association mapping table between port(s) and multicast group.

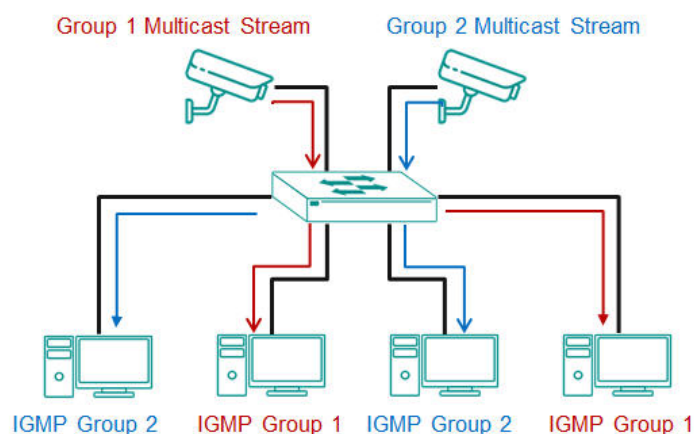
How IGMP Snooping Works

A switch will, by default, flood multicast traffic to all the other ports, aside ingress, in a broadcast domain (or the VLAN equivalent). Multicast can cause unnecessary loading for host devices by requiring them to process packets they have not solicited. IGMP snooping prevents hosts on a local network from receiving traffic for a multicast group they have not joined. It provides switches with a mechanism to forward multicast traffic to specific ports that receive IGMP hosts. Hence, IGMP snooping can use the network bandwidth more efficiently.

Without IGMP Snooping



With IGMP Snooping



Differences Between IGMP Snooping V1, V2, and V3

IGMP protocols regulate the communication mechanism between querier and listener. IGMP Snooping has three different versions. Refer to the following table for the detailed differences.

IGMP Version	Main Features	Reference
V1	The IGMPv1 querier will periodically send out a "query". Listeners can solicit a "report" of their interested group. However, IGMPv1 does not have a "leave group" message, and the querier might need to implement a timeout mechanism for each registered group.	RFC-1112
V2	Compatible with V1 and the following functions: a. Group-specific query b. Leave group messages c. Resends specific queries to verify leave message was the last one in the group d. Querier election if multiple capable queries are present.	RFC-2236
V3	Compatible with V1, V2, and the following functions: Source filtering enables hosts to specify: - the multicast traffic from a specified source - the multicast traffic from any source except a specified source	RFC-3376

IGMP Snooping Settings

First, select **IGMP Snooping** on the menu and then the **General** tab on the configuration page.

IGMP Snooping

General

VLAN Settings

Group Table

Forwarding Table

IGMP Snooping
Disabled

APPLY

Enable

Setting	Description	Factory Default
Enabled	Enable IGMP Snooping on a specific VLAN.	Disabled
Disabled	Disable IGMP Snooping on a specific VLAN.	

Configuring VLAN Setting

Select the **VLAN Setting** tab, and then select the edit icon to configure the VLAN settings.

VLAN	Enable	Version	Query Interval	Config Role	Active Role	Static Router Port
1	Disabled	2	125	Querier	Non-Querier	
2	Disabled	2	125	Querier	Non-Querier	

Edit VLAN 1 Settings

IGMP Snooping
Disabled

Version *
2

Query Interval *
125
20 - 600 sec.

Static Router Port

Config Role *
Querier

CANCEL APPLY

Enable

Setting	Description	Factory Default
Enabled	Enable IGMP Snooping on a switch.	Disabled
Disabled	Disable IGMP Snooping on a switch.	

Version

Setting	Description	Factory Default
1, 2, 3	Specify the IGMP version of the packets that the switch listens to and sends queries for.	2

Query Interval (sec)

Setting	Description	Factory Default
20 to 600	Specify the query interval for the Querier function globally (Querier must be enabled.)	125

Static Router Port

Setting	Description	Factory Default
Check the port from the drop-down list	The router port is the port that connects to the upper-level router (or IGMP querier), or to the upper-level router of downstream multicast streams. All of the received IGMP signaling packets or multicast streams will be forwarded to those static router ports.	None

Config Role

Setting	Description	Factory Default
Querier	The switch will act as the Querier role.	Querier
Non-querier	The switch will not act as the Querier role.	

When finished, select **APPLY** to save your changes.



NOTE

To ensure stable multicast stream transmission during topology changes with redundant protocols, it is recommended to configure a static router port.

Viewing the Group Table

Select the **Group Table** tab, which allows you to view the current Group Table status.

IGMP Snooping

General	VLAN Setting	Group Table	Forwarding Table	
---------	--------------	-------------	------------------	--

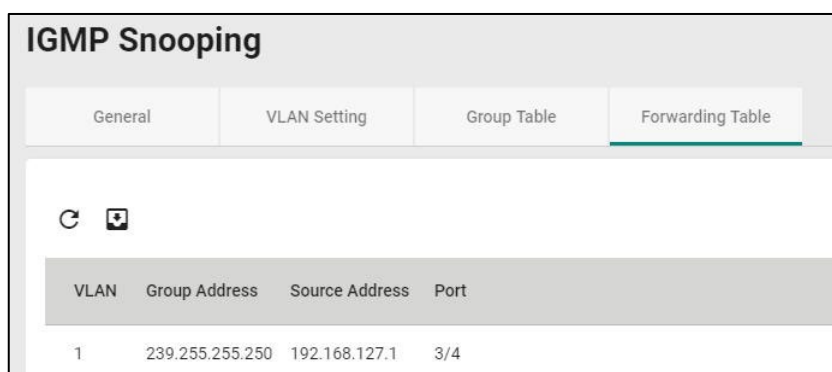
VLAN	Group Address	Filter Mode	Port	Source Address
1	239.255.255.250	Exclude	3/4	0.0.0.0

Refer to the following table for the detailed description for each item.

Item	Description
VLAN	The VLAN ID.
Group Address	The registered multicast group.
Filter Mode	Only applicable to IGMPv3. (v1 and v2 will display "N/A") Include: source-specific multicast address group Exclude: source-specific exclusive multicast address group
Port	The forwarded port.
Source Address	Only applicable to IGMPv3. (v1 and v2 will display N/A)

Viewing the Forwarding Table

Select the **Forwarding Table** tab to view the current forwarding table.



VLAN	Group Address	Source Address	Port
1	239.255.255.250	192.168.127.1	3/4

Refer to the following table for a description of each item.

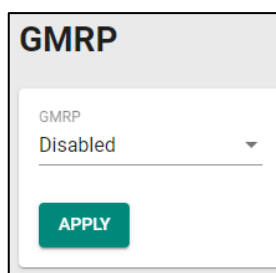
Item	Description
VLAN	The VLAN ID.
Group Address	The associated multicast group address of the streaming data.
Source Address	The source address of the streaming data.
Port	The forwarded port.

GMRP

GMRP stands for GARP Multicast Registration Protocol, which is a Generic Attribute Registration Protocol (GARP) application that can be used to prevent multicast from data flooding. Both GMRP and GARP are defined by the IEEE 802.1P, and widely used as a standard protocol in various industrial-related applications. GMRP allows bridges and the devices at the edge of the network to perform a dynamic group membership information registration with the MAC bridges connected to the same LAN section. The information can be transmitted among all bridges in the Bridge LAN that is implemented with extended filtering features. To operate GMRP, the GARP service must be established first.

Configuring GMRP Setting

To configure the GMRP settings, select **GMRP** on the menu.



Configure the following settings.

Enable

Setting	Description	Factory Default
Enabled	Enable GMRP.	Disabled
Disabled	Disable GMRP.	

When finished, select **APPLY** to save your changes.

Configuring GMRP Settings for Each Port

Next, select the edit icon on the port you want to configure.

	Port	Enable	Group Restrict
	1/3	Disabled	Disabled
	1/4	Disabled	Disabled

Configure the following settings.

Edit Port 2 Settings

GMRP
Disabled

Group Restrict
Disabled

Copy Config to Ports 

CANCEL APPLY

Enable

Setting	Description	Factory Default
Enabled	Enable GMRP for this port.	Disabled
Disabled	Disable GMRP for this port.	

Group Restrict

Setting	Description	Factory Default
Enabled	Enable Group Restrict on the port. This specific port will not process any GMRP control packets.	Disabled
Disabled	Disable Group Restrict on the port. The specific port will receive and process incoming GMRP control packets.	

Copy Config to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Allows you to copy the configurations to other port(s).	None

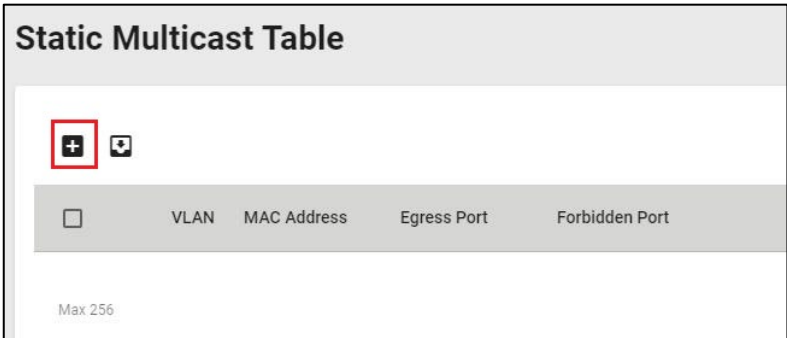
When finished, select **APPLY** to save your changes.

Static Multicast

Select Static Multicast on the menu to view the current multicast table.

Adding Static Multicast Entry

To add more tables, select the + icon.



Configure the following settings.

Add Static Multicast Entry

VLAN ID *

▼

MAC Address *

Port *

▼

Forbidden Port

▼

CANCEL

CREATE

VID (VLAN ID)

Setting	Description	Factory Default
Input the VID	Specify the multicast group's associated VLAN ID.	None

MAC Address

Setting	Description	Factory Default
Input the MAC address	Specify the multicast MAC address.	None

Egress Port

Setting	Description	Factory Default
Input the port from the drop-down list	Set the port(s) as an egress port(s) so that multicast streams can be forwarded to this port.	None

Forbidden Port

Setting	Description	Factory Default
Input the port from the drop-down list	Set the port as forbidden so that packets cannot be forwarded to this port.	None

When finished, select **CREATE**.

Network Redundancy

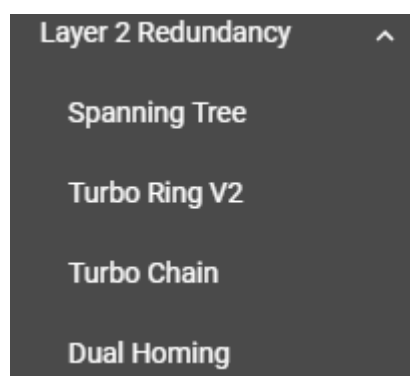
Setting up the Redundancy Protocol on your network helps protect critical links against failure, protects against network loops, and keeps network downtime to a minimum.

The Redundancy Protocol allows you to set up redundant paths on the network to provide a backup data transmission route if a cable or one of the switches is inadvertently disconnected or damaged. This is a particularly important feature for industrial applications, since it can take several minutes to address the link down port or failed switch. For example, if a switch module is used as a key communications device for a production line, several minutes of downtime can cause a big loss in production and revenue. Switch modules support the following Redundancy Protocol functions:

- **Spanning Tree**
- **Turbo Ring V2**
- **Turbo Chain**
- **Dual Homing**

Layer 2 Redundancy

First select **Network Redundancy** on the menu and then select **Layer 2 Redundancy**.



Spanning Tree

Spanning Tree Overview

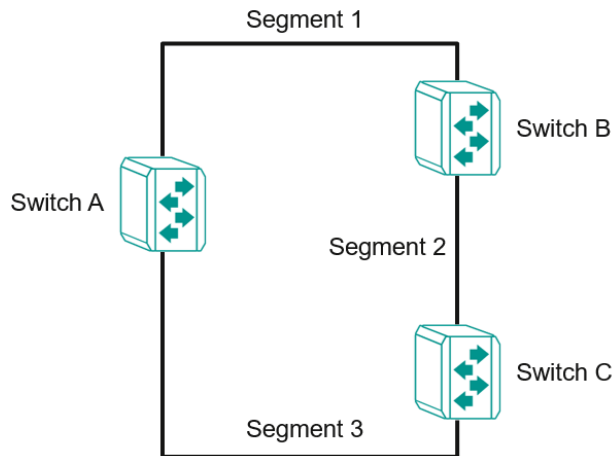
Spanning Tree Protocol (STP) helps construct a loop-free logical topology on an Ethernet network and provides an automatic means of avoiding any network loops. This is particularly important for networks that have a complicated architecture, since unintended loops in the network can cause broadcast storms. Switch modules' STP feature is disabled by default. To be completely effective, enable STP/RSTP on every switch module connected to your network.

STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

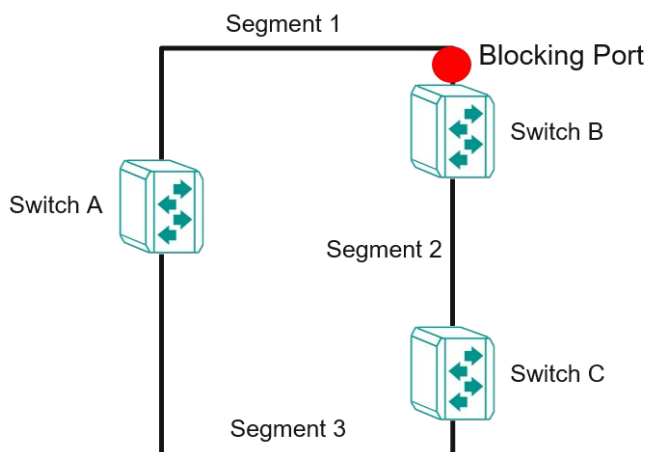
- Locate and then disable less efficient paths (e.g., paths that have lower bandwidth).
- Enable one of the less efficient paths if a more efficient path fails.

How STP Works

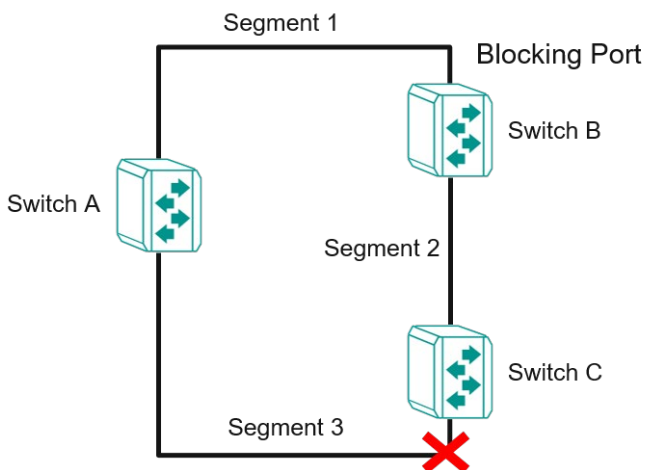
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is not enabled.



If STP is enabled, it will detect duplicate paths or block one of the paths from forwarding traffic. In the following example, STP determined that traffic from segment 2 to segment 1 flows through switches C and A since this path is in a forwarding state and is processing BPDUs. However, switch B on segment 1 is in a blocking state.



What happens if a link failure is detected? As shown in the figure below, the STP will change the blocking state to a forwarding state so that traffic from segment 2 flows through switch B to segment 1 through a redundant path.



STP will determine which path between each segment is most efficient and then assign a specific reference point on the network. When the most efficient path has been identified, the other paths are blocked. In the previous three figures, STP first determined that the path through switch C was the most efficient, and as a result, blocked the path through switch B. After the failure of switch C, STP re-evaluated the situation and opened the path through switch B.

Difference Between STP and RSTP

RSTP is like STP but includes additional information in the BPDUs that allows each bridge to confirm that it has taken action to prevent loops from forming when it decides to enable a link to a neighboring bridge. Adjacent bridges connected via point-to-point links will enable a link without waiting to ensure that all other bridges in the network have had time to react to the change. The main benefit of RSTP is that the configuration decision is made locally rather than network-wide, allowing RSTP to carry out automatic configuration and restore a link faster than STP.

STP and RSTP spanning tree protocols operate without regard to a network's VLAN configuration and maintain one common spanning tree throughout a bridged network. Thus, these protocols map one loop-free, logical topology on a given physical topology.

STP/RSTP Settings and Status

This section describes how to configure **Spanning Tree** settings.

General

Select Spanning Tree on the menu and then the **General** tab.

Configure the following settings.

STP Mode

Setting	Description	Factory Default
Disabled	Disable Spanning Tree.	Disabled
STP/RSTP	Specify STP/RSTP as the STP mode.	
MSTP	Specify MSTP as the STP mode.	

Select **APPLY** to save your changes. When **STP/RSTP** has been selected, configure the following settings.

STP Mode

Setting	Description	Factory Default
STP/RSTP	Use the STP/RSTP mode as the Spanning Tree protocol.	STP/RSTP

Compatibility

Setting	Description	Factory Default
STP	To be compatible with STP mode only	RSTP
RSTP	To be compatible with RSTP and STP modes	

Bridge Priority

Setting	Description	Factory Default
0 to 61440	Increase this device's bridge priority by selecting a lower number. A device with a higher bridge priority has a greater chance of being established as the root of the Spanning Tree topology.	32768

Forwarding Delay Time (sec.)

Setting	Description	Factory Default
4 to 30	The time the device waits before checking to see if it should change to a different state.	15

Hello Time (sec.)

Setting	Description	Factory Default
1 or 2	The root of the Spanning Tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy. The "hello time" is the time the root waits between sending hello messages.	2

Max Age (sec.)

Setting	Description	Factory Default
6 to 40	If this device is not the root, and it has not received a hello message from the root in the time equal to "Max. Age," then this device will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate a new Spanning Tree topology.	20

Error Recovery Time (sec.)

Setting	Description	Factory Default
30 to 65535	If the BPDU guard is triggered on a port, it will automatically recover to the normal state after the Error Recovery Time.	300

When finished, select **APPLY** to save your changes.

If you select **MSTP** as the STP mode, configure the following settings.

Spanning Tree

General

Guard

Status

STP Mode *

Compatibility *

MSTP

MSTP

Forward Delay Time *

Hello Time *

Max. Age *

Error Recovery Time *

15

2

20

300

4 - 30 sec.

1 - 2 sec.

6 - 40 sec.

30 - 65535 sec.

Region Name

Region Revision *

Max. Hops *

MSTP

0

20

4 / 32

0 - 65535

6 - 40

APPLY

STP Mode

Setting	Description	Factory Default
MSTP	Use the MSTP mode as the Spanning Tree protocol.	MSTP

Compatibility

Setting	Description	Factory Default
MSTP	Only compatible with MTP mode.	MSTP
STP	Only compatible with STP mode.	
RSTP	Compatible with RSTP and STP modes.	

Forwarding Delay Time (sec.)

Setting	Description	Factory Default
4 to 30	The amount of time the device waits before checking to see if it should change to a different state.	15

Hello Time (sec.)

Setting	Description	Factory Default
1 or 2	The root of the Spanning Tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy. The "hello time" is the amount of time the root waits between sending hello messages.	2

Max Age (sec.)

Setting	Description	Factory Default
6 to 40	If this device is not the root, and it has not received a hello message from the root in the amount of time equal to "Max. Age," then this device will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate a new Spanning Tree topology.	20

Error Recovery Time (sec.)

Setting	Description	Factory Default
30 to 65535	If the BPDU guard is triggered on a port, it will automatically recover to the normal state after the Error Recovery Time.	300

Region Name

Setting	Description	Factory Default
0 to 32 characters	Provides the region's name.	MSTP

Region Revision

Setting	Description	Factory Default
0 to 65535 (characters)	Provides the regional revision.	0

Max. Hops

Setting	Description	Factory Default
6 to 40	Provides the maximum hops value.	20

When finished, select **APPLY** to save your changes.

Editing Spanning Tree for a Port

To edit the spanning tree settings for a specific port, select the edit icon on the port you want to configure.

	Port	Enable	Edge	Priority	Path Cost	Link Type
	2	Disabled	Auto	128	0	Auto
	3	Disabled	Auto	128	0	Auto
	4	Disabled	Auto	128	0	Auto
	po1	Disabled	Auto	128	0	Auto

Configure the following settings.

Edit Port 2 Settings

Enable

Disabled

Edge

Auto

Priority *

128

0 - 240, multiples of 16

Path Cost *

0

0 - 200000000

Link Type

Auto

Copy Config to Ports

CANCEL

APPLY

Enable

Setting	Description	Factory Default
Enabled	Enables Spanning Tree.	Disabled
Disabled	Disables Spanning Tree.	

Edge

Setting	Description	Factory Default
Auto	Automatically detects to be the edge port.	Auto
Yes	Set as an edge port.	
No	Does not set as an edge port.	

Priority

Setting	Description	Factory Default
0 to 255 (multiples of 16)	Increases the priority of a port by selecting a lower number. A port with a higher priority has a greater chance of being a root port.	128

Path Cost

Setting	Description	Factory Default
0 to 200000000	The path cost value will be automatically assigned according to the different port speed if the value is set to zero.	0

Link Type

Setting	Description	Factory Default
Force True	Set to Force True when port operating in full-duplex mode, such as a switch.	Auto
Force False	Set to Force False when port operating in half-duplex mode, such as a hub.	
Auto	Automatically select Force True or Force False mode.	

Copy Config to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configurations to other port(s).	None

Select **APPLY** to finish.

BPDU Overview

BPDUs (Bridge Protocol Data Units) are the network communication frames used in the STP (Spanning Tree Protocol). When two switches exchange messages, BPDUs are used to calculate the STP topology and determine the network communication route. A BPDU filter is often used to screen sending or receiving BPDUs on a specific port of the switch.

BPDU Guard

BPDU Guard is a protection mechanism that prevents a port from receiving BPDUs. When an RSTP-enabled port receives BPDUs, it will automatically be in the error-disable state, which means the port will in turn switch to Block state. When STP is enabled, all ports are involved in the STP domain, sending and receiving BPDUs. However, when BPDU Guard is enabled, all ports will not receive or send any BPDUs, as all computers and unmanaged switches do not support STP. When BPDU Guard is enabled, all communications will be treated as error-disabled, and the related ports will be blocked, therefore no more data will be sent or received, protecting the network from a loop chain.

Root Guard

Root Guard prevents a designated port role in changing to a root port role on reception of superior information.

Loop Guard

Loop Guard prevents temporary loops in a network caused by **non-designated ports** changing to the spanning-tree **forwarding** state because of a link failure in the topology.

BPDU Filter

BPDU Filter prevents a port from sending and processing BPDUs. A BPDU filter enabled port cannot transmit any BPDUs and drop all received BPDUs.

Configuring BPDU Filter, BPDU/Root/Loop Guard Settings

First select **Spanning Tree** on the menu and then the **Guard** tab. Next, select the edit icon on the port you want to configure.

Spanning Tree					
General		Guard		Status	
Port		BPDU Guard	rootGuard	Loop Guard	BPDU Filter
 2		Disabled	Disabled	Disabled	Disabled
 3		Disabled	Disabled	Disabled	Disabled
 4		Disabled	Disabled	Disabled	Disabled
 po1		Disabled	Disabled	Disabled	Disabled

Configure the following settings.

Edit Port 2 Settings

BPDU Guard

Disabled

Root Guard

Disabled

Loop Guard

Disabled

BPDU Filter

Disabled

Copy Config to Ports

CANCEL

APPLY

BPDU Guard

Setting	Description	Factory Default
Enabled	Enables BPDU Guard.	Disabled
Disabled	Disables BPDU Guard.	



NOTE

To establish a redundant port, e.g., it is highly recommended that you do not enable the BPDU filter.

Root Guard

Setting	Description	Factory Default
Enabled	Enables Root Guard.	Disabled
Disabled	Disables Root Guard.	

Loop Guard

Setting	Description	Factory Default
Enabled	Enables Loop Guard.	Disabled
Disabled	Disables Loop Guard.	

BPDU Filter

Setting	Description	Factory Default
Enabled	Enables BPDU Filter.	Disabled
Disabled	Disables BPDU Filter.	

Copy Config to Port

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copies the same settings as other port(s).	None

When finished, select **APPLY** to save your changes.

Viewing Current Spanning Tree Status

Select the Status tab to view the current Spanning Tree status.

Spanning Tree

GeneralGuardStatus

Root Information

Bridge ID
32768/00:90:e8:90:a6:7c

Root Path Cost
0

Forward Delay Time
15 (sec.)

Hello Time
2 (sec.)

Max. Age
20 (sec.)

Bridge Information

Bridge ID
32768/00:90:E8:90:A6:7C

Running Protocol
RSTP

Forward Delay Time
15 (sec.)

Hello Time
2 (sec.)

Max. Age
20 (sec.)

In addition, the status for each port will also be shown below.

Port	Edge	Port Role	Port State	Root Path Cost	Path Cost	Link Type	BPDU Inconsistency	Root Inconsistency	Loop Inconsistency
2	No	Disabled	Discarding	0	200000	Shared-LAN	No	No	No
3	No	Disabled	Discarding	0	200000	Shared-LAN	No	No	No
4	No	Disabled	Discarding	0	200000	Shared-LAN	No	No	No
po1	No	Disabled	Forwarding	0	199900	Point-to-Point	No	No	No

Refer to the following table for a detailed description of each item.

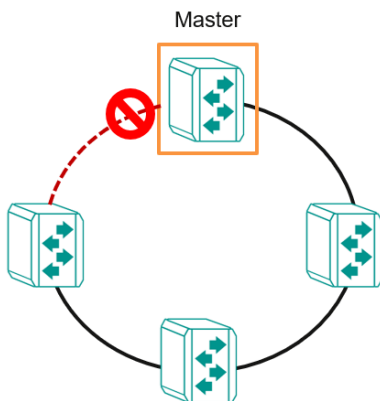
Item	Description
Port	The port number on this device.
Edge	Shows if this port is connected to an edge device.
Port Rule	Root: The port is connected directly or indirectly to the root device. Designated: The port is designated if it can send the best BPDU on the segment to which it is connected. Alternate: The alternate port receives more useful BPDU from another bridge and is a blocked port. Backup: The backup port receives more useful BPDU from the same bridge and is the blocked port. Disabled: The function is disabled.
Port State	Forwarding: The traffic can be forwarded through this port. Blocked: The traffic will be blocked. Disabled: The function is disabled.
Root Path Cost	The total path cost to the root bridge.
Path Cost	The path cost on this link.
Link Type	Edge Port: The port is connected to an edge device. Point-to-Point Non-edge Port: The port is connected to another bridge and is full duplex. Shared Non-edge Port: The port is connected to another bridge and is half duplex.
BPDU Inconsistency	BPDU is received in a port enabled by a BPDU guard.
Root Inconsistency	A port is changed to a root port when enabled by a loop guard.
Loop Inconsistency	A loop is detected on this port by a loop guard.

Turbo Ring v2

Turbo Ring v2 Overview

Moxa Turbo Ring is a proprietary self-healing technology that enables fast fault recovery of under 20 ms for Fast Ethernet, and 50 ms for Gigabit Ethernet. Turbo Ring supports two topology expansions—ring coupling and dual-ring—to reduce redundant network cabling and network planning costs and to ensure high reliability of your industrial network applications.

The Turbo Ring v2 protocols identify one switch as the client of the network, and then automatically block one port beside the client on the ring (red line) to avoid network's redundant loops. If one branch of the ring gets disconnected from the rest of the network, the protocol automatically readjusts the ring so that the part of the network that was disconnected can reestablish contact with the rest of the network.

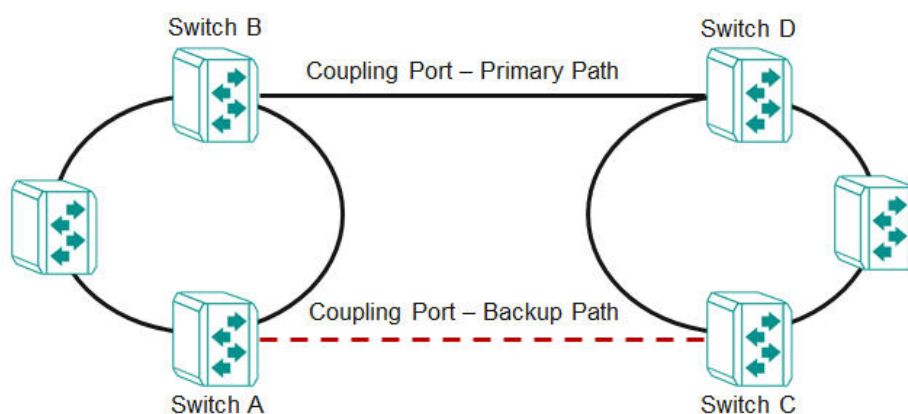


How Turbo Ring v2 Works

Turbo Ring v2 is an advanced technology for network redundancy, which ensures recovery times of less than 20 ms for Fast Ethernet, and 50 ms for Gigabit Ethernet when the network is down. In addition, it allows more switches within the network rings. You can select different network typologies for Turbo Ring redundancy to allow more network reliability and reduce cabling costs. Below are three examples of how Turbo Ring v2 works.

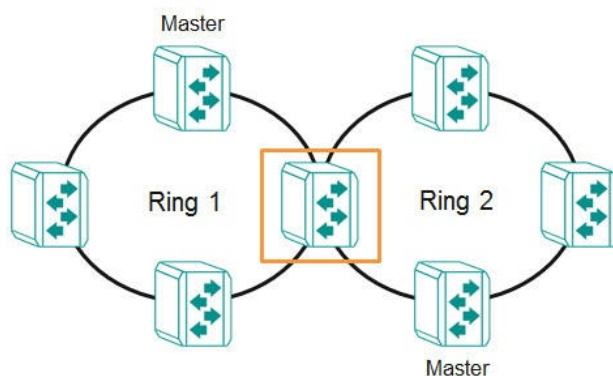
Ring Coupling

Ring Coupling helps you separate distributed devices into different smaller redundant rings, but in such a way that the smaller rings at different remote sites will be able to communicate with each other. This is useful for applications where some devices are at remote sites.



Dual-Ring

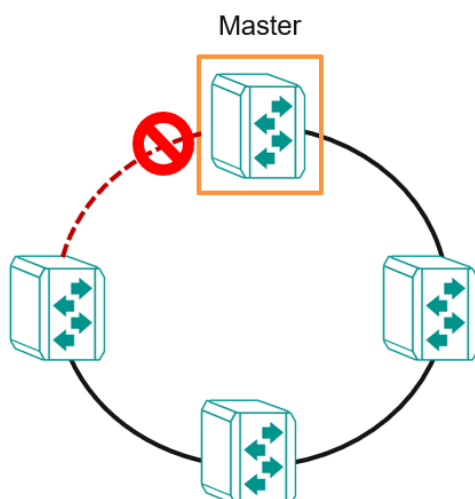
Dual-ring adds reliability by using a single switch module to connect two separate rings for applications that present cabling difficulties. It provides another ring coupling configuration where two adjacent rings can share one switch. This typology is an ideal solution for applications that have inherent cabling difficulties.



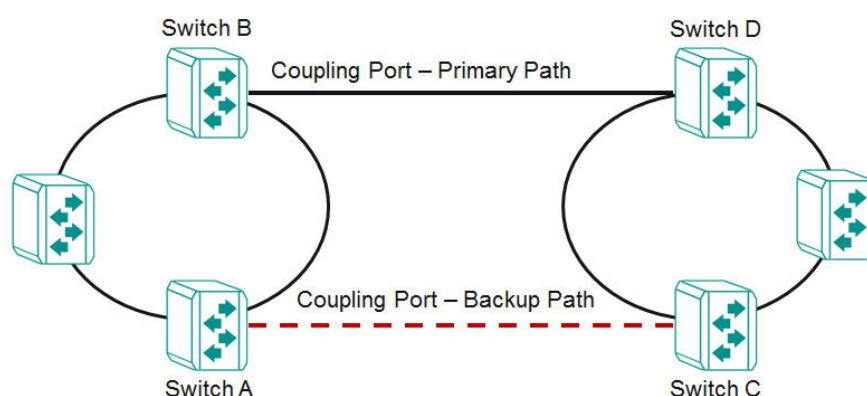
How to Determine the Redundant Path

For Turbo Ring v2, the client is determined by two methods: one is a system MAC address election, the smallest MAC address will play the client role; the other is user manual configuration to enable the client role on the switch.

The redundant path is determined by "Ring Port 2", which means the port set on "Ring Port 2" will become the blocking port.



Ring Coupling for a "Turbo Ring V2" Ring



For Turbo Ring V2, Ring Coupling is enabled by configuring the **Coupling Port (Primary)** on Switch B, and the **Coupling Port (Backup)** on Switch A only.

The **Coupling Port (Backup)** on Switch A is used for the backup path, and connects directly to an extra network port on Switch C. The **Coupling Port (Primary)** on Switch B monitors the status of the main path, and connects directly to an extra network port on Switch D. With ring coupling established, Switch A can activate the backup path as soon as it detects a problem with the main path.



ATTENTION

Ring Coupling needs to be enabled on one coupling primary switch and one coupling backup switch as the Ring Coupler. The Coupler must designate different ports, such as the two Turbo Ring ports and the coupling port.



NOTE

1. You do not need to use the same switch for both Ring Coupling and Ring Master.
2. To achieve optimal redundancy performance, it is recommended to use 1G fiber for Turbo Ring.

Turbo Ring V2 Settings and Status



NOTE

If you connect the EDR-G9010 Series in your topology, ensure it is not set as the client.

Select **Turbo Ring V2** on the menu, and then select the **Setting** tab.

Configure the following setting.

Enable

Setting	Description	Factory Default
Enabled	Enable Turbo Ring V2.	Disabled
Disabled	Disable Turbo Ring V2.	

When finished, select **APPLY** to save your changes.

Ring Settings

In **Ring Setting**, select the edit icon.

Ring ID	Enabled	Master	Ring Port 1	Ring Port 2
 Ring 1	Disabled	Disabled	G1	G2
 Ring 2	Disabled	Disabled	G3	G4

Configure the following settings. When finished, select **Apply** to save your changes.

Ring 1 Settings

Enabled

Disabled

Master

Disabled

Ring Port 1

G1

Ring Port 2

G2

CANCEL

APPLY

Enable

Setting	Description	Factory Default
Enabled	Enables Ring Setting.	Disabled
Disabled	Disables Ring Setting.	

Master

Setting	Description	Factory Default
Enabled	Enables this Ring as the client.	Disabled
Disabled	Disables this Ring as the client.	

Ring Port 1

Setting	Description	Factory Default
Select the port from the list	Specifies this port as the first redundant port.	1/1

Ring Port 2

Setting	Description	Factory Default
Select the port from the list	Specifies this port as the second redundant port.	1/2

Ring Coupling Overview

Ring Coupling helps you separate distributed devices into different smaller redundant rings, but in such a way that the smaller rings at different remote sites will be able to communicate with each other. This is useful for applications where some devices are at remote sites.

Ring Coupling Settings and Status

In the **Ring Coupling Setting**, select the edit icon.

Ring Coupling Settings

Coupling Mode

Enabled

Coupling Port

Primary Path

Disabled

2

Configure the following settings.

Ring Coupling Settings

Enabled

Disabled

Coupling Mode

Coupling Primary Path

Coupling Port

2

CANCEL

APPLY

Enable

Setting	Description	Factory Default
Enabled	Enables Ring Coupling.	Disabled
Disabled	Disables Ring Coupling.	

Coupling Mode

Setting	Description	Factory Default
Coupling Backup Path	Selects Coupling Mode to assign the coupling port as the backup path.	Coupling Primary Path
Coupling Primary Path	Selects Coupling Mode to assign the coupling port as the primary path.	

Coupling Port

Setting	Description	Factory Default
Select the port from the list	Selects the port as the coupling port.	2/1

When finished, select **APPLY** to save your changes.

Ring Settings and Ring Coupling Setting Status

Select **Status** in the Turbo Ring V2 menu to view the current Ring settings and the Ring Coupling Status.

Turbo Ring V2

Settings

Status

Ring Status

Ring ID	Master ID	Status	Master	Ring Port 1	Ring Port 2
Ring 1	00:00:00:00:00:00	Disabled	Slave	Blocking	Blocking
Ring 2	00:00:00:00:00:00	Disabled	Slave	Blocking	Blocking

Ring Coupling Status

Coupling Mode	Coupling Port
Disabled	Blocking

Refer to the following table for a detailed description of each item of the Ring status.

Item	Description
Ring ID	The ID number of the Ring.
Master ID	The MAC address of the Ring client.
Status	Healthy: The Ring and the ports are working properly. Break: One or more rings has been broken.
Master	The device is a client/server on this ring.
Ring Port 1	The port of the first ring port.
Ring Port 2	The port of the second ring port.

Refer to the following table for a detailed description of the status of Coupling Mode and Coupling Port.

Item	Description
Coupling Mode	Primary: The main path of Ring Coupling. Backup: The backup path of Ring Coupling.
Coupling Port	The port of the Ring Coupling.

Turbo Chain

Turbo Chain Overview

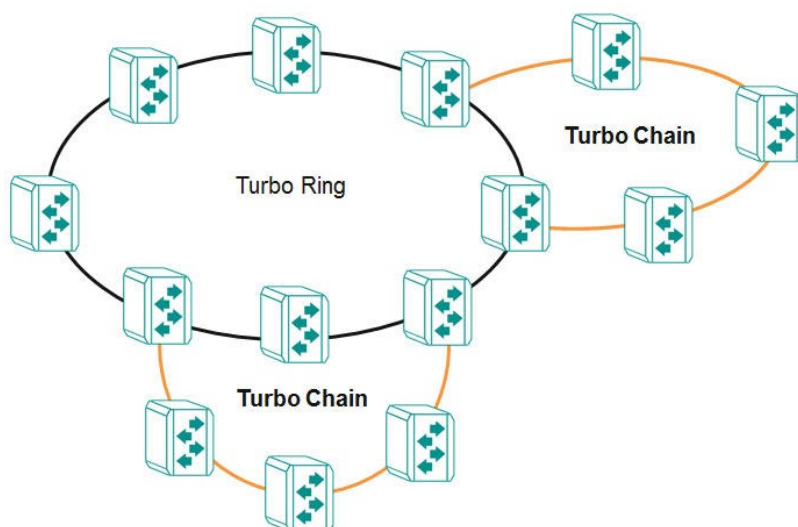
Moxa's Turbo Chain is an advanced software technology that gives network administrators the flexibility of constructing any type of redundant network topology. In addition, it offers system recovery time under 20 ms for Fast Ethernet, and 50 ms for Gigabit Ethernet for member port link environments. When using the "chain" concept, you first connect the Ethernet switches in a chain and then simply link the two ends of the chain to an Ethernet network.

Turbo Chain can be used on industrial networks that have a complex topology. If the industrial network uses multi-ring architecture, Turbo Chain can be used to create flexible and scalable topologies with a fast media-recovery time.

How Turbo Chain Works

Moxa's Turbo Chain outperforms traditional ring topologies by providing great flexibility, unrestricted expansion, and cost-effective configurations when connecting separate redundant rings together—in a simplified manner. With Turbo Chain, you can create any complex redundant network that corresponds to your needs, while still ensuring great reliability and availability for your industrial Ethernet network applications.

With Moxa's Turbo Chain, network engineers have the flexibility to construct any type of redundant topology with minimum effort by simply linking Turbo Chain to the Ethernet Network. Turbo Chain allows for unrestricted network expansion. Network engineers no longer need to go through the hassle of reconfiguring the existing network and can simply use Turbo Chain to scale up their redundant networks.

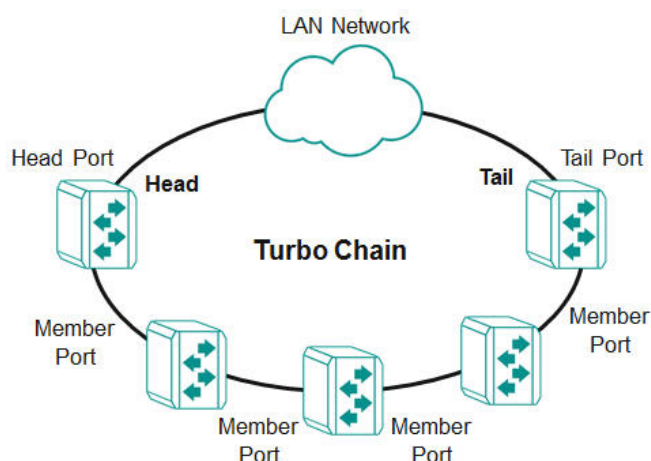


How to Determine the Redundant Path

Here is an example of how to set up Turbo Chain and determine the redundant path.

1. Select the head switch, tail switch, and member switches.
2. Configure one port as the head port and one port as the member port in the head switch, configure one port as the tail port and one port as the member port in the tail switch, and configure two ports as Member ports in each of the member switches.
3. Connect the head switch, tail switch, and member switches, as shown in the diagram below.

The path connecting to the head port is the main path, and the path connecting to the tail port is the backup path of Turbo Chain. Under normal conditions, packets are transmitted through the head port to the LAN network. If any Turbo Chain path is disconnected, the Tail Port will be activated so that packet transmission can continue.



There are two points to note:

1. Two chain ports must have the same PVID.
2. Chain ports must join the untagged members of PVID VLAN before being assigned to be a chain port.

Turbo Chain V2 Settings and Status

First select **Turbo Chain** on the menu and then **Setting**.

Turbo Chain

Settings

Status

Turbo Chain

Disabled

Chain Role

Member

Member Port 1

G1

Member Port 2

G2

APPLY

Configure the following settings.

Enable

Setting	Description	Factory Default
Enabled	Enables Turbo Chain.	Disabled
Disabled	Disables Turbo Chain.	

Chain Role

Setting	Description	Factory Default
Head	Enables chain role as the head.	Member
Member	Enables chain role as a member.	
Tail	Enables chain role as the tail.	

Head/Member/Tail Port

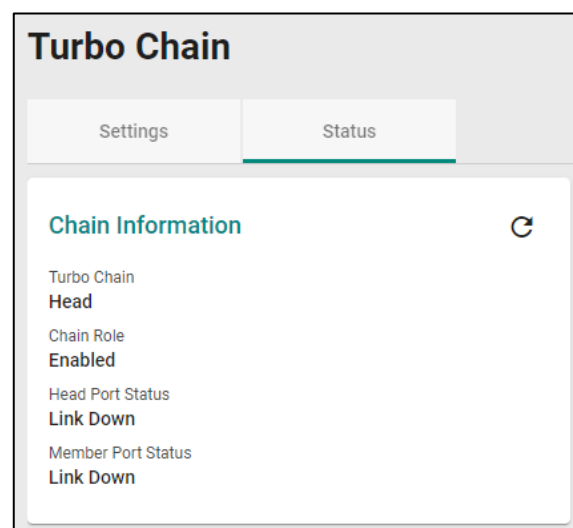
Setting	Description	Factory Default
Select the port from the list	Specifies the port as the head/member/tail port.	1/1

Member Port

Setting	Description	Factory Default
Select the port from the list	Specifies the port as the member port.	1/2

When finished, select **APPLY** to save your changes.

Select **Turbo Chain** on the menu and then **Status** to view the current Turbo Chain status.



Refer to the following table for a detailed description of each item.

Item	Description
Turbo Chain	Head: The device is the head of this chain. Member: The device is a member of this chain. Tail: The device is the tail of this chain.
Chain Role	Healthy: The Chain and the ports are working properly. Break: The chain or the ports are broken.
Head/Member/Tail 1 Port Status	The status of the first Head/Member/Tail port.
Head/Member/Tail 2 Port Status	The status of the second Head/Member/Tail port.

Dual Homing

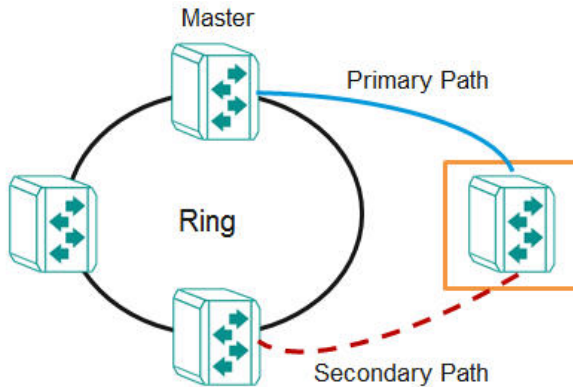
Dual Homing Overview

Dual Homing is a layer 2 function, which uses a single Ethernet switch to connect two network topologies, both of which can run any redundancy protocols. It involves coupling two separate devices or even coupling to two separate rings with a single switch connecting to two independent connection points. The secondary path will be activated if the primary path fails.

How Dual Homing Works

Dual Homing is a redundant path technology that allows a single switch to connect to any topology.

The primary and secondary paths require manual configuration: Select a primary port as the primary path and the secondary port as the secondary path. The default path switching mode is "primary path always first", which means when failover occurs, the primary path will switch to the secondary path, but if the primary path recovers, the path will switch back to the primary path again even if the secondary path is healthy.



Path Switching Mode

There are two path switch modes that you can configure:

Primary path always first: Always select the path switching mode as the primary path first. When path switching occurs, the primary path will always be the first path for data communication.

Maintain current path: Select the path switching mode to maintain the current path. When path switching occurs, maintain the current path to keep the network stable and do not change paths for data communication.

Dual Homing Settings and Status

Select **Dual Homing** in the menu and then **Setting**.

Dual Homing

Settings

Status

Dual Homing

Disabled

Primary Port

G1

Secondary Port

G2

i

Path Switching Mode

Primary path always ...

APPLY

Configure the following settings.

Enable

Setting	Description	Factory Default
Enabled	Enables Dual Homing.	Disabled
Disabled	Disables Dual Homing.	

Primary Port

Setting	Description	Factory Default
Select the port from the list	Specifies the port as the primary port.	1/1

Secondary Port

Setting	Description	Factory Default
Select the port from the list	Specifies the port as the secondary port.	1/1

Path Switching Mode

Setting	Description	Factory Default
Primary path always first	Always select path switching mode as the primary path first.	Primary path always first
Maintain current path	Always select the path switching mode to maintain the current path.	

When finished, select **APPLY** to save your changes.

First, select **Dual Homing** in the menu and then **Status** to view the current Dual Homing Settings.

Dual Homing

Settings

Status



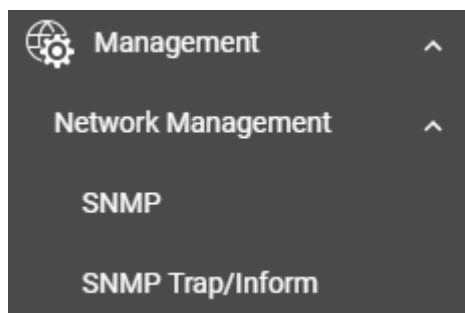
Path	Port	Link Status	Port State
Primary	G1	Link Down	Link Down
Secondary	G2	Link Down	Link Down

Refer to the following table for a detailed description of each item.

Item	Description
Path	Primary: The primary path of dual homing. Secondary: The secondary path of dual homing.
Port	The port that is used as the primary/secondary path.
Link Status	Link Up: The port is connected. Link Down: The port is disconnected.
Port State	Forwarding: The port is forwarding traffic. Blocking: The port is blocking traffic.

Management

This section describes how to configure **Network Management** including SNMP and **SNMP Trap/Inform**.



Network Management

This section demonstrates how to configure **SNMP** and **SNMP Trap/Inform** settings.

SNMP

The ioPAC 6500 Layer 2 Managed Ethernet Switch Module support SNMP V1, V2c, and V3. SNMP V1 and SNMP V2c use a community string match for authentication, so SNMP servers access all objects with read-only or read/write permission using the community strings public and private by default. SNMP V3 requires that you select an authentication level of MD5 or SHA. You can also enable data encryption to enhance data security.

Supported SNMP security modes and levels are shown in the table below. Select the security mode and level that will communicate between the SNMP agent and manager.

Protocol Version	UI Setting	Authentication	Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Uses a community string match for authentication.
	V1, V2c Write/Read Community	Community string	No	Uses a community string match for authentication.
SNMP V3	None	No	No	Uses an account with admin or user to access objects.
	MD5 or SHA	Authentication based on MD5 or SHA	Disabled	Uses authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key: DES, AES	Uses authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication .and encryption.

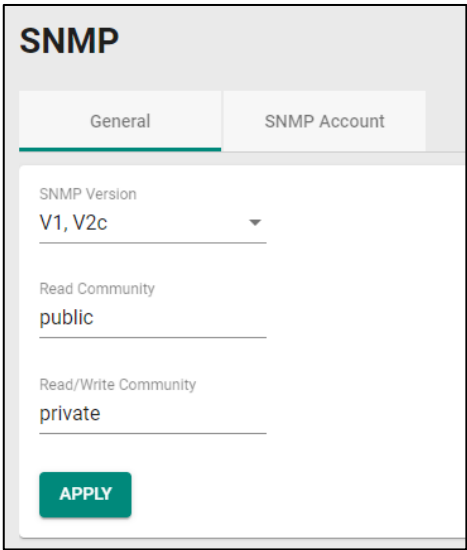


NOTE

SNMPv3 enhances security, as it includes authentication and data privacy. If you require a higher level of security, it is recommended to install additional security mechanisms, such as a firewall, to protect critical infrastructure.

General Settings

First select **SNMP** on the menu and then **General**.

The image shows the 'SNMP' configuration page with the 'General' tab selected. It contains three input fields: 'SNMP Version' with a dropdown menu showing 'V1, V2c', 'Read Community' with the text 'public', and 'Read/Write Community' with the text 'private'. An 'APPLY' button is at the bottom left.

Configure the following settings.

SNMP Version

Setting	Description	Factory Default
V1, V2c, V3	Specify V1, V2c, and V3 as the SNMP version.	V1, V2c
V1, V2c	Specify V1 and V2c as the SNMP version.	
V3 only	Specify V3 as the SNMP version.	

Read Community

Setting	Description	Factory Default
Max. 30 characters	Specifies the community string to authenticate the SNMP agent for read-only access. The SNMP agent will access all objects with read-only permissions using this community string.	Public

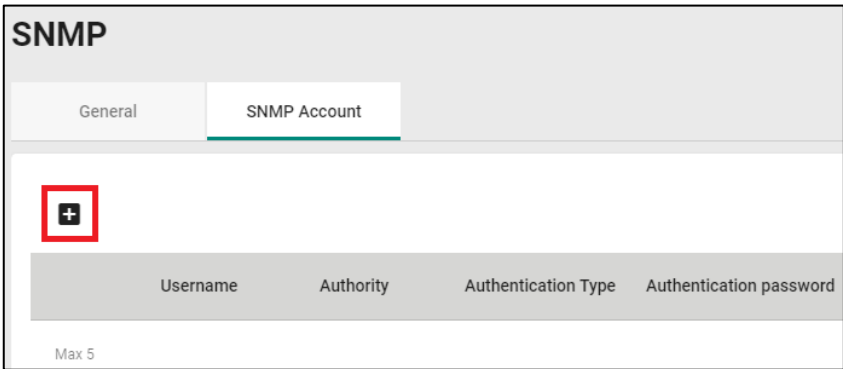
Read/Write Community

Setting	Description	Factory Default
Max. 30 characters	Specifies the community string to authenticate the SNMP agent for read/write access. The SNMP server will access all objects with read/write permissions using this community string.	Private

When finished, select **Apply** to save your changes.

Creating an SNMP Account

Select **SNMP** on the menu and then **SNMP Account**. Next, select the **+** icon on the page.

The image shows the 'SNMP Account' configuration page. At the top, there's a '+ ' icon in a red square. Below it is a table with four columns: 'Username', 'Authority', 'Authentication Type', and 'Authentication password'. At the bottom left, it says 'Max 5'.

Configure the following settings.

Create SNMP Account Settings

Username *

At least 4 characters0 / 32

Authority

Read/Write

Authentication Type

None

Encryption Method

Disabled

CANCEL

CREATE

Username

Setting	Description	Factory Default
At least 4 characters, (max. 32 characters)	Input a username.	None

Authority

Setting	Description	Factory Default
Read Write	The user has read/write access.	None
Read Only	The user only has read access.	

Authentication type

Setting	Description	Factory Default
None	No authentication will be used.	None
MD5	MD5 is the authentication type.	
SHA	SHA is the authentication type.	

Authentication password

Setting	Description	Factory Default
8 to 64 characters	Input the authentication password.	None

Encryption Method

Setting	Description	Factory Default
Disabled	Disables the encryption method.	None
DES	DES is the encryption method.	
AES	AES is the encryption method.	

Encryption Key

Setting	Description	Factory Default
8 to 30 characters	Enables data encryption.	None

When finished, select **CREATE**.

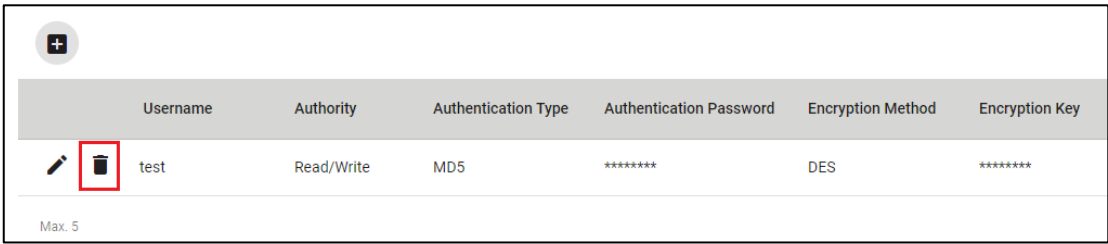


NOTE

SNMPv3 enhances security management by using authentication and ensuring data privacy. If you intend to pursue a higher level of security, it is recommended to install additional security mechanisms, such as a firewall, to protect critical infrastructure.

Deleting an Existing SNMP Account

To delete an existing SNMP account, select the delete icon on the account.

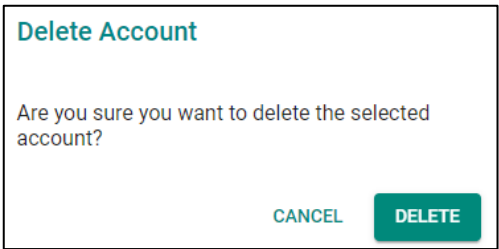


A table showing a list of SNMP accounts. The first row is a header with columns: Username, Authority, Authentication Type, Authentication Password, Encryption Method, and Encryption Key. The second row contains the values: test, Read/Write, MD5, *****, DES, and *****. To the left of the 'test' username is a delete icon (a trash can) which is highlighted with a red square. Above the table is a plus icon in a circle. Below the table, it says 'Max. 5'.

Username	Authority	Authentication Type	Authentication Password	Encryption Method	Encryption Key
test	Read/Write	MD5	*****	DES	*****

Max. 5

Select **DELETE** to delete the SNMP account.



A dialog box titled 'Delete Account'. It contains the text 'Are you sure you want to delete the selected account?'. At the bottom right, there are two buttons: 'CANCEL' and 'DELETE'.

Delete Account

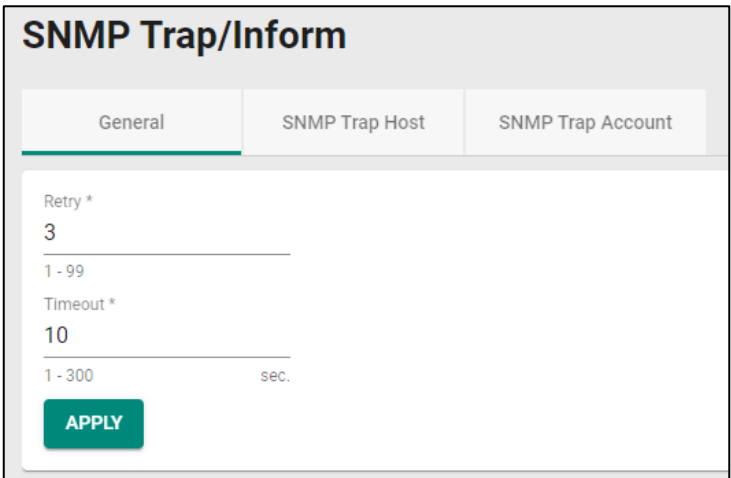
Are you sure you want to delete the selected account?

CANCEL DELETE

SNMP Trap/Inform

General Settings

First select **SNMP Trap/Inform** on the menu and then **General**.



A form titled 'SNMP Trap/Inform'. It has three tabs: 'General', 'SNMP Trap Host', and 'SNMP Trap Account'. The 'General' tab is selected. It contains two input fields: 'Retry *' with the value '3' and a range '1 - 99', and 'Timeout *' with the value '10' and a range '1 - 300 sec.'. There is an 'APPLY' button at the bottom.

SNMP Trap/Inform

General SNMP Trap Host SNMP Trap Account

Retry *
3
1 - 99

Timeout *
10
1 - 300 sec.

APPLY

Configure the following settings.

Retry

Setting	Description	Factory Default
1 to 99	Input the retry value.	3

Timeout

Setting	Description	Factory Default
1 to 300	Input the timeout value.	10

When finished, select **APPLY** to save your changes.

SNMP Trap Host Settings

SNMP Trap allows an SNMP agent to notify the NMS of a significant event. The switch supports two SNMP modes: **Trap** mode and **Inform** mode. Select **SNMP Trap/Inform** on the menu and then **SNMP Trap Host**. Then select the **+** icon on the page.

SNMP Trap/Inform

General

SNMP Trap Host

SNMP Trap Account

Host IP/Name

Mode

Trap Community

Max 2

Configure the following settings.

Create Host Settings

Host IP/Name *

0 / 32

Mode *

Trap Community *

At least 4 characters0 / 32

CANCEL

CREATE

Host IP/Name

Setting	Description	Factory Default
Input a host IP or name, (max. 32 characters)	Specify the name of the primary trap server used by your network.	None

Mode

Setting	Description	Factory Default
Trap V1	Set the trap version to Trap V1.	None
Trap V2c	Set the trap version to Trap v2c.	
Inform V2c	Set the inform version to Inform V2c.	
Trap V3	Set the trap version to Trap V3.	
Inform V3	Set the inform version to Inform V3.	

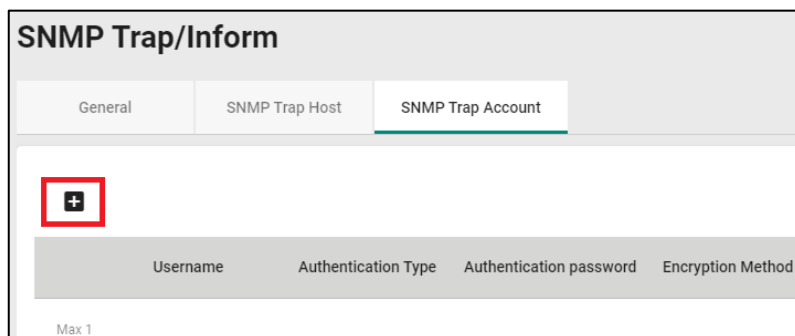
Trap Community

Setting	Description	Factory Default
At least 4 characters, (max. 30 characters)	Specify the community string that will be used for authentication.	None

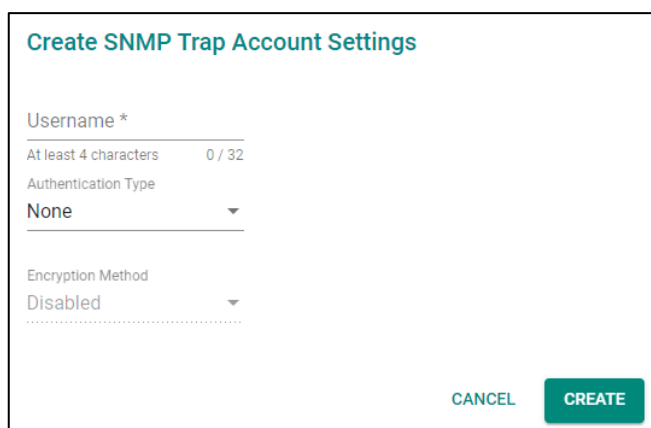
When finished, select **CREATE**.

SNMP Trap Account Settings

Select **SNMP Trap/Inform** on the menu and then **SNMP Trap Account**. Next, select the + icon on the page.



Configure the following settings:



Username

Setting	Description	Factory Default
At least 4 characters, (max. 30 characters)	Input a username.	None

Authentication type

Setting	Description	Factory Default
None	No authentication type will be used.	None
MD5	MD5 is the authentication type.	
SHA	SHA is the authentication type.	

Authentication Password

Setting	Description	Factory Default
8 to 64 characters	Input the authentication password.	None

Encryption Method

Setting	Description	Factory Default
Disabled	Disable the encryption method.	None
DES	DES is the encryption method.	
AES	AES is the encryption method.	

Encryption Key

Setting	Description	Factory Default
8 to 64 characters	Enable data encryption.	None

When finished, select **CREATE**.

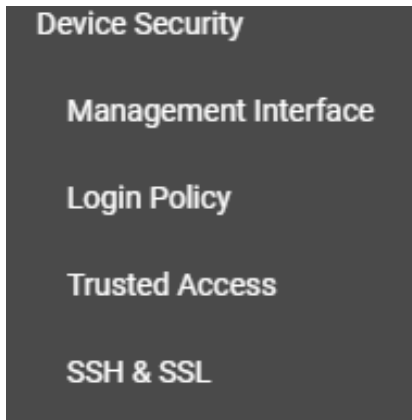
Security

This section describes how to configure **Device Security**, **Network Security**, and **Authentication**.



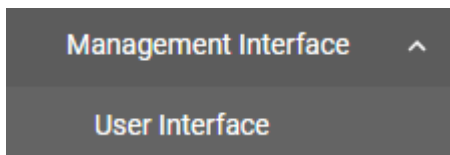
Device Security

This section includes information about the **Management Interface**, **Login Policy**, **Trusted Access**, and **SSH and SSL** configurations.



Management Interface

Select **Management Interface** to configure the settings for **User Interface**.



User Interface

User Interface

HTTP

Enabled

▼

HTTP - TCP Port *

80

1 - 65535

HTTPS

Enabled

▼

HTTPS - TCP Port *

443

1 - 65535

Telnet

Enabled

▼

Telnet - TCP Port *

23

1 - 65535

SSH

Enabled

▼

SSH - TCP Port *

22

1 - 65535

SNMP

Disabled

▼

SNMP - UDP Port *

161

1 - 65535

Moxa Service

Enabled

▼

Moxa Service(Encrypted) - TCP Port

443

1 - 65535

Moxa Service(Encrypted) - UDP Port

40404

1 - 65535

Maximum number of Login Sessions For HTTP+HTTPS *

5

1 - 10

Maximum number of Login Sessions For Telnet+SSH *

1

1 - 5

APPLY

Configure the following settings.

HTTP

Setting	Description	Factory Default
Enabled	Enable the HTTP connection.	Enabled
Disabled	Disable the HTTP connection.	



NOTE

An HTTP session will be redirected to HTTPS if both HTTP and HTTPS are enabled.

HTTP – TCP Port

Setting	Description	Factory Default
0 to 47808	Specify the HTTP connection port number.	80

HTTPS

Setting	Description	Factory Default
Enabled	Enable the HTTPS connection.	Enabled
Disabled	Disable the HTTPS connection.	

HTTPS – TCP Port

Setting	Description	Factory Default
1 to 65535	Specify the HTTP connection port number.	443

Telnet

Setting	Description	Factory Default
Enabled	Enable a Telnet connection.	Disabled
Disabled	Disable a Telnet connection.	

Telnet – TCP Port

Setting	Description	Factory Default
1 to 65535	Specify the Telnet connection port number.	23

SSH

Setting	Description	Factory Default
Enabled	Enable the SSH connection.	Enabled
Disabled	Disable the SSH connection.	

SSH – TCP Port

Setting	Description	Factory Default
1 to 65535	Input the SSH connection port number.	22

SNMP

Setting	Description	Factory Default
Enabled	Enable the SNMP connection.	Disabled
Disabled	Disable the SNMP connection.	

SNMP – Port

Setting	Description	Factory Default
0 to 47808	Input the SNMP connection port number.	161

Moxa Service

Setting	Description	Factory Default
Enabled	Enable Moxa Service.	Enabled
Disabled	Disable Moxa Service.	

When you enable a non-secure protocol, such as Telnet, a warning screen will appear. Select **CONFIRM** to make sure you want to enable the protocol.

Enable Telnet Interface

Are you sure you want to enable non-secure interface Telnet ?

CANCEL CONFIRM



NOTE

Moxa Service is only for Moxa network management software suite.

Moxa Service (Encrypted)—TCP Port

Setting	Description	Factory Default
443 (read only)	Enable a Moxa Service TCP port.	443

Moxa Service (Encrypted)—UDP Port

Setting	Description	Factory Default
40404 (read only)	Enable a Moxa Service UDP port.	40404

Maximum number of Login Sessions for HTTP+HTTPS

Setting	Description	Factory Default
1 to 10	Specify the maximum amount of HTTP and HTTPS login sessions that can happen simultaneously.	5

Maximum number of Login Sessions for Telnet+SSH

Setting	Description	Factory Default
1 to 5	Specify the maximum amount of Telnet and SSH login sessions that can happen simultaneously.	1

When finished, select **APPLY** to save your changes.

Login Policy

Select **Login Policy** on the menu.

Login Policy

Login Message

0 / 500

Login Authentication Failure Message

0 / 500

Account Login Failure Lockout

Disabled

Retry Failure Threshold *

5

1 - 10 times

Lockout Time *

5

1 - 10 min.

Auto Logout Setting *

0

0 - 1440 min.

APPLY

Configure the following settings.

Login Message

Setting	Description	Factory Default
0 to 500 characters	Input the message that will be displayed to users when they log in.	None

Login Authentication Failure Message

Setting	Description	Factory Default
0 to 500 characters	Input the message that will be displayed when users cannot log in.	None

Account Login Failure Lockout

Setting	Description	Factory Default
Enabled	Enables the lockout function when a user cannot log in. Note that this will work on web, command-line interface, and SNMP V3 protocols.	Disabled
Disabled	Disables the lockout function when a user cannot log in.	

Retry Failure Threshold (times)

Setting	Description	Factory Default
1 to 10	Input the maximum number of retry failure times.	5

Lockout Time (min.)

Setting	Description	Factory Default
1 to 60	Specifies the time (in minutes) that a user cannot log in after the retry failure threshold is achieved.	5

Auto Logout Setting (min.)

Setting	Description	Factory Default
0 to 1440	Specify how long a user must be inactive before getting logged out.	5

When finished, select **APPLY** to save your changes.

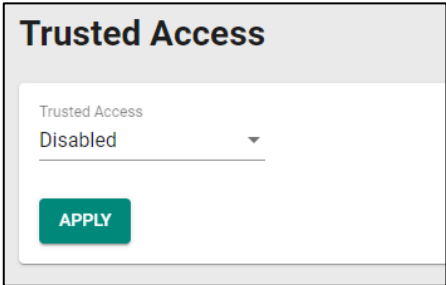
Trusted Access

Trusted Access Overview

Trusted Access is a mechanism that provides a secure connection to the switch module. Use this method to allow the connection from the assigned IP address to ensure safe data transmission.

Trusted Access Settings and Status

Select **Trusted Access** on the menu.



Configure the following settings.

Enable

Setting	Description	Factory Default
Enabled	Enables Trusted Access.	Disabled
Disabled	Disables Trusted Access.	

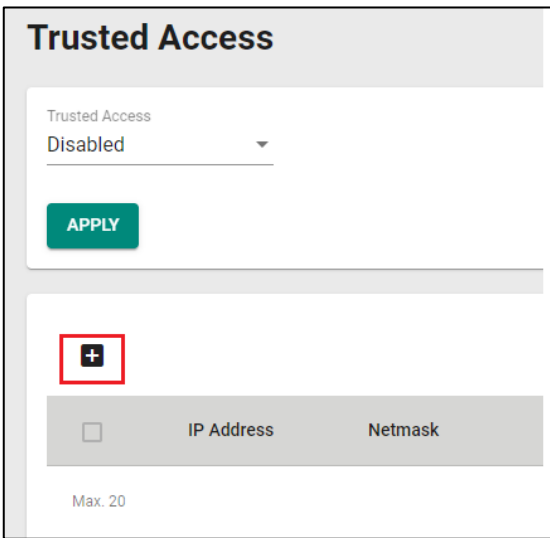


NOTE

1. Trusted Access must be added before it can be enabled.
2. To avoid being disconnected after you enable Trusted Access, you must first add the current IP subnet to Trusted Access. To use this function, you should use an RS-232 console to log in or set the device to factory default.

When finished, select **APPLY** to save your changes.

Next, select the **+** icon.



Configure the following settings.

Create Entry

IP Address *

Netmask *

CANCEL

CREATE

IP Address

Setting	Description	Factory Default
Input IP address	Specifies the IP address that is allowed to connect to switch module.	None

Netmask

Setting	Description	Factory Default
Input Netmask	Specifies the Netmask that is allowed to connect to switch module.	None

When finished, select **CREATE**.

View the Trusted Access status in the figure below.

☐	IP Address	Netmask
☐	192.168.127.1	255.255.255.0
Max 32		

To delete the trusted access source, select the item and then delete the icon on the top of the page.

☐

☒

☒	IP Address	Netmask
☒	192.168.127.1	255.255.255.0
Max. 20		

Select **DELETE** to delete the item.

Delete Entry

Are you sure you want to delete the selected entry?

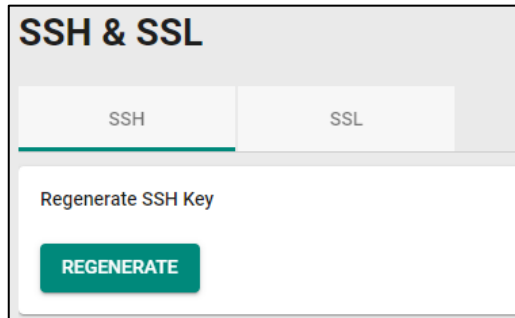
CANCEL

DELETE

SSH & SSL

SSH Key Regeneration

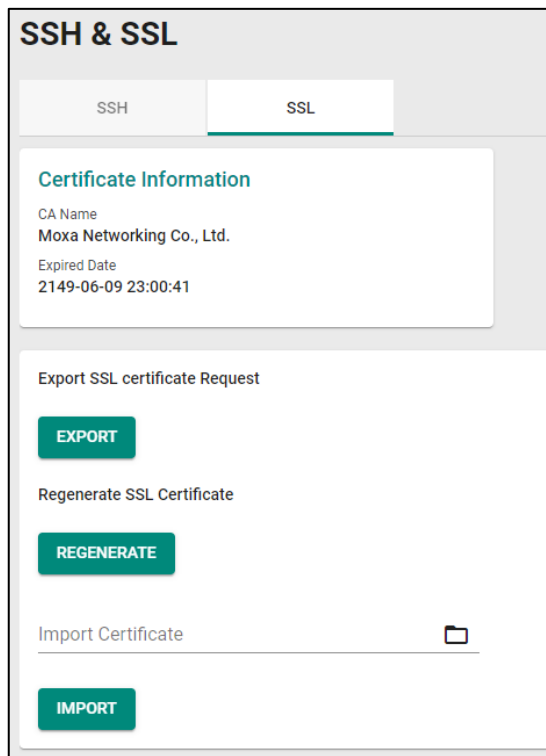
Select **SSH & SSL** on the menu and then the **SSH** tab.



Select **REGENERATE** to regenerate the key.

SSL Certification Regeneration

Select **SSH & SSL** on the menu and the **SSL** tab. The Certificate Information is shown on this screen.



We recommend using a certificate that is signed by the certification authority to enhance security. Configure the following settings and use the steps below to import the certificate.

1. Export the CSR file from the switch and provide it to the certification authority to generate the certificate.
2. Import the certificate signed by the certification authority to the switch.

Export SSL Certificate Request

Setting	Description	Factory Default
Export	Export the SSL certificate to your local computer.	None

Regenerate SSL Certificate

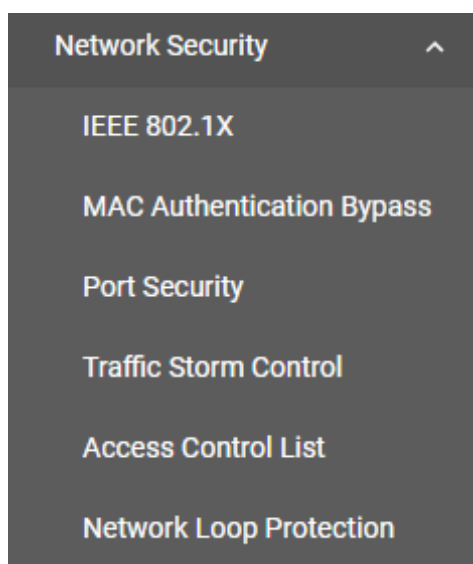
Setting	Description	Factory Default
Regenerate	Regenerates the SSL certificate.	None

Import Certificate

Setting	Description	Factory Default
Select the file	Imports the SSL certificate from the location where the SSL certificate is located.	None

Network Security

This section shows how to configure network security settings, including **IEEE802.1X, MAC Authentication Bypass, Port Security, Traffic Storm Control, Access Control List, and Loop Protection**.



IEEE 802.1X

Port-based IEEE 802.1X Overview

The IEEE 802.1X standard defines a protocol for client/server-based access control and authentication. The protocol restricts unauthorized clients from connecting to a LAN through ports that are open to the Internet, and which otherwise would be readily accessible. The purpose of the authentication server is to check each client that requests access to the port. The client is only allowed access to the port if the client's permission is authenticated.

Three components are used to create an authentication mechanism based on 802.1X standards: Client/Supplicant, Authentication Server, and Authenticator.

Client/Supplicant: The end station that requests access to the LAN and switch services and responds to the requests from the switch.

Authentication Server: The server that performs the actual authentication of the supplicant.

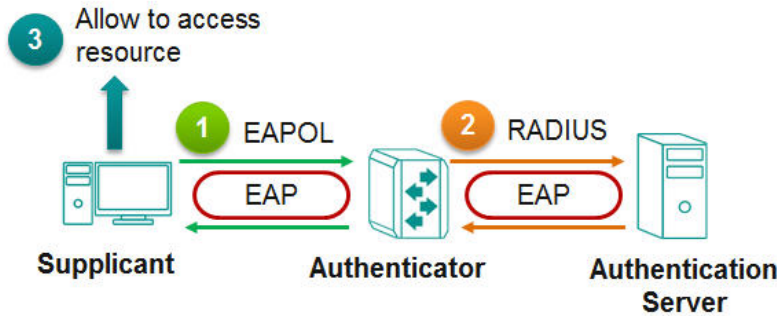
Authenticator: Edge switch or wireless access point that acts as a proxy between the supplicant and the authentication server, requesting identity information from the supplicant, verifying the information with the authentication server, and relaying a response to the supplicant.

The switch module acts as an authenticator in the 802.1X environment. A supplicant and an authenticator exchange EAPOL (Extensible Authentication Protocol over LAN) frames with each other. We can either use an external RADIUS server as the authentication server or implement the authentication server in the switch module by using a Local User Database as the authentication look-up table. When we use an external RADIUS server as the authentication server, the authenticator and the authentication server exchange EAP frames.

Authentication can be initiated either by the supplicant or the authenticator. When the supplicant starts the authentication process, it sends an **EAPOL-Start** frame to the authenticator. When the authenticator starts the authentication process or when it receives an **EAPOL Start** frame, it sends an **EAP Request/Identity** frame to ask for the username of the supplicant.

How IEEE 802.1X Works

802.1X authentication requires three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device that wishes to connect to the LAN or WLAN. The supplicant can also use the software to run on the client that offers credentials to the authenticator. Network administrators usually use an Ethernet switch or wireless access point as the authenticator and running software supporting RADIUS and EAP protocols in the authentication server.



The authenticator serves as a security guard to a protected network. The supplicant is not allowed access through the authenticator to the protected side of the network unless the supplicant's identity has been validated and authorized. With 802.1X port-based authentication, the supplicant provides credentials, such as username/password or digital certificate, to the authenticator, and the authenticator transmits the credentials to the authentication server for verification. If the authentication server approves the credentials as valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

IEEE 802.1X Settings

Select **IEEE802.1X** on the menu and then the **General** tab.



NOTE

Only ports 1 to 10 support 802.1X setting. SW1, SW2, CPU1, CPU2 are internal communication ports. This function cannot be edited in these ports.

IEEE 802.1X

General

RADIUS

Local Database

IEEE 802.1X

Disabled

Authentication Mode

Local Database

APPLY

Configure the following settings.

IEEE 802.1X

Setting	Description	Factory Default
Enabled	Enables IEEE 802.1X.	Disabled
Disabled	Disables IEEE 802.1X.	

Authentication Mode

Setting	Description	Factory Default
Local Database	Uses the local database as the authentication mode.	Local Database
RADIUS	Uses the RADIUS as the authentication mode.	

When finished, select **APPLY** to save your changes.

To configure the IEEE 802.1X settings for the specific port, select the edit icon on the port.

	Port	Enable	Port Control	Max. Request	Quiet Period	Reauthentication	Reauth Period	Server Timeout	Supp Timeout	Tx Period	Port Status
	1	Disabled	Auto	2	60	Disabled	3600	30	30	30	Authorized
	2	Disabled	Auto	2	60	Disabled	3600	30	30	30	Authorized
	3	Disabled	Auto	2	60	Disabled	3600	30	30	30	Authorized
	4	Disabled	Auto	2	60	Disabled	3600	30	30	30	Authorized

Configure the following settings.

Port 1 Settings

Enabled

Disabled

Port Control

Auto

Max. Request *

2

1 - 10

times

Quiet Period *

60

0 - 65535

sec.

Reauthentication

Disabled

Reauth Period *

3600

1 - 65535

sec.

Server Timeout *

30

1 - 65535

sec.

Supp Timeout *

30

1 - 65535

sec.

Tx Period *

30

1 - 65535

sec.

Copy Config to Ports

CANCEL

APPLY

Enable

Setting	Description	Factory Default
Enabled	Enables IEEE 802.1X.	Disabled
Disabled	Disables IEEE 802.1X.	

Port Control

Setting	Description	Factory Default
Force Unauthorized	The controlled port must be held in the Unauthorized state.	Auto
Auto	The controlled port is set to the authorized or unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the Authentication Server.	
Force Authorized	The controlled port is required to be held in the authorized state.	

Max Request (times)

Setting	Description	Factory Default
1 to 10	Enables re-authentication request time.	2

Quiet Period (sec.)

Setting	Description	Factory Default
0 to 65535	Specifies the duration of time that the switch remains in the muted state following a failed authentication exchange with the client.	60

Reauthentication

Setting	Description	Factory Default
Enabled	Enables re-authentication.	Disabled
Disabled	Disables re-authentication.	

Reauth Period (sec.)

Setting	Description	Factory Default
1 to 65535	Input the duration of time between re-authentication attempts.	3600

Server Timeout (sec.)

Setting	Description	Factory Default
1 to 65535	Input the duration of time that the switch will re-transmit the packets from the switch to the authentication server.	30

Supp (Supplicant, such as Client PC) Timeout (sec.)

Setting	Description	Factory Default
1 to 65535	Input the duration of time that the switch will re-transmit the packets from the switch to the client.	30

Tx Period (sec.)

Setting	Description	Factory Default
1 to 65535	Input the duration of time that the switch will re-transmit the data to the client.	30

Copy Config to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Allows users to copy configurations to other port(s).	None

When finished, select **APPLY** to save your changes.

IEEE 802.1X Database

RADIUS

RADIUS **Remote Authentication Dial in User Service** is a protocol that involves three services in one network protocol: Authentication, Authorization, and Accounting (AAA). The protocol operates in port 1812, and the AAA management for users connecting to a network service.

RADIUS is based on a client/server protocol that runs in the application layer and can use either TCP or UDP as the mode of transport. The network access servers that contain the RADIUS protocol can allow the client to communicate with the RADIUS server. Through Authentication, Authorization, and Accounting, RADIUS is used to monitor access to the network.

To configure RADIUS settings, select the **RADIUS** tab.

IEEE 802.1X

General

RADIUS

Local Database

Server Address 1

Auth Port

1 - 65535

Share Key

i

0 / 46

Timeout

i

1 - 120

sec.

Retransmit

i

1 - 254

sec.

Server Address 2

Auth Port

1 - 65535

Share Key

i

0 / 46

Timeout

i

1 - 120

sec.

Retransmit

i

1 - 254

sec.

APPLY

Configure the following settings.

Server Address 1

Setting	Description	Factory Default
To input server address 1	Specifies the first server address.	None

Auth Port

Setting	Description	Factory Default
1 to 65535	Specifies the authentication port number for the first server address.	None

Share Key

Setting	Description	Factory Default
Input the share key for the first server, (0 to 46)	Specifies the share key for the first server.	None

Timeout (sec.)

Setting	Description	Factory Default
1 to 120	Specifies the duration of time before a device is logged out.	None

Retransmit (sec.)

Setting	Description	Factory Default
1 to 254	Specifies the time for data retransmission.	None

Server Address 2

Setting	Description	Factory Default
To input server address 2	Specify the second server address.	None

Auth Port

Setting	Description	Factory Default
1 to 65535	Specifies the authentication port number for the first server address.	None

Share Key

Setting	Description	Factory Default
Input the share key for the second server (0 to 46)	Specifies the share key for the second server.	None

Timeout

Setting	Description	Factory Default
1 to 120	Specifies the duration of time before the device is timed out.	None

Retransmit (sec.)

Setting	Description	Factory Default
1 to 254	Specifies the time for data re-transmission.	None

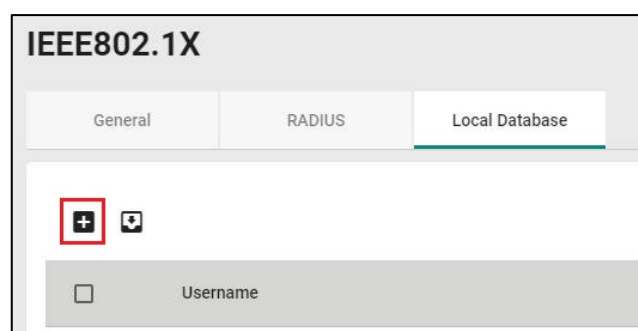
When finished, select **APPLY** to save your changes.

**NOTE**

The RADIUS service will be operated via the first server first; if it fails, it will be run on the second server.

Local Database

First, select the **Local Database** tab and then the + icon.



Configure the following settings.

Account Settings

Username

0 / 20

Password

At least 4 characters0 / 20

Confirm Password

At least 4 characters0 / 20

CANCEL

APPLY

Username

Setting	Description	Factory Default
0 to 20 characters	Specifies the username for the local database.	None

Password

Setting	Description	Factory Default
At least 4 characters, (max. 64 characters)	Specifies the password for the local database user.	None

Confirm Password

Setting	Description	Factory Default
At least 4 characters, (max. 64 characters)	Confirms the password for the local database user.	None

When finished, select **APPLY** to save your changes.

MAC Authentication Bypass

Select **MAC Authentication Bypass** on the function menu.



NOTE

Only ports 1 to 10 support MAC Authentication Bypass setting. SW1, SW2, CPU1, and CPU2 are internal communication ports. This function cannot be edited in these ports.

General

Select the **General** tab for general settings.

MAC Authentication Bypass

General

RADIUS

Local Database

MAC Authentication ...

Authentication Mode *

APPLY

MAC Authentication Bypass

Setting	Description	Factory Default
Enabled	Enables the MAC authentication bypass function.	None
Disabled	Disables the MAC authentication bypass function.	

Authentication Mode

Setting	Description	Factory Default
RADIUS	Selects RADIUS as the authentication mode.	None
Local Database	Selects local database as the authentication mode.	

When finished, select **APPLY** to save your changes.

RADIUS

Select the **RADIUS** tab to perform further configurations.

MAC Authentication Bypass

General

RADIUS

Local Database

Server Address 1

Auth Port

1 - 65535

Share Key

0 / 46

Timeout

1 - 120

sec.

Retransmit

1 - 254

sec.

Server Address 2

Auth Port

1 - 65535

Share Key

0 / 46

Timeout

1 - 120

sec.

Retransmit

1 - 254

sec.

APPLY

Configure the following settings.

Server Address 1

Setting	Description	Factory Default
To input server address 1	Specifies the first server address.	None

Auth Port

Setting	Description	Factory Default
1 to 65535	Specifies the authentication port number for the first server address.	None

Share Key

Setting	Description	Factory Default
Input the share key for the first server, (0 to 46)	Specifies the share key for the first server.	None

Timeout (sec.)

Setting	Description	Factory Default
1 to 120	Specifies the duration of time before a device is logged out.	None

Retransmit (sec.)

Setting	Description	Factory Default
1 to 254	Specifies the time for data retransmission.	None

Server Address 2

Setting	Description	Factory Default
To input server address 2	Specifies the second server address.	None

Auth Port

Setting	Description	Factory Default
1 to 65535	Specifies the authentication port number for the first server address.	None

Share Key

Setting	Description	Factory Default
Input the share key for the second server (0 to 46)	Specifies the share key for the second server.	None

Timeout

Setting	Description	Factory Default
1 to 120	Specifies the duration of time before the device is timed out.	None

Retransmit (sec.)

Setting	Description	Factory Default
1 to 254	Specifies the time for data retransmission.	None

When finished, select **APPLY** to save your changes.



NOTE

The RADIUS service will be operated via the first server first. If it fails, it will be run on the second server.

Local Database

Select **Local Database** tab and then select  icon for further configurations.

MAC Authentication Bypass

General

RADIUS

Local Database



☐ MAC Address

Max. 1024

Configure the following setting.

Create Entry

MAC Address * 

CANCEL

CREATE

MAC Address

Setting	Description	Factory Default
MAC Address	Specifies the MAC address used for MAC authentication bypass.	None

When finished, select **CREATE** to complete.

Port Security



NOTE

Only port 1 to 10 support Port Security setting. SW1, SW2, CPU1, CPU2 are internal communication ports. This function cannot be edited in these ports.

MAC Sticky Overview

MAC Sticky is a function that allows users to configure the maximum number of MAC addresses (the Limit) that a port can "learn". Users can configure what action should be taken (under Secure Action) when a new MAC address tries to access a port after the maximum number of MAC addresses have already been learned. The total number of allowed MAC addresses cannot exceed 1024.

How MAC Sticky Works

In MAC Sticky mode, administrators can set a proper limit number and then configure trust devices manually, or let the system configure trust devices automatically. Except for dropping packets as a response to any violations, administrators can set 'port shutdown' on a port and achieve a strict security guarantee. When a violation is registered on a port, the port will shut down and an administrator will receive a notification to perform a check.

MAC Sticky Settings and Status

To configure the MAC Sticky settings, select the **General** tab in **Port Security**.

Port Security

General

Static Port Lock

Port Security
Enabled

Port Security Mode
Static Port Lock 

APPLY

Configure the following settings.

Enable

Setting	Description	Factory Default
Enabled	Enables port security.	Enabled
Disabled	Disables port security.	

Port Security Mode

Setting	Description	Factory Default
MAC Sticky	Specifies MAC Sticky as the port security mode.	Static Port Lock
Static Port Lock	Specifies Static Port Lock as the port security mode.	

Select **MAC Sticky** and then **APPLY**.



NOTE

When you change the Port Security Mode, the settings in the table will be deleted.

Select the edit icon on the port you want to edit.

	Port	MAC Sticky	Address Limit	Secure Action	Current Address	Manual Configured Address	Violation
	1	Disabled	1	Packet Drop	0	0	No
	2	Disabled	1	Packet Drop	0	0	No
	3	Disabled	1	Packet Drop	0	0	No
	4	Disabled	1	Packet Drop	0	0	No

Configure the following settings.

Edit Port 1 Settings

MAC Sticky
Disabled

Address Limit *
1

Secure Action
Packet Drop

CANCEL

APPLY

MAC Sticky

Setting	Description	Factory Default
Enabled	Enables Static Port Lock for this port.	Disabled
Disabled	Disables Static Port Lock for this port.	

Address Limit

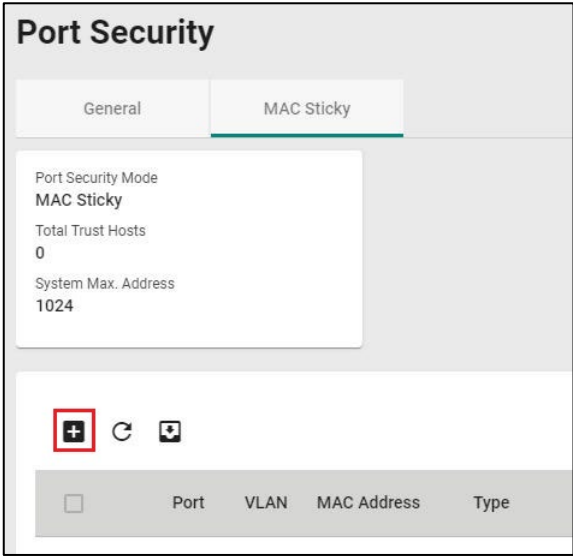
Setting	Description	Factory Default
1 to 1017	Specifies the maximum numbers of the learned MAC address.	1

Secure Action

Setting	Description	Factory Default
Port Shutdown	Enables port shutdown when a violation occurs.	Packet Drop
Packet Drop	Drops the packets when a violation occurs.	

When finished, select **APPLY** to save your changes.

Next, select the **MAC Sticky** tab and then the + icon to add the MAC Sticky entries.



Configure the following settings.

Create Entry

Port *

VLAN ID *

MAC Address * i

CANCEL

CREATE

Port		
Setting	Description	Factory Default
Select the port from the drop-down list	Selects the port(s) that will be used with the MAC Sticky function.	None
VLAN ID		
Setting	Description	Factory Default
Input the VLAN ID	Specifies the VLAN ID that will be used with MAC Sticky.	None
MAC Address		
Setting	Description	Factory Default
Input the MAC address that will be used	Specifies the MAC Address of the device that will be used as the reliable source for network access.	None

When finished, select **CREATE**.

You can view the MAC Sticky settings in the figure below.

Port Security

General

MAC Sticky

Port Security Mode

MAC Sticky

Total Trust Hosts

1

System Max. Address

1024

Port

VLAN

MAC Address

Type

Effective

3/4

1

c8:cb:b8:02:26:5f

Sticky Dynamic

Yes

Static Port Lock Overview

To provide a port-based security function, switch modules have implemented Static Port Lock function; the main idea is to allow configured devices, 128 at most, to access the network through a specific port. Packets sent from unknown devices or from configured devices with mismatching ports will be dropped. In other words, only the packets from the devices pre-configured with the specific MAC addresses can be sent to the specific port to ensure a secure network data transmission scenario.

Static Port Lock Settings and Status

To configure these settings, first select the **Port Security** tab and then **General**.

Port Security

General

MAC Sticky

Port Security

Enabled

Port Security Mode

Static Port Lock

APPLY

Configure the following settings.

Enable

Setting	Description	Factory Default
Enabled	Enables port security.	Enabled
Disabled	Disables port security.	

Port Security Mode

Setting	Description	Factory Default
MAC Sticky	Selects MAC Sticky as the port security mode.	Static Port Lock
Static Port Lock	Selects Static Port Lock as the port security mode.	

Select **Static Port Lock** and then **APPLY**.

Select the edit icon on the port you want to edit.

	Port	Static Port Lock	Manual Configured Address
	1	Disabled	0
	2	Disabled	0
	3	Disabled	0
	4	Disabled	0

Configure the following settings.

Edit Port 1 Settings

Static Port Lock
Disabled

CANCEL

APPLY

Enable

Setting	Description	Factory Default
Enabled	Enables Static Port Lock.	Disabled
Disabled	Disables Static Port Lock.	

When finished, select **APPLY** to save your changes.

Next, select the **Static Port Lock** tab and then the + icon to perform further settings.

Port Security

General

Static Port Lock

Port Security Mode
Static Port Lock

Total Trust Hosts
0

System Max. Address
1024

☐

Port

VLAN

MAC Address

Type

Configure the following settings.

Create Entry

Port *

VLAN ID *

MAC Address *

i

CANCEL

CREATE

Port

Setting	Description	Factory Default
Select the port from the drop-down list	Specifies the port(s) that will be used with Static Port Lock.	None

VLAN ID

Setting	Description	Factory Default
Input the VLAN ID	Specifies the VLAN ID that will use Static Port Lock.	None

MAC Address

Setting	Description	Factory Default
Input the MAC address that will be used	Specifies the MAC Address of the device that will be used as the reliable source for network access.	None

When finished, select **CREATE**.

View the Static Port Lock setting status from the following figure.

Traffic Storm Control

A traffic storm can happen when packets flood the network; this causes excessive traffic and slows down the network performance. To counter this, Traffic Storm Control provides an efficient design to prevent the network from flooding caused by a broadcast, multicast, or unicast traffic storm on a physical network layer. The feature can handle packets from both ingress and egress data.

First select **Traffic Storm Control** on the menu and then the edit icon on the specific port you want to configure.



NOTE

Only ports 1 to 10 support Traffic Storm Control setting. SW1, SW2, CPU1, CPU2 are internal communication ports. This function cannot be edited in these ports.

Traffic Storm Control					
	Port	Broadcast	Multicast	DLF	Threshold (fps)
	1	Enabled	Disabled	Disabled	12700
	2	Enabled	Disabled	Disabled	12700
	3	Enabled	Disabled	Disabled	12700
	4	Enabled	Disabled	Disabled	12700

Configure the following settings.

Edit Port QG1 Settings

Broadcast

Enabled

▼

Threshold

12700

.....

fps

Multicast

Disabled

▼

Threshold

12700

.....

fps

DLF

Disabled

▼

Threshold

12700

.....

fps

Threshold *

12700

1000 - 3720250

fps



Copy Config to Ports

▼



CANCEL

APPLY

Three methods that can be used for traffic storm control: Broadcast, Multicast, and Destination Lookup Failure (DLF).

Broadcast

Setting	Description	Factory Default
Enabled	Enables Broadcast when a traffic storm occurs.	Disabled
Disabled	Disables Broadcast when a traffic storm occurs.	

Multicast

Setting	Description	Factory Default
Enabled	Enables multicast when a traffic storm occurs.	Disabled
Disabled	Disables multicast when a traffic storm occurs.	

DLF

Setting	Description	Factory Default
Enabled	Enables DLF when a traffic storm occurs.	Disabled
Disabled	Disables DLF when a traffic storm occurs.	

Threshold (fps)

Setting	Description	Factory Default
1 to 1488100	Define the threshold for a traffic storm.	12700

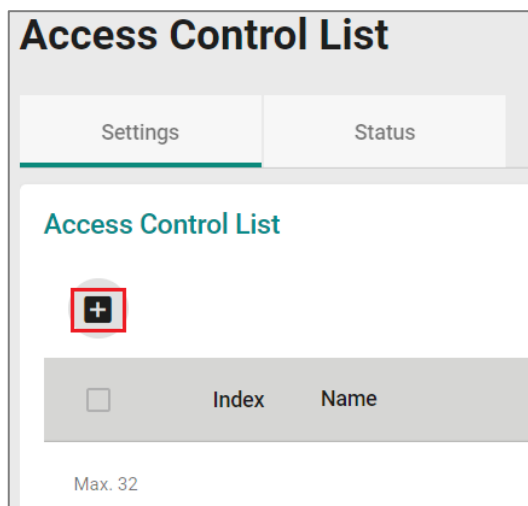
Copy Config to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) you want to have the same configurations for.	None

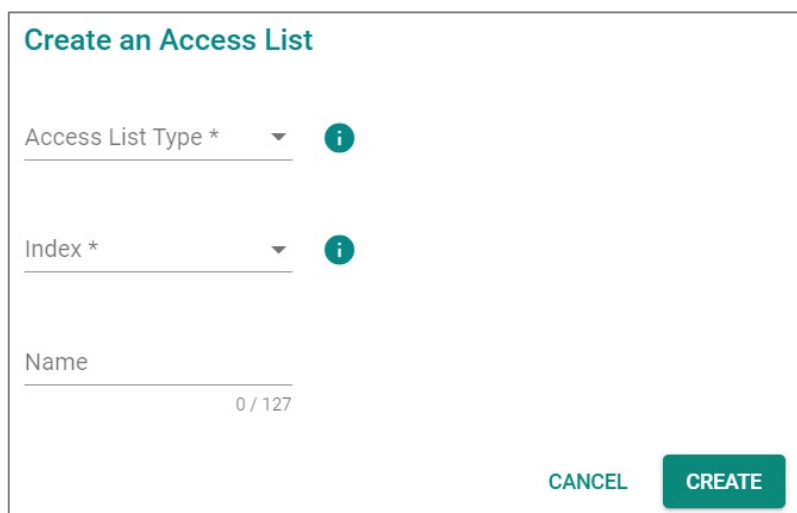
When finished, select **APPLY** to save your changes.

Access Control List

Select **Access Control List** on the function menu and then  to perform further configurations.



The screenshot shows the 'Access Control List' configuration page. It has two tabs: 'Settings' (selected) and 'Status'. Under the 'Settings' tab, there is a section titled 'Access Control List' with a red square icon containing a plus sign. Below this is a table with two columns: 'Index' and 'Name'. The table is currently empty, and a note 'Max. 32' is visible at the bottom left of the table area.



The screenshot shows the 'Create an Access List' dialog. It contains three input fields: 'Access List Type *' with a dropdown arrow and an information icon, 'Index *' with a dropdown arrow and an information icon, and 'Name' with a text input field and a character count '0 / 127'. At the bottom right, there are two buttons: 'CANCEL' and 'CREATE'.

Configure the following settings.

Access List Type

Setting	Description	Factory Default
IP-based	Specify IP-based as the access list type.	None
MAC-based	Specify MAC-based as the access list type.	

Index (For IP-based type)

Setting	Description	Factory Default
Select from IP-1 to IP-16	Select from the drop-down list for index.	None

Index (For MAC-based type)

Setting	Description	Factory Default
Select from MAC-1 to MAC-16	Select from the drop-down list for index.	None

Name

Setting	Description	Factory Default
0 to 127 characters	Provide a name for this access list.	None

IP-based ACL Table Configurations

Configure the following settings for the IP-based access list.

Active Interface Type

Setting	Description	Factory Default
Port-based	Specify Port-based as the active interface type.	None
VLAN-based	Specify VLAN-based as the active interface type.	

Active Ingress Ports (For Port-based type)

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) as the active ingress port(s).	None

Active Ingress VLAN (For VLAN-based type)

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) as the active ingress VLAN.	None

When finished, select **APPLY** to save your changes.

IP-based Rule Index Settings

Select the  icon for Rule Index settings.



Create Rule Index 1 Settings of IP-1

Rule Index 1 *

Enabled ▼

Rule Type *

Protocol

Any ▼

Source IP Address

Any Source IP Mask ▼

Destination IP Address

Any Destination IP Mask ▼

DSCP

Any

0 - 63

CANCEL CREATE

Configure the following settings.

Rule Index 1

Setting	Description	Factory Default
Enabled	Enable Rule Index 1 settings.	Enabled
Disabled	Disable Rule Index 1 settings.	

Rule Type

Setting	Description	Factory Default
Permit	Permit the rule type.	None
Deny	Deny the rule type.	

Protocol

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the protocol used for this rule index.	Any

Source IP Address

Setting	Description	Factory Default
IP address	Provide the IP address as the source IP address.	Any

Source IP Mask

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the source IP mask from the list.	None

Destination IP Address

Setting	Description	Factory Default
IP address	Provide the IP address as the destination IP address.	Any

Destination IP Mask

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the destination IP mask from the list.	None

DSCP

Setting	Description	Factory Default
0 to 63	Specify the DSCP value.	Any

When finished, select **CREATE** to complete.

Note that the following system packets are not included in the ACL operation.

Item	Destination/Source Port Number
DHCP Server	67
DHCP Client	68
Moxa Service	40404

MAC-based ACL Table Configurations

Configure the following settings for MAC-based access list.

ACL Table of MAC-1 ▼

Active Interface Type *
Port-based ▼

Active Ingress Ports ▼

APPLY

Active Interface Type

Setting	Description	Factory Default
Port-based	Specify Port-based as the active interface type.	None
VLAN-based	Specify VLAN-based as the active interface type.	

Active Ingress Ports (For Port-based type)

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) as the active ingress port(s).	None

Active Ingress VLAN (For VLAN-based type)

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) as the active ingress VLAN.	None

When finished, select **APPLY** to save your changes.

MAC-based Rule Index Settings

Select the  icon for Rule Index settings.



Create Rule Index 1 Settings of MAC-1

Rule Index 1 *
Enabled

Rule Type *
Any

EtherType
Any

Source MAC Address
Any

Source MAC Mask
.....

Destination MAC Address
Any

Destination MAC Ma...
.....

VLAN ID
Any

1 - 4094

CoS
Any

0 - 7

CANCEL CREATE

Configure the following settings.

Rule Index 1

Setting	Description	Factory Default
Enabled	Enable Rule Index 1 settings.	Enabled
Disabled	Disable Rule Index 1 settings.	

Rule Type

Setting	Description	Factory Default
Permit	Permit the rule type.	None
Deny	Deny the rule type.	

EtherType

Setting	Description	Factory Default
User defined	Select User defined as the Ethernet type.	Any

EtherType Value (For User defined type only)

Setting	Description	Factory Default
In hex digit	Provide the Ethernet type value for the user defined type.	0x

Source MAC Address

Setting	Description	Factory Default
MAC address	Provide the MAC address as the source MAC address.	Any

Source MAC Mask

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the source MAC mask from the list.	None

Destination MAC Address

Setting	Description	Factory Default
MAC address	Provide the MAC address as the destination MAC address.	Any

Destination MAC Mask

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the destination MAC mask from the list.	None

VLAN ID

Setting	Description	Factory Default
Select the VLAN ID by using the up/down arrows	Select the VLAN ID.	Any

CoS

Setting	Description	Factory Default
Select the CoS value by using the up/down arrows	Specify the DSCP value.	Any

When finished, select **CREATE** to complete.

Note that the following system packets are not included in the ACL operation.

Item	MAC Address
IEEE reserved Multicast MAC address	01:80:C2:XX:XX:XX
IP Multicast MAC address	01:00:5E:XX:XX:XX
Broadcast MAC address	FF:FF:FF:FF:FF:FF
L2 Multicast MAC address	01:XX:XX:XX:XX

Item	Ether Type
LLDP	0x88CC
EAPOL	0x888E
LACP	0x8809
LLC Jumbo Frame	0x8870
ARP	0x0806
MRP	0x88E3
PROFINET	0x8892
PTP	0x88B5
PTP	0x88F7
GOOSE	0x88B8
SMV	0x88BA
Ethernet Configuration Testing Protocol	0x9000

Access Control List Status

Select **Status** to view the Access Control List status.

Access Control List

Settings

Status

ACL Summary

Number of activate ACL (Max. 16)

1

Access Control List

Index	Name	Activated	Activate Direction
MAC-1	test	Inactivated	---
IP-1	test	Activated	Both

Loop Protection

Select **Loop Protection** on the function menu.

Settings

Select **Settings** for further configurations.

Loop Protection

Settings

Status

Loop Protection *

Disabled

Detect Interval *

10

1 - 30 sec.

APPLY

Configure the following settings.

Loop Protection

Setting	Description	Factory Default
Enabled	Enable the Loop Protection function.	Disabled
Disabled	Disable the Loop Protection function.	

Detect Interval

Setting	Description	Factory Default
1 to 30	Specify the detect interval value.	10

When finished, select **APPLY** to complete.

Status

Select **Status** tab to view the Loop Protection status.

Loop Protection

Settings

Status

Ports	Loop Status	Port Status	Peer Port
1/1	Normal	--	--
1/2	Normal	--	--
1/3	Normal	--	--
1/4	Normal	--	--

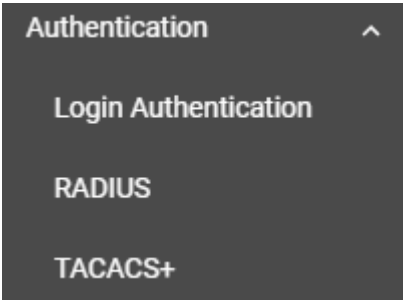
Authentication

This section describes how to configure system authentication including RADIUS and TACACS+. Switch modules have three different user login authentications: TACACS+ (Terminal Access Controller Access-Control System Plus), RADIUS (Remote Authentication Dial In User Service), and Local. The TACACS+ and RADIUS mechanisms are centralized "AAA" (Authentication, Authorization, and Accounting) systems for connecting to network services. The fundamental purpose of both TACACS+ and RADIUS is to provide an efficient and secure mechanism for user account management.

Five combinations are available to choose from.

1. **TACACS+, Local:** Check the TACACS+ database first. If checking the TACACS+ database fails, then check the Local database.
2. **RADIUS, Local:** Check the RADIUS database first. If checking the RADIUS database fails, then check the Local database.
3. **TACACS+:** Only check TACACS+ database.
4. **RADIUS:** Only check the RADIUS database.
5. **Local:** Only check the Local database.

This section includes the configurations for Login Authentication, RADIUS, and TACACS+.



Login Authentication

This section allows you to select the login authentication protocol.

Select **Login Authentication**.

Login Authentication

Authentication Protocol

Local

APPLY

Configure the following settings.

Authentication Protocol

Setting	Description	Factory Default
Local	Select Local as the authentication protocol.	Local
RADIUS	Select RADIUS as the authentication protocol.	
TACACS+	Select TACACS+ as the authentication protocol.	
RADIUS, Local	Select RADIUS and Local as the authentication protocol.	
TACACS+, Local	Select TACACS+ and Local as the authentication protocol.	

When finished, select **APPLY** to save your changes.

RADIUS

Select RADIUS on the menu and configure the following settings.

RADIUS Server

Server Address 1 *

0.0.0.0

UDP Port *

1812

Share Key

At least 60 characters0 / 60

Auth Type *

CHAP

Timeout *

5

5 - 180sec.

Retry *

1

0 - 5times

Server Address 2 *

0.0.0.0

UDP Port *

1812

Share Key

At least 60 characters0 / 60

Auth Type *

CHAP

Timeout *

5

5 - 180sec.

Retry *

1

0 - 5times

APPLY

Server Address 1

Setting	Description	Factory Default
Input the server address	Specify the first server address as the authentication database.	0.0.0.0

UDP Port

Setting	Description	Factory Default
Input the port number	Specify the UDP port.	1812

Share Key

Setting	Description	Factory Default
Input the key	Input the share key for first server authentication verification.	None

Authentication Type

Setting	Description	Factory Default
PAP	PAP is the authentication type.	CHAP
CHAP	CHAP is the authentication type.	
MS-CHAPv1	MS-CHAPv1 is the authentication type.	

Timeout (sec.)

Setting	Description	Factory Default
5 to 180	When waiting for a response from the server, set the time before timeout.	5

Retry (sec.)

Setting	Description	Factory Default
0 to 5	Define the retry interval when reconnecting to a server.	1

Server Address 2

Setting	Description	Factory Default
Input the server address	Specify the second server address as the authentication database.	0.0.0.0

UDP Port

Setting	Description	Factory Default
Input the port number	Specify the UDP port.	1812

Share Key

Setting	Description	Factory Default
Input the key	Specify the share key for second server authentication verification.	None

Authentication Type

Setting	Description	Factory Default
PAP	PAP is the authentication type.	CHAP
CHAP	CHAP is the authentication type.	
MS-CHAPv1	MS-CHAPv1 is the authentication type.	

Timeout (sec.)

Setting	Description	Factory Default
5 to 180	When waiting for a response from the server, set the time before the device is timed out.	5

Retry (sec.)

Setting	Description	Factory Default
0 to 5	Set the retry interval when reconnecting to a server.	1

When finished, select **APPLY** to save your changes.

**NOTE**

The RADIUS service will be operated via the first server; if it fails, it will run on the second server.

TACACS+

Select **TACACS+** on the menu and then configure the following settings.

TACACS+ Server

Server Address 1 *

0.0.0.0

TCP Port *

49

Share Key

i

At least 60 characters0 / 60

Auth Type *

CHAP

Timeout *

5

5 - 180sec.

Retry *

1

0 - 5times

Server Address 2 *

0.0.0.0

TCP Port *

49

Share Key

i

At least 60 characters0 / 60

Auth Type *

CHAP

Timeout *

5

5 - 180sec.

Retry *

1

0 - 5times

APPLY

Server Address 1

Setting	Description	Factory Default
Input the server address	Specify the first server address as the authentication database.	0.0.0.0

TCP Port

Setting	Description	Factory Default
Input the port number	Specify the UDP port.	49

Share Key

Setting	Description first	Factory Default
Input the key	Specify the share key for first server authentication verification.	None

Authentication Type

Setting	Description	Factory Default
ASCII	ASCII is the authentication type.	CHAP
PAP	PAP is the authentication type.	
CHAP	CHAP is the authentication type.	

Timeout (sec.)

Setting	Description	Factory Default
Input the value	When waiting for a response from the server, set the time before the device is timed out.	5

Retry

Setting	Description	Factory Default
Input the value	Set the retry interval when reconnecting to a server.	1

Server Address 2

Setting	Description	Factory Default
Input the server address	Specify the second server address as the authentication database.	0.0.0.0

TCP Port

Setting	Description	Factory Default
Input the port number	Specify the UDP port.	49

Share Key

Setting	Description	Factory Default
Input the key	Specify the share key for second server authentication verification.	None

Authentication Type

Setting	Description	Factory Default
ASCII	ASCII is the authentication type.	CHAP
PAP	PAP is the authentication type.	
CHAP	CHAP is the authentication type.	

Timeout (sec.)

Setting	Description	Factory Default
Input the value	When waiting for a response from the server, set the time before the device is timed out.	5

Retry

Setting	Description	Factory Default
Input the value	Set the retry interval when reconnecting to a server.	1

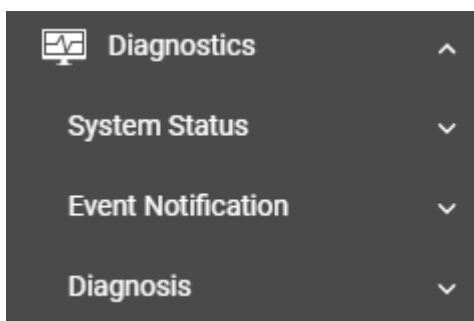
When finished, select **APPLY** to save your changes.

**NOTE**

The TACACS+ service will be operated via the first server; if it fails, it will run on the second server.

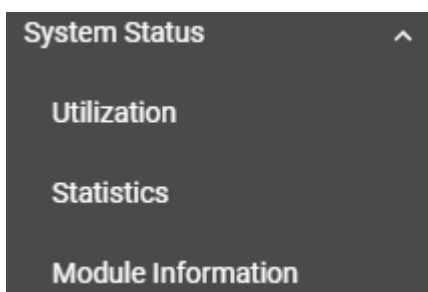
Diagnostics

This section describes the diagnostics functions of the switch module. Select **Diagnostics** from the function menu.



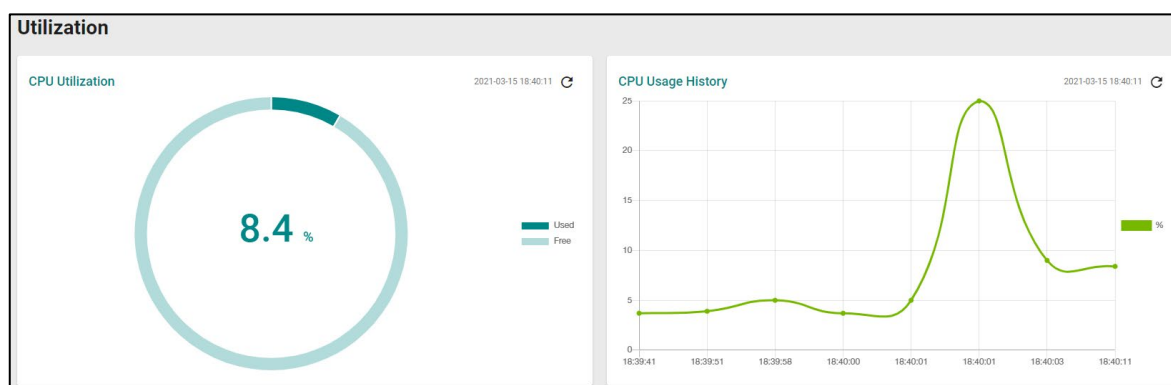
System Status

This section allows you to view the current system status, including **Utilization**, **Statistics**, and **Module Information**.



Utilization

Select **Utilization** on the function menu to view the current utilization status, including CPU utilization, memory history, power consumption, and power history. All the information is displayed via graphics, making it easier for you to view the system's status. In addition, a refresh icon is available on the upper right corner of each figure, which allows you to view the latest status for each function.

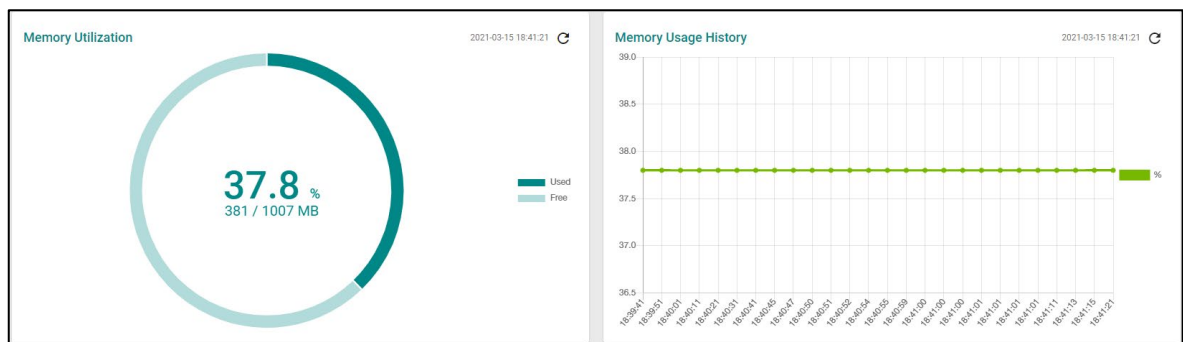


CPU Utilization

Setting	Description	Factory Default
Read-only	Displays the current utilization of the CPU.	None

CPU Usage History

Setting	Description	Factory Default
Read-only	Displays the CPU usage history trend in a chart.	None

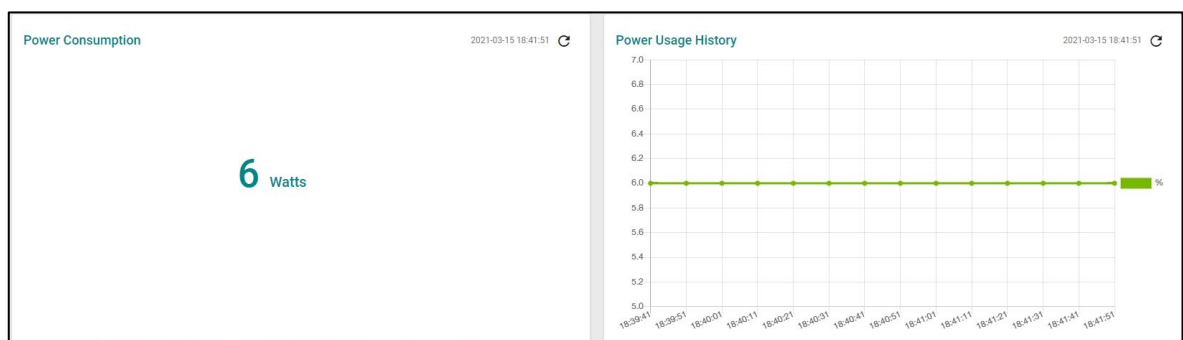


Memory Utilization

Setting	Description	Factory Default
Read-only	Displays the memory status.	None

Memory Usage History

Setting	Description	Factory Default
Read-only	Displays the history of memory usage.	None



Power Consumption (watt)

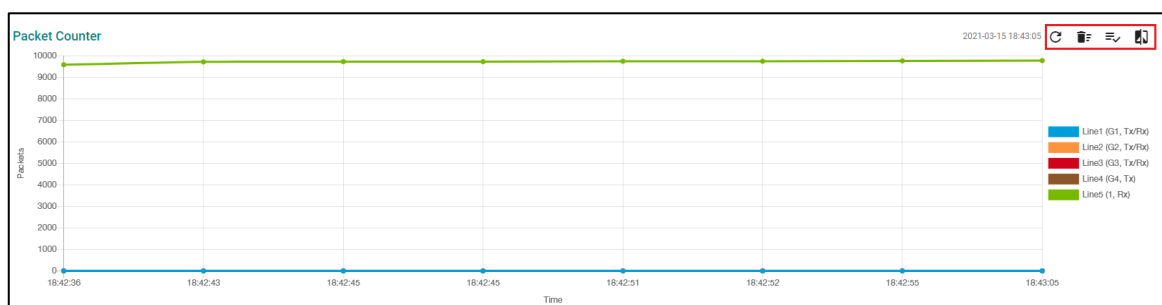
Setting	Description	Factory Default
Read-only	Displays the power consumption status.	None

Power Usage History

Setting	Description	Factory Default
Read-only	Displays the history of power usage.	None

Statistics

Select **Statistics** on the function menu. The first figure shows the packet counter status.



The status of the different ports will be shown in different colors. A maximum of five ports will have their information displayed.

	Line1 (G1, Tx/Rx)
	Line2 (G2, Tx/Rx)
	Line3 (G3, Tx/Rx)
	Line4 (G4, Tx)
	Line5 (1, Rx)

There are four icons on the right upper corner of the page. The table below describes each one.

Item	Name	Description
	Refresh	All statistical data will be refreshed.
	Reset Statistics Graph	The packet counter will be cleared, and the graphs will be reset.
	Display Setting	All selected setting items will be shown here.
	Data Comparison	Select the data you want to compare.

Refreshing the Statistics

Select the **Refresh** button and all statistical data will be refreshed immediately.

Resetting Statistics Graph

Select the **Reset** button and then **CLEAR** to clear the packet counter and reset the graph.

Reset Statistics Graph

Are you sure to clear all graph data?

CANCELCLEAR

Display Setting

Select the **Display Setting** icon and all settings will be displayed. Select the display mode from the drop-down list.

Display Settings

Display Mode *

Packet Counter

Line 1 Monitoring Port *

1

Line 1 Sniffer *

Tx/Rx

Line 2 Monitoring Port *

2

Line 2 Sniffer *

Tx/Rx

Line 3 Monitoring Port *

3

Line 3 Sniffer *

Tx/Rx

Line 4 Monitoring Port *

4

Line 4 Sniffer *

Tx

Line 5 Monitoring Port *

5

Line 5 Sniffer *

Rx

CANCEL

APPLY

The Monitoring Port is the port you want to view or monitor. The sniffer port is the port you can choose to view its receiving or transmission status, or both.

Display Mode

Setting	Description	Factory Default
Packet Counter	The packet statistics will be displayed.	Packet Counter
Bandwidth Utilization	The bandwidth statistics will be displayed.	

Select **APPLY** to complete.

Comparing Data

Select the **Data Comparison** icon and then select the items from the relevant fields.

Data Comparison

Benchmark Line *

Comparison Line *

Benchmark Line - Time *

Comparison Line - Time *

CLOSE

Select **CLOSE** to complete.

The data comparison figure will be shown. Select **Close** to finish.

Compare Data

Benchmark *

1, Tx/Rx

Benchmark Line - Time *

22:32:13

Comparison *

2, Tx/Rx

Comparison Line - Time

22:32:22

Tx Total Octets	0	$\frac{\downarrow}{\uparrow}$	▼
Tx Total Packets	0	$\frac{\downarrow}{\uparrow}$	▼
Tx Unicast Packets	0	$\frac{\downarrow}{\uparrow}$	▼
Tx Multicast Packets	0	$\frac{\downarrow}{\uparrow}$	▼
Tx Broadcast Packets	0	$\frac{\downarrow}{\uparrow}$	▼
Rx Total Octets	0	$\frac{\downarrow}{\uparrow}$	▼
Rx Total Packets	0	$\frac{\downarrow}{\uparrow}$	▼

CLOSE

The detailed packet transmission activity for each port can be seen in the table below.

Port	Tx Total Octets	Tx Total Packets	Tx Unicast Packets	Tx Multicast Packets	Tx Broadcast Packets	Rx Total Octets	Rx Total Packets	Rx Unicast Packets	Rx Multicast Packets	Rx Broadcast Packets
1	11843056	15111	13375	1736	0	1974621	10329	10041	282	6
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
po1	11843056	15111	13375	1736	0	1974621	10329	10041	282	6

Rx Pause Packets	Collision Packets	Late Collision Packets	Excessive Collision Packets	CRC Align Error Packets	Drop Packets	Undersize	Oversize Packets	Fragment Packets	Jabber Packets
1	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0

Port: port number

Tx Total Octets: Number of octets transmitted, including bad packets and FCS octets. Framing bits are not included.

Tx Total Packets: Number of packets transmitted.

Tx Unicast Packets: Number of Unicast packets transmitted.

Tx Broadcast Packets: Number of good Broadcast packets transmitted. Multicast packets are not included.

Rx Total Octets: Number of octets received, including bad packets and FCS octets. Framing bits are not included.

Rx Unicast Packets: Number of Unicast packets received.

Rx Multicast Packets: Number of Multicast packets received.

Rx Broadcast Packets: Number of good Broadcast packets received. Multicast packets are not included.

Rx Pause Packets: Number of pause packets received.

Collision Packets: Number of collisions received. If Jumbo Frames are enabled, the threshold of Jabber Frames is raised to the maximum size of Jumbo Frames.

Late Collision Packets: Number of late collision packets.

Excessive Collision Packets: Number of excessive collision packets.

CRC Align Error Packets: Number of CRC and Align errors that have occurred.

Drop Packets: Number of packets that were dropped.

Undersize: Number of undersized packets (less than 64 octets) received.

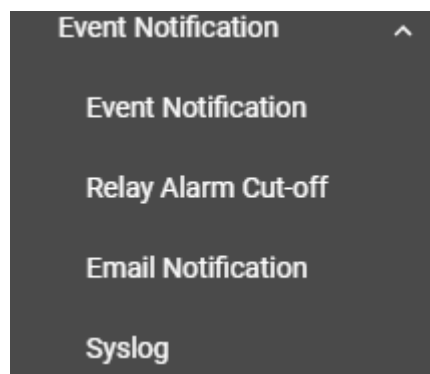
Oversize Packets: Number of oversized packets (over 1518 octets) received.

Fragment Packets: Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received.

Jabber Packets: Number of received packets that were longer than 1632 octets. This number excludes frame bits but includes FCS octets that had either a bad FCS (Frame Check Sequence) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number.

Event Notification

This section includes the information regarding **Event Notification**, **Email Notification**, and **Syslog**.



Event Notification

Event Notification includes two functions: System and Function, and Port.

In the **Event Notification** menu, select the **System and Function** tab and then the edit icon on the specific event you want to configure. For example, select the edit icon for warm start when the switch reboots.

Event Notification					
System and Function		Port			
Group	Event Name	Enabled	Severity	Registered Action	
	General	Warm start	Enabled	Notice	Trap, Email
	General	Password changed	Enabled	Notice	Trap, Email
	General	Login success	Enabled	Notice	Trap, Email
	General	Configuration changed	Enabled	Notice	Trap, Email
	General	Configuration imported	Enabled	Notice	Trap, Email

Configure the following settings.

Edit Event Notification

Event Name

Cold start

Enabled

Enabled

Registered Action

Trap, Email

CANCEL

APPLY

Enable

Setting	Description	Factory Default
Enabled	Enable Event Notification for this event.	Enabled
Disabled	Disable Event Notification for this event.	

Registered Action

Setting	Description	Factory Default
Trap	Send SNMP Trap for event notifications.	Trap/Email
Email	Send an email for event notifications.	

When finished, select **APPLY** to save your changes.

In addition, use the same method to edit other events, such as login logout, warm start, password changed, etc.

Next, in the **Event Notification** menu, select the **Port** tab, and then select the edit icon on the specific port status on **Event Name**. For example, select the edit icon for event notifications when the port status is on.

Event Notification

System and Function

Port

Event Name	Enable	Severity	Registered Action
 Port On	Enabled	Notice	Trap, Email
 Port Off	Enabled	Notice	Trap, Email
 Port shutdown by Port Security	Enabled	Warning	Trap, Email
 Port shutdown by Rate Limit	Enabled	Warning	Trap, Email
 Port recovery by Rate Limit	Enabled	Warning	Trap, Email

Configure the following settings.

Edit Event Notification

Event Name

Port On

Enabled

Enabled

Registered Action

Trap, Email

Registered Port

All Ports

CANCEL

APPLY

Enable		
Setting	Description	Factory Default
Enabled	Enable Event Notification for this event.	Enabled
Disabled	Disable Event Notification for this event.	

Registered Action		
Setting	Description	Factory Default
Trap	Send SNMP Trap for event notifications.	Trap/Email
Email	Send an email for event notifications.	

Registered Port		
Setting	Description	Factory Default
Select port(s) from the drop-down list	Specify the port(s) that use the registered action.	All Ports

When finished, select **APPLY** to save your changes.

In addition, use the same method to edit other events such as, port status is off, port shutdown by port security, and port recovery by rate limit, etc.

Check the following table for the severity degree of each event.

System & Function	
Event Name	Severity
Cold start	Critical
Warm start	Notice
Configuration changed	Notice
Login success	Notice
Login fail	Warning
Login lockout	Warning
Account setting changed	Notice
Configuration imported	Notice
SSL certification changed	Notice
Log capacity threshold	Warning
Password changed	Notice
PWR Off->On	Notice
PWR On->Off	Notice
Topology changed	Warning
Coupling changed	Warning
Master changed	Warning
Master mismatch	Warning
RSTP topology changed	Warning
RSTP root changed	Warning
RSTP migration	Warning
RSTP invalid BPDU	Warning
RSTP new port role	Warning
Redundant port health check fail	Error
Dual homing path changed	Warning
Dot1X auth fail	Warning
LLDP table changed	Information
RMON raising alarm	Warning
RMON failing alarm	Warning

Port	
Event Name	Severity
Port On	Notice
Port Off	Notice
Port shutdown by Port Security	Warning
Port shutdown by Rate Limit	Warning
Port recovery by Rate Limit	Warning

Email Notification

Select **Email Notification** on the function menu and configure the following settings.

Email Notification

Mail Server *

0.0.0.0

7 / 60

TCP Port

25

1 - 65535

Username

0 / 60

Password

0 / 60

TLS Enable

Disabled

Sender Address

admin@localhost.com

19 / 60

1st Recipient Email Add...

0 / 60

2nd Recipient Email Ad...

0 / 60

3rd Recipient Email Add...

0 / 60

4th Recipient Email Add...

0 / 60

5th Recipient Email Add...

0 / 60

APPLY

Mail Server

Setting	Description	Factory Default
IP address or URL	The IP Address or URL of the email server.	0.0.0.0

TCP Port

Setting	Description	Factory Default
1 to 65535	The TCP port number of your email server.	25

User Name

Setting	Description	Factory Default
Max. of 60 characters	Your email account name.	None

Password

Setting	Description	Factory Default
Max. of 60 characters	Your email account password.	None

TLS Enable

Setting	Description	Factory Default
Enabled	Enable TLS (Transport Layer Security).	Disabled
Disabled	Disable TLS (Transport Layer Security).	

Sender Address

Setting	Description	Factory Default
Max. 60 characters	The sender's email address.	admin@localhost

First to Fifth Email Addresses

Setting	Description	Factory Default
Max. of 60 characters	Set up maximum five email addresses to receive alert emails from the switch module.	None

When finished, select **APPLY** to save your changes.

Syslog Settings

Select the **General** tab on the function menu and configure the following settings.

Syslog

General Authentication

Syslog
Disabled

Syslog Server 1
Disabled

Address 1
514

Syslog Server 2
Disabled

Address 2
514

Syslog Server 3
Disabled

Address 3
514

APPLY

Logging Enable

Setting	Description	Factory Default
Enabled	Enable logging.	Disabled
Disabled	Disable logging.	

Syslog Server 1

Setting	Description	Factory Default
Enabled	Enable the first log server.	Disabled
Disabled	Disable the first log server.	

Address 1

Setting	Description	Factory Default
IP Address	Input the IP address of the Syslog first server that is used by your network.	None

UDP Port

Setting	Description	Factory Default
1 to 65535	Input the UDP port number.	514

Syslog Server 2

Setting	Description	Factory Default
Enabled	Enable the second syslog server.	Disabled
Disabled	Disable the second syslog server.	

Address 2

Setting	Description	Factory Default
IP Address	Input the IP address of Syslog second server that is used by your network.	None

UDP Port

Setting	Description	Factory Default
1 to 65535	Input the UDP port number.	514

Syslog Server 3

Setting	Description	Factory Default
Enabled	Enable the third syslog server.	Disabled
Disabled	Disable the third syslog server.	

Address 3

Setting	Description	Factory Default
IP Address	Input the IP address of the Syslog third server that is used by your network.	None

UDP Port

Setting	Description	Factory Default
1 to 65535	Input the UDP port number.	514

When finished, select **APPLY** to save your changes.



NOTE

If the syslog server cannot receive the previous logs, it is possible that the receiving port of the syslog server is not ready. We suggest you enable the Linkup Delay function to delay the log delivery time.

Select **Authentication** tab and add the icon in the function menu.

Syslog

General

Authentication

Common Name	Start Time	Expire Time
Max. 1		

Configure the following settings.

Add Certificate and Key

Client Certificate *

Client Key *

CA Key *

CANCEL

CREATE

Client Certificate

Setting	Description	Factory Default
Select the import icon and then the file from your computer.	Import the client certificate file.	None

Client Key

Setting	Description	Factory Default
Select the import icon and then the file from your computer.	Import the client key file.	None

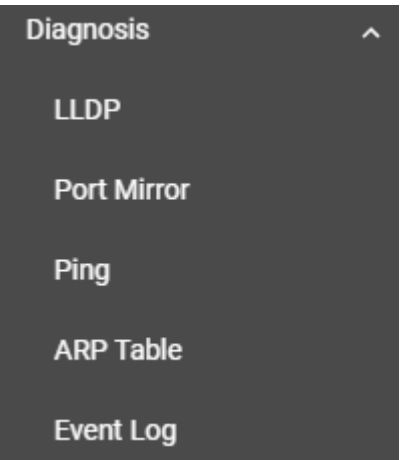
CA Key

Setting	Description	Factory Default
Select the import icon and then select the file from your computer.	Import the CA key file.	None

When finished, select **CREATE** to save your changes.

Diagnosis

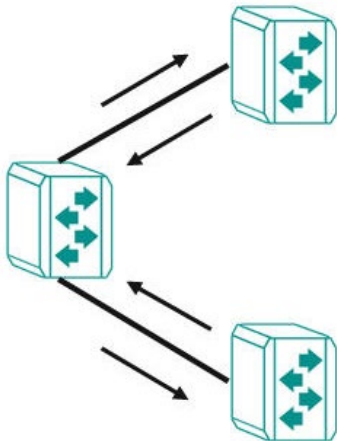
This section explains the configurations for system diagnoses, such as **LLDP**, **Port Mirror**, **Ping**, **ARP Table**, and **Event Log**.



LLDP Overview

LLDP is an OSI Layer 2 protocol defined by IEEE 802.11AB. LLDP standardizes the self-identification advertisement method, and allows each networking device, such as a Moxa managed switch, to periodically send its system and configuration information to its neighbors. Because of this, all LLDP devices are kept informed of each other's status and configurations. With SNMP, this information can be transferred to Moxa's MXview for auto-topology and network visualization.

From the switch's web interface, enable or disable LLDP, and set the LLDP transmit interval. In addition, you can view each switch's neighbor-list, which is reported by its network neighbors. Most importantly, enabling the LLDP function allows Moxa's MXview to automatically display the network's topology and system setup details, such as VLAN and trunking for the entire network.



LLDP Settings and Status

Select **LLDP** on the menu and then the **Setting** tab to configure the following settings.

LLDP

Settings

Status

Enable

Enabled

LLDP Version

2005

Transmit Interval

30

sec.

Notification Interval

5

sec.

Tx Delay

2

sec.

Reinitialization Delay

2

sec.

Holdtime Multiplier

4

times

Chassis ID Subtype

MAC-Addr

APPLY

Enable

Setting	Description	Factory Default
Enabled	Enable LLDP.	Disabled
Disabled	Disable LLDP.	

LLDP Version

Setting	Description	Factory Default
Show the LLDP version	Show the LLDP version automatically.	2005

Transmit Interval (sec.)

Setting	Description	Factory Default
5 to 32768	Set the transmit interval of LLDP messages	30

Notification Interval (sec.)

Setting	Description	Factory Default
5 to 3600	Specify the notification interval.	5

Tx Delay (sec.)

Setting	Description	Factory Default
1 to 8192	Specify the Tx delay interval.	2

Reinitialization Delay (sec.)

Setting	Description	Factory Default
1 to 10	Specify the LLDP reinitialization delay interval.	2

Holdtime Multiplier

Setting	Description	Factory Default
2 to 10	Specify the holdtime multiplier value.	4

Chassis ID Subtype

Setting	Description	Factory Default
Chassis-Component	Select Chassis-Component as Chassis ID subtype.	Mac-Addr
If-Alias	Select If-Alias as Chassis ID subtype.	
Port-Component	Select Port-Component as Chassis ID subtype.	
MAC-Addr	Select MAC-Address as Chassis ID subtype.	
Network Address	Select Network Address as Chassis ID subtype.	
If-Name	Select If-Name as Chassis ID subtype.	
Local	Select Local as Chassis ID subtype.	

When finished, select **APPLY** to save your changes.

Each port for the LLDP settings can also be configured. Select the edit icon for the port you want to configure.

Port	Port Status
 1	Tx and Rx
 2	Tx and Rx
 3	Tx and Rx
 4	Tx and Rx

Configure the following settings.

Edit Port 1 Settings

Port Status
Tx and Rx

Subtype
If-Alias

TLV
Basic

Transmit TLVs

☒ Port Description
☒ System Name
☐ System Description
☐ System Capability

Copy Config to Ports

CANCEL

APPLY

Port Status

Setting	Description	Factory Default
Tx Only	Set Tx as the port status.	Tx and Rx
Rx Only	Set Rx as the port status.	
Tx and Rx	Set both Tx and Rx as the port status.	

Subtype

Setting	Description	Factory Default
If-Alias	Select If-Alias as the subtype.	If-Alias
Port-Component	Select Port-Component as the subtype.	
MAC-Addr	Select MAC-Address as the subtype.	
If-Name	Select If-Name as the subtype.	
Local	Select Local as the subtype.	

TLV

Setting	Description	Factory Default
Basic	Set TLV as Basic.	Basic
802.1	Set TLV as 802.1.	
802.3	Set TLV as 802.3.	

Transmit TLVs

Setting	Description	Factory Default
Port Description	Add a port description for the TLV.	Port Description System Name
System Name	Add a system name for the TLV.	
System Description	Add a system description for the TLV.	
System Capability	Add a system capability for the TLV.	

Copy Config to Port

Setting	Description	Factory Default
Select the port from the list	Copy the same configurations to other port(s).	None

When finished, select **APPLY** to save your changes.

To view the LLDP status, select the **Status** tab on the LLDP page, and the status of all LLDP will be shown on the page.

LLDP		
Setting	Status	
Local Information Enable Enabled LLDP Version v1(2005) Chassis Id Subtype MAC-Addr Chassis ID 00:01:02:03:04:05	Local Timer Transmit Interval 30 (sec) Notification Interval 5 (sec) Tx Delay 2 (sec) Reinitialization Delay 2 (sec) Holdtime Multiplier 4 (x)	Remote Table Statistics Last Change Time (ms) 1300 Inserts 1 Drops 0 Delete 0 Ageouts 0

Refer to the following table for the detailed description of each item.

Local Information	
Enable	Show if LLDP has been enabled or disabled.
LLDP Version	Show the LLDP version.
Chassis ID Subtype	Show the chassis ID subtype.
Chassis ID	Show the chassis ID.

Local Timer	
Transmit Interval (sec.)	The interval between regular LLDP packet transmissions.
Notification Interval (sec.)	The interval that notifications will be sent.
Tx Delay (sec.)	The delay period between successive LLDP frame transmissions initiated by changes.
Reinitialization Delay (sec.)	The interval of an LLDP port waits before re-initializing an LLDP packet transmission.
Holdtime Multiplier	The time that the receiving device holds an LLDP packet before discarding it.

Remote Table Statistics	
Last Change Time (ms.)	The last time the remote table changed.
Inserts	How many inserts have occurred.
Drop	How many drops have occurred.
Delete	How many deletes have occurred.
Age-outs	How many age-outs have occurred.

To view the LLDP status for a specific port, select the detailed information icon on the port. All information will be shown on the right side of the page.

LLDP
Enabled

LLDP Version
v1(2005)

Chassis ID Subtype
MAC-Addr

Chassis ID
00:90:e8:90:a6:7c

Transmit Interval
30 (sec.)

Notification Interval
5 (sec.)

Tx Delay
2 (sec.)

Reinitialization Delay
2 (sec.)

Holdtime Multiplier
4 (times)

Last change time (ms)
0

Inserts
0

Drops
0

Delete
0

Ageouts
0

Detailed Information

Port Local Interface

Port ID SubType
Chassis-Component

Port ID
Eth1/5

Port Description
Ethernet Interface Port 05

Extended 802.1 TLV

Port VLAN ID
1

VLAN ID / Name

Extended 802.3 TLV

Aggregated and Status
Enabled

Aggregated Port ID
9

Maximum Frame Size
9216

Port Traffic Statistics

Total Frames Out
611

Total Entries Aged
0

Total Frames In
0

Total Frames Received In Error

Port

Tx Status

Rx Status

Neighbor Port ID

Neighbor Chassis ID

1	Enabled	Enabled		
2	Enabled	Enabled		
3	Enabled	Enabled		
4	Enabled	Enabled		

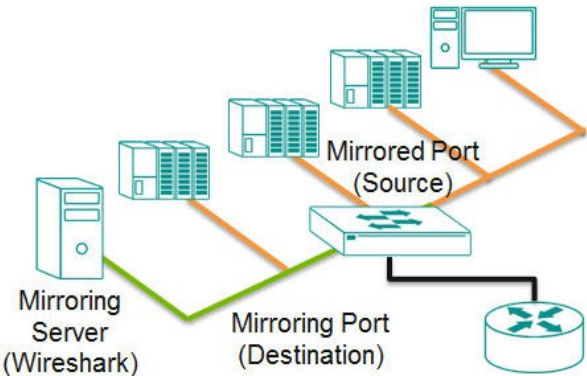
Port Mirroring

Port Mirroring Overview

The Port Mirroring function can be used to monitor data being transmitted through a specific port. This is done by setting up another port (the mirror port) to receive the same data being transmitted from, or both to and from, the port under observation. Using a mirror port allows the network administrator to sniff the observed port to keep tabs on network activity.

How Port Mirror Works

Port Mirroring can configure to copy one or more packets from various ports to a single port, so that you can check if there are problems occurring in these ports. For example, the following figure demonstrates how the packets transmitted in the four mirrored ports (marked in orange) are copied (mirrored) to a single mirroring port (marked in green). These packets will be sent to a monitoring computer and then software is used to check if there is something wrong with these packets. It is a useful function to troubleshoot or debug a network data transmission issue.



Port Mirror Settings and Status

Select Port Mirror on the menu and then configure the settings.

Port Mirror

Enabled

APPLY

Enable

Setting	Description	Factory Default
Enabled	Enable Port Mirror.	Enabled
Disabled	Disable Port Mirror.	

When finished, select **APPLY** to save your changes.

To configure the specific port, select the edit icon next to the port.

	Session ID	Enable	Tx Source Port
	1	Disabled	
	2	Disabled	
	3	Disabled	
	4	Disabled	
	5	Disabled	

Configure the following settings.

Edit Session 1 Settings

Port Mirror *

Disabled

Tx Source Port

Rx Source Port

Destination Port *

CANCEL

APPLY

Enable

Setting	Description	Factory Default
Enabled	Enable Port Mirror for this session.	Disabled
Disabled	Disable Port Mirror for this session.	

Tx Source Port

Setting	Description	Factory Default
Select the port from the list	Select this option to monitor only those data packets being sent out through the switch's port.	None

Rx Source Port

Setting	Description	Factory Default
Select the port from the list	Select this option to monitor only those data packets coming into the switch's port.	None

Destination Port

Setting	Description	Factory Default
Select the port from the list	Specify this port as the destination port.	None

When finished, select **APPLY** to save your changes.



NOTE

The RSTP ports and Port Mirror destination port cannot be enabled on the same port.

The Port Mirror status can be seen in the figure below.

	Session ID	Enable	Tx Source Port(s)	Rx Source Port(s)	Destination Port
	1	Enabled	1, 2	1, 4	3
	2	Disabled			

Ping

The **Ping** function uses the ping command to give you a simple but powerful tool for troubleshooting network problems. The unique feature of the function is that even though the ping command is entered from the your PC, the actual ping command originates from the switch module itself. This allows you to essentially sit on top of the switch module and send ping commands out through its ports.

To use the Ping function, select **Ping** on the menu, and enter the IP address or domain name you want to ping. After selecting **Ping**, the result will be shown.

Ping

PING

ARP Table

To view the ARP Table, select **ARP Table** and the information will be displayed.

ARP Table		
 		
Index	MAC Address	IP Address
1	28:d2:44:5e:8b:40	192.168.127.99
Max 2000		

Event Log

To edit the event log oversize-action, select **Event Log** on the menu and then **Event Log** on the page.

Event Log

Event Log

Threshold Settings

Oversize-Action

Overwrite the oldest event log

APPLY

Configure the following settings when the event log file is full.

Oversize-action

Setting	Description	Factory Default
Overwrite the oldest event log	Overwrite the oldest event log.	Overwrite the oldest event log
Stop recording event log	Disable Port Mirror for this port.	

Select **APPLY** to finish.

To view all the event formation, check the lower part of the event log page.

Index	Bootup Number	Severity	Timestamp	Uptime	Message
1	16	Notice	2018-12-27 21:47:10	0d4h52m3s	Configuration [Account] changed by admin.
2	16	Notice	2018-12-27 21:41:20	0d4h46m13s	Configuration [Port Security] changed by admin.
3	16	Notice	2018-12-27 21:36:48	0d4h41m41s	Configuration [Port Security] changed by admin.
4	16	Notice	2018-12-27 21:21:34	0d4h26m27s	Configuration [Trusted Access] changed by admin.
5	16	Notice	2018-12-27 21:12:24	0d4h17m17s	Configuration [Mgmt Interface] changed by admin.
6	16	Notice	2018-12-27 21:05:41	0d4h10m34s	Configuration [SNMP] changed by admin.
7	16	Notice	2018-12-27 21:04:13	0d4h9m6s	Configuration [SNMP] changed by admin.
8	16	Notice	2018-12-27 20:57:08	0d4h2m1s	Configuration [L2 Redundancy] changed by admin.
9	16	Notice	2018-12-27 20:56:09	0d4h1m2s	Port 1/2 has restarted by Turbo Chain.
10	16	Notice	2018-12-27 20:56:08	0d4h1m1s	Port 1/1 has restarted by Turbo Chain.
11	16	Notice	2018-12-27 20:56:06	0d4h0m59s	Configuration [L2 Redundancy] changed by admin.
12	16	Warning	2018-12-27 20:55:11	0d4h0m4s	Topology has been changed by Turbo Chain.
13	16	Notice	2018-12-27 20:55:11	0d4h0m4s	Port 1/2 has restarted by Turbo Chain.
14	16	Notice	2018-12-27 20:55:11	0d4h0m4s	Port 1/1 has restarted by Turbo Chain.
15	16	Notice	2018-12-27 20:55:08	0d4h0m1s	Configuration [Turbo Chain] changed by admin.
16	16	Notice	2018-12-27 20:54:54	0d3h59m47s	Configuration [L2 Redundancy] changed by admin.

Threshold Settings

To configure the event log threshold, select the **Threshold Setting** tab on the Event Log Page. The event log threshold can be set up to send an early warning when the event log entries have reached the percentage of the threshold. The maximum recorded event log entries are 10,000.

Event Log

Event Log

Threshold Settings

Capacity Warning

Disabled

Warning Threshold *

80

50 - 100

%

APPLY

Configure the following settings.

Capacity Warning

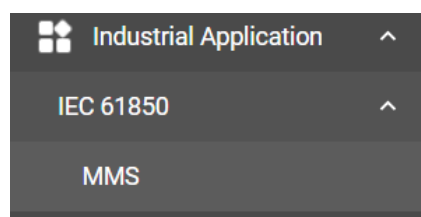
Setting	Description	Factory Default
Enabled	Enable capacity warning event log.	Disabled
Disabled	Disable capacity warning event log.	

Warning Threshold (%)

Setting	Description	Factory Default
50 to 100	Set the warning threshold as a percentage.	80

Industrial Applications

This section introduces the settings for the MMS of the IEC 61850 standard. Select **MMS** in the function menu under **Industrial Application** and **IEC 61850**.



General Settings

Select the **General** tab for further configurations.

A screenshot of the 'MMS' configuration page. At the top, there are two tabs: 'General' (which is selected) and 'Security'. Below the tabs, there is a dropdown menu labeled 'MMS *' with 'Disabled' selected. Below that is a text input field labeled 'IED Name *' containing '65M5011M'. To the right of the input field is a character count '8 / 20'. At the bottom left of the form is a green button labeled 'APPLY'.

Configure the following settings.

MMS

Setting	Description	Factory Default
Enabled	Enable the MMS function on the switch.	Disabled
Disabled	Disable the MMS function on the switch.	

IED Name

Setting	Description	Factory Default
0 to 20 characters	Provide the IED name for your switch.	RKS-G4000 (Will vary depending on the switch models)

When finished, select **APPLY** to save your changes.

CID File Settings

Select the edit icon  on the page.

CID File Settings	
Report Control Block	Data Change
 urcbLnkSt	Enabled
 brcbLnkSt	Enabled
 urcbSysSt	Enabled
 brcbSysSt	Enabled

Configure the following settings.

Edit urcbLnkSt

Data Change *

Enabled

Data Update *

Disabled

Quality Change *

Disabled

Integrity *

Enabled

Buffer Time *

1000

1 - 4294967295ms

Integrity Period *

5000

1 - 4294967295ms

CANCEL

APPLY

Data Change

Setting	Description	Factory Default
Enabled	Enable the Data Change function.	Enabled
Disabled	Disable the Data Change function.	

Data Update

Setting	Description	Factory Default
Enabled	Enable the Data Update function.	Disabled
Disabled	Disable the Data Update function.	

Quality Change

Setting	Description	Factory Default
Enabled	Enable the Quality Change function.	Disabled
Disabled	Disable the Quality Change function.	

Integrity

Setting	Description	Factory Default
Enabled	Enable the Integrity function.	Enabled
Disabled	Disable the Integrity function.	

Buffer Time

Setting	Description	Factory Default
1 to 4294967295 (ms)	Provide the buffer time value.	1000

Integrity Period

Setting	Description	Factory Default
1 to 4294967295 (ms)	Provide the integrity period value.	5000

When finished, select **APPLY** to save your changes.

Exporting CID File

To export the CID file, select **EXPORT CID FILE**.



The file will be downloaded to your local computer.

Security Settings

Select the **Security** tab, where you can view the information for **T-Profile** and **A-Profile** Certificates.

MMS

General

Security

T-Profile Certificate Information

CA Name
moxa

Expired Date
2200-08-06 06:54:19

A-Profile Certificate Information

CA Name
moxa

Expired Date
2200-08-06 06:54:19

T-Profile Security

T-Profile Security *

Disabled

Import Client CA

Import Client Certificate

APPLY

EXPORT SERVER CA

EXPORT SERVER CERTIFICATE

T-Profile Security Settings

Configure the following settings for T-Profile Security.

T-Profile Security

T-Profile Security *
Disabled

Import Client CA

Import Client Certificate

APPLY

EXPORT SERVER CA

EXPORT SERVER CERTIFICATE

T-Profile Security

Setting	Description	Factory Default
Enabled	Enable T-Profile Security.	Disabled
Disabled	Disable T-Profile Security.	

Import Client CA

Setting	Description	Factory Default
Select the import icon  on the right.	Import Client CA file from your local computer	None

Import Client Certificate

Setting	Description	Factory Default
Select the import icon  on the right.	Import Client Certificate file from your local computer	None

When finished, select **APPLY** to complete.

Export Server CA

To export the Server CA, select **EXPORT SERVER CA**, the file will be downloaded to your local computer.

EXPORT SERVER CA

Export Server Certificate

To export the Server Certificate, select **EXPORT SERVER CERTIFICATE**, the file will be downloaded to your local computer.

EXPORT SERVER CERTIFICATE

A-Profile Security Settings

Configure the following settings for A-Profile Security.

A-Profile Security

A-Profile Security *
Disabled

Import Client CA

Import Client Certificate

APPLYEXPORT SERVER CAEXPORT SERVER CERTIFICATE

A-Profile Security

Setting	Description	Factory Default
Enabled	Enable A-Profile Security	Disabled
Disabled	Disable A-Profile Security	

Import Client CA

Setting	Description	Factory Default
Select the import icon on the right	Import Client CA file from your local computer	None

Import Client Certificate

Setting	Description	Factory Default
Select the import icon on the right	Import Client Certificate file from your local computer	None

When finished, select **APPLY** to complete.

Exporting Server CA

To export Server CA, select **EXPORT SERVER CA**. The file will be downloaded to your local computer.

EXPORT SERVER CA

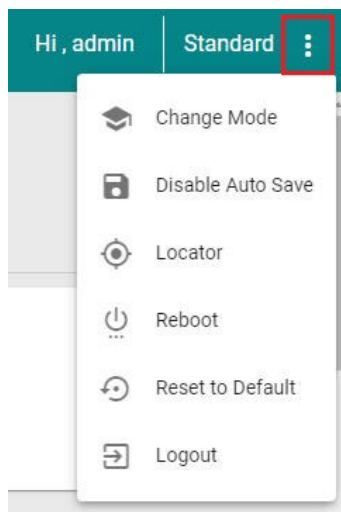
Exporting Server Certificate

To export Server Certificate, select **EXPORT SERVER CERTIFICATE**. The file will be downloaded to your local computer.

EXPORT SERVER CERTIFICATE

Maintenance and Tool

This section explains how to maintain the switch module and the tools that help you operate the switch. Select the icon on the upper right corner of the page.

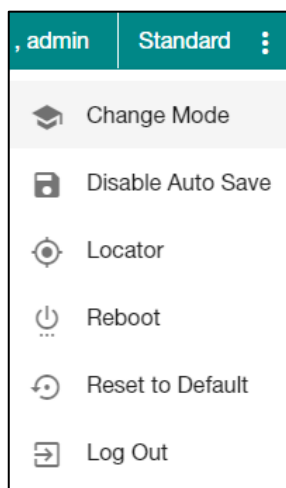


Standard/Advanced Mode

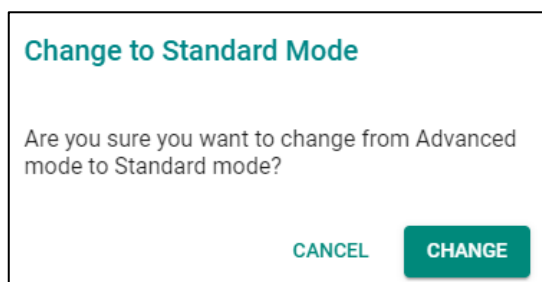
Two configuration modes are available: **Standard Mode** and **Advanced Mode**.

1. In **Standard Mode**, some of the features/parameters will be hidden to make it easier to perform configurations (this is the default setting).
2. In **Advanced Mode**, some advanced features/parameters will be available for you to adjust these settings.

To switch to Advanced Mode, select the change mode icon on the upper right corner of the page and then **Change Mode**.



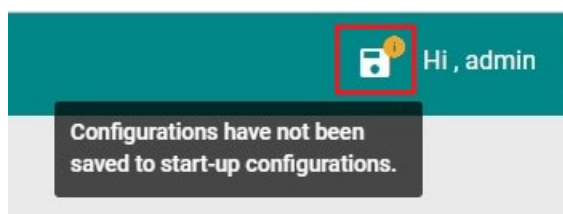
Select **CHANGE** to change to **Advanced Mode**.



Advanced Mode offers more detailed system configurations for specific functions. Use the same process if you want to return to Standard Mode.

Disable Auto Save

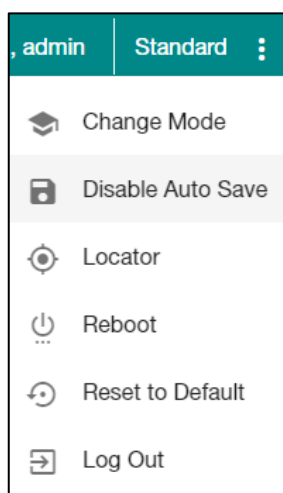
Auto Save allows you to save the settings to the start-up configurations; all parameters will be effective when applied immediately, even when the switch has restarted. When you select **Disable Auto Save**, all parameters will be temporarily stored in the running config (memory), and a disk icon will appear on the upper right corner of the page. You need to save the running-configuration to the startup-configuration when changing any parameters or function after selecting **Apply**.



It is highly recommended that you always manually save all configurations by selecting the Save Disk icon when **Disable Auto Save** is applied, or all information will have disappeared after the switch has restarted.

When **Disable Auto Save** is applied, only the configurations that are running will be saved; you can unplug the power or perform a warm recovery to the network before manually saving the configurations. When Auto Save is enabled, the start-up configurations will be saved in the switch.

To disable the **Auto Save** function, select **Disable Auto Save** in the menu.



Select **DISABLE**.

Disable Auto Save Mode

Are you sure you want to disable auto save mode?

CANCEL

DISABLE

Locator

You can trigger the device locator by selecting this icon. This will cause the LED indicators on the switch to flash for one minute. This helps you easily find the location of the switch on a field site.

, adminStandard

Change Mode

Disable Auto Save

Locator

Reboot

Reset to Default

Log Out

Select **LOCATE**.

Switch Locator

Duration *

60

30 - 300sec.

CANCEL

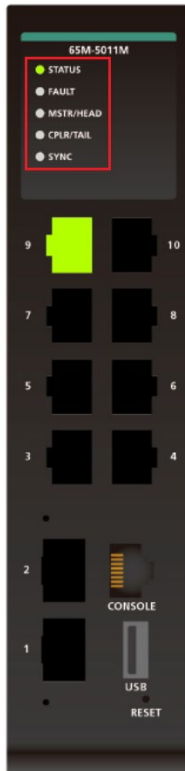
LOCATE

Duration (sec.)

Setting	Description	Factory Default
30 to 300	Specify the time the indicators will remain flashing.	60

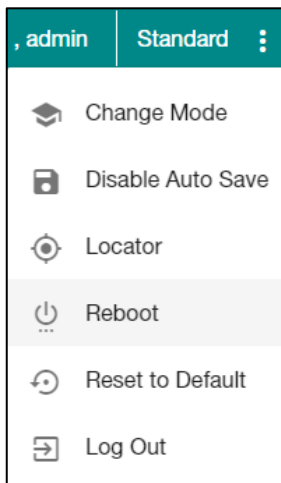
Select **LOCATE** to activate the switch locator.

The LED indicators are on the top of the front panel of the switch, as shown in the following figure.

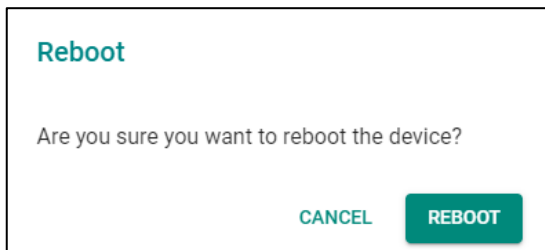


Reboot

To reboot the device, select **Reboot**.

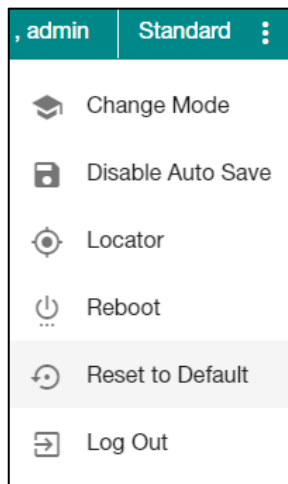


Select **REBOOT** to reboot the device.

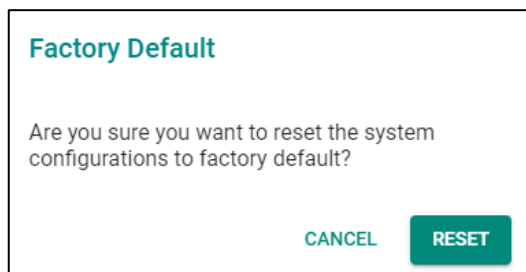


Reset to Default

To reset the switch to the default status, select **Reset to Default**.

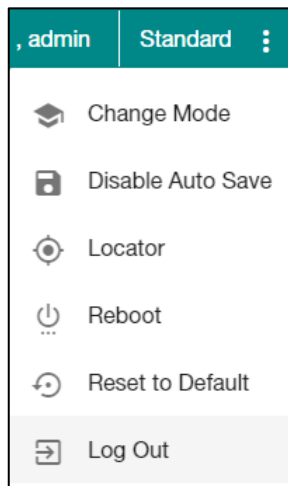


To return the switch to factory default settings, select **Reset**.



Log Out of the Switch

To log out of the switch, select **Log Out**.



Select **LOG OUT** to log out of the switch.

Log Out

Are you sure you want to log out?

CANCEL **LOG OUT**

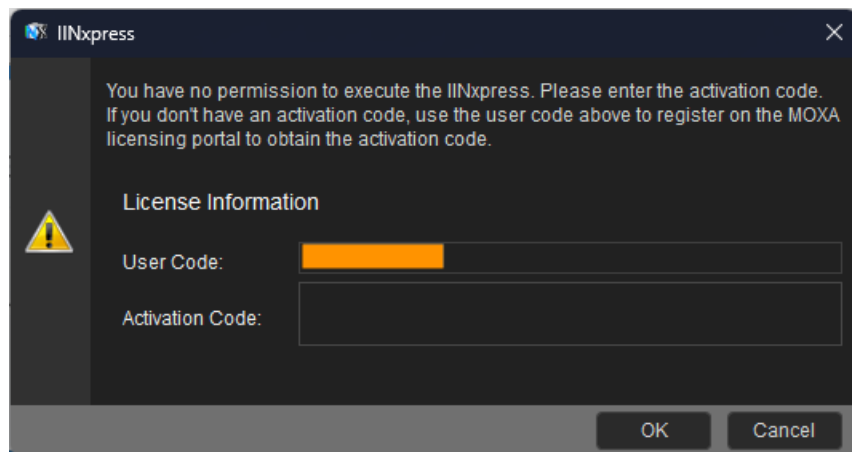
A. Activate and Transfer the IINxpress

In this appendix, we demonstrate how to activate the IINxpress and transfer the activation code between the IINxpress.

Activate the IINxpress

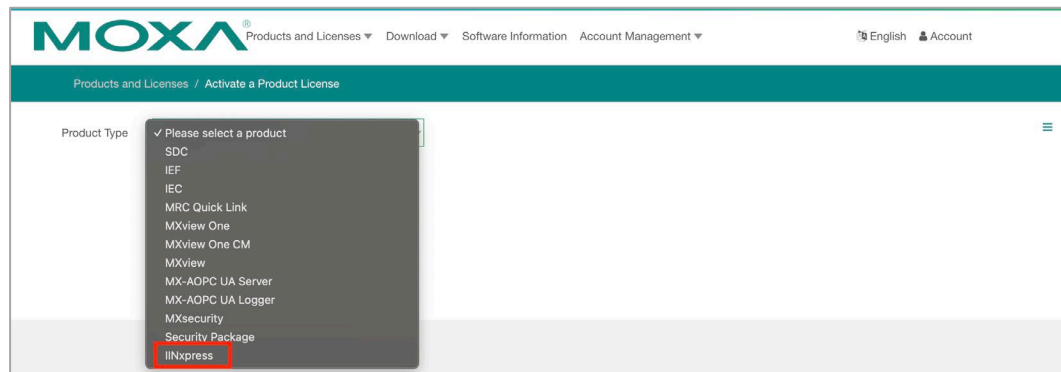
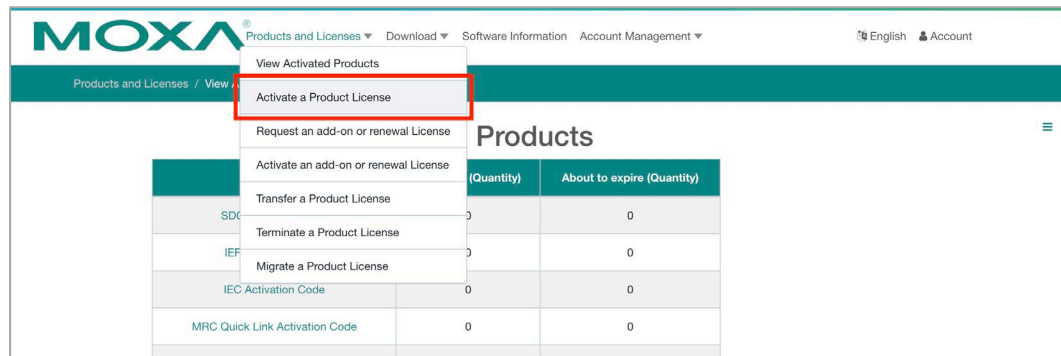
The activation code is needed to activate the IINxpress. Follow the steps to complete the activation in your computer.

- Step 1:** Contact Moxa sales representatives or Moxa official distributors to purchase the license of IINxpress. One computer is required for one license. Once the license procurement is complete, the **Registration Code** will be mailed to you.
- Step 2:** Download the IINxpress from the Moxa website (<https://www.moxa.com/>) and install in the computer. When a first-time user opens IINxpress, the user can find the **User Code** in the pop-up window.

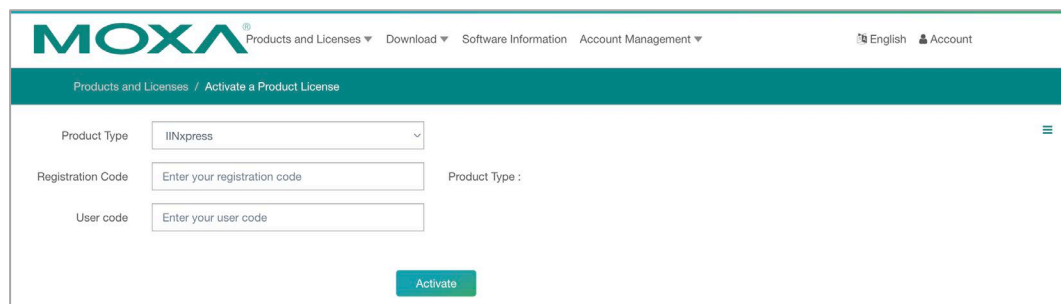


- Step 3:** Create an account on Moxa Software Licensing System. (<https://netsecuritylicense.moxa.com/Account/Login>)

Step 4: Go to **Products and Licenses > Activate a Product License** and select the **IINxpress**.



Step 5: Enter the Registration Code and User Code. Select the **Activate**.



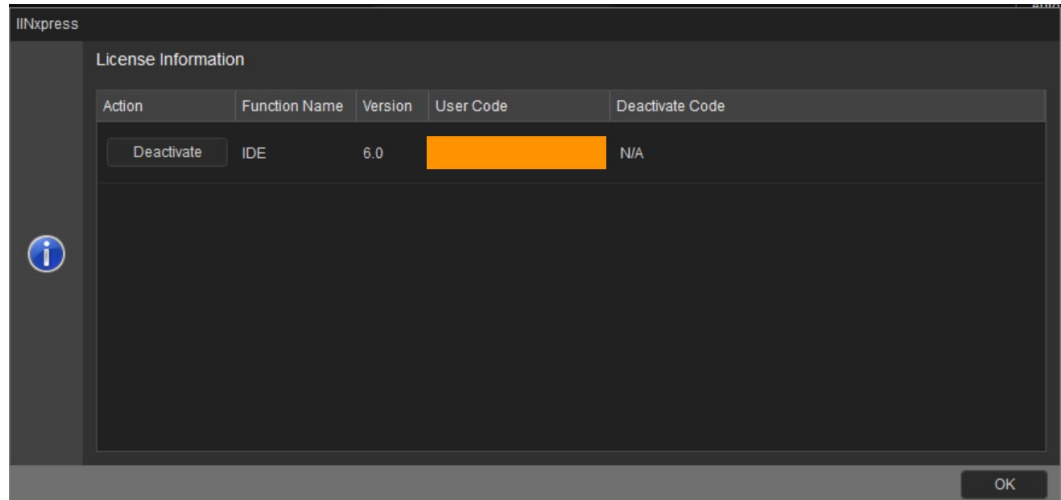
Step 6: If activated successfully, you will receive a mail notice with the **Activation Code**.

Step 7: Activate the IINxpress with the Activation Code.

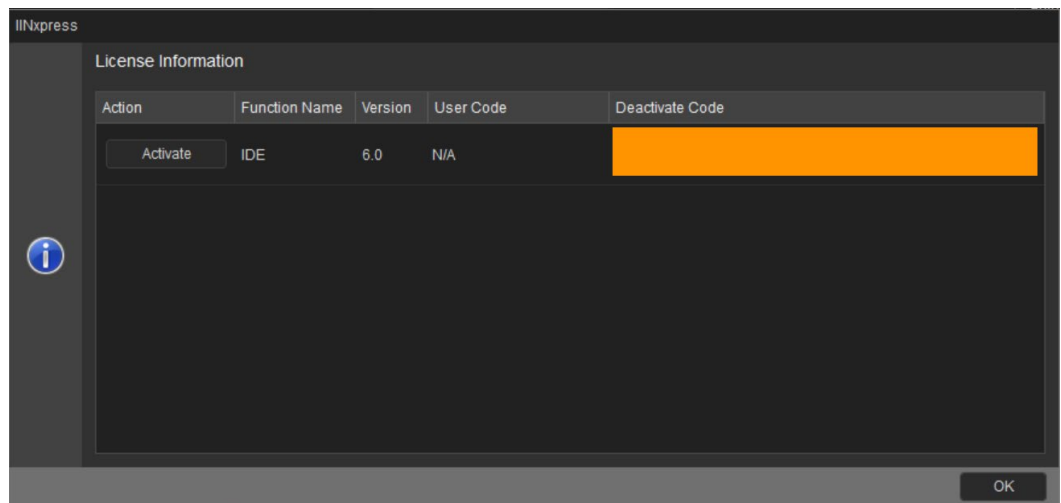
Transfer the Activation Code Between IINxpress

When you want to change the development environment to a new computer, the IINxpress can transfer to a new computer accordingly. Follow the steps to complete the transfer between the IINxpress.

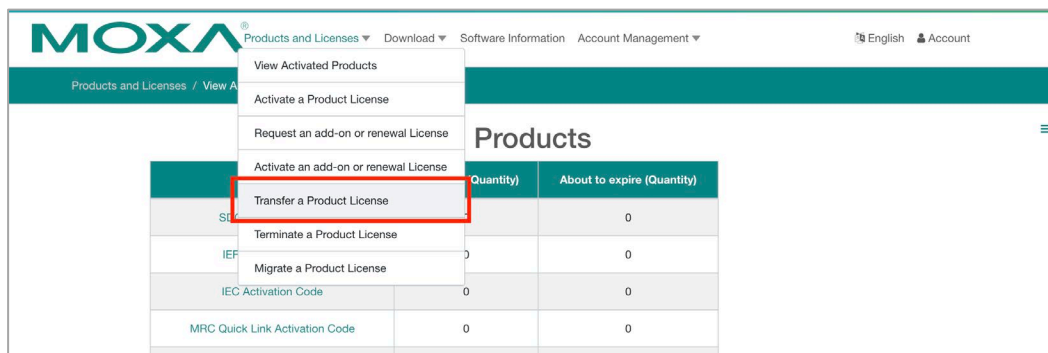
- Step 1:** Download the IINxpress and complete the installation on the new computer. Get the new User Code from the IINxpress on the new computer.
- Step 2:** Open the IINxpress on the old computer, go to **Help > License Information**, and launch the license management tool.



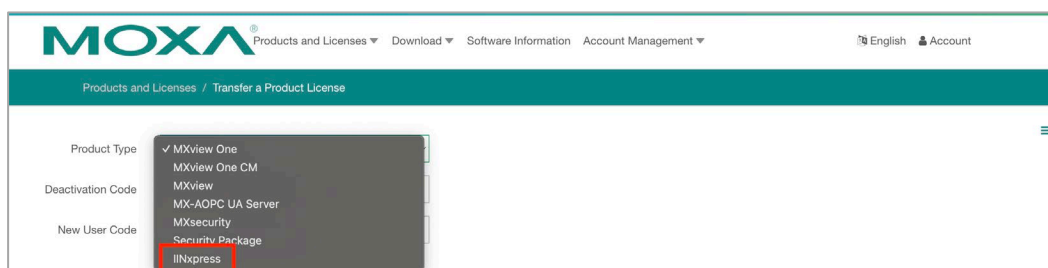
- Step 3:** Select the **Deactivate** button, the IINxpress will ask you to reconfirm again. Select OK and the IINxpress will provide a **Deactivation Code**.



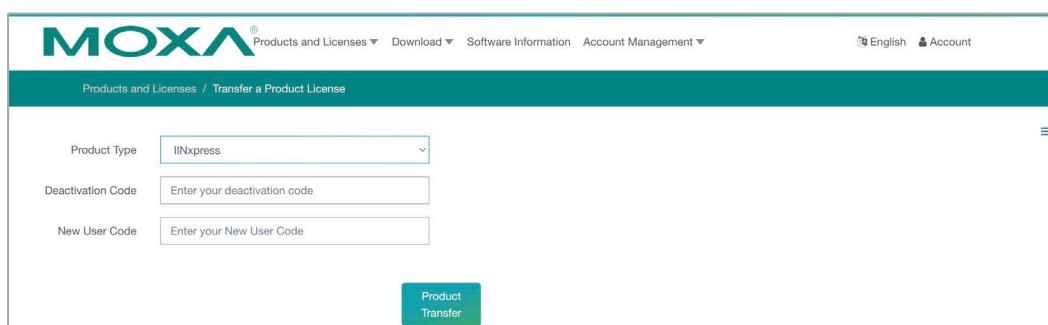
Step 4: Go to Moxa Software Licensing System and find the Transfer page via **Products and Licenses > Transfer a Product License**.



Step 5: Select the IINxpress.



Step 6: Enter the Deactivation Code and New User Code. Then, select the **Product Transfer**.



Step 7: If the transfer is successful, you will receive a mail notice with new **Activation Code**.

Step 8: Activate the IINxpress on a new computer with the new Activation Code.

B. Account Privileges List of 65M-5011M (Managed Switch Module)

This appendix describes the read/write access privileges for different accounts on the ioPAC 6500 Layer 2 Managed Ethernet Switch Module.

Account Privileges List

This appendix lists the privileges for different account roles.

Note, **R** stands for **Read** and **W** stands for **Write**.

Function	Account Privilege		
System	Admin	Supervisor	User
Information Setting	R/W	R/W	R/W
Firmware Upgrade	Execute	No Access	No Access
Configuration Backup and Restore (including File Signature)	Execute	No Access	No Access
Event log backup	Execute	Execute	Execute
User Account	R/W	No Access	No Access
Password Policy	R/W	No Access	No Access
Online Accounts	R/w	No Access	No Access
IP Configuration	R/W	R/W	R
DHCP Server	R/W	R/W	R
Time Zone	R/W	R/W	R
System Time	R/W	R/W	R
Port			
Port Setting	R/W	R/W	R
Linkup Delay	R/W	R/W	R
Link Aggregation (Port Channel)	R/W	R/W	R
VLAN			
IEEE 802.1Q	R/W	R/W	R
GARP	R/W	R/W	R
MAC			
Static Unicast	R/W	R/W	R
MAC Address Table	R/W	R/W	R
QoS			
Classification	R/W	R/W	R
Ingress Rate Limit (port shutdown only)	R/W	R/W	R
Scheduler	R/W	R/W	R
Multicast			
IGMP Snooping	R/W	R/W	R
Static Multicast	R/W	R/W	R
GMRP	R/W	R/W	R
Layer 2 Redundancy			
Spanning Tree	R/W	R/W	R
Turbo Ring v2	R/W	R/W	R
Turbo Chain	R/W	R/W	R
Dual Homing	R/W	R/W	R
Network Management			
SNMP	R/W	No Access	No Access
SNMP Trap/Inform	R/W	No Access	No Access

Function	Account Privilege		
Security	Admin	Supervisor	User
Management Interface	R/W	R/W	R
Login Policy	R/W	R	R
Trusted Access	R/W	R/W	R
SSH & SSL	Execute	Execute	No Access
IEEE802.1X	R/W	R/W	R
Port Security	R/W	R/W	R
Traffic Storm Control	R/W	R/W	R
Authentication			
RADIUS	R/W	No Access	No Access
TACACS+	R/W	No Access	No Access
Login Authentication	R/W	No Access	No Access
Diagnostics			
Event Notification	R/W	R/W	R
Email Notification	R/W	R	R
Syslog (including authentication)	R/W	R	R
Event Log	R/W	R/W	R
LLDP	R/W	R/W	R
Port Mirror	R/W	R/W	R
Ping	Execute	Execute	Execute
ARP Table	R	R	R
Utilization	R	R	R
Statistics	R/W	R/W	R
Maintenance and Tool			
Standard/Advance Mode	Execute	Execute	Execute
Disable Auto Save	R/W	R/W	R
Locator	R/W	R/W	Execute
Reboot	Execute	Execute	No Access
Reset to Default	Execute	Execute	No Access
Logout	Execute	Execute	Execute

C. Event Log Description of 65M-5011M (Managed Switch Module)

This appendix describes all the information for the event logs. When an event occurs, it will be recorded in the event log files. Check the event log name and its event log description.

Event Log Description

Event Name	Severity	Event Description
802.1X Auth Failed	Warning	802.1x authentication failed on port {{index}}/{{number}} with {{buffer}}
ABC-02 is inserted or unplugged	Notice	ABC-02 is {{inserted/unplugged}}.
Account log out	Notice	[Account:{{user_name}}] logged out.
Account removed	Notice	[Account:{{user_name}}] has been removed by admin.
Account settings changed	Notice	Account settings of [Account:{{user_name}}] has been updated. Account settings of [Account:{{user_name}}] has been deleted. Account settings of [Account:{{user_name}}] has been created.
Announce message with different interval	Warning	An Announce message with a different interval has been received from port {{index}}/{{number}}
Check if hardware revision is valid	Notice	The hardware revision of Power Module {{index}} is not allowed.
Cold start	Critical	System has performed a cold start.
Configuration changed	Notice	Configuration {{modules}} changed by {{username}}.
Configuration exported	Notice	Configurations exported {{successful /failed}} by {{username}} via {{method}}.
Configuration imported	Notice	Configuration import {{successful /failed}} by {{username}} via {{method}}.
Coupling changed	Warning	Turbo Ring v2 coupling path status has changed.
dhcpsnp untrust mac discards	Warning	VLAN {{Vlan Id}} dropped packets due to violation of DHCP Snooping rule. Total mac discards: {{number}}.
dhcpsnp untrust server discards	Warning	VLAN {{Vlan Id}} dropped packets due to a violation of the DHCP Snooping rule. Total server discards: {{number}}.
Dual homing path changed	Warning	Dual Homing path has switched.
Event log export	Notice	Event Log export {{successful /failed}} by {{username}} via {{method}}.
Firmware upgrade failed	Warning	Firmware failed to upgrade.
Firmware upgrade successful	Notice	Firmware successfully upgraded
Hardware revision is not allowed	Error	The hardware revision of Line Module %d is not allowed.
Interface link down	Notice	Interface{{number}} down.
Interface link up	Notice	Interface {{number}} up.
LLDP table changed	Info	LLDP remote table has changed.
Log capacity threshold	Warning	Number of event log entries {{logEntryNum}} has reached the threshold.

Event Name	Severity	Event Description
Log Turbo Chain Port Restart	Notice	Port-Channel {{channel id}} has restarted by Turbo Chain. Port {{index}}/{{number}} has restarted by Turbo Chain.
Login failed	Warning	[Account {{user_name}}] log in failed via {{interface}}.
Login lockout	Warning	[Account {{user_name}}] locked due to {{failed_times}} failed login attempts.
Login successful	Notice	[Account {{user_name}}] successfully logged in via {{interface}}.
Master changed	Warning	Ring {{Index}} client has changed.
Master mismatch	Warning	Ring {{Index}} client setting does not match.
MSTP new port role	Warning	MSTP (MST{{Index}}) port {{number}} role changed from {{role}} to {{role}}.
MSTP root changed	Warning	MSTP (MST{{Index}}) new root has been elected in topology.
MSTP topology changed	Warning	Topology (MST{{Index}}) has been changed by MSTP.
Packet dropped by Port Security	Warning	Port {{index}}/{{number}} dropped packets due to violation of Port Security rule.
Password changed	Notice	Password of [Account: {{user_name}}] has been changed.
Port Link Down	Notice	Port {{index}}/{{number}} link down. Port-channel {{Channel id}} link down.
Port Link Up	Notice	Port {{index}}/{{number}} link up. Port-channel {{Channel id}} link up.
Port recovery by Rate Limit	Warning	Port {{index}}/{{number}} has recovered by rate limit.
Port shutdown by Loop	Critical	Port {{index}}/{{number}} looping and shutdown.
Port shutdown by Port Security	Warning	Port {{index}}/{{number}} has shut down due to a violation of the Port Security rule.
Port shutdown by Rate Limit	Warning	Port {{index}}/{{number}} has excessive traffic and shutdown.
Power Off->On	Notice	Power {{index}} has turned off.
Power On->Off	Notice	Power {{index}} has turned on.
Redundant port health check failed	Error	Redundant port {{index}}/{{number}} health check fail.
RMON failing alarm	Warning	{{user defined}}.
RMON raising alarm	Warning	{{user defined}}.
RSTP invalid BPDU	Warning	RSTP Port-Channel {{channel id}} received an invalid BPDU (type: {{type}}, value: {{value}}). RSTP port {{index}}/{{number}} received an invalid BPDU (type: {{type}}, value: {{value}}).
RSTP migration	Warning	Port-Channel {{channel id}} changed to {{rstp/stp}}. Port {{index}}/{{number}} changed to {{rstp/stp}}.
RSTP new port role	Warning	RSTP Port-Channel {{channel id}} role changed from {{role}} to {{role}}. RSTP port {{index}}/{{number}} role changed from {{role}} to {{role}}.
RSTP root changed	Warning	RSTP new root has been elected in topology.
RSTP topology changed	Warning	Topology has been changed by RSTP.
SSH Key generated	Notice	SSH key has been regenerated.
SSL certification changed	Notice	SSL certificate has been changed. SSL certificate has been regenerated.
Topology changed (RSTP)	Warning	Topology has been changed by RSTP.
Topology changed (Turbo Chain)	Warning	Topology has been changed by Turbo Chain.

Event Name	Severity	Event Description
Topology changed (Turbo Ring)	Warning	Topology change has been detected on Ring {{RingIndex}} of Turbo Ring v2.
Topology changed (MSTP)	Warning	Topology (MST{{Index}}) has been changed by MSTP.
Warm start	Notice	System has performed a warm start.
When the trust host moves, it will send a log to Moxa log handler.	Warning	A trust host, MAC is {{mac address}} with VLAN {{Vlan Id}}, moved from port {{index}}/{{number}} to port {{index}}/{{number}}.

D. SNMP MIB File of 65M-5011M (Managed Switch Module)

This appendix contains the SNMP MIB file for the managed switch.

Standard MIB Installation Order

If you need to import the MIB one-by-one, install the MIBs in the following order.

1. RFC1213-MIB.mib
2. SNMP-FRAMEWORK-MIB.mib
3. SNMPv2-SMI.mib
4. SNMPv2-TC.mib
5. SNMPv2-CONF.mib
6. SNMPv2-MIB.mib
7. IANAifType-MIB.mib
8. IEEE8023-LAG-MIB.mib
9. IF-MIB.mib
10. EtherLike-MIB.mib
11. IEEE8021-PAE-MIB.mib
12. BRIDGE-MIB.mib
13. P-BRIDGE-MIB.mib
14. RFC1271-MIB.mib
15. RMON-MIB.mib
16. TOKEN-RING-RMON-MIB.mib
17. RMON2-MIB.mib
18. Q-BRIDGE-MIB.mib
19. INET-ADDRESS-MIB.mib
20. IEEE8021-TC-MIB.mib
21. IEEE8021-SPANNING-TREE-MIB.mib
22. IANA-ADDRESS-FAMILY-NUMBERS-MIB.mib
23. LLDP-MIB.mib
24. LLDP-EXT-DOT1-MIB.mib
25. LLDP-EXT-DOT3-MIB.mib

MIB Tree

Refer to the following content for the MIB Tree structure.

```
iso(1)
|-std(0)-iso8802(8802)-ieee802dot1(1)-ieee802dot1mibs(1)
    |-ieee8021paeMIB(1): IEEE8021-PAE-MIB.mib
    |-ieee8021SpanningTreeMib(3): IEEE8021-SPANNING-TREE-MIB.mib
|-org(3)
|-dod(6)-internet(1)
    |-mgmt(2)-mib-2(1): SNMPv2-MIB.mib
        |-system(1): RFC1213-MIB.mib
            |-interface(2): RFC1213-MIB.mib
        |-at(3): RFC1213-MIB.mib
        |-snmp(11): RFC1213-MIB.mib
        |-rmon(16): RMON-MIB.mib
        |-dot1dBridge(17): BRIDGE-MIB.mib, P-BRIDGE-MIB.mib, Q-BRIDGE-MIB.mib
        |-ifMIB(31): IF-MIB.mib
        |-etherMIB(35): EtherLike-MIB.mib
|-private(4)-moxa(8691)
    |-product(600): mxGeneralInfo.mib, mxProductInfo.mib,
    |-general(602): mxGeneral.mib, mxDeviceIo.mib, mxDhcpSvr.mib, mxEmailC.mib,
        mxEventLog.mib,
        : mxGene.mib, mxLocator.mib, mxManagementIp.mib, mxPorte.mib,
        : mxSnmp.mib, mxSwe.mib, mxSysLoginPolicySvr.mib,
        : mxSyslogSvr.mib, mxSysPasswordPolicySvr.mib, mxSystemInfo.mib,
        : mxSysTrustAccessSvr.mib, mxSysUtilSvr.mib, mxTimeSetting.mib,
        : mxTimeZone.mib, mxTrapC.mib, mxUiServiceMgmt.mib
    |-switching(603): mxSwitching.mib
        |- portInterfacce : mxPort.mib, mxLa.mib
        |- basicLayer2: mxLhc.mib, mxQos, mxVlan.mib
        |- layer2Redundancy: mxRstp.mib, mxTrv2.mib, mxTurboChain.mib,
            mxDualHoming.mib
        |- layer2Security: mxStcl.mib, mxRlps.mib, mxPssp.mib, mxPsms.mib, mxDot1x.mib,
            mxRadius.mib
        |- layer2Diagnostic: mxLldp.mib, mxTcst.mib, mxPortMirror.mib, mxRmon.mib
        |- layer2Multicast: mxIgmpSnp.mib
|-snmpV2(6)-snmpModules(3)
    |-snmpFrameworkMIB(10): SNMP-FRAMEWORK.mib
|-ieee(111)-standards-association-numbers-series-standards(2)-lan-man-stds(802)-ieee802dot1(1)-
    ieee802dot1mibs(1)-ieee8021SpanningTreeMib(3): IEEE8021-SPANNING-TREE-MIB.mib
```

E. Security Guidelines of 65M-5011M (Managed Switch Module)

This appendix explains security practices for installing, operating, maintaining, and decommissioning the device. We strongly recommend that our customers follow these guidelines to enhance network and equipment security.

Installation

Physical Installation

1. The device **MUST** be installed in an access-controlled area, where only the necessary personnel have physical access to the device.
2. The device **MUST NOT** be directly connected to the Internet, which means switches **MUST** be installed within a security perimeter, which can be implemented by a firewall at the border since the device is not classified as zone/boundary equipment.
3. Follow the instructions in the Quick Installation Guide, which is included in the package, to ensure you install the device correctly in your environment.
4. The device has anti-tamper labels on the enclosures. This allows an administrator to tell whether the device has been tampered with.
5. The ports that are not in use should be deactivated. Refer to **Port Interface** section for detailed instructions.

Account Management

Follow these best practices when setting up an account.

1. Each account should be assigned the correct privileges: Only allow the minimum number of people to have admin privilege so they can perform device configuration or modifications, while other users should only have read access privilege. The device supports both local account authentication and remote centralized mechanism, including Radius and TACACS+.
2. Change the default password, and strengthen the account password complexity by:
 - a. Enabling the "Password Policy" function.
 - b. Increasing the minimum password length to at least eight characters.
 - c. Defining a password policy to ensure that it contains at least an uppercase and lowercase letter, a digit, and a special character.
 - d. Setting user passwords to expire after a certain period.
3. Enforce regulations that ensure that only a trusted host can access the device. Refer to the **Trusted Access** section for detailed instructions.

Vulnerable Network Ports

1. For network security concerns, we strongly recommend that you change the port numbers, such as TCP port numbers for HTTP, HTTPS, Telnet, and SSH, for the protocols that are in use; ports that are not in use but are still reachable pose an unacceptable security risk and should be disabled. Refer to the **Management Interface** section for detailed instructions.
2. To avoid eavesdropping from snooping confidential information, you should adopt encryption-based communication protocols, such as HTTPS instead of HTTP, SSH instead of Telnet, SFTP instead of TFTP, SNMPv3 instead of SNMPv1/v2c, etc. In addition, the maximum number of sessions should be kept to an absolute minimum. Refer to **Management Interface** section for detailed instructions.
3. Generate the SSL certificate for the device before commissioning HTTPS or SSH applications. Refer to **SSH & SSL** section for detailed instructions.

Operation

1. To ensure that communications are properly protected, use a strong cryptographic algorithm for key exchange or encryption protocols for HTTPS/SSH applications. The device follows the NIST SP800-52 and SP800-131 standards and supports TLS v1.2 and v1.3 with the following cipher suites:

TLS V1.2				
Cipher suite name	Key exchange	Authentication	Encryption	Hash function
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE	RSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE	ECDSA	AES128	SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE	RSA	AES128	SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE	RSA	AES256	SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Ephemeral DH	RSA	AES128	SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Ephemeral DH	RSA	AES256	SHA384
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Ephemeral DH	RSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE-RSA_WITH_AES256-SHA384	ECDHE	RSA	AES256	SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE	RSA	AES128	SHA256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE	ECDSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE	RSA	AES256	SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE	ECDSA	AES256	SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE	ECDSA	AES128	SHA256

TLS V1.3				
Cipher suite name	Key exchange	Encryption	Mode	Hash function
TLS_AES_256_GCM_SHA384	any	AES256	GCM	SHA384
TLS_CHACHA20_POLY1305_SHA256	any	CHACHA20-POLY1305	N/A	SHA256
TLS_AES_128_GCM_SHA256	any	AES128	GCM	SHA256

2. Below is a list of the recommended secure browsers that support TLS v1.2 or above:

Browser	Version
Microsoft Edge	All
Microsoft Internet Explorer	v11 or above
Mozilla Firefox	v27 or above
Google Chrome	v38 or above
Apple Safari	v7 or above

Reference: <https://support.globalsign.com/ssl/general-ssl/tls-protocol-compatibility#Browsers>

3. The device supports event logs and syslog for SIEM integration:
- Event log: Because of limited storage capacity, the event log can only accommodate a maximum of 10,000 entries. Administrators can set a warning for a pre-defined threshold. We recommend that you regularly back up system event logs. Refer to **Event Log** section for detailed instructions.
 - Syslog: the device supports syslog, and advanced secure TLS-based syslog for centralized SIEM integration. Refer to **Syslog Settings** section for detailed instructions.
4. The device can provide information for control system inventory:
- SNMPv1, v2c, v3: We recommend administrators use SNMPv3 with authentication and encryption to manage the network. Refer to the **MIB File** for detailed instructions.
 - Telnet/SSH: We recommend that administrators use SSH with authentication and encryption to retrieve device properties.
 - HTTP/HTTPS: We recommend that administrators use HTTPS with a certificate that has been granted by a Certificate Authority to configure the device.
5. Denial of Service protection: To avoid disruption of normal operation of the switch, administrators should configure the QoS function. The device supports the ingress rate limit and egress shaped. Administrators can decide how to deal with excess data flow and configure the device accordingly. This process will regulate the resulting data rate per port. Refer to **QoS** section for detailed instructions.
6. Time synchronization with authentication: Time synchronization is crucial for process control. To prevent malicious attacks, whereby the settings are changed without permission, authentication must be in place between the NTP server and client. The device supports NTP with a pre-shared key. Refer to **NTP** section for detailed instructions.
7. Periodically regenerate the SSH and SSL certificates: Even though the device supports RSA 2048-bit and SHA-256 to ensure sufficient complexity, we strongly recommend that you frequently renew their SSH key and SSL certificate in case the key is compromised. Refer to **SSH & SSL** section for detailed instructions.
8. Below is the list of the protocol port numbers used for all external interfaces.

Protocol	Service Type	Port Number
TCP	SSH	22
	Telnet	23
	HTTP	80
	HTTPS	443
UDP	DHCP	67
	NTP	123
	SNMP	161
	Moxa Service	40404

Maintenance

- Perform firmware upgrades frequently to enhance features, deploy security patches, or fix bugs.
- Frequently back up the system configurations: In order to properly protect the system configuration files from being tampered with, the device supports password encryption and signature authentication for backup files.
- Examine event logs frequently to detect any anomalies.
- To report vulnerabilities of Moxa products, submit your findings on the following web page: <https://www.moxa.com/en/support/product-support/security-advisory/report-a-vulnerability>.

Decommission

To avoid any sensitive information such as your account password or certificate from being disclosed, always reset the system settings to factory default before decommissioning the device.

F. SFP Module List of 65M-5011M (Managed Switch Module)

This appendix lists the supported SFP module for the managed switch module

Model	Description
SFP-1GLHLC-T	SFP module with 1 1000BaseLH port with LC connector for 30 km transmission, -40 to 85°C operating temperature
SFP-1GLSXLC-T	SFP module with 1 1000BaseLSX port with LC connector for 1km/2km transmission, -40 to 85°C operating temperature
SFP-1GLXLC-T	SFP module with 1 1000BaseLX port with LC connector for 10 km transmission, -40 to 85°C operating temperature
SFP-1GSXLC-T	SFP module with 1 1000BaseSX port with LC connector for 300m/550m transmission, -40 to 85°C operating temperature
SFP-1GZXLC-T	SFP module with 1 1000BaseZX port with LC connector for 80 km transmission, -40 to 85°C operating temperature
SFP-1G10ALC-T	WDM-type (BiDi) SFP module with 1 1000BaseSFP port with LC connector for 10 km transmission; TX 1310 nm, RX 1550 nm, -40 to 85°C operating temperature
SFP-1G10BLC-T	WDM-type (BiDi) SFP module with 1 1000BaseSFP port with LC connector for 10 km transmission; TX 1550 nm, RX 1310 nm, -40 to 85°C operating temperature
SFP-1G20ALC-T	WDM-type (BiDi) SFP module with 1 1000BaseSFP port with LC connector for 20 km transmission; TX 1310 nm, RX 1550 nm, -40 to 85°C operating temperature
SFP-1G20BLC-T	WDM-type (BiDi) SFP module with 1 1000BaseSFP port with LC connector for 20 km transmission; TX 1550 nm, RX 1310 nm, -40 to 85°C operating temperature
SFP-1G40ALC-T	WDM-type (BiDi) SFP module with 1 1000BaseSFP port with LC connector for 40 km transmission; TX 1310 nm, RX 1550 nm, -40 to 85°C operating temperature
SFP-1G40BLC-T	WDM-type (BiDi) SFP module with 1 1000BaseSFP port with LC connector for 40 km transmission; TX 1550 nm, RX 1310 nm, -40 to 85°C operating temperature
SFP-1FELLC-T	SFP module with 1 100Base single-mode with LC connector for 80 km transmission, -40 to 85°C operating temperature
SFP-1FEMLC-T	SFP module with 1 100Base multi-mode with LC connector for 2/4 km transmission, -40 to 85°C operating temperature
SFP-1FESLC-T	SFP module with 1 100Base single-mode with LC connector for 40 km transmission, -40 to 85°C operating temperature