

ioLogik 2500 Series User's Manual

Third Edition, July 2015

www.moxa.com/product

MOXA®

© 2015 Moxa Inc. All rights reserved.

ioLogik 2500 Series User's 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

© 2015 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

Moxa Americas

Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa Europe

Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa India

Tel: +91-80-4172-9088
Fax: +91-80-4132-1045

Moxa China (Shanghai office)

Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

Moxa Asia-Pacific

Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Table of Contents

1. Overview	1-1
ioLogik 2500 Overview	1-2
Appearance	1-2
Dimensions Diagram	1-3
Package Checklist	1-3
Product Features	1-3
I/O Channels Available on ioLogik 2500 Models	1-3
Communication Interface	1-4
Product Specifications	1-4
Common Specifications	1-4
ioLogik 2512 Specifications	1-6
ioLogik 2542 Specifications	1-7
2. Installation	2-1
Hardware Installation	2-2
Installing the ioLogik 2500 on a DIN Rail	2-2
Removing the ioLogik 2500 from a DIN Rail	2-2
Powering on the ioLogik 2500	2-3
Grounding the Unit	2-3
Installing a microSD Card and SIM Cards (cellular models only)	2-3
I/O Wiring Diagrams	2-3
LED Indicators	2-4
Daisy-Chaining for I/O Expansion	2-4
Reset to Factory Defaults	2-6
Network Installation	2-6
Ethernet Communication	2-6
TCP/IP Settings	2-6
Serial Communication	2-7
Installing the IOxpress Utility	2-7
System Requirements	2-7
Installing IOxpress from the CD	2-7
Installing IOxpress from the Internet	2-8
3. The IOxpress Utility	3-1
Introduction	3-2
Application Interface	3-2
Using IOxpress	3-3
Offline Configuration	3-3
Creating a Project	3-3
Adding an ioLogik 2500 Device to a Project	3-4
Adding E1200 Devices to a Project	3-4
Setting Up a Device	3-5
Settings	3-6
General Device Settings	3-6
Network	3-6
General	3-6
Click&Go Plus	3-21
Click&Go Plus Simulator	3-21
Peer-to-Peer	3-21
General Settings	3-22
P2P Rule Settings	3-23
Online Configuration	3-24
Introduction	3-24
Searching for Online Devices	3-25
Deploying Individual Devices	3-28
IO Status	3-28
4. Cellular Network Setup and Configuration (for cellular models)	4-1
IOxpress Settings for a Cellular Network	4-2
Select Major Network Interface	4-2
Cellular	4-3
Cellular Network Connection	4-10
MX-AOPC Server (for SCADA/HMI users)	4-10
With DDNS (for SCADA/HMI users)	4-11
Moxa Cellular Data Access Utility (for mobile devices/PCs)	4-11
5. Wireless LAN Network Setup and Configuration (for Wireless LAN models)	5-1
Deploying the ioLogik 2500-WL1	5-2
IOxpress Settings for a Wireless LAN Network	5-2
Wireless LAN	5-2

A. Network Port Usage A-1

The ioLogik 2500 is a smart remote I/O product with unique hardware and software designs, making it an ideal solution for a variety of industrial data acquisition applications. The ioLogik 2500's hardware design includes a 4-port unmanaged Ethernet switch and 2 serial ports, enabling the ioLogik 2500 to seamlessly connect to a variety of field devices. One of the Ethernet ports can be used to link to 8 daisy-chained ioLogik E1200 expansion modules to provide more than 100 channels. The ioLogik 2500 acts as the "head" unit, with Click&Go Plus logic used to control the entire I/O array. Most importantly, the ioLogik 2500's single IP is all that's required to connect the entire I/O array to your network, providing the perfect solution for industrial field sites that have an insufficient number of IP addresses.

For cellular connections, the ioLogik 2500 supports Moxa's patented MX-AOPC Server with push communications technology, and provides an economical solution for accessing multiple remote I/O devices connected to the same private IP network, which itself links to the outside world over a cellular connection using dynamic IP addresses.

The following topics are covered in this chapter:

▣ **ioLogik 2500 Overview**

- Appearance
- Dimensions Diagram
- Package Checklist
- Product Features
- I/O Channels Available on ioLogik 2500 Models
- Communication Interface

▣ **Product Specifications**

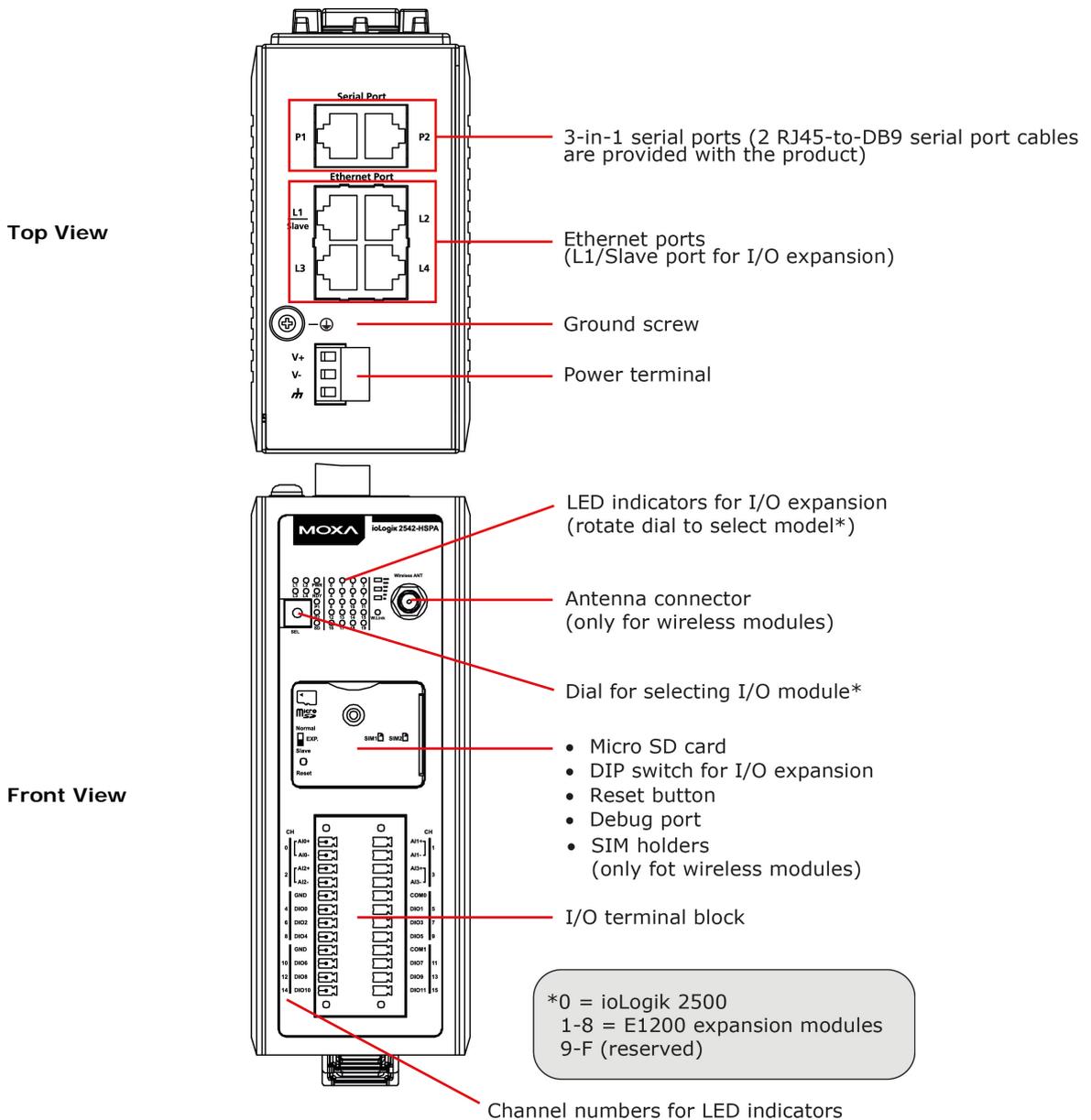
- Common Specifications
- ioLogik 2512 Specifications
- ioLogik 2542 Specifications

ioLogik 2500 Overview



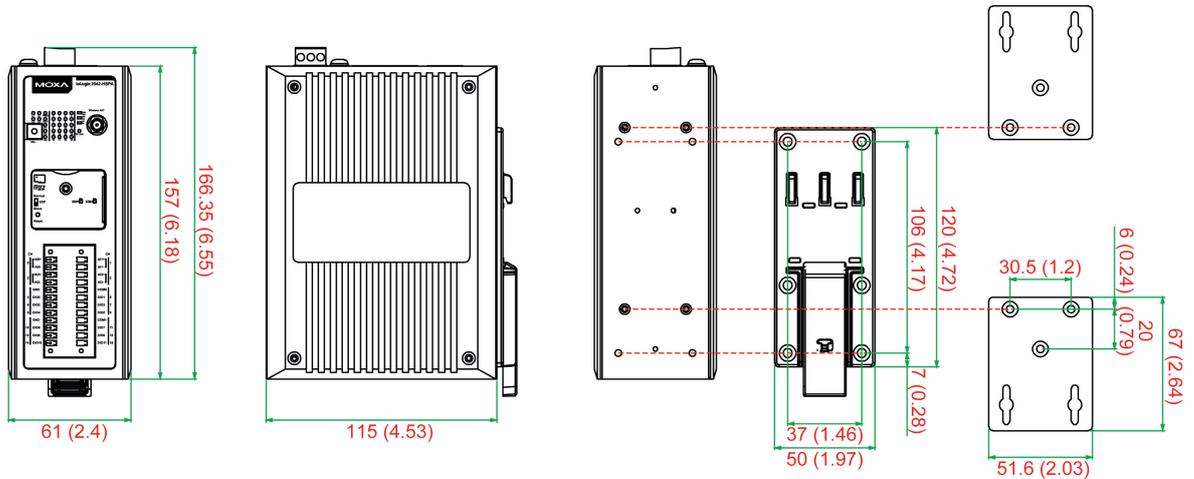
The ioLogik 2500 combines a remote I/O device and data logger into one box, dramatically reducing the amount of effort required to integrate devices from multiple vendors. I/O and serial data can be logged onto a Micro SD card (supports cards with up to 32 GB of storage space), and the ioLogik 2500 can be programmed with Moxa's convenient Click&Go™ Plus control logic, which can be used to easily construct customized control systems. As a rugged industrial device, the ioLogik 2500 operates reliably at a wide range of temperatures, and is well suited for hard-to-wire remote monitoring and alarm applications at unmanned sites like riversides and pipelines.

Appearance



Dimensions Diagram

Units: mm (in)



Package Checklist

The ioLogik 2500 is shipped with the following items:

- ioLogik 2500 series device
- 3-pin screw terminal block (for power input)
- 2 12-pin screw terminal blocks (for I/O)
- 2 8-pin RJ45-to-DB9 cables (CBL-RJ45M9-150)
- 1 antenna (only for wireless modules)
- Documentation and software CD
- Hardware installation guide

NOTE: Please notify your sales representative if any of the above items are missing or damaged.

Product Features

- Supports cellular (HSPA/GPRS), Ethernet, and serial communication (ioLogik 2500-HSPA/GPRS only)
- New Click&Go Plus logic provides powerful front-end intelligence
- Supports wireless LAN communication (ioLogik 2500-WL1 only)
- 4-port unmanaged switch built in for linking to Ethernet devices
- Optimized I/O expansion port for daisy chaining up to 8 ioLogik E1200 units
- 2 serial ports (RS-232/422/485) for connecting field devices
- Built-in data logger supports an FTP server/client and microSD™ card with up to a 32 GB
- Transforms Modbus RTU into Modbus TCP or Active Tags
- Active communication with patented MX-AOPC UA Server
- Smart alarm management: Email, SNMP traps, TCP, UDP, SMS
- Wide operating temperature: -40 to 75°C (-40 to 167°F)

I/O Channels Available on ioLogik 2500 Models

Model Name	Digital Inputs	DI/DO (DIO) Configurable	Analog Inputs
ioLogik 2512	8	8	–
ioLogik 2542	–	12	4

Communication Interface

Model Name	Communication Interface
ioLogik 2512 ioLogik 2542	Serial / Ethernet
ioLogik 2512-GPRS ioLogik 2542-GPRS	Serial / Ethernet / GPRS (2G)
ioLogik 2512-HSPA ioLogik 2542-HSPA	Serial / Ethernet / GPRS (2G) /HSPA (3G)
ioLogik 2512-WL1 ioLogik 2542-WL1	Serial / Ethernet / Wireless LAN

Product Specifications

Common Specifications

Cellular (ioLogik 2500-HSPA/GPRS only)

ioLogik 2500-HSPA:

- Five-Band UMTS/HSPA+ (WCDMA/FDD), 800/850/AWS1700/1900/2100 MHz
- Quad-band GSM/GPRS/EDGE, 850/900/1800/1900 MHz

ioLogik 2500-GPRS: • Quad-band GSM/GPRS/EDGE 850/900/1800/1900 MHz

HSPA data rates:

- Up to 5.76 Mbps upload speed (max.)
- Up to 14.4 Mbps download speed (max.)

EDGE Class 12 data rates:

- Up to 237 kbps upload speed (max.)
- Up to 237 kbps download speed (max.)

GPRS Class 12 data rates:

- Up to 85.6 kbps upload speed (max.)
- Up to 85.6 kbps download speed (max.)

SIM Control Voltage: 3.0/1.8 V

LAN

Ethernet:

- 4 switched 10/100 Mbps RJ45 ports
- 1 slave port for communications with daisy-chained ioLogik E1200 units

Note: The slave daisy-chain port is not supported on wind industry devices (ioLogik E1261W-T, E1261H-T, or E1263H-T).

Protection: 1.5 kV magnetic isolation

Protocols: Modbus/TCP, TCP/IP, UDP, DHCP, BOOTP, SNMP, HTTP, CGI, SNTP, SMTP

802.11 WLAN (For ioLogik 2512-WL1, ioLogik 2542-WL1)

Standards:

IEEE 802.11a/b/g for Wireless LAN

IEEE 802.11i for Wireless Security

Spread Spectrum and Modulation (typical):

- DSSS with DBPSK, DQPSK, CCK
- OFDM with BPSK, QPSK, 16QAM, 64QAM
- 802.11b/g: CCK @ 11/5.5 Mbps, DQPSK @ 2 Mbps, DBPSK @ 11 Mbps
- 802.11a/g: 64QAM @ 54/48 Mbps, 16 QAM @ 36/24 Mbps, QPSK @ 18/12 Mbps, BPSK @ 9/6 Mbps

Operating Channels (central frequency):

US: 2.412 to 2.462 GHz (11 channels), 5.18 to 5.24 GHz (4 channels)

EU: 2.412 to 2.472 GHz (13 channels), 5.18 to 5.24 GHz (4 channels)

Security:

Firewall for MAC, IP, protocol, or port-based filtering;
64- and 128-bit WEP encryption; full WPA/WPA2 Personal or
Enterprise Security (IEEE 802.1X/RADIUS, TKIP and AES)

Transmission Rates:

802.11b: 1, 2, 5.5, 11 Mbps
802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps

TX Transmit Power:

802.11b: Typ. 18 ± 1.5 dBm @ 1 to 11 Mbps
802.11g: Typ. 18 ± 1.5 dBm @ 6 to 24 Mbps, Typ. 17 ± 1.5 dBm @ 36 Mbps, Typ. 16 ± 1.5 dBm @ 48 Mbps,
Typ. 16 ± 1.5 dBm @ 54 Mbps
802.11a: Typ. 18 ± 1.5 dBm @ 6 to 24 Mbps, Typ. 16 ± 1.5 dBm @ 36 Mbps, Typ. 15 ± 1.5 dBm @ 48 Mbps,
Typ. 14 ± 1.5 dBm @ 54 Mbps

RX Sensitivity:

802.11b: -97 dBm @ 1 Mbps, -94 dBm @ 2 Mbps, -92 dBm @ 5.5 Mbps, -90 dBm @ 11 Mbps
802.11g: -88 dBm @ 6 to 24 Mbps, -85 dBm @ 36 Mbps, -75 dBm @ 48 Mbps, -70 dBm @ 54 Mbps
802.11a: -88 dBm @ 6 to 24 Mbps, -85 dBm @ 36 Mbps, -75 dBm @ 48 Mbps, -70 dBm @ 54 Mbps

Serial Communication

Serial Ports: 2, RJ45, 3-in-1 interface
Protocols: Modbus/RTU (master), serial tunnel mode (client/server)
Serial Line Protection: ≥ 8 kV ESD for all signals

Serial Communication Parameters

Parity: None, Odd, Even
Data Bits: 5, 6, 7, 8
Stop Bits: 1, 1.5, 2
Flow Control: None, RTS/CTS
Baudrate: 300 to 115200 bps
Protocol: Modbus/RTU

Power Requirements

Power Input: 24 VDC nominal, 9 to 48 VDC
Power Consumption:
ioLogik 2512: 340 mA @ 24 VDC
ioLogik 2542: 450 mA @ 24 VDC
ioLogik 2512-GPRS: 420 mA @ 24 VDC
ioLogik 2512-HSPA: 460 mA @ 24 VDC
ioLogik 2542-GPRS: 500 mA @ 24 VDC
ioLogik 2542-HSPA: 540 mA @ 24 VDC

Physical Characteristics

Wiring: I/O cable max. 14 AWG
Mounting: DIN rail, wall

Storage

Expansion Slot: Up to 32 GB microSD™ memory card (SDHC compatible)

Note: For units operating in extreme temperatures, industrial grade, wide-temperature SD cards are required.

Environmental Limits

Operating Temperature:
Standard Models: -10 to 60°C (14 to 140°F)
Wide Temp. Models: Ethernet: -40 to 75°C (-40 to 167°F)
Wireless: -30 to 70°C (-22 to 158°F)

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

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

Altitude: Up to 2000 m

Note: Please contact Moxa if you require products guaranteed to function properly at higher altitudes.

Standards and Certifications

Safety: UL 508, EN 60950-1, NCC

EMI: EN 55022; EN 61000-3-2; EN 61000-3-3; FCC Part 15, Subpart B, Class A

EMS: EN 55024, EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11, EN 61000-6-2

Radio: FCC Part 22H, FCC Part 24E, EN 301 489-1, EN 301 489-7, EN 301 511

Shock: IEC 60068-2-27

Fre fall: IEC 60068-2-32

Vibration: IEC 60068-2-6

Green Product: RoHS, CRoHS, WEEE

Note: Please check Moxa's website for the most up-to-date certification status.

Warranty

Warranty Period: 5 years

Details: See www.moxa.com/warranty

ioLogik 2512 Specifications

Inputs and Outputs

Digital Inputs: 8 channels

Configurable DI/DOs (DIO): 8 channels

Isolation: 3k VDC or 2k Vrms

Digital Input

Sensor Type: Wet Contact (NPN or PNP) and Dry Contact

Input Leakage Current: < 1 mA (@ 30 VDC)

I/O Mode: DI or Event Counter

Dry Contact:

- On: short to GND
- Off: open

Wet Contact (DI to COM):

- On: 10 to 30 VDC
- Off: 0 to 3 VDC

Common Type: 8 points per COM

Counter Frequency: 2.5 kHz

Digital Filtering Time Interval: Software configurable

Digital Output

Type: Sink

I/O Mode: DO or Pulse Output

Pulse Output Frequency: 5 kHz

Over-voltage Protection: 45 VDC

Over-current Protection: 1.5 A per channel @ 25°C

Over-temperature Shutdown: 175°C (min.)

Current Rating: 500 mA per channel @ 25°C

ioLogik 2542 Specifications

Inputs and Outputs

Analog Inputs: 4 channels

Configurable DI/DOs (DIO): 12 channels

Isolation: 3k VDC or 2k Vrms

Analog Input

Type: Differential input

Resolution: 16 bits

I/O Mode: Voltage / Current (software selectable)

Input Range: ± 10 V, 0 to 10 V, 0 to 20 mA, 4 to 20 mA (with burn-out detection)

Accuracy:

- $\pm 0.1\%$ FSR @ 25°C
- $\pm 0.3\%$ FSR @ -10 and 60°C
- $\pm 0.5\%$ FSR @ -30 and 70°C

Sampling Rate:

- All channels: 400 samples/sec
- Per channel: 100 samples/sec

Input Impedance: > 1M ohms (min.)

Built-in Resistor for Current Input: 120 ohms

Digital Input

Sensor Type: Wet Contact (NPN or PNP) and Dry Contact

Input Leakage Current: < 1 mA (@ 30 VDC)

I/O Mode: DI or Event Counter

Dry Contact:

- On: short to GND
- Off: open

Wet Contact (DI to COM):

- On: 10 to 30 VDC
- Off: 0 to 3 VDC

Common Type: 6 points per COM

Counter Frequency: 2.5 kHz

Digital Filtering Time Interval: Software configurable

Digital Output

Type: Sink

I/O Mode: DO or Pulse Output

Pulse Output Frequency: 5 kHz

Over-voltage Protection: 45 VDC

Over-current Protection: 1.5 A per channel @ 25°C

Over-temperature Shutdown: 175°C (min.)

Current Rating: 500 mA per channel @ 25°C

Installation

In this chapter, we provide instructions on how to install the ioLogik 2500 I/O server to connect to the network and serial devices.

The following topics are covered in this chapter:

❑ **Hardware Installation**

- Installing the ioLogik 2500 on a DIN Rail
- Removing the ioLogik 2500 from a DIN Rail

❑ **Powering on the ioLogik 2500**

❑ **Grounding the Unit**

❑ **Installing a microSD Card and SIM Cards (cellular models only)**

❑ **I/O Wiring Diagrams**

❑ **LED Indicators**

❑ **Daisy-Chaining for I/O Expansion**

❑ **Reset to Factory Defaults**

❑ **Network Installation**

- Ethernet Communication
- TCP/IP Settings
- Serial Communication

❑ **Installing the IOxpress Utility**

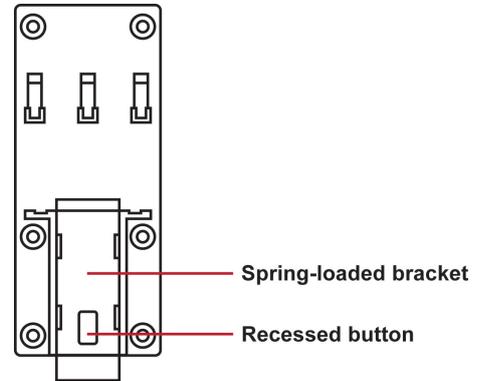
- System Requirements
- Installing IOxpress from the CD
- Installing IOxpress from the Internet

Hardware Installation

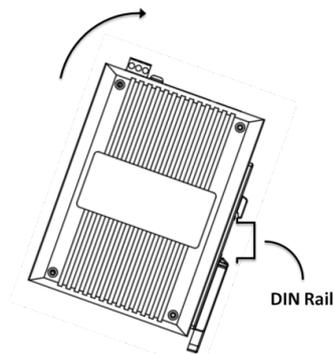
Installing the ioLogik 2500 on a DIN Rail

The DIN-rail attachment plate should already be fixed to the back panel of your ioLogik 2500. If you need to reattach the plate, be sure the spring-loaded bracket is oriented towards the bottom, as shown in the figures below.

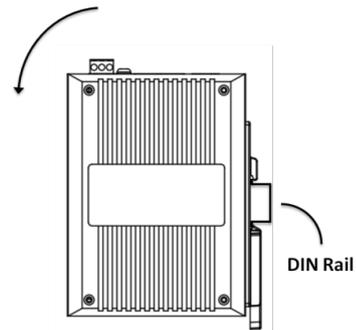
STEP 1: If the spring-loaded bracket is locked in place, push the recessed button to release it. Once released, you should feel some resistance from the spring as you slide the bracket up and down a few millimeters in each direction.



STEP 2: Insert the top of the rail into the upper lip of the attachment plate's slot.

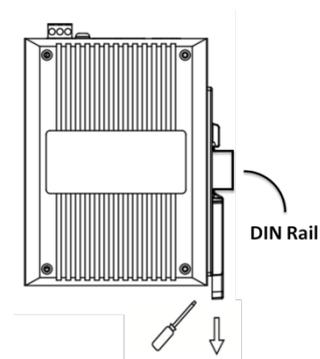


STEP 3: The attachment unit should now snap into place along the rail, as shown below.



Removing the ioLogik 2500 from a DIN Rail

To remove the ioLogik 2500 from a DIN rail, use a screwdriver to pull down the spring-loaded bracket until it locks in place, as shown in the diagram at the right. Next, rotate the bottom of the ioLogik 2500 upwards until you can remove it from the DIN rail.



WARNING

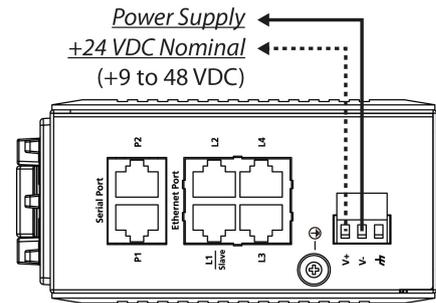
This equipment is intended to be used in Restricted Access Locations. External metal parts will be hot! Maintenance personnel should wear protective gear before touching outside surface.



Powering on the ioLogik 2500

The ioLogik 2500 can receive power from a 9 to 48 VDC power source. Input power is applied to the positive (V+) and negative (V-) terminals on the connector.

After connecting the ioLogik 2500 to the power supply, it will take 30 to 60 seconds for the operating system to boot up. The green Ready LED will illuminate continuously until the operating system is ready.



Grounding the Unit

The ioLogik 2500 is equipped with a ground connector labeled .

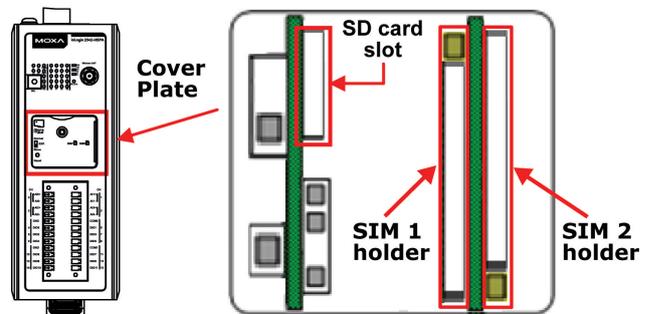


ATTENTION

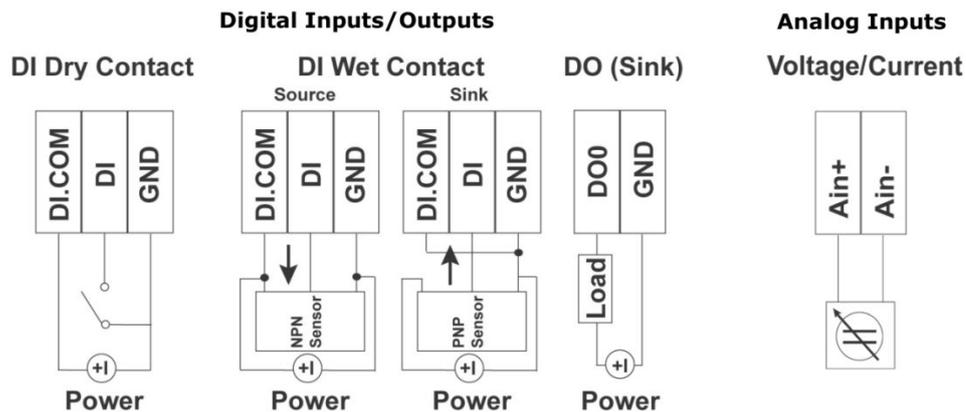
Be sure to note the maximum possible current for each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size. If currents exceed the maximum rating the wires will overheat, and may cause serious damage to the equipment. For safety reasons, wires connecting the power supply should be at least 2 mm in diameter (e.g., 12 gauge).

Installing a microSD Card and SIM Cards (cellular models only)

The ioLogik 2500 supports a single microSD card and two SIM cards (cellular models only). The card slots are located inside the ioLogik 2500, as shown here. The card slot is hidden beneath a cover plate attached by a screw that must first be removed before the slot can be accessed. After removing the screw holding the cover plate in place you can insert or remove the microSD/SIM cards. Be sure to refasten the cover plate when you are done.



I/O Wiring Diagrams



**ATTENTION**

When connecting the I/O device to the ioLogik's dry contacts, we strongly recommend connecting DI.Com to the power of the external sensor to avoid affecting other channels. DI.Com input power should be limited to 12 to 36 VDC.

LED Indicators

Type	Color	Description
Power (PWR)	Green	System power is ON
	Off	System power is OFF
Ready (RDY)	Green	System is ready
	Red	System error
	Flashing	Locating device
	Off	System is not ready
Ethernet Port (L1/L2/L3/L4)	Green	Ethernet connection enabled at 100 Mbps
	Amber	Ethernet connection enabled at 10 Mbps
	Flashing	Data is being transmitted
	Off	Disconnected
Serial Port (P1/P2)	Green	Tx
	Amber	Rx
	Flashing	Data is being transmitted
	Off	Disconnected
SD (Micro SD)	Green	SD card inserted
	Off	SD card is being accessed
I/O Channel Status* (0 to 15)	Green	Channel ON or Counter/Pulse signal
	Off	Channel OFF or No Counter/Pulse signal
W.Link**	Green	Cellular connection established
	Off	Off
Signal Status**	Off	No signal, or No SIM card
	1 LED	Weak or insufficient (SMS only)
	2 LEDs	Average (good for cellular connections)
	3 LEDs	Excellent signal

*Use the rotary switch to select which module's I/O channel status is displayed.

0 = ioLogik 2500
 1 to 8 = E1200 expansion
 9 to F = Reserved

**Wireless modules only

Daisy-Chaining for I/O Expansion

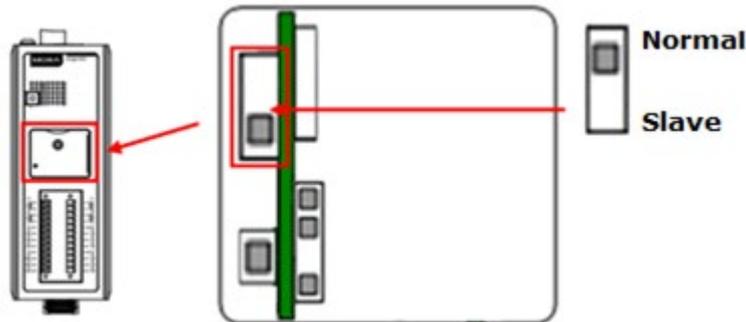
Up to 8 ioLogik E1200 devices can be connected in a daisy chain configuration to the ioLogik 2500 via the L1/Slave port on the ioLogik 2500. An IOxpress configuration scheme is called a project. If the IOxpress project includes expansion devices, the ioLogik 2500 will automatically start running in expansion mode.

If the ioLogik 2500 is running, you can replace one of the expansion units without powering down the ioLogik 2500. Take the following steps to replace an expansion unit:

1. Power-off the expansion unit.
2. Replace the unit with another expansion unit of the same model.
3. Access the DIP switch beneath the cover plate (as shown below).

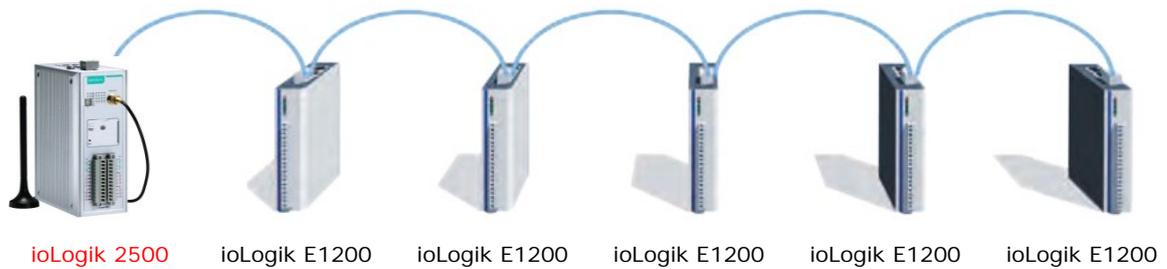
4. Move the DIP switch from the down position to the up position to trigger the ioLogik 2500 to refresh its connection with the expansion units. If the DIP switch is already in the up position, move it down and then back up again.
5. The expansion unit will start running.

You may also use the ioLogik 2500's web console to reconnect the expansion units.

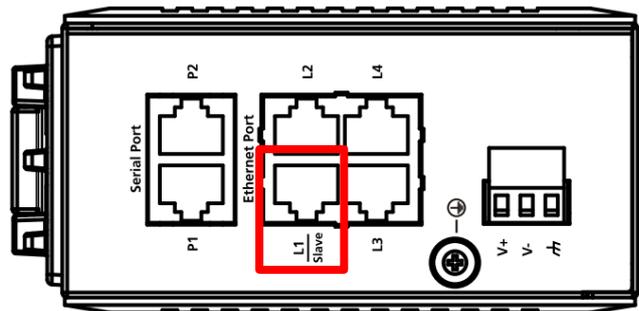


NOTE Expansion units must be replaced with the same model of expansion unit. If you would like to use a different expansion unit model, you must first change the relevant IOxpress settings.

The following figure illustrates a simple daisy-chain of I/O modules using the ioLogik 2500 for wireless connectivity.



When daisy-chaining an array of devices, the first device in the chain (after the ioLogik 2500) must be connected to the L1 Slave port on the top of the ioLogik 2500 (outlined in red in the diagram).

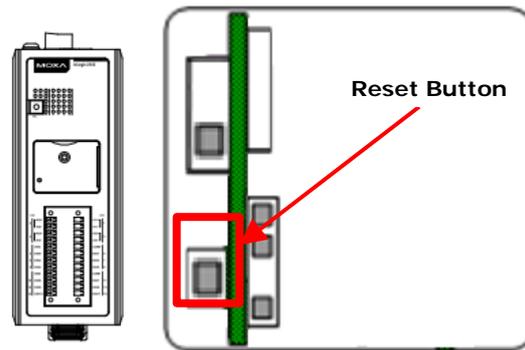


ATTENTION When using the ioLogik 2500 as the wireless head of an array of ioLogik E1200 modules, make sure that:

1. You connect the first E1200 expansion module in the array to the ioLogik 2500's L1 Slave port.
2. A maximum of 8 ioLogik E1200 devices are connected in a single array.

Reset to Factory Defaults

If you need to reset the ioLogik 2500 to factory defaults, press and hold the reset button (located under the cover-plate, as shown in the diagram) for 5 seconds.



WARNING

Resetting your device to factory defaults will result in the loss of all configuration settings and any Click&Go Plus logic settings that have already been configured.

Network Installation

Ethernet Communication

Connections to the LAN port are made through an RJ45 connector on the ioLogik 2500 device. The wiring and pin connections for these connectors are described in separate sections below.



ATTENTION

The maximum cable length of a 10/100BaseT connection is 100 m (350 feet), but the actual limit could be 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 cables that generate electrical noise.

TCP/IP Settings

The following table shows the TCP/IP parameters supported by the LAN port. The ioLogik 2500 will revert to these default values whenever it is reset to factory defaults.

LAN Port	
Parameter	Supported Values
IP Address	Default: 192.168.127.253
Subnet Mask	Default: 255.255.255.0
Gateway	Default: 0.0.0.0

IP Address

The ioLogik 2500's IP address.

Subnet Mask

Determines the subnet on which the device is located.

Gateway

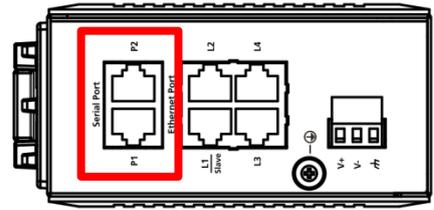
The gateway IP address, which determines how the controller communicates with devices outside its subnet.

The IP address, subnet mask, and gateway are static; contact your network administrator to obtain these addresses for the ioLogik 2500 device.

Serial Communication

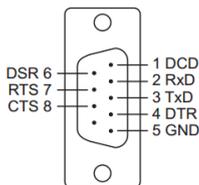
The ioLogik 2500 is equipped with two 3-in-1 software-selectable RS-232/422/485 serial ports, making it more convenient to connect serial devices.

If required, the RJ45 to 8-pin male DB9 converter cables can be used to connect to serial devices.



NOTE The ioLogik 2500 is shipped with 2 RJ45 to DB9 connection cables. If you need additional cables, contact your Moxa sales representative.

The model name of the connection cable is CBL-RJ45M9-150.



Pin	RS-232	RS-422 and 4-wire RS-485	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	—	—

Installing the IOxpress Utility

The ioLogik 2500 can be remotely managed and configured over an Ethernet with Moxa's **IOxpress** utility. IOxpress is a Windows utility provided for the configuration and management of the ioLogik 2500. IOxpress can be used to remotely monitor and configure devices from any location on the network. The IOxpress graphical user interface provides easy access to all status information and configuration settings, and can also be used to configure Click&Go Plus rules, and to handle front-end events.

System Requirements

Hardware Requirements	
CPU	Intel Pentium 4 CPU and above
RAM	Min. 512 MB, 1024 MB is recommended
Network Interface	10/100 Ethernet
Software Requirements	
Operating System	Microsoft Windows 2000, XP or later
Editor (not required)	Microsoft Office 2003 (Access 2003) or later

Installing IOxpress from the CD

Insert the documentation and software CD into the host computer. Locate the Software/Utility_IOxpress directory and run SETUP.EXE from that location.

The installation program will guide you through the installation process and install the **IOxpress** utility. After the installation is finished, run IOxpress from the Windows Start menu.

Installing IOxpress from the Internet

You can also download IOxpress from Moxa's website. To do this, first click on the following link to access the website's search utility:

<http://www.moxa.com/support/search.aspx?type=soft>

When the web page opens, enter the model name of your product in the search box. Navigate to the product page, and then click on **Utilities** (in the middle of the page), located in the box titled **Software**.

NOTE Additional information on using IOxpress can be found in **Chapter 3: The IOxpress Utility**.

The IOxpress Utility

In this chapter, we explain how to configure the ioLogik 2500.

The following topics are covered in this chapter:

- ❑ **Introduction**
 - Application Interface
- ❑ **Using IOxpress**
- ❑ **Offline Configuration**
 - Creating a Project
 - Adding an ioLogik 2500 Device to a Project
 - Adding E1200 Devices to a Project
- ❑ **Setting Up a Device**
- ❑ **Settings**
- ❑ **General Device Settings**
 - Network
 - General
- ❑ **Click&Go Plus**
- ❑ **Click&Go Plus Simulator**
- ❑ **Peer-to-Peer**
 - General Settings
 - P2P Rule Settings
- ❑ **Online Configuration**
 - Introduction
 - Searching for Online Devices
 - Deploying Individual Devices
 - IO Status

Introduction

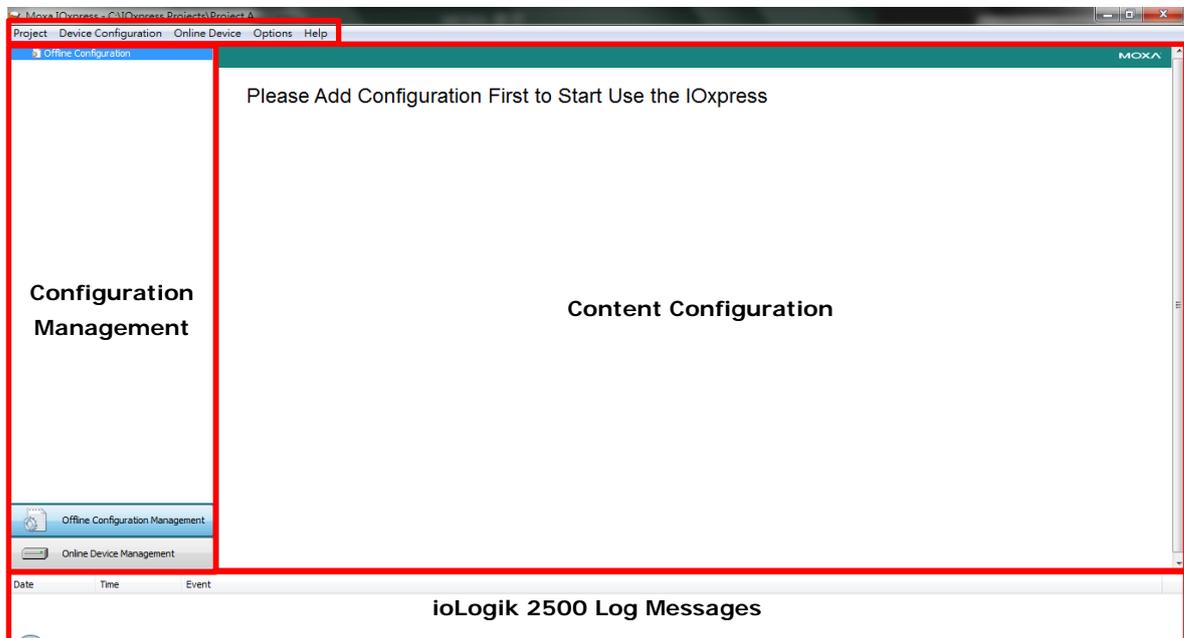
The ioLogik 2500 can be managed and configured over an Ethernet using the IOExpress utility. IOExpress's graphical user interface provides easy access to all status information and settings, and can also be used to configure Click&Go Plus rules to handle front-end events.

Application Interface

Main screen

The following figure shows the main screen of the IOExpress utility. There are four main areas:

- **Menu Bar**
- **Configuration Management**
- **Content Configuration**
- **Log Messages**



Menu Bar

There are five tabs in the menu bar:

- **Project:** For managing projects.
- **Device Configuration:** Functions for offline configuration.
- **Online Device:** Functions for online configuration.
- **Options:** Preferences and network interface.
- **Help:** Version information

NOTE If the host computer has multiple interfaces, be sure to select the correct network interface before searching for online devices.

Using IOxpress

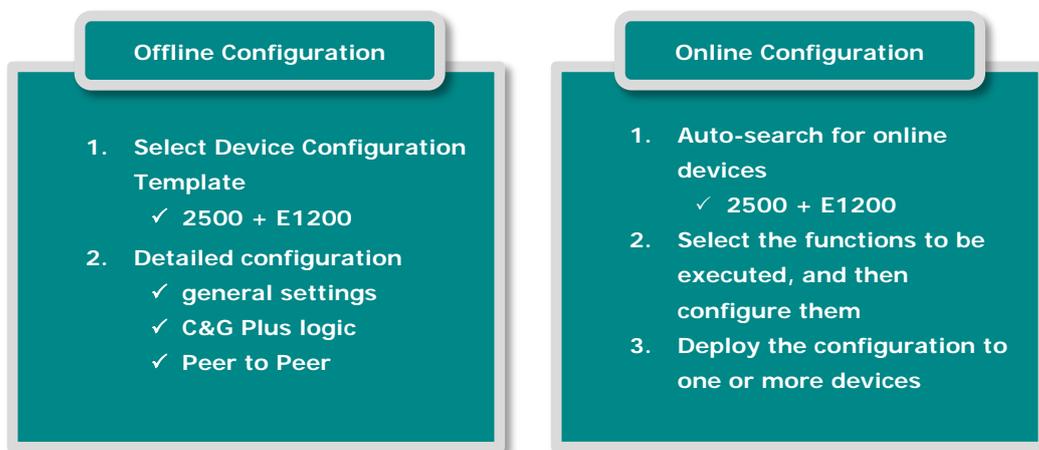
IOxpress is usually configured in two steps:

1. **Offline Configuration:** The operator uses IOxpress to configure settings, which are stored on a local computer.
2. **Online Configuration:** The operator uses IOxpress to export the configuration to devices on the network.

The basic idea is to use a project created offline to set up all of your devices. That is, the settings configured offline are exported over the network to online devices. This can be done either in batch mode, or on a case-by-case basis.

IOxpress can also be used to access online devices directly to check I/O status, upgrade firmware, export configurations, and restart the device.

The following flowchart gives an overview of the IOxpress configuration process. Once offline configuration is completed, you can start online configuration.



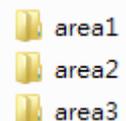
Offline Configuration

Creating a Project

IOxpress configuration schemes are called **Projects** (saved as *.prj files). The first step to using IOxpress is to create a project for automating your device configuration processes. This can be done offline, after which the project can be exported to other devices over the network during the online configuration phase, discussed later in this chapter.

Projects are automatically saved in the following folder:

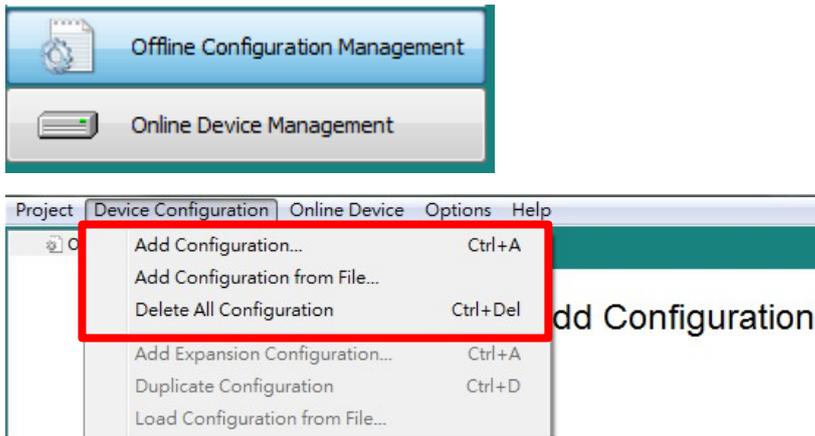
C:\Users\Public\Documents\Moxa\IOxpress\Database



We recommend using folder names to manage your projects. For example, if you would like to create three projects for three different segments of the network, you could create three folders named area1, area2, and area3.

The first time you use offline configuration, create a new project by clicking New from the dropdown menu under the Project tab.

Click **Offline Configuration Management**, or select **Device Configuration** from the tool bar. You may click on either the **Add Configuration** or **Add Configuration from File...** option to add a device to the new project.



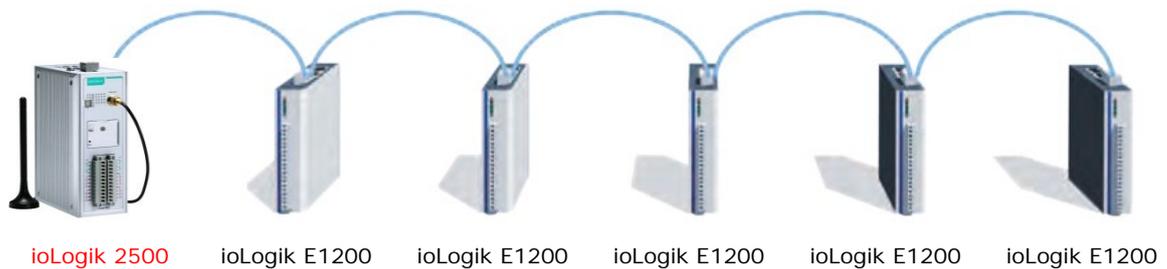
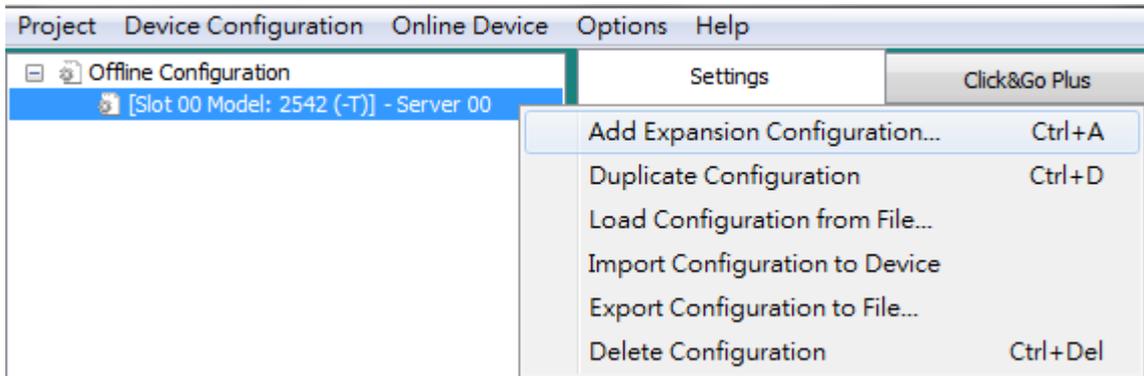
Adding an ioLogik 2500 Device to a Project

The ioLogik 2500 can be used as the head of a cascaded array of ioLogik E1200 modules, with Click&Go Plus logic used to extend communication capability to the all of the expansion units.

Adding E1200 Devices to a Project

Up to 8 ioLogik E1200 series devices can be connected to the ioLogik 2500 in a daisy-chain configuration.

Right click on the ioLogik 2500 device you have just added, and then select **Add Expansion Configuration**. After adding an E1200, the settings for the added device can be found in the **I/O settings**, **Tag selection**, and **data logging – profile** areas.



ATTENTION

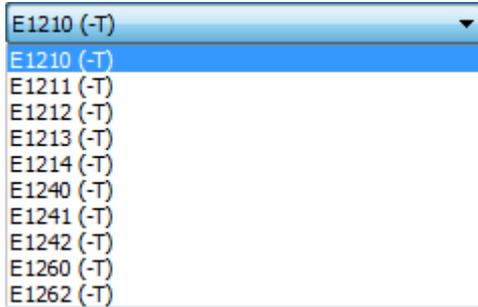
If the IOxpress project includes expansion devices, the L1/slave port will automatically run in expansion mode.



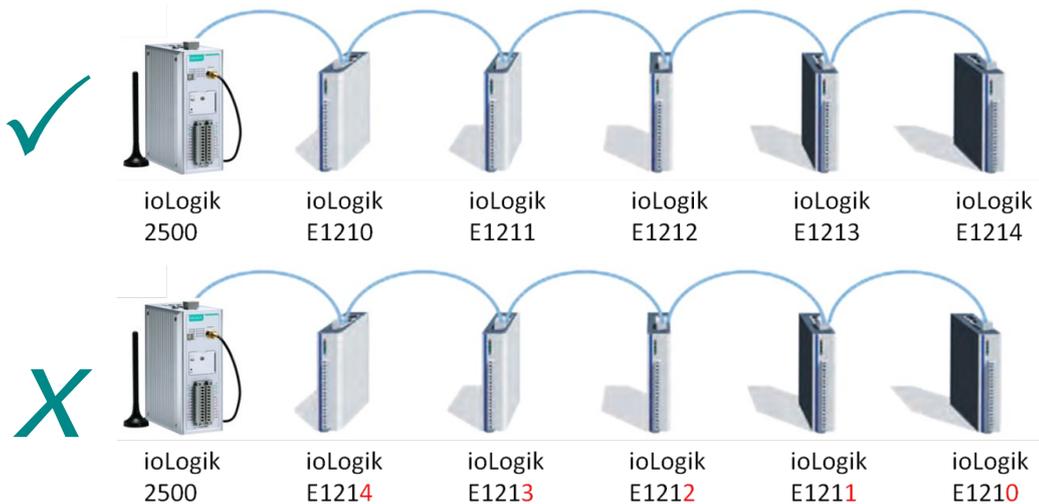
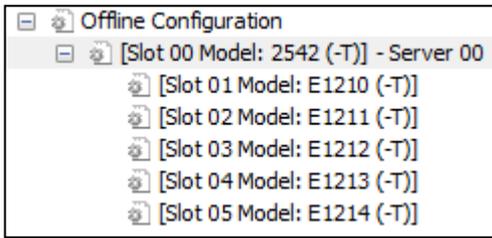
ATTENTION

The IP address of the ioLogik 2500 should not be the same as its E1200 expansion units.

NOTE The following ioLogik E1200 models can be used for ioLogik 2500 I/O arrays:



NOTE The location of each model is fixed. If you would like to change a device in an E1200 array, make sure that the order of the expansion modules is the same as in the Expansion Configuration list you just modified. An example is shown below:



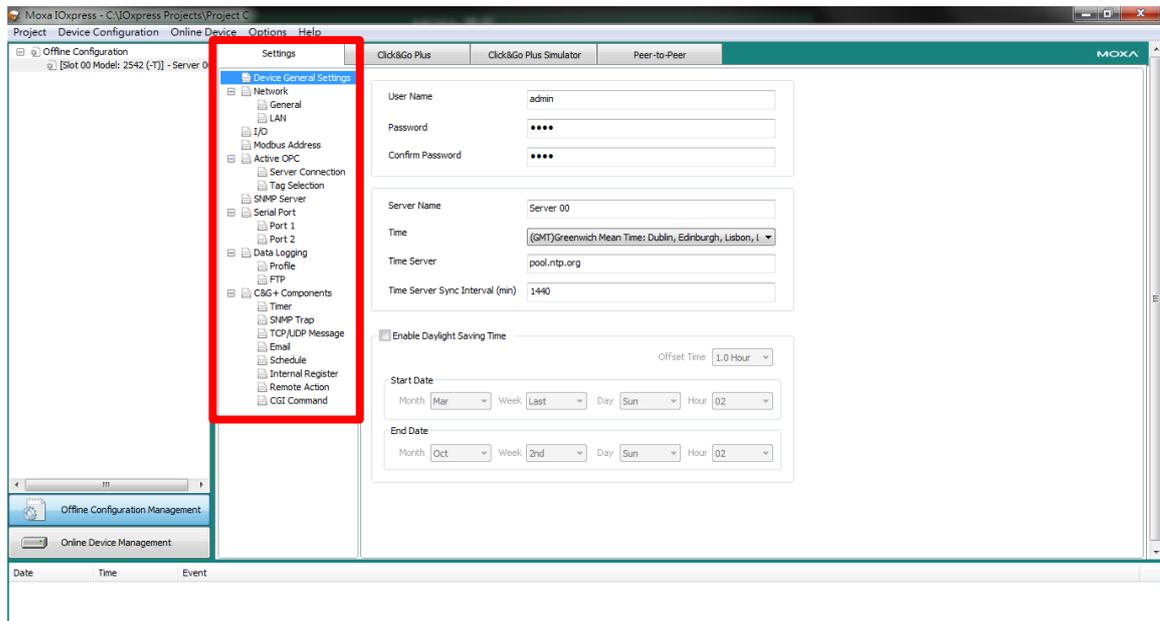
Setting Up a Device

After you have created the project, you can start to configure each device in the project. The configuration window has four tabs:

- **Settings**
- **Click&Go Plus**
- **Click&Go Plus Simulator**
- **Peer-to-Peer**

Settings

In the **Settings** section, you will find basic settings used to set up a selected device.



General Device Settings

The User Name, Password, Server Name, Time, Time Server, and Daylight Saving functions can be accessed from under the General Settings tab.

Server Name

IOxpress supports long server names and a location description with up to 30 characters.

Daylight Saving Time

To set up the Daylight saving schedule, check the Enable Daylight Saving Time checkbox, and then configure Offset Time, Start Date, and End Date.

User Name	admin
Password	••••
Confirm Password	••••

Server Name	Server 00
Time	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, L
Time Server	pool.ntp.org
Time Server Sync Interval (min)	1440

<input type="checkbox"/> Enable Daylight Saving Time	Offset Time: 1.0 Hour
Start Date	Month: Mar, Week: Last, Day: Sun, Hour: 02
End Date	Month: Oct, Week: 2nd, Day: Sun, Hour: 02

Network

There are three sub-pages under the **Network** item tab: **General**, **LAN**, **Cellular** (applies to the ioLogik 2500-GPRS/HSPA only) and **Wireless Lan** (applies to the ioLogik 2500-WL1 only).

General

There are two columns under general tab: **Select major network Interface** and **General Settings**.

Select Major Network Interface

Select major network Interface is only available for the ioLogik 2500-GPRS/HSPA models. See **Chapter 4: Cellular Network Setup and Configuration** for details.

General Settings

General Settings

Enable Web Access

Enable Server Socket Idle Connection Timeout (sec.)

Private IP for First Module

Enable Web Access

Use this checkbox to enable or disable the web console. When enabled, the ioLogik can be configured from a web browser. If not enabled, you will not be able to open the web console.

Enable Server Socket Idle Connection Timeout

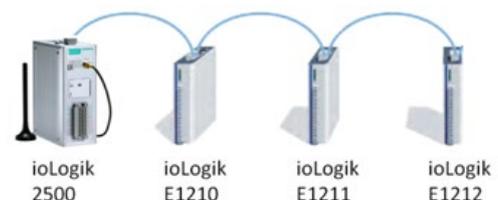
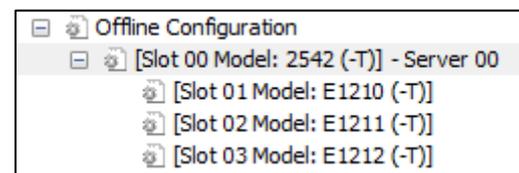
Server Socket Idle Connection Timeout is designed to avoid TCP connection failures when the network host is unable to respond due to a hardware failure or network problem.

If **Server Socket Idle Connection Timeout** is enabled: When the server's connection to the ioLogik 2500 exceeds the specified time period the device will automatically release its TCP connection to the server to free up the port for the next connection.

If **Server Socket Idle Connection Timeout** is not enabled: If the network host is unable to respond due to a hardware failure or network problem, the ioLogik will continue to wait for a response from the host, causing the TCP port to be occupied indefinitely by the host.

Private IP for First Slot of Slave Module

An array of up to 8 modules can be connected to the ioLogik 2500. The Private IP for First Slot of Slave Module assigns an IP to the first E1200 device. The IPs for subsequent devices in the chain will be automatically assigned consecutively. For example, if the IP of the first E1200 device is set to 192.168.120.1, the IP of the second E1200 will be 192.168.120.2, the third IP will be 192.168.120.3, and so on.



LAN

IP Settings

You can set up a static or dynamic IP address for the ioLogik, as well as the subnet mask and gateway address.

Use this field to specify the IP addresses of one or two DNS servers. DNS servers can be used to find available e-mail addresses when setting up Click & Go plus rules.

IP Setting

IP Configuration: Static IP

IP Address: 192 . 168 . 125 . 1

Netmask: 255 . 255 . 0 . 0

Gateway: . . .

DNS1: . . .

DNS2: . . .

Cellular (ioLogik 2500-GPRS/HSPA only)

Cellular is only available for the ioLogik 2500-GPRS/HSPA models. See **Chapter 4: Cellular Network Setup and Configuration** for details.

Wireless LAN

Wireless LAN is only available for the ioLogik 2500-WL1 models. See **Chapter 5: Wireless LAN Network Setup and Configuration** for details.

I/O

In the I/O section, you can configure I/O settings for ioLogik 2500 devices. Items that can be modified will be shown in **black**. Items that cannot be modified will be shown in **light gray**.

Slot Number	Channel No	Channel Type	Channel Mode	Name
[Slot 00 Model: 2542 (-T)]	0	AI	0-10V	AI-00
[Slot 00 Model: 2542 (-T)]	1	AI	0-10V	AI-01
[Slot 00 Model: 2542 (-T)]	2	AI	0-10V	AI-02
[Slot 00 Model: 2542 (-T)]	3	AI	0-10V	AI-03
[Slot 00 Model: 2542 (-T)]	4	DIO	DI	DIO-00
[Slot 00 Model: 2542 (-T)]	5	DIO	DI	DIO-01
[Slot 00 Model: 2542 (-T)]	6	DIO	DI	DIO-02
[Slot 00 Model: 2542 (-T)]	7	DIO	DI	DIO-03
[Slot 00 Model: 2542 (-T)]	8	DIO	DI	DIO-04
[Slot 00 Model: 2542 (-T)]	9	DIO	DI	DIO-05
[Slot 00 Model: 2542 (-T)]	10	DIO	DI	DIO-06
[Slot 00 Model: 2542 (-T)]	11	DIO	DI	DIO-07
[Slot 00 Model: 2542 (-T)]	12	DIO	DI	DIO-08
[Slot 00 Model: 2542 (-T)]	13	DIO	DI	DIO-09
[Slot 00 Model: 2542 (-T)]	14	DIO	DI	DIO-10
[Slot 00 Model: 2542 (-T)]	15	DIO	DI	DIO-11
[Slot 00 Model: 2542 (-T)]	16	Virtual Channel	Disable	Virtual Channel-00
[Slot 00 Model: 2542 (-T)]	17	Virtual Channel	Disable	Virtual Channel-01
[Slot 00 Model: 2542 (-T)]	18	Virtual Channel	Disable	Virtual Channel-02
[Slot 00 Model: 2542 (-T)]	19	Virtual Channel	Disable	Virtual Channel-03
[Slot 00 Model: 2542 (-T)]	20	Virtual Channel	Disable	Virtual Channel-04
[Slot 00 Model: 2542 (-T)]	21	Virtual Channel	Disable	Virtual Channel-05
[Slot 00 Model: 2542 (-T)]	22	Virtual Channel	Disable	Virtual Channel-06
[Slot 00 Model: 2542 (-T)]	23	Virtual Channel	Disable	Virtual Channel-07
[Slot 00 Model: 2542 (-T)]	24	Virtual Channel	Disable	Virtual Channel-08
[Slot 00 Model: 2542 (-T)]	25	Virtual Channel	Disable	Virtual Channel-09

Setting	Functions
IO Mode Setting	Channel Mode Name
DI Setting	Filter
Counter Setting	Filter Initial Value Active Mode Power On Status Scaling Enable Scaling Offset Scaling Interval
DO Setting	Enable Communication Watchdog for Safe Mode Enable Auto Clear Safe Mode Power On Status Power On Delay Safe Mode Status
Pulse Setting	On Width Off Width Count Power On Status Power On Delay Safe Mode Status
AI Setting	Input Range Burnout Value Scaling Slope Scaling Offset Scaling Unit
Virtual Channel Setting	Enable Slot No. Channel No. Function Interval (min) Sampling Time (min)

Select module

Select the module that you would like to configure. You may select **All** modules, in which case information on all I/O channels in the project will be displayed.

Select Module

IO Mode Setting

- Channel Mode**

DIO channels can be set to one of four modes: **DI**, **Event Counter**, **DO**, or **Pulse output**. AI channels can be set to one of five modes: **±10 V**, **0 to 10 V**, **0 to 20 mA**, **4 to 20 mA**, or **4 to 20 mA (Burnout)**. AO channels can be set to one of two modes: **0 to 10 V** and **4 to 20 mA**.

NOTE Since the ioLogik 2500 does not have AO channels, the AO setting will only show up when the project contains E1200 AO modules, such as the E1241.

- Name**

The name will be attached to the AOPC tag to help users identify channel information in MX-AOPC.

DI Setting

Filter: Software filtering is used to avoid switch bounces. The filter is configurable in multiples of 100 μ s and accepts values between 1 and 65535.

Detail Setting DI Setting

Enable Communication Watchdog for Safe Mode sec Enable Auto Clear Safe Mode

Slot Number	Channel No	Filter	Filter Unit
[Slot 00 Model: 2542 (-T)]	4	1	100 us
[Slot 00 Model: 2542 (-T)]	5	1	100 us
[Slot 00 Model: 2542 (-T)]	6	1	100 us
[Slot 00 Model: 2542 (-T)]	7	1	100 us
[Slot 00 Model: 2542 (-T)]	8	1	100 us
[Slot 00 Model: 2542 (-T)]	9	1	100 us
[Slot 00 Model: 2542 (-T)]	10	1	100 us
[Slot 00 Model: 2542 (-T)]	11	1	100 us
[Slot 00 Model: 2542 (-T)]	12	1	100 us
[Slot 00 Model: 2542 (-T)]	13	1	100 us
[Slot 00 Model: 2542 (-T)]	14	1	100 us
[Slot 00 Model: 2542 (-T)]	15	1	100 us

Counter Setting

Counter refers to an **Event Counter** channel. Counts are stored internally.

Detail Setting Counter Setting

Enable Communication Watchdog for Safe Mode sec Enable Auto Clear Safe Mode

Slot Number	Channel No	Filter	Filte...	Initial Value	Active Mode	Power On Status	Scaling Enable	Scaling Slope	Scaling Offset	Scaling Interval .
[Slot 00 Model: 2542 (-T)]	4	1	100 us	0	Raising edge	Stop	Disable	1	0	5
[Slot 00 Model: 2542 (-T)]	5	1	100 us	0	Raising edge	Stop	Disable	1	0	5
[Slot 00 Model: 2542 (-T)]	6	1	100 us	0	Raising edge	Stop	Disable	1	0	5
[Slot 00 Model: 2542 (-T)]	7	1	100 us	0	Raising edge	Stop	Disable	1	0	5

- **Filter**

Software filtering is used to avoid switch bounces. The filter is configurable in multiples of 100 μ s and accepts values between 1 and 65535.

- **Initial Value**

The initial value is the start value in counter mode.

- **Active Mode**

In **Active mode**, the channel accepts limit or proximity switches and counts events according to the ON/OFF status. When **Rising edge** is selected, the counter value increases when the attached switch is pushed. When **Falling edge** is selected, the counter value increases when the switch is released. When **Both** is selected, the counter value increases when the attached switch is pushed or released.

- **Power On Status**

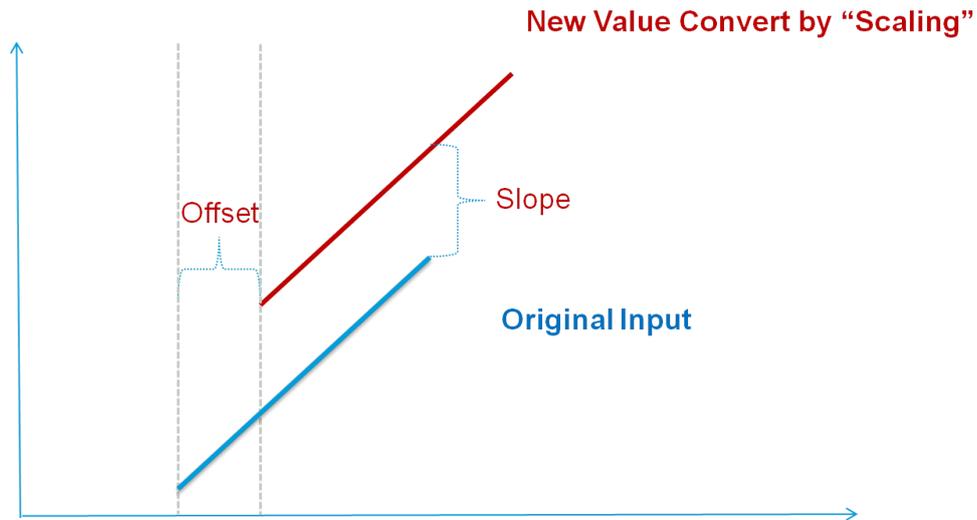
To enable the counter to resume counting immediately upon powering up, enable the **Power On Status**.

Stop: The counter starts logging signals only after configured to do so by a Modbus or a Click&Go Plus command.

Start: Counting begins automatically whenever the ioLogik is powered on.

- **Scaling Enable / Scaling Slope / Scaling Offset / Scaling Interval (sec)**

Set the **Slope & Offset** to convert the Counter value to new units.



DO Setting

Detail Setting DO Setting

Enable Communication Watchdog for Safe Mode sec Enable Auto Clear Safe Mode

Slot Number	Channel No	Power On Status	Power On Delay (s)	Safe Mode Status
[Slot 00 Model: 2542 (-T)]	8	Off	0	Off
[Slot 00 Model: 2542 (-T)]	9	Off	0	Off
[Slot 00 Model: 2542 (-T)]	10	Off	0	Off
[Slot 00 Model: 2542 (-T)]	11	Off	0	Off

- **Enable Communication Watchdog for Safe Mode**

When the watchdog is enabled, any disconnection from the network will activate a safe state. In the safe mode, DO channels can be configured to turn on, turn off, or commence pulse output during the safe state. If the watchdog is not enabled, then DO channel status will remain unchanged during a network disconnection.

To configure a DO for safe mode, set the corresponding value in the **Safe Mode Status** column to ON.

- **Enable Auto Clear Safe Mode**

When detecting the reconnection of Ethernet signals, the device will auto clear the safe mode status.

- **Power On Status**

When the device is first powered on, the status of each DO channel is set to **OFF** by default. This behavior can be modified using the **Power On Status**.

- **Power On Delay**

The time delay from tuning DO channels when the power is turned on.

- **Safe Mode Status**

Enable Communication Watchdog for Safe Mode allows you to control how DO and pulse output channels act when the network is disconnected.

If the Communication Watchdog is enabled, a network disconnection will activate a safe state. The DO channel can be configured to turn on / turn off during the safe state.

If the Communication Watchdog is not enabled, then the DO channel status will remain unchanged during a network disconnection.

Pulse Setting

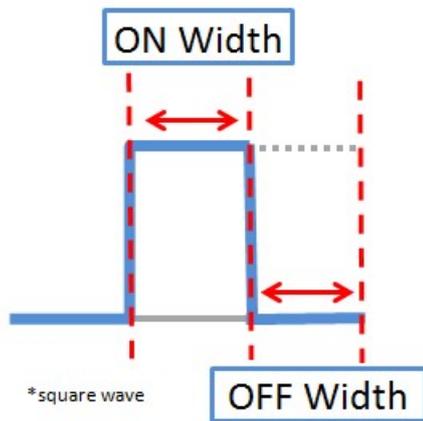
Detail Setting Pulse Setting

Enable Communication Watchdog for Safe Mode sec Enable Auto Clear Safe Mode

Slot Number	Channel No	On Width	Off Width	Width Unit	Count	Power On Status	Power On Delay (s)	Safe Mode Status
[Slot 00 Model: 2542 (-T)]	12	1	1	100 us	0	Stop	0	Stop
[Slot 00 Model: 2542 (-T)]	13	1	1	100 us	0	Stop	0	Stop
[Slot 00 Model: 2542 (-T)]	14	1	1	100 us	0	Stop	0	Stop
[Slot 00 Model: 2542 (-T)]	15	1	1	100 us	0	Stop	0	Stop

• **On Width / Off Width**

In **Pulse Output mode**, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The low and high level widths are specified in multiples of 100 μs for Digital Output, with a maximum setting of 65,535.



• **Count**

You can specify between 1 and 4,294,967,295 pulses or enter "0" for continuous pulse output.

• **Power On Status**

When the device is first powered on, the status of each pulse output channel is set to **OFF** by default. This behavior can be modified using the **Power On Status**.

You can set a pulse output channel to turn **ON** when the ioLogik is powered on, or to commence pulse output.

• **Power On Delay**

The time delay from tuning DO channels when the power is turned on.

• **Safe Mode Status**

If the Communication Watchdog is enabled, a network disconnection will activate a safe state. The pulse output channel can be configured to turn on / turn off during the safe state.

AI Setting

Detail Setting AI Setting

Enable Communication Watchdog for Safe Mode sec Enable Auto Clear Safe Mode

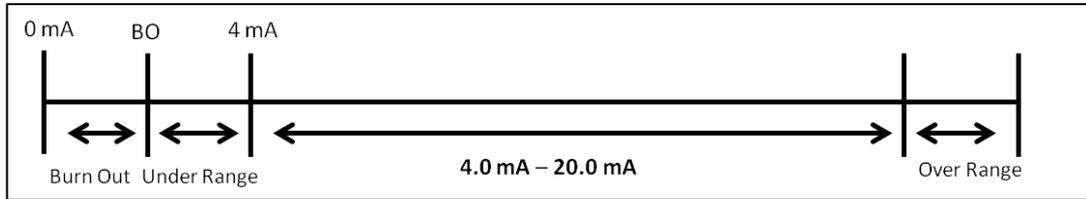
Slot Number	Channel No	Channel Mode	Burnout Value	Scaling Slope	Scaling Offset	Scaling Unit
[Slot 00 Model: 2542 (-T)]	0	0-10V		1.000000	0.000000	V
[Slot 00 Model: 2542 (-T)]	1	0-10V		1.000000	0.000000	V
[Slot 00 Model: 2542 (-T)]	2	0-10V		1.000000	0.000000	V
[Slot 00 Model: 2542 (-T)]	3	0-10V		1.000000	0.000000	V

• **Channel Mode**

The input channels can be set individually to ±10 V, 0 to 10 V, 0 to 20 mA, 4 to 20 mA, and 4 to 20 mA (Burnout).

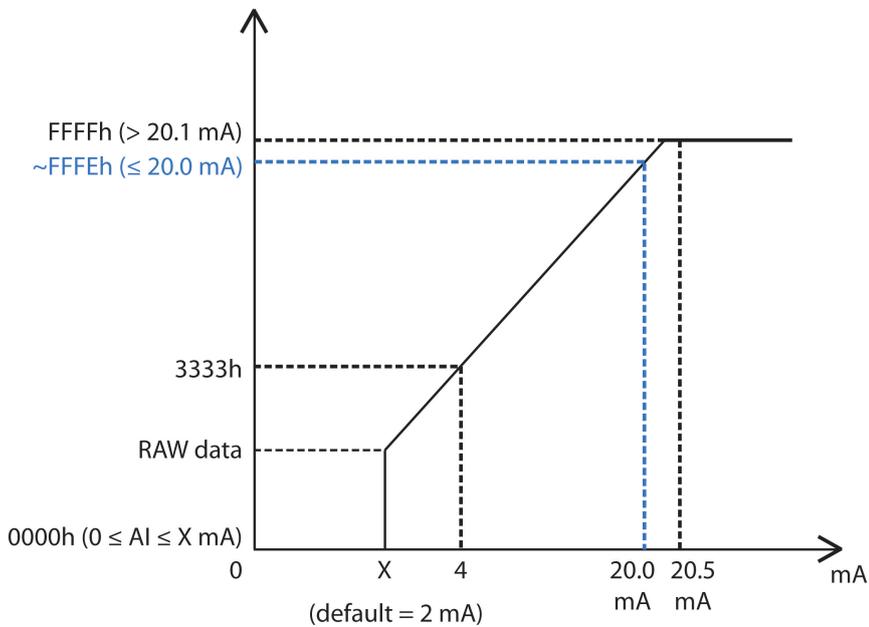
• **Burn-out Value**

Burn Out mode indicates when the Current AI has burned out. For example, the 4–20 mA Burn-out mode is defined in the following diagram:



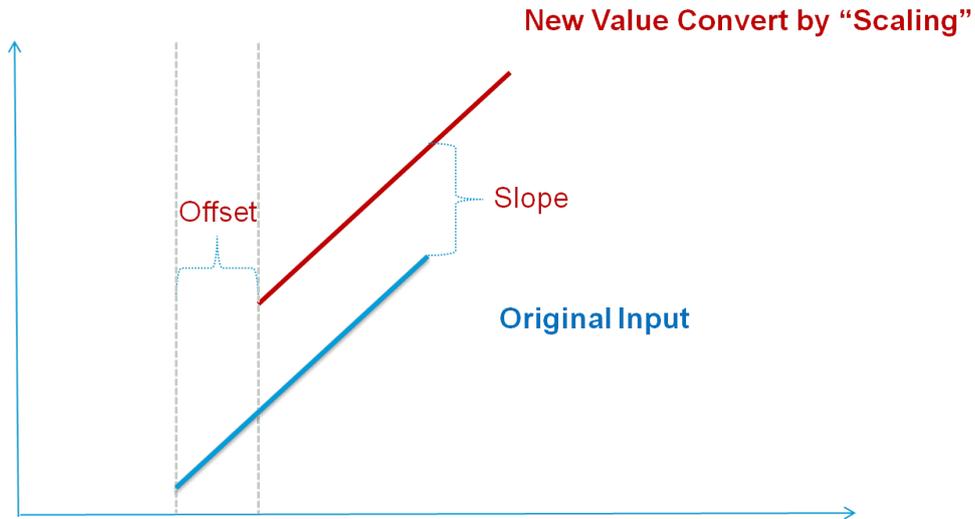
Users can define Burn-out (BO) values (default = 2 mA) for selected ranges. When input values are in the Burn Out range, raw data will register as 0000h to indicate that the analog input has burned out. The definition of raw data is as follows:

Burnout Value (BO)	0.0 < BO < 4.0	User defined (default 2 mA)
Burnout State	0 ≤ AI < BO mA	Modbus output 0000h
Under Range	BO ≤ AI < 4 mA	Modbus output raw data
Normal Range	4 ≤ AI ≤ 20.00 mA	Modbus output raw data until FFFEh
Over Range	XX > 20.00 mA	Modbus output FFFFh



- **Scaling Slope / Scaling Offset /Scaling Unit**

Enabling the Scaling functions will linearly convert the actual current or voltage value into other user-defined units, such as percentage or ppm (parts per million).



AO Setting

Detail Setting AO Setting

Enable Communication Watchdog for Safe Mode 30 sec Enable Auto Clear Safe Mode

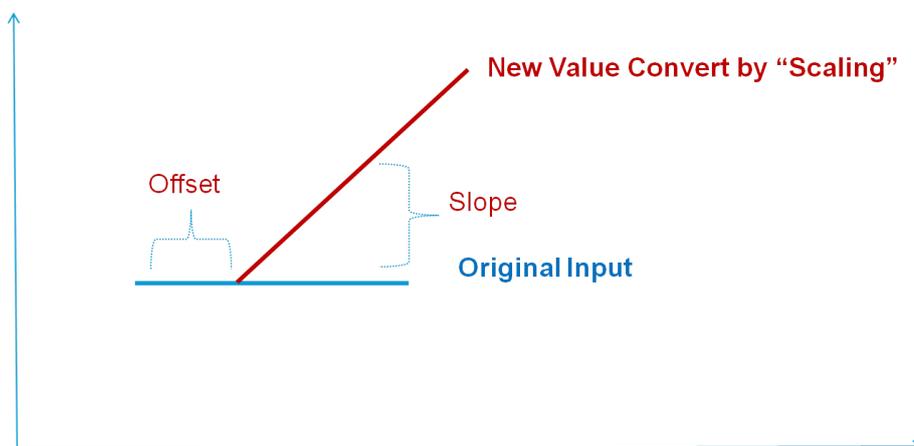
Slot Number	Channel No	Channel Mode	Scaling Slope	Scaling Offset	Scaling Unit	Power On Status	Safe Mode Status
[Slot 02 Model: E1241 (-T)]	0	4-20mA	1.000000	0.000000	mA	4.000000	4.000000
[Slot 02 Model: E1241 (-T)]	1	4-20mA	1.000000	0.000000	mA	4.000000	4.000000
[Slot 02 Model: E1241 (-T)]	2	4-20mA	1.000000	0.000000	mA	4.000000	4.000000
[Slot 02 Model: E1241 (-T)]	3	4-20mA	1.000000	0.000000	mA	4.000000	4.000000

- **Channel Mode**

There are two modes for the AO channels: Voltage Mode (V) and Current Mode (mA).

- **Scaling Slope / Scaling Offset / Scaling Unit**

Enabling the Scaling functions will linearly convert the actual current or voltage value into other user-defined units, such as percentage or ppm (parts per million).



- **Power On Status**

When the device is first powered on, the status of each AO channel can be modified using the **Power On Status**.

• **Safe Mode Status**

Enable Communication Watchdog for Safe Mode allows you to control how an AO channel acts when the network is disconnected.

If the Communication Watchdog is enabled, a network disconnection will activate a safe state. The AO channel can be configured to a defined value during the safe state.

NOTE Since the ioLogik 2500 does not have AO channels, the AO setting will only show up when the project contains E1200 AO modules (such as the E1241).

Virtual Channel Setting

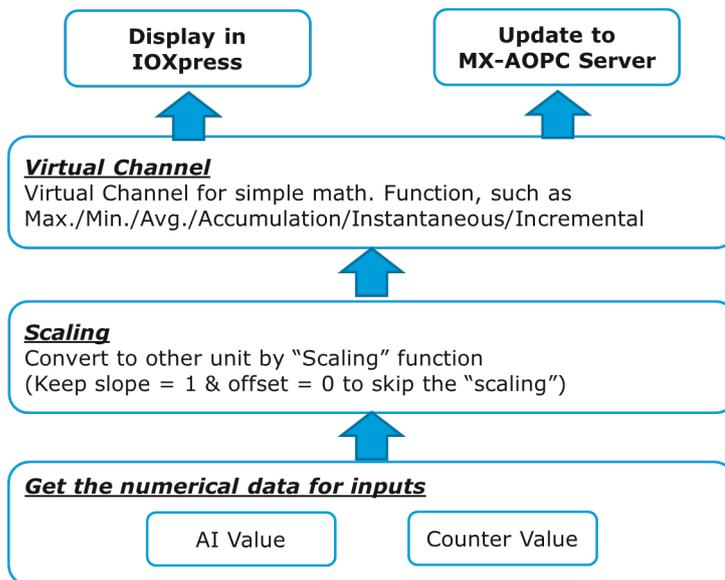
Detail Setting Virtual Channel Setting

Enable Communication Watchdog for Safe Mode sec Enable Auto Clear Safe Mode

Slot Number	Channel No	Enable	Slot No	Channel No	Function	Interval (min.)	Sampling Time (min.)
[Slot 00 Model: 2542 (-T)]	16	Disable	2542 (-T)	None	Maximum	1	
[Slot 00 Model: 2542 (-T)]	17	Disable	2542 (-T)	None	Maximum	1	
[Slot 00 Model: 2542 (-T)]	18	Disable	2542 (-T)	None	Maximum	1	
[Slot 00 Model: 2542 (-T)]	19	Disable	2542 (-T)	None	Maximum	1	
[Slot 00 Model: 2542 (-T)]	20	Disable	2542 (-T)	None	Maximum	1	
[Slot 00 Model: 2542 (-T)]	21	Disable	2542 (-T)	None	Maximum	1	
[Slot 00 Model: 2542 (-T)]	22	Disable	2542 (-T)	None	Maximum	1	
[Slot 00 Model: 2542 (-T)]	23	Disable	2542 (-T)	None	Maximum	1	
[Slot 00 Model: 2542 (-T)]	24	Disable	2542 (-T)	None	Maximum	1	
[Slot 00 Model: 2542 (-T)]	25	Disable	2542 (-T)	None	Maximum	1	

The ioLogik 2500 has 10 internal virtual channels to support front-end statistics functions.

The data source is the real I/O channel, such as AI and DI counters, some of which need to be converted to the appropriate time unit. The operation is illustrated below.



NOTE For AI/Counter scaling, configure Scaling on the AI or Counter Configuration panel before selecting operations in the virtual channels.

For example, if you want to monitor the daily flow at a point in a pipeline, you can use a pulse output flow meter, where 1 pulse indicates 5 ml. You can set the virtual channel's **scaling function** so that 1 tick of counter input equals 5 ml. Next, set the **Accumulation** flag, and configure the **Time Interval** to 24 hours. This will set up the virtual channel to log the total water flow volume over a period of 24 hours.

- **Status**

Enable/Disable virtual channels.

- **Slot No.**

If you have connected E1200 expansion modules, select the device you would like to configure here.

Slot No
2542 (-T)
2542 (-T)
[Slot 01 Model: E1210 (-T)]

- **Channel No.**

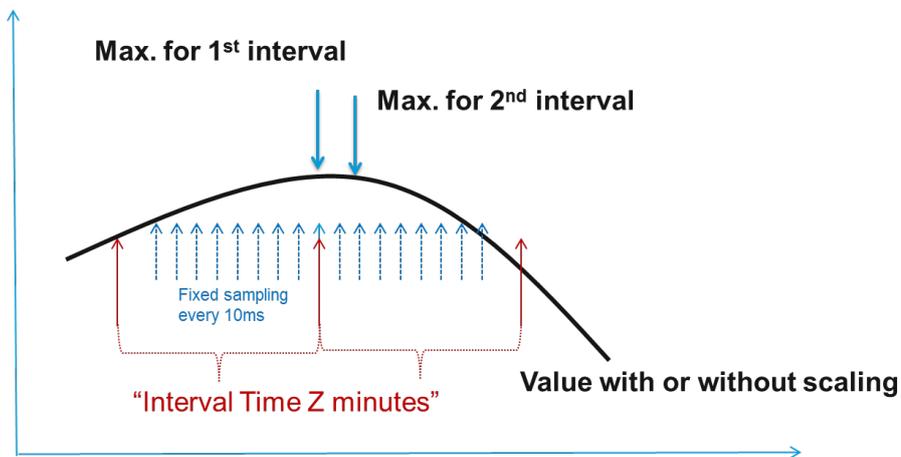
Virtual channels are required to configure AI or counter channels.

- **Function**

There are six functions: Max, Min, Average, Accumulation, Instantaneous, and Incremental.

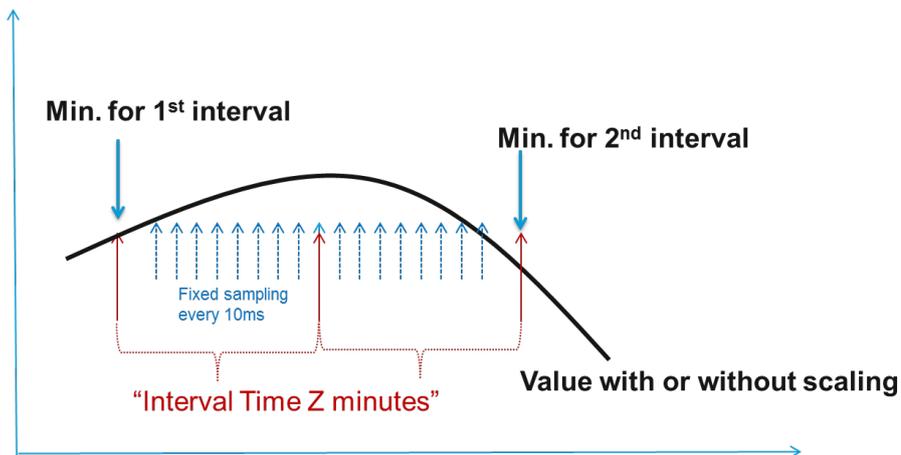
Maximum:

The maximum value within Z sec, with sampling done every 10 ms.



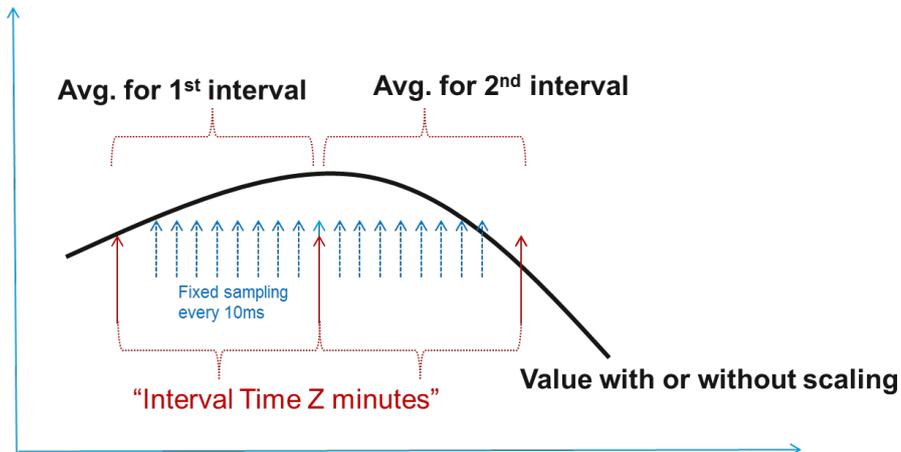
Minimum:

The minimum value within Z sec, with sampling done every 10 ms.



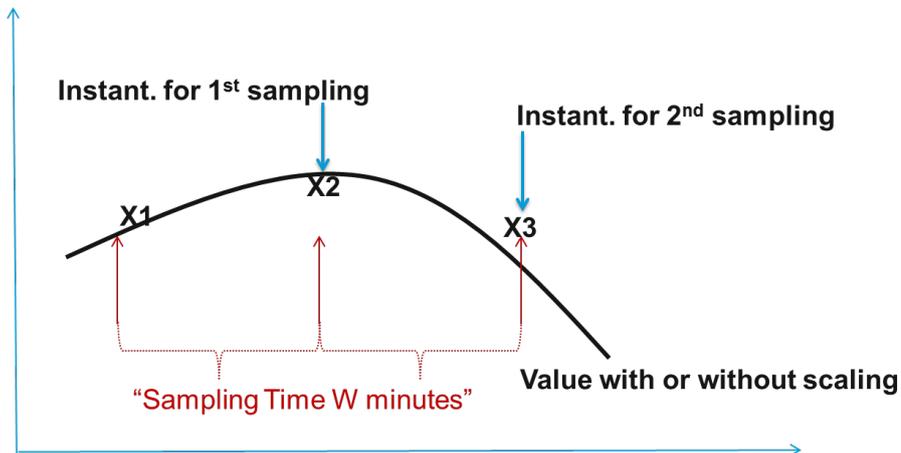
Average:

The average value within Z sec, with sampling done every 10 ms.



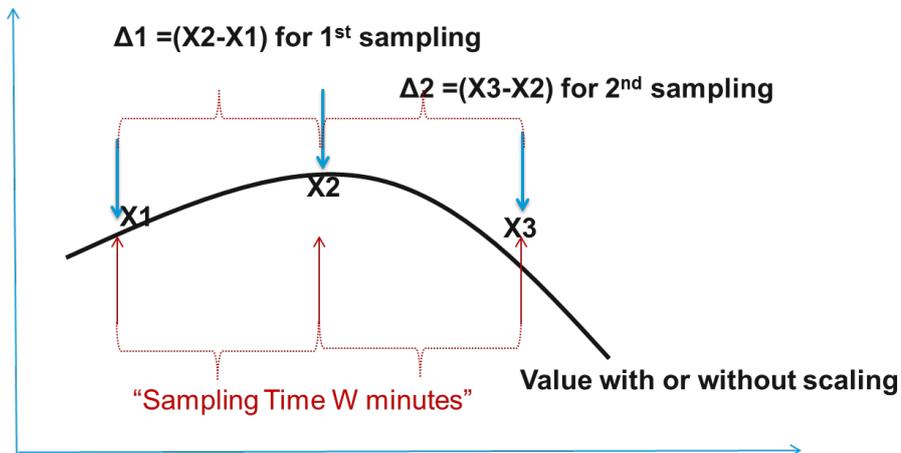
Instantaneous:

The instantaneous value when a sample is taken.



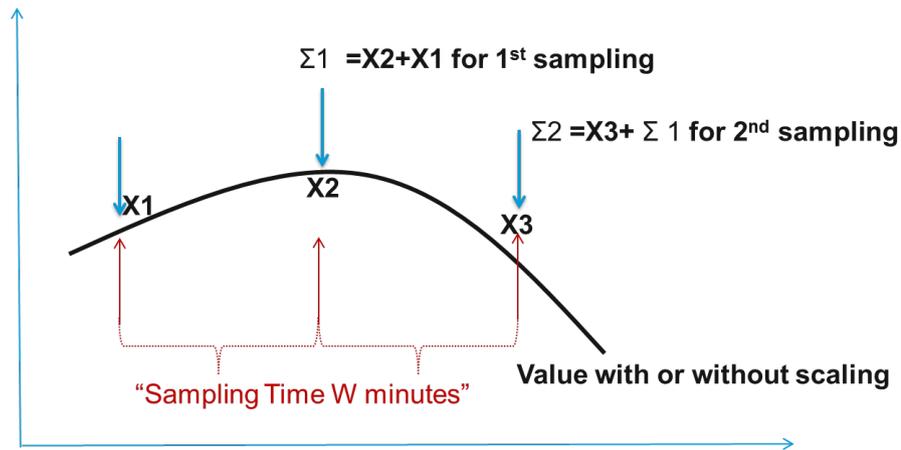
Incremental:

The difference (Δ) between two samples.



Accumulation:

The sum (Σ) of all sampling values.



- **Interval (min.)**
Set the interval time (Minutes) for Maximum, Minimum, and Average functions.
- **Sampling Time (min.)**
Set the sampling time (Minutes) for Instantaneous and Incremental functions.

Modbus Address (Dynamic Address/ User Defined)

In this section, I/O addresses can be configured for different formats. Check the **Enable Modbus Service** box, select the Modbus function, and then configure the start address of each item.

Enable Modbus Service All

No.	Slot Number	Description	Point Type	Read/Write	Start Address (DEC)	Reference Address (DEC)	Total Channels
0	[Slot 00 Mo...	DI Value	02:INPUT STATUS	Read Only	0	10001	8
1	[Slot 00 Mo...	DI Counter Value	04:INPUT REGISTER	Read Only	0	30001	8
2	[Slot 00 Mo...	DIO Value	01:COIL STATUS	Read/Write	0	00001	8
3	[Slot 00 Mo...	DIO Counter Value	04:INPUT REGISTER	Read Only	100	30101	8
4	[Slot 00 Mo...	DIO Pulse Value	01:COIL STATUS	Read/Write	100	00101	8
5	[Slot 00 Mo...	Internal Register	03:HOLDING REGIS...	Read/Write	500	40501	48
6	[Slot 00 Mo...	Float Internal Register	03:HOLDING REGIS...	Read/Write	1000	41001	48

Active OPC Server

Moxa MX-AOPC Server is a software package operated as an OPC driver of an HMI or SCADA system. It offers seamless connection from Moxa ioLogik series products to SCADA systems.

Server Connection

Fill in the fixed IP address on the panel to configure the MX-AOPC Address and Port settings. The default port number is 9900. The port number should be the same as the setting in MX-AOPC Server.

Enable Connection to Active OPC Server, with Heartbeat sec.

Redundant mode

Single server mode 1st AOPC Server
 Synchronicity mode 2nd AOPC Server
 Fail-over mode Port

- **Heartbeat Interval**

The **Heartbeat Interval** can be used to determine the connection status between the ioLogik 2500 and MX-AOPC Server, and to ensure that the ioLogik 2500 is connected and alive. If the heartbeat interval is set and the network between the ioLogik 2500 and MX-AOPC Server is down, MX-AOPC Server will detect the stopped heartbeat and the Quality column in the MX-AOPC will display BAD to indicate the loss of connectivity.

- **Single server mode:**

No redundancy: connects to a single MX-AOPC.

- **Synchronicity mode:**

Synchronize with 2 MX-AOPC servers at the same time.

- **Fail-over mode:**

The ioLogik 2500 will try to connect with the first MX-AOPC Server IP. If it cannot connect, it will automatically connect with the second IP, and when the connection to the second IP fails, it will switch back to the first IP.

Tag Selection

The I/O status of a channel can be updated to the MX-AOPC Server once it is changed, or updated periodically.

- **On Change / Percentage**

The On Change / Percentage setting forces an update when there is a signal change for that channel (percentage change is available for analog channels).

- **Interval / Interval Time**

To periodically update the status of the MX-AOPC Server, enable the **Interval** and specify a time interval in the **Interval Time** column.

NOTE If AI is configured to update on change, the percentage settings represent the percentage of the full analog range. For example, if the AI is configured to 0 to 10 V, "On Change 1%" means the ioLogik will update the MX-AOPC Server every time there is 0.1 V change.

NOTE The ioLogik 2500 supports Moxa's MX-AOPC UA server.

SNMP Server

The ioLogik supports SNMP (Simple Network Management Protocol) V1, V2c, and V3 to monitor network and I/O devices with SNMP Network Management software. It is useful in building automation and telecom applications. Use these fields to enable SNMP and set the read and write community strings for SNMP V1 and V2c, or use authentication for SNMP V3.

<input checked="" type="checkbox"/> Enable SNMP	
Version	<input type="text" value="V1 and V2c and V3"/>
Contact	<input type="text"/>
Location	<input type="text"/>
SNMP V1, V2c	
Read Community	<input type="text" value="public"/>
Write Community	<input type="text" value="private"/>
SNMP V3 Read Only	
User Name	<input type="text"/>
Authentication Protocol	<input type="text" value="DISABLE"/>
Authentication Password	<input type="text"/>
Privacy Protocol	<input type="text" value="DISABLE"/>
Privacy Password	<input type="text"/>
SNMP V3 Read/Write	
User Name	<input type="text"/>
Authentication Protocol	<input type="text" value="DISABLE"/>
Authentication Password	<input type="text"/>
Privacy Protocol	<input type="text" value="DISABLE"/>
Privacy Password	<input type="text"/>

Serial Port

The ioLogik 2500 has a built-in 3-in-1 serial port that supports attaching field serial Modbus/RTU meters (either RS-232, RS-422, or RS-485), and allows the integration of this serial data so that it can be uploaded to the SCADA system.

Step 1: Set the serial port parameters: RS-232, RS-422, RS-485, Baudrate, Stop Bits, etc.

Port Setting

Mode	RS-232	Flow Control	None
Baudrate	115200	Data Bits	8
Stop Bits	1	Parity	None

Step 2: Choose the operation mode. There are four modes to choose from:

Dropdown menu showing operation modes:

- Disable
- Transparent Serial Tunnel (TCP Client)
- Transparent Serial Tunnel (TCP Server)
- Modbus TCP Gateway
- Modbus Serial Tag

Data Logging

Profile

The Profile List defines how to log the I/O data into the Micro SD card. A total of 10 profiles can be created, and multiple/duplicate channels can be included in different profiles.

Step1: Define how to log the data by specifying the Logging Type. Users can choose to log from different I/O channels.

Step2: Check mark I/O channels that you would like to add in the profile, and click **Add** to create a profile.

Step3: Click **Apply** to save the profile settings.

No.	Profile Name	Initial State	Total Profile Size (MB)	Records Pe...

Profile Settings

Name:

Enable at Power On

Total Profile Size in MB (512-32768):

Records Per File (1000-65000):

Select Tag

Select Module:

I/O Type:

Slot No.	Channel No.	Name	On Change

FTP

The FTP tab defines how to log I/O data into an FTP server. The FTP Service function provides upload service for data log files stored on the Micro SD card.

FTP Client Settings		FTP Server Settings	
IP (or URL) ftp://	<input type="text"/>	User Name	<input type="text" value="admin"/>
Port	<input type="text" value="21"/>	Password	<input type="password" value="••••"/>
User Name	<input type="text"/>	Confirm Password	<input type="password" value="••••"/>
Password	<input type="password"/>		
Confirm Password	<input type="password"/>		

NOTE default user name: admin
default password: moxa

Click & Go Component

Click&Go components are designed for Click&Go Plus rules. When a set of rules (known as a rule-set) is defined using Click&Go Plus, the ioLogik can perform local and remote I/O control, report I/O status, and actively send out messages, e-mails, or SNMP traps to a host as soon as the user-defined I/O conditions have been met.

For a detailed introduction on how to use this function, refer to Chapter 2 of the [Click&Go Plus User's Manual](#).

Click&Go Plus

Click&Go Plus logic provides an easy way to program your ioLogik 2500 product for smarter I/O functionality over an Ethernet network. For a detailed introduction on how to use Click&Go Plus, refer to Chapter 3 of the [Click&Go Plus User's Manual](#).

Click&Go Plus Simulator

When you finish defining your Click&Go rules, you can use the Click & Go plus Simulation tool to test the rules. For a detailed introduction of how to use this function, refer to Chapter 4 of the Click & Go Plus User's Manual.

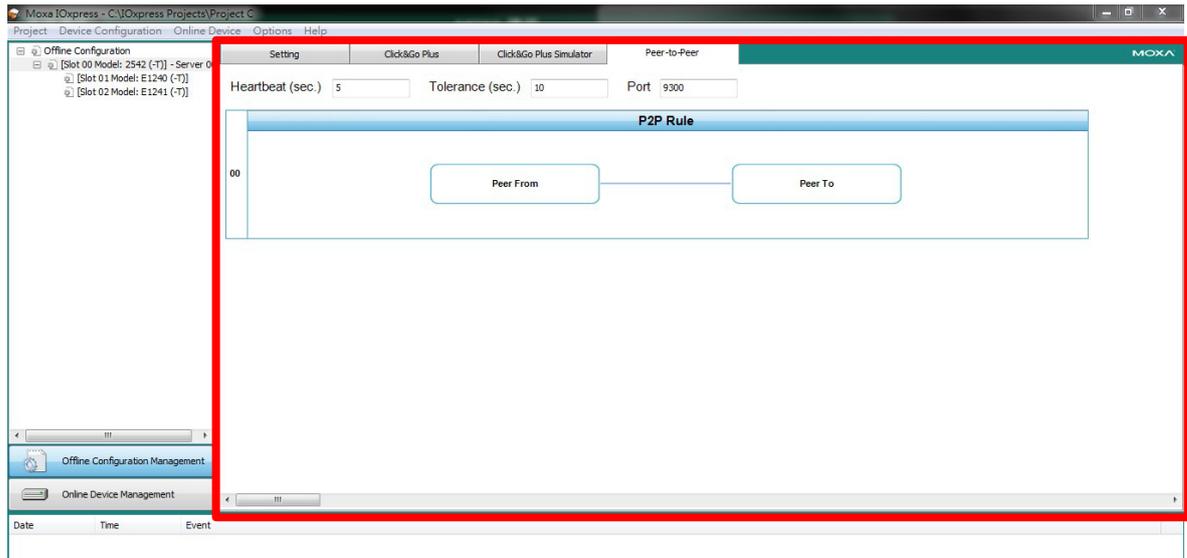
Peer-to-Peer

In some remote automation implementations, the control room and field sensors may be located far apart from each other, often with only a single remote I/O module to collect data from all the sensors.

Peer-to-peer communication has little or no limitation since it replaces cable by integrating multiple I/O signals over a single network cable to transmit input-to-output controls without the aid of PLCs or controllers.

With peer-to-peer communication and support for channel-to-channel mapping, the ioLogik 2500 allows simultaneous multiple target transmissions. In addition, the ioLogik 2500 supports up to 16 channels for transmission over Ethernet (based on an emitter and receiver I/O pair).

Click on **Peer to Peer** in the menu bar to configure basic device settings.



General Settings

Heartbeat (Sec)

Heartbeat is used to determine the connection status between P2P devices and to ensure that the ioLogik 2500 is connected and alive.

NOTE If the heartbeat interval is set and the network between the P2P devices is down, the ioLogik 2500 will detect lack of heartbeat, and then disconnect the P2P connection.

Tolerance (Sec)

Tolerance allows you to define an additional timeout interval to wait for a heartbeat signal from P2P devices.

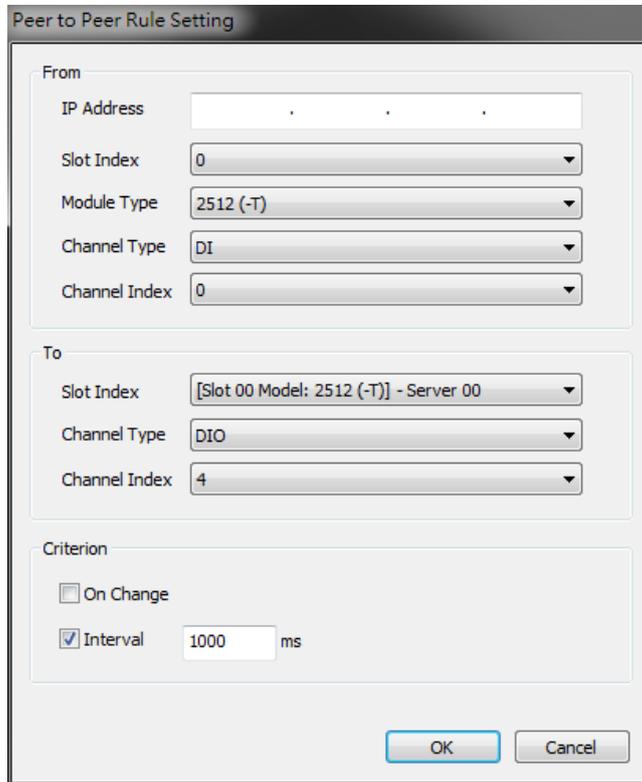
Port

The default local listen port number is 9300; this value can be set from 1 to 65535.

P2P Rule Settings

With peer-to-peer communication and support for channel-to-channel mapping, the ioLogik 2500 allows simultaneous multiple target transmissions.

In a P2P rule, the ioLogik 2500 can be configured to receive a signal from a remote site and output the signal at the local site, allowing you to configure the remote site information by configuring the IP address, slot index (for expanded E1200 units), and module type.



The image shows a 'Peer to Peer Rule Setting' dialog box with the following fields:

- From:**
 - IP Address: [. . .]
 - Slot Index: 0
 - Module Type: 2512 (-T)
 - Channel Type: DI
 - Channel Index: 0
- To:**
 - Slot Index: [Slot 00 Model: 2512 (-T)] - Server 00
 - Channel Type: DIO
 - Channel Index: 4
- Criterion:**
 - On Change
 - Interval: 1000 ms

Buttons: OK, Cancel

IP Address

The IP address of the device that collects and sends signals.

Slot Index

An integer used to represent the ioLogik 2500 and its E1200 expansion units.

- 0: represents the ioLogik 2500 head unit
- 1 to 8: represents an E1200 expansion unit

Module Type

The module type of the source ioLogik 2500.

Channel Type

The DI or DIO channel of the selected unit.

Slot Index

The channel index of the unit.

On change/Interval

You can set the Interval Time and On change percentage on the local ioLogik 2500 to trigger the transmission of a mapping signal to the remote ioLogik 2500.

NOTE Up to 16 P2P rules can be set (a set of ioLogik2500 + up to 8 x E1200).

NOTE As you configure a DI or AI channel in the Local Channel field, you also need to configure the DO or AO channel on the remote ioLogik devices.

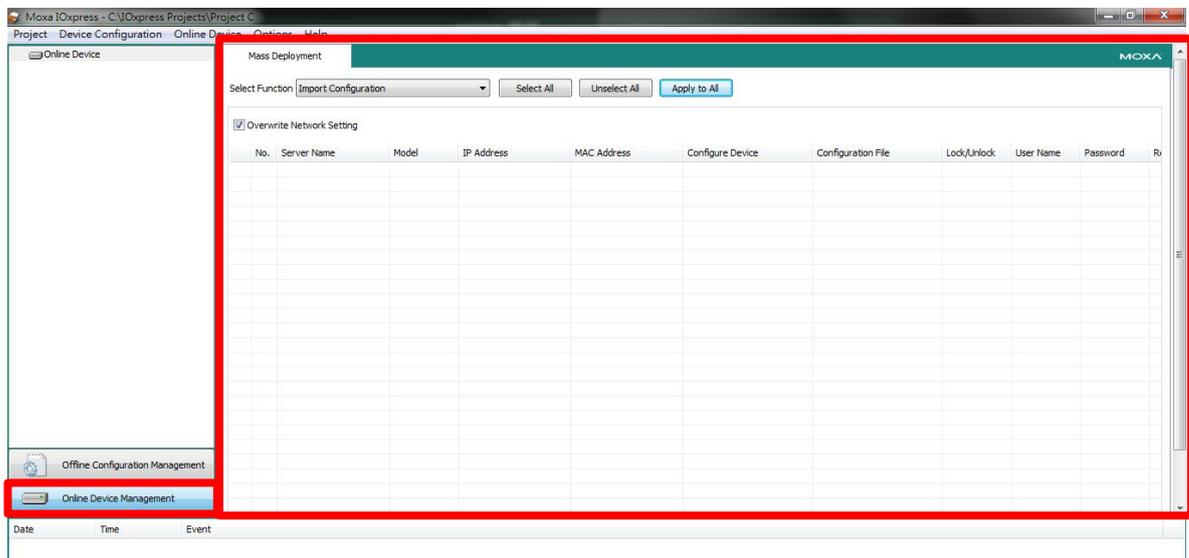
NOTE The peer to peer channel at the remote field site will be mapped automatically. Peer-to-peer settings only need to be configured in the local ioLogik 2500 devices.

Online Configuration

Introduction

Online configuration provides two main functions:

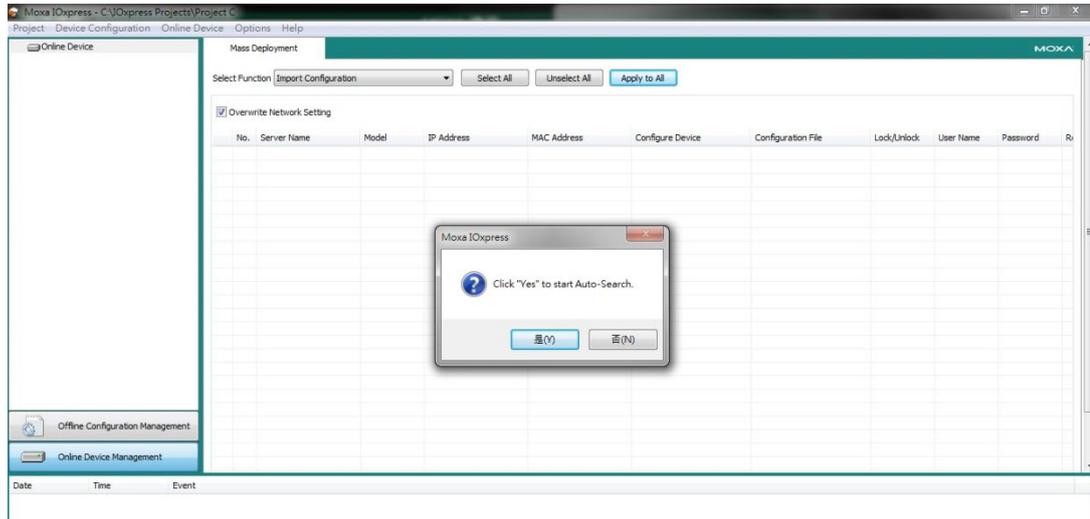
- Importing offline configurations to online devices.
- Monitoring all online devices, such as I/O status, upgrade firmware, import configuration, export configuration, and device reset.



Searching for Online Devices

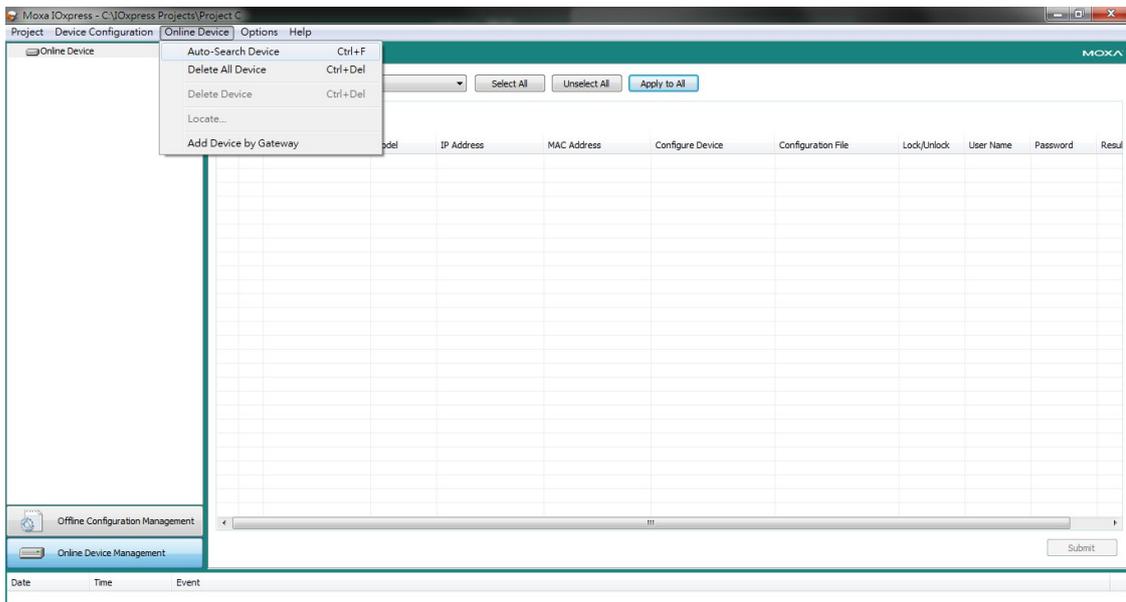
First Time Searching for Devices

- When you click **Online Device Management**, IOExpress will automatically display an auto-search information popup window.
- Click **Yes** to start searching for devices.
- The search information will be displayed in the Log.



Conducting Another Search for Online Devices

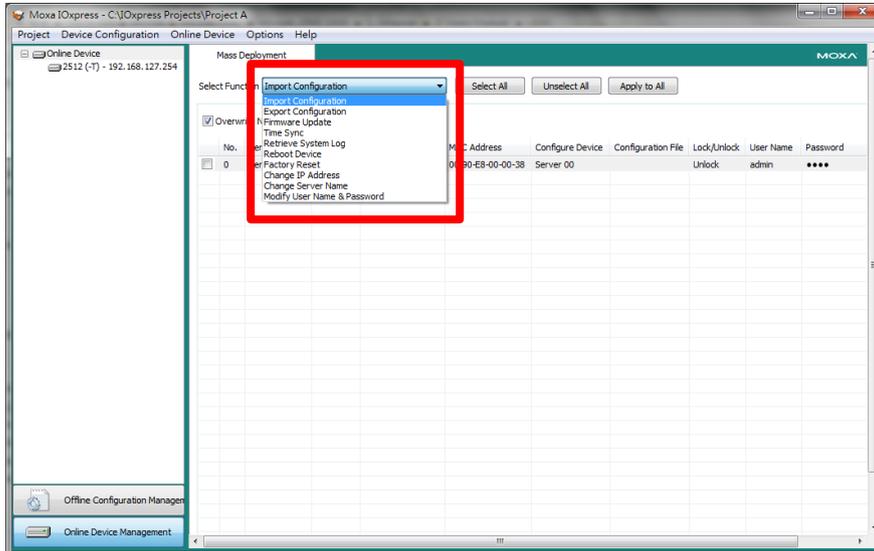
If you would like to conduct another search for online devices, click **Auto-search Device** in the **Online Device** menu.



Mass Deployment

Mass deployment allows you to deploy multiple devices at the same time. To execute a mass deployment, first click **Online Device** in the left panel, and then click **Import Configuration** to open the dropdown box. Ten different functions can be used for mass deployment, including **Firmware Update**, **Reboot Device**, and **Change IP Address**, as shown in the figure below.

The following sections will introduce how these functions work.



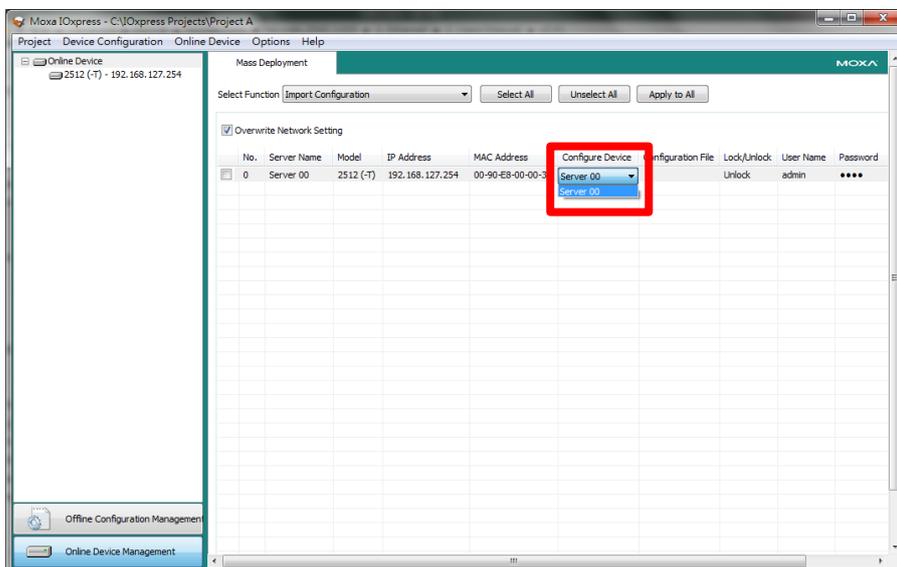
Import Configuration

The ioLogik's system configuration, including the current Click&Go Plus rule-set, can be imported and exported to the ioLogik 2500 device. You will need to know the user name and password to use this functionality.

There are two ways to import a configuration:

Configure Device:

To import from a preset offline configuration, click the **Configure Device** column and select the configuration you created.



Configuration File:

Import from configuration files saved on your computer.

NOTE If the device is Locked, you must log in as administrator to gain access to the ioLogik's configuration options. If you have not updated the username and password, use the default:

Default User Name: admin

Default password: moxa

NOTE If you do not want to change a device's network settings, uncheck the **Overwrite Network Setting** checkbox.

Overwrite Network Setting

Export Configuration

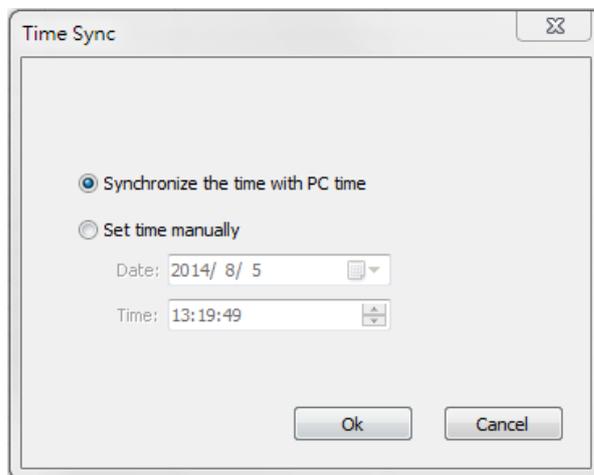
After you make changes to a rule-set, you can export the system configuration to save the updated rule-set.

Firmware Update

The **Firmware Update** tab is available after you log in as administrator. Enter the path to the firmware file or click on the icon to browse for the file. Click **Update** to update the ioLogik firmware. The wizard will lead you through the entire process, including restarting the ioLogik.

Time Sync

The ioLogik 2500 can be set to be synchronized with PC time, or the time can be set manually.



Retrieve System Log

You can retrieve the system logs from selected devices and save the logs as Notepad files on your computer. System logs contain system operations information, like firmware upgrades, restarts, and configuration imports.

Reboot Device

Select this command to restart a selected ioLogik 2500.

Factory Reset

Select this command to reset all settings on the selected ioLogik, including the password and all configuration settings, to factory default values.

Change IP Address

Use this function to change the IP address.

Change Server Name

Use this function to change the server name.

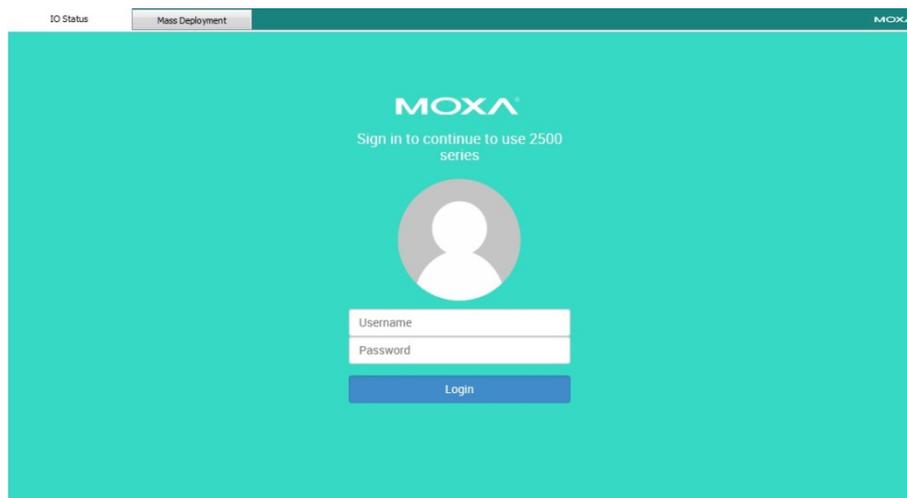
Modify User Name & Password

Use this function to change the User Name & Password.

Deploying Individual Devices

To check device information for individual devices, click the device listed in the Online Device column and then log in to the device.

Online Device
2542 (-T) - 192.168.127.254



- NOTE**
- Default user name: admin
 - Default password: moxa

Note: The user name and password are **case-sensitive**.

IO Status

The IO status tab allows you to execute the following information:

I/O information

The following information will appear at the top of the page.

MOXA®		ioLogik 2542		www.moxa.com	
■ Name	- ioLogik 2542-T	■ IP	- 192.168.127.254	■ MAC address	- 00-90-E8-00-00-00
■ Firmware	- V1.0.0.0	■ Click & Go	- Stop	■ Connection status	- Connecting

I/O status

Check the complete I/O status.

Upgrade

Click this icon to upgrade the firmware.

Import

Click this icon to import a device configuration.

Export

Click this icon to export a device configuration.

Reset

Click this icon to reset the device to factory default.

Cellular Network Setup and Configuration (for cellular models)

In this chapter, we introduce how to set up your ioLogik 2500-GPRS/HSPA device.

The following topics are covered in this chapter:

- ❑ **IOxpress Settings for a Cellular Network**
 - Select Major Network Interface
 - Cellular
- ❑ **Cellular Network Connection**
 - MX-AOPC Server (for SCADA/HMI users)
 - With DDNS (for SCADA/HMI users)
 - Moxa Cellular Data Access Utility (for mobile devices/PCs)

I Opress Settings for a Cellular Network

When you add an ioLogik 2500-GPRS/HSPA model, the following two functions will be available (in addition to the functions discussed in Chapter 3).

Select Major Network Interface

Configure your device's cellular network settings on the **Select Major Network Interface** page, which is located under the **Network-General** sub-page.

The screenshot shows the 'Select Major Network Interface' configuration page. At the top, there are tabs for 'Click&Go Plus', 'Click&Go Plus Simulator', and 'Peer-to-Peer'. On the left, a navigation tree shows 'Setting' > 'Network' > 'General' selected. The main content area is titled 'Select Major Network Interface' and contains the following sections:

- Cellular Only** (selected):
 - Cellular Always On
 - Cellular On Demand
 - By Click&Go Plus
 - Wake On Call
- Ethernet as Primary and Cellular as Backup** (not selected):
 - Dest IP/URL: (Active OPC Server or any public URL)
 - Continuous check until: fails (1 to 255)
 - Retry Interval: (10 to 600 sec.)
- General Settings**:
 - Enable Web Access
 - Enable Server Socket Idle Connection Timeout (sec.):
 - Private IP for First Module:

Cellular Only

You can configure under what conditions the ioLogik 2500-GPRS/HSPA will connect to the cellular network. For example, the device could be triggered by a Click&Go Plus rule or by wake on call.

Cellular ON Demand

This mode allows the ioLogik 2500-GPRS/HSPA to conserve power by flipping into sleep mode whenever there is no need to transmit information. When in sleep mode, the ioLogik 2500-GPRS/HSPA disables the cellular connection and stays in standby mode, saving all I/O records in the data log on the SD card. The ioLogik 2500-GPRS/HSPA will only wake up when either:

1. It receives an activate message from Click&Go, or
2. It receives a call from an authorized caller phone number.

Ethernet as Primary and Cellular as Backup

By selecting this function, a remote destination is used in this setting to indicate if the Internet connection is still alive. The user can specify a public IP or URL and the number of retries that are allowed. If the Ethernet is disconnected, the cellular connection will be triggered as a backup.

Dest IP/URL

This option, which can be configured to either an AOPC server IP or any public URL, will be used by the device to determine whether or not it is connected to the Internet.

Continuous Check Until 3 failures

The ioLogik 2500-GPRS/HSPA continuously check its connection with the IP/URL to ensure that it is constantly connected to the internet (could incur a high cost, depending on your cellular plan).

Retry Interval

The "retry interval" is the time interval between retries.

Cellular

Cellular network settings are configured on the "cellular" page, which is located under "Network."

General

To set up your cellular connection, click the **Cellular Settings** tab and enter your **User name**, **Password**, **SIM pin code**, and **APN** of your Cellular Provider (contact your local Cellular Service Provider for assistance).

Cellular Data Network Settings (SIM1)		Cellular Data Network Settings (SIM2)	
Username	<input type="text"/>	Username	<input type="text"/>
Password	<input type="text"/>	Password	<input type="text"/>
SIM PIN	<input type="text"/>	SIM PIN	<input type="text"/>
APN	internet	APN	internet
Band	Auto	Band	Auto
PPP Authentication	Auto mode	PPP Authentication	Auto mode
Dial AT Command	ATD*99***1#	Dial AT Command	ATD*99***1#

VPN

In this section, we explain how to set up a VPN connection for the ioLogik 2500-GPRS/HSPA.

Enable VPN

<input type="checkbox"/> Enable VPN			
VPN Tunnel Mode	Manual Key		
Remote Endpoint IP	. . .	Local Subnet IP	. . .
Remote Subnet IP	. . .	Local Subnet Netmask	255 . 255 . 255 . 0
Remote Subnet Netmask	255 . 255 . 255 . 0		

VPN Tunnel Mode

The type of VPN tunnel policy to be used; either manual key IPsec or ISAKMP with Pre-shared Keys (PSK).

Remote Endpoint IP

Enter the **WAN IP** of the remote VPN server endpoint.

Remote Subnet IP:

Enter the remote VPN server subnet (LAN) IP of the remote network.

Remote Subnet netmask

Enter the remote VPN server subnet netmask of the remote network.

Local subnet IP

Enter the ioLogik 2500's subnet (LAN) IP.

Local Subnet netmask

Enter the ioLogik 2500's subnet netmask.

Manual Key

Manual Key			
Incoming Security Settings			
SPI	<input type="text"/>	Encryption Mode	DES
Encryption Key	<input type="text"/>	Authentication Mode	MD5
Authentication Key	<input type="text"/>		
Outgoing Security Settings			
SPI	<input type="text"/>	Encryption Mode	DES
Encryption Key	<input type="text"/>	Authentication Mode	MD5
Authentication Key	<input type="text"/>		

SPI

Set the VPN manual key for incoming/outgoing SPI between 257 and 4294967295.

Encryption mode

Select the incoming/outgoing encryption mode.

Encryption key

Enter the incoming/outgoing encryption key.

Encryption mode	Length (bytes)
DES	8
3DES	24
AES 128bit	16
AES 192bit	24
AES 256bit	32

Authentication mode

Select the incoming/outgoing authentication mode.

Authentication key

Enter the incoming/outgoing authentication key.

Authentication mode	Length (bytes)
MDS	16
SHA1	20

ISAKMP/PSK

ISAKMP/PSK

ISAKMP (Key Management)

Pre-Share Key (PSK)

Perfect Forward Secrecy (PFS)

Local Identify

Identity Option Default IP

IP/FQDN/User-FQDN

ISAKMP Phase 1

Operation Mode Main

NAT Traversal (NAT-T)

Encryption Mode DES

Authentication Mode MD5

Diffie-Hellman Group Group1-768 bits

SA Lifetime 86400 (600-86400 sec.)

ISAKMP Phase 2

Encryption Mode DES

Authentication Mode MD5

Diffie-Hellman Group Group1-768 bits

SA Lifetime 28800 (600-86400 sec.)

Advanced Settings

Anti-Replay Dead Peer Detection (DPD)

ISAKMP (Key Management)

Pre-shared key (PSK): Sets the VPN ISAKMP Pre-Shared key settings.

Perfect forward secrecy (PFS) (default = Disable): Enable or disable the Perfect Forward Secrecy. PFS as an additional security protocol.

Local Identity

Identity option: Select additional ID authentication requirements for the VPN using a specific IP Address, FQDN, or User FQDN settings.

IP/FQDN/User_FQDN: Enter an ID (IP/FQDN/User_FQDN) to identify and authenticate the local VPN endpoint.

ISAKMP phase 1

Operation mode: Select main mode or aggressive mode to configure the standard negotiation parameters for IKE Phase 1 of the VPN Tunnel.

NAT-T (default = Disable): Enabling this option will allow IPSec traffic from this endpoint to traverse through the translation process during NAT. The remote VPN endpoint must also support this feature and it must be enabled to function properly over the VPN.

Encryption mode: Select the VPN ISAKMP phase 1 encryption mode. **Authentication mode:** Select the VPN ISAKMP phase 1 authentication mode. **Diffie-Hellman group:** Select the VPN ISAKMP phase 1 DH group. As the DH Group number increases, the higher the level of encryption implemented for PFS.

SA life time (default = 86400): Enter the number of seconds for the VPN ISAKMP phase 1 Lifetime. This is the period of time that passes before establishing a new IPSec security association (SA) with the remote endpoint.

ISAKMP phase 2

Encryption mode: Select the VPN ISAKMP phase 2 encryption mode. **Authentication mode:** Select the VPN ISAKMP phase 2 authentication mode.

Diffie-Hellman group: Select the VPN ISAKMP phase 2 DH group. As the DH Group number increases, the higher the level of encryption implemented for PFS.

SA life time (default = 28800): Enter the number of seconds for the VPN ISAKMP phase 2 Lifetime. This is the period of time that passes before establishing a new IPSec security association (SA) with the remote endpoint.

Advanced settings

Anti-replay (default = Disable): Anti-replay is the method of not allowing an intercepted packet message to be sent to the recipient multiple times without the original sender knowing about it.

Dead Peer Detection (DPD) (default = Disable): Enable or disable Dead Peer Detection. DPD is a method of detecting a dead Internet Key Exchange (IKE) peer. It sends a DPD packet to the peer every 60 seconds under no traffic and attempts to connect normally. If the DPD packet fails 5 times the VPN will continuously re-establish a connection.

Reconnection

Carriers disconnect idle mobile device connections in order to save bandwidth for other on-line users and applications. To keep the ioLogik 2500-GPRS/HSPA always On, the ioLogik 2500-GPRS/HSPA must not only have the capability to detect the cellular connection and reconnect to the network once it is disconnected, but also needs to send out signals (ICMP package) to notify carriers that the ioLogik 2500-GPRS/HSPA is still alive.

Cellular Network Reconnection Settings

Timeout (30 to 65535 sec.)

Retries (3 - 65535, 10 to 30 sec. per retry)

Ping Settings

Dest. IP/URL (Any public URL)

Retry Interval (10 to 600 seconds)

Note: Cellular modem will be restarted after pinging the URL fails 3 times.

Enable SIM Failover Mode

Reboot system after Hours (1 to 24)

System automatically reboots if reconnection and ping fail after the defined period.

Cellular Network Reconnection Settings

This setting defines the timeout for detecting the physical cellular connection. Once the ioLogik reaches the timeout, it will perform a system restart.

Timeout

When you turn on the ioLogik 2500-GPRS/HSPA, the device will continue to connect to the GSM for a period of 60 seconds (the default setting). If it fails to connect, the device will automatically restart the modem board after 60 seconds.

Retries

After the connection between the device and GSM (carrier) has been made, the device will try to connect with the Internet. After 5 times (the default setting) of failed retry, the ioLogik 2500-GPRS/HSPA will restart the modem board.

Ping Settings

A remote destination is used in this setting to indicate if the Internet connection is still alive. The user can specify a public IP or URL and the number of retries that are allowed.

Dest IP/URL

Can either be an AOPC server IP or any public URL for the device to check its connection with the internet.

Retry Interval

The retry will be activated when the AOPC can't connect with the AOPC server. The ioLogik 2500-GPRS/HSPA will tell the machine to ping the Dest IP/URL to check for an Internet connection.

Enable SIM Failover Mode

When the **Enable SIM Failover Mode** checkbox is selected, the ioLogik 2500-GPRS/HSPA will switch from one SIM card to the other when a connection cannot be established using the active SIM card.

System Reconnect after 1 hours (1 to 24)

If **Carrier Check before system restart** or **PING Check before system restart** is selected, the system will check if there is still a wireless connection.

If the wireless signal is unstable and disconnects, the ioLogik 2500-GPRS/HSPA will first reboot the modem to restore the physical layer connection. Enable **System Reconnect** to reinitiate the ioLogik 2500-GPRS/HSPA. If rebooting the modem does not recover your connection, the disconnection may be caused by a higher layer communication problem. You may select a **System Reconnect** interval from 1 to 24 hours.

Port Forwarding

The ioLogik 2500-GPRS/HSPA supports port forwarding on its cellular and Ethernet interfaces for WAN-to-LAN communication. Using port forwarding, the ioLogik W5300 allows external WAN hosts such as SCADA/HMI systems to connect to specific field devices within the LAN by linking with the ioLogik 2500-GPRS/HSPA.

Enable Port Forwarding

Enabled	Index	Protocol	Public Port	Internal IP	Internal Port
<input type="checkbox"/>	0	TCP	0	0.0.0.0	0
<input type="checkbox"/>	1	TCP	0	0.0.0.0	0
<input type="checkbox"/>	2	TCP	0	0.0.0.0	0
<input type="checkbox"/>	3	TCP	0	0.0.0.0	0
<input type="checkbox"/>	4	TCP	0	0.0.0.0	0
<input type="checkbox"/>	5	TCP	0	0.0.0.0	0
<input type="checkbox"/>	6	TCP	0	0.0.0.0	0
<input type="checkbox"/>	7	TCP	0	0.0.0.0	0
<input type="checkbox"/>	8	TCP	0	0.0.0.0	0
<input type="checkbox"/>	9	TCP	0	0.0.0.0	0

Note: The Internal IP cannot be on the same subnet as the IO expansion module (currently 192.168.120.1).

DDNS

The purpose of DDNS is to provide you with an alternative cost effective cellular plan. You will not need to establish a server or pay for a Static IP. Setting up DDNS allows the ioLogik 2500-GPRS/HSPA to behave like a server and perform functions such as email, ftp, etc. Regardless of whether the device has a floating IP or a private IP, the user can establish a connection with their remote device through DDNS. DDNS allows the SCADA/HMI server to establish a connection through the DDNS server to find the remote device.

Enable DDNS

Service Provider: DynDns.org

Host Name:

Username:

Password:

Service Provider (default=DynDns.org)

Currently, DynDns.org is the only option available for Server address.

Host name

Enter the name you created on www.dyndns.com in this field. The ioLogik 2500-GPRS/HSPA will update the DynDNS server with this host name.

Username

This is the user name used for updating DDNS Server authentication.

Password

This is the password used for updating DDNS Server authentication.

Cellular Data Access

The **Cellular Data Access** setting is used for connecting to Moxa cellular data access utilities.

For detailed information on how to set up the cellular data access server, see the next section, **Moxa Cellular Data Access Utility**.

Enable Cellular Data Access

IP Address: 0 . 0 . 0 . 0

Port: 9401

Unique ID: 0

Heartbeat (sec.): 30

IP address

Enter the IP address of the cellular data access server.

Port

Enter the port number of the cellular data access server.

Unique ID

The unique ID is used for remote action functions. For detailed information, refer to the Click&Go Plus User's Manual.

Heartbeat (sec.)

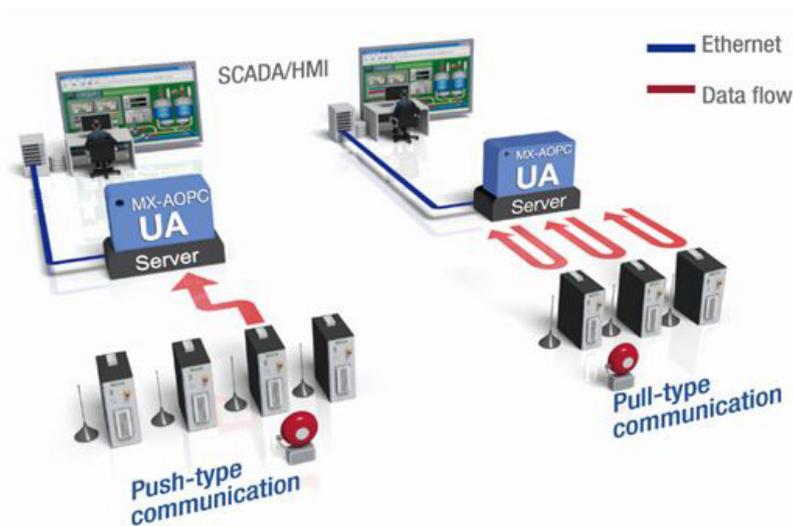
The heartbeat is used to determine whether or not the connection between an ioLogik device and the cellular data access server is still active.

Cellular Network Connection

The dynamic IP addresses commonly used for cellular connections make it hard for control systems to link to cellular data acquisition devices. With Moxa's MX-AOPC server, SCADA/HMI users can easily connect to field I/O devices. For web-based applications, Moxa's cellular data access utility provides an ideal way to seamlessly connect to remote cellular IO units.

MX-AOPC Server (for SCADA/HMI users)

To allow private networks to get around the connectivity issues raised by edge devices configured with dynamically assigned private IP addresses, typically operators purchase high-cost static IP addresses for each device, with IPs provided by a DDNS or VPN service purchased from an MVNO (Mobile Virtual Network Operator). Even with DDNS technology, SCADA systems need to assign resources to manage the DDNS servers. As an alternative, Moxa's Cellular remote I/O devices use Moxa's proprietary "push" technology, called MX-AOPC Server.



With Moxa's powerful MX-AOPC Server support, communications efficiency between ioLogik 2500-GPRS/HSPA devices and the central SCADA are substantially improved. Moxa's MX-AOPC Server's non-polling communications architecture supports the standard OPC protocol, but instead of requiring the SCADA to poll edge devices it allows edge devices to actively push communications to the central HMI/SCADA system, empowering the network with real time I/O updates while substantially cutting network overhead.

Unlike the requirements of a traditional OPC server (where remote I/O devices must use a static IP so they may be successfully polled), MX-AOPC Server and ioLogik products allow engineers the flexibility of configuring edge devices with dynamic IP addresses. Even when using DHCP addressing, ioLogik devices can push messages back to the OPC server, allowing wide area I/O networks using dynamic IP cellular accounts. Using traditional polling OPC applications, I/O devices cannot make use of this approach.

With DDNS (for SCADA/HMI users)

In addition to using MX-AOPC Server to register an ioLogik ioLogik 2500-GPRS/HSPA with SCADA over a dynamic IP cellular connection, you may also use DDNS to configure the device with a unique URL. The ioLogik 2500-GPRS/HSPA can be configured to register a DNS hostname (i.e. – URL) with DDNS, and thereby convert a dynamic IP to a publicized address. In this way, centralized control software will be able to connect to the remote ioLogik W5300 without requiring a fixed IP or VPN service from a network provider.

Moxa Cellular Data Access Utility (for mobile devices/PCs)

With the Moxa cellular data access utility, you can configure the ioLogik 2500-GPRS/HSPA using the IOxpress utility over the cellular network. You can also log on to selected ioLogik 2500 devices by using a specific URL port. In this section, we explain how to use these two methods to connect devices.

Step1: Installing Cellular Data Access Utility on a server PC

Cellular Data Access Utility is a Windows utility provided for connecting and managing the ioLogik 2500-GPRS/HSPA over a cellular network. Cellular Data Access Utility can be used from anywhere on the network to monitor and configure the ioLogik 2500-GPRS/HSPA.

Installing from the CD

Insert the Document and Software CD into the host computer. In the Software/Utility directory of the CD, locate and run **SETUP.EXE**. The installation program will guide you through the installation process and install the ioAdmin utility. After the installation is finished, run ioAdmin from the Windows Start menu.

Downloading from Moxa's Website

Click the following link: <http://www.moxa.com/support/search.aspx?type=soft>.

Enter the name of the product you have purchased into the search bar or select it from the dropdown menu, and after navigating to the product page click on Utilities, in the middle of the page, located in the box titled Software.

Step2: Use “offline configuration” to set up the ioLogik 2500-GPRS/HSPA

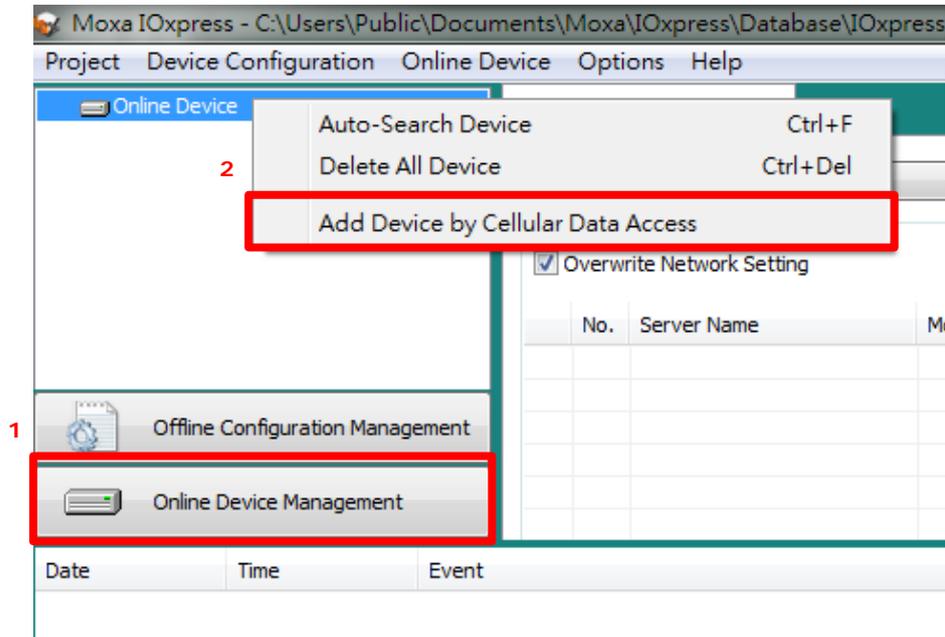
Before you start using the cellular data access utility, set up the “cellular data access” function. See the **Cellular Data Access** section in this chapter for details.

Step3: Connect to the device over the cellular network

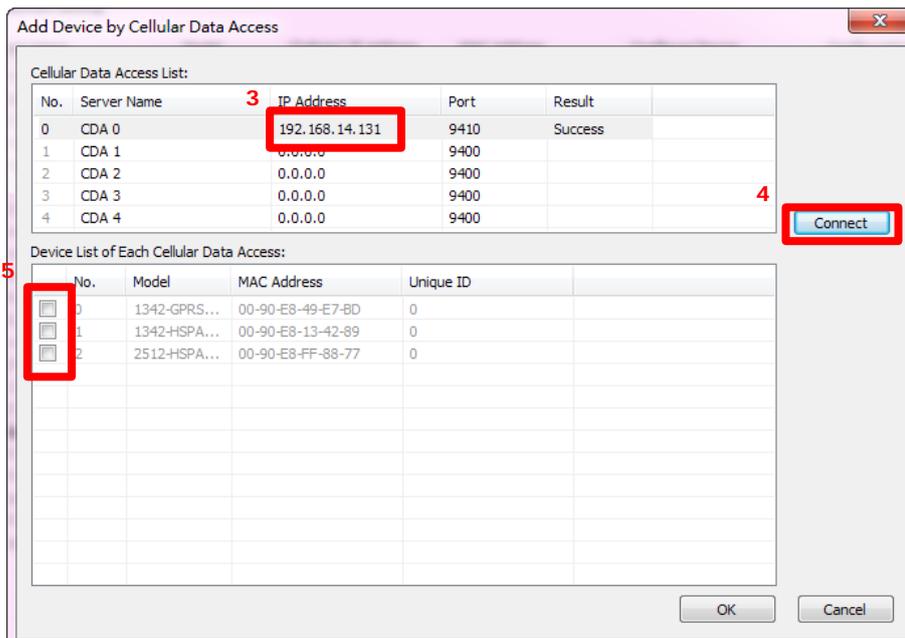
Using IOxpress

Connect to the cellular Data Access server using Online Device Management, as described below:

1. Click **Online Device Management**.
2. Select **Add Device by Cellular Data Access**.



3. Type in the server's IP address and port number.
4. Click the **Connect** checkbox.
5. Select the cellular device that you would like to connect to.

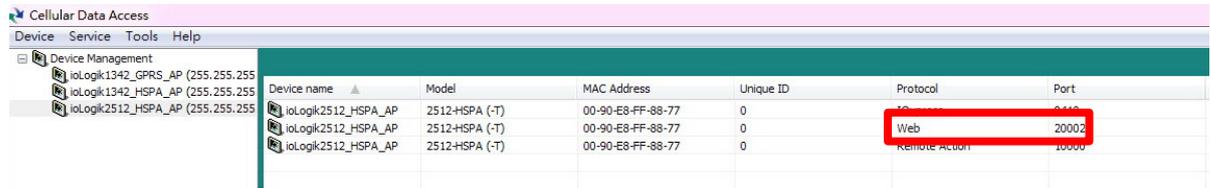


6. The selected devices have been added to the online device list, and you can start to upload/configure your devices over the cellular network.

Using a browser URL

1. Check the port number in the cellular data access utility.

Once the devices are connected, the utility will automatically assign URL ports to the devices.



Device name	Model	MAC Address	Unique ID	Protocol	Port
ioLogik2512_HSPA_AP	2512-HSPA (-T)	00-90-E8-FF-88-77	0	Web	20002
ioLogik2512_HSPA_AP	2512-HSPA (-T)	00-90-E8-FF-88-77	0	Remote Action	10000

2. Access the device via the browser.

You can use the URL to connect to the device by typing **http://[IP address]** of Moxa Cellular access server port : number of the device assigned by the server.

E.g., 192.168.17.253:20002

Wireless LAN Network Setup and Configuration (for Wireless LAN models)

In this chapter, we introduce how to set up your ioLogik 2500-WL1 device.

The following topics are covered in this chapter:

- ❑ **Deploying the ioLogik 2500-WL1**
- ❑ **IOxpress Settings for a Wireless LAN Network**
 - Wireless LAN

Deploying the ioLogik 2500-WL1

For testing requirements, we strongly suggest that you prepare a wireless LAN adapter. After finishing the installation and configuration, you should test the ioLogik 2500-WL1 to make sure the wireless transmission is working normally.

Step 1: Set up the computer's IP address, and the connect ioLogik 2500-WL1 to a notebook or PC.

In a Windows environment, the computer's IP address can be changed in the TCP/IP settings window. Select an IP address on the same subnet as the ioLogik 2500-WL1. Since the ioLogik 2500-WL1's default IP address is 192.168.127.253, and the subnet mask is 255.255.255.0, you should set the IP address of the computer to 192.168.127.xxx.

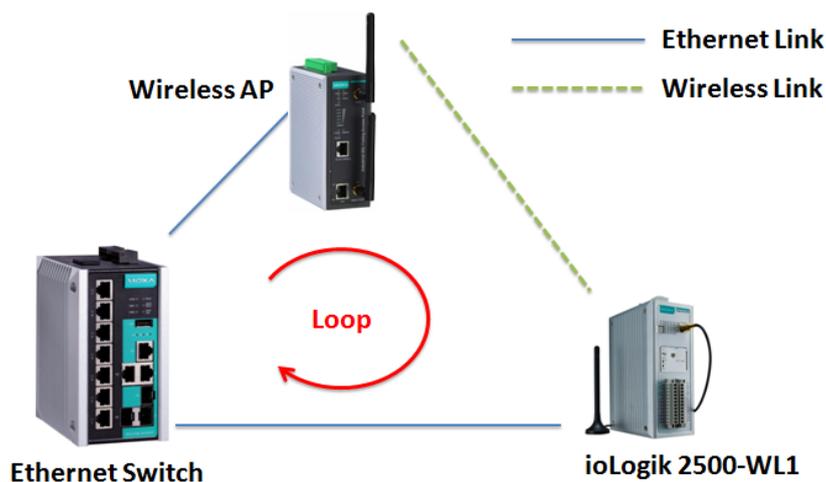
Step 2: Use the IOxpress utility to configure the ioLogik 2500-WL1.

See the following section to learn how to use IOxpress to configure the ioLogik 2500-WL1's functions.



ATTENTION

Be sure to eliminate loops from networks that consist of wireless bridges, Ethernet switches, Ethernet links, and Wireless LAN links. If any loops exist, packets will circle around the loops and network performance will be seriously degraded. The following figure shows a network topology containing a loop.



IOxpress Settings for a Wireless LAN Network

When you add an ioLogik 2500-WL1 model to your network, the following two functions will be available (in addition to the functions discussed in Chapter 3).

Wireless LAN

Cellular network settings are configured on the "cellular" page, which is located under "Network."

Basic

The Basic tab is used to add and edit RF type, channel width, and SSID.

RF Type

SSID

Setting	Description	Factory Default
B	Supports IEEE 802.11b only	B/G Mixed
G	Supports IEEE 802.11g only	
B/G Mixed	Supports both IEEE 802.11b/g standards, but 802.11g will operate more slowly when 802.11b clients are on the network	
A Only	Supports IEEE 802.11a only	

Channel Width

Channel Width

Setting	Description	Factory Default
20 MHz	Select your channel width. If you are not sure which option to use, select 20/40 MHz (Auto)	20 MHz
20/40 MHz		

SSID

An SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSIDs.

SSID

Setting	Description	Factory Default
Max. of 31 characters	The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other.	MOXA

NOTE The model name of the ioLogik 2500-WL1 is shown as ioLogik 2500-WL-XX in IOxpress, where XX indicates the country code. The country code indicates the ioLogik 2500-WL1 version and which bandwidth it uses. We use ioLogik 2500-WL1-US as an example in the following figures. (The country code and model name that appear on your computer screen may be different than the ones shown here.)

Security

The ioLogik 2500-WL1 provides four standardized wireless security modes: Open, WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), and WPA2.

Security Mode

Open

No authentication, no data encryption.

For security reasons, users should NOT set the security mode to Open System, since authentication and data encryption are NOT performed in Open System mode.

WEP

Static WEP (Wired Equivalent Privacy) keys must be configured manually.

According to the IEEE 802.11 standard, WEP can be used for authentication and data encryption to maintain confidentiality. **Shared** (or **Shared Key**) authentication type is used if WEP authentication and data encryption are both needed. Normally, **Open** (or **Open System**) authentication type is used when WEP data encryption is run with authentication.

When WEP is enabled as a security mode, the length of a key (the so-called WEP seed) can be specified as 64/128 bits, which is actually a 40/104-bit secret key with a 24-bit initialization vector. The ioLogik 2500-WL1 provides 4 entities of WEP key settings that can be selected to use with **Key index**. The selected key setting specifies the key to be used as a send-key for encrypting traffic from the AP side to the wireless client side. All 4 WEP keys are used as receive-keys to decrypt traffic from the wireless client side to the AP side.

The WEP key can be presented in two **Key types**, HEX and ASCII. Each ASCII character has 8 bits, so a 64-bit WEP key contains 5 characters, and a 128-bit key has 13 characters. In hex, each character uses 4 bits, so a 64-bit key has 10 hex characters, and a 128-bit key has 26 characters.

Authentication type

Setting	Description	Factory Default
Open	Data encryption is enabled, but without authentication	Open
Shared	Data encryption and authentication are both enabled.	

Key type

Setting	Description	Factory Default
HEX	Specifies WEP keys in hex-decimal number format	HEX
ASCII	Specifies WEP keys in ASCII format	

Key length

Setting	Description	Factory Default
64 bits	Uses 40-bit secret keys with 24-bit initialization vector	64 bits
128 bits	Uses 104-bit secret key with 24-bit initialization vector	

Key index

Setting	Description	Factory Default
1-4	Specifies which WEP key is used	Open

WEP key 1-4

Setting	Description	Factory Default
	A string that can be used as a WEP seed for the RC4 encryption engine. ASCII type: 64 bits: 5 chars / 128 bits: 13chars HEX type: 64 bits: 10 hex chars / 128 bits: 26 hex chars	None

WPA/WPA2-Personal

Also known as WPA/WPA2-PSK. You will need to specify the Pre-Shared Key in the Passphrase field, which will be used by the TKIP or AES engine as a master key to generate keys that actually encrypt outgoing packets and decrypt incoming packets.

WPA (Wi-Fi Protected Access) and WPA2 represent significant improvements over the WEP encryption method. WPA is a security standard based on 802.11i draft 3, while WPA2 is based on the fully ratified version of 802.11i. The initial vector is transmitted, encrypted, and enhanced with its 48 bits, twice as long as WEP. The key is regularly changed so that true session is secured.

Even though AES encryption is only included in the WPA2 standard, it is widely available in the WPA security mode of some wireless APs and clients as well. The ioLogik 2500-WL1 also supports AES algorithms in WPA and WPA2 for better compatibility.

Personal versions of WPA/WPA2, also known as WPA/WPA-PSK (Pre-Shared Key), provide a simple way of encrypting a wireless connection for high confidentiality. A **Passphrase** is used as a basis for encryption methods (or cipher types) in a WLAN connection. The passphrases should be complicated and as long as possible. The Passphrase must have at least 8 ASCII characters, and can have as many as 63. For security reasons, this passphrase should only be disclosed to users who need it, and it should be changed regularly.

WPA/WPA2-Enterprise

WPA type

Setting	Description	Factory Default
Personal	Provides Pre-Shared Key-enabled WPA and WPA2	Personal
Enterprise	Provides enterprise-level security for WPA and WPA2	

Encryption method

Setting	Description	Factory Default
TKIP	Temporal Key Integrity Protocol is enabled	TKIP
AES	Advanced Encryption System is enabled	

Passphrase

Setting	Description	Factory Default
8 to 63 characters	Master key to generate keys for encryption and decryption	None

EAP Protocol

Setting	Description	Factory Default
TLS	Specifies Transport Layer Security protocol	TLS
TTLS	Specifies Tunneled Transport Layer Security	
PEAP	Specifies Protected Extensible Authentication Protocol, or Protected EAP	

WPA/WPA2-Enterprise

Also called WPA/WPA2-EAP (Extensible Authentication Protocol). In addition to device-based authentication, WPA/WPA2-Enterprise enables user-based authentication via IEEE 802.1X. The ioLogik 2500-WL1 can support three EAP methods: EAP-TLS, EAP-TTLS, and EAP-PEAP.

By setting **WPA type** to **Enterprise**, you can use EAP (Extensible Authentication Protocol), a framework authentication protocol used by 802.1X to provide network authentication. In these Enterprise-level security modes, a back-end RADIUS (Remote Authentication Dial-In User Service) server is needed if IEEE 802.1X functionality is enabled in WPA /WPA2. The IEEE 802.1X protocol also offers the possibility of carrying out an efficient connection authentication on a large-scale network. It is not necessary to exchange keys or passphrases.

WPA type

Setting	Description	Factory Default
Personal	Provides Pre-Shared Key-enabled WPA and WPA2	Personal
Enterprise	Provides enterprise-level security for WPA and WPA2	

Encryption method

Setting	Description	Factory Default
TKIP	Temporal Key Integrity Protocol is enabled	TKIP
AES	Advanced Encryption System is enabled	

Passphrase

Setting	Description	Factory Default
8 to 63 characters	Master key to generate keys for encryption and decryption	None

EAP-TLS

TLS is the standards-based successor to Secure Socket Layer (SSL). It can establish a trusted communication channel over a distrusted network. TLS provides mutual authentication through certificate exchange. EAP-TLS is also secure to use. You are required to submit a digital certificate to the authentication server for validation, but the authentication server must also supply a certificate.

EAP Protocol

Setting	Description	Factory Default
TLS	Specifies Transport Layer Security protocol	TLS
TTLS	Specifies Tunneled Transport Layer Security	
PEAP	Specifies Protected Extensible Authentication Protocol, or Protected EAP	

EAP-TTLS

It is usually much easier to re-use existing authentication systems, such as a Windows domain or Active Directory, LDAP directory, or Kerberos realm, rather than creating a parallel authentication system. As a result, TTLS (Tunneled TLS) and PEAP (Protected EAP) are used to support the use of so-called “legacy authentication methods.” TTLS and PEAP work in a similar way. First, they establish a TLS tunnel (EAP-TLS for example), and validate whether the network is trustworthy with digital certificates on the authentication server. This step establishes a tunnel that protects the next step (or “inner” authentication), and consequently is sometimes referred to as “outer” authentication. The TLS tunnel is then used to encrypt an older authentication protocol that authenticates the user for the network.

As you can see, digital certificates are still needed for outer authentication in a simplified form. Only a small number of certificates are required, which can be generated by a small certificate authority. Certificate reduction makes TTLS and PEAP much more popular than EAP-TLS.

The ioLogik 2500-WL1 provides some non-cryptographic EAP methods, including **PAP**, **CHAP**, **MS-CHAP**, and **MS-CHAP-V2**. These EAP methods are not recommended for direct use on wireless networks. However, they may be useful as inner authentication methods with TTLS and PEAP.

Because the inner and outer authentications can use distinct user names in TTLS and PEAP, you can use an anonymous user name for the outer authentication, with the true user name only shown through the encrypted channel. Keep in mind that not all client software supports anonymous alteration. Confirm this with the network administrator before you enable identity hiding in TTLS and PEAP.

TTL Inner Authentication

Setting	Description	Factory Default
PAP	Password Authentication Protocol is used	MS-CHAP-V2
CHAP	Challenge Handshake Authentication Protocol is used	
MS-CHAP	Microsoft CHAP is used	
MS-CHAP-V2	Microsoft CHAP version 2 is used	

Anonymous

Setting	Description	Factory Default
Max. of 31 characters	A distinct name used for outer authentication	None

User name & Password

Setting	Description	Factory Default
	User name and password used in inner authentication	None

PEAP

There are a few differences in the TLS and PEAP inner authentication procedures. TLS uses the encrypted channel to exchange attribute-value pairs (AVPs), while PEAP uses the encrypted channel to start a second EAP exchange inside of the tunnel. The ioLogik 2500-WL1 provides **MS-CHAP-V2** merely as an EAP method for inner authentication.

Inner EAP protocol

Setting	Description	Factory Default
MS-CHAP-V2	Microsoft CHAP version 2 is used	MS-CHAP-V2

Anonymous

Setting	Description	Factory Default
Max. of 31 characters	A distinct name used for outer authentication	None

User name & Password

Setting	Description	Factory Default
	User name and password used in inner authentication	None

Advanced

Additional wireless-related parameters are presented in this section to help you set up your wireless network in detail.

Advanced Settings

Transmission Rate

Setting	Description	Factory Default
Auto	The device senses and adjusts the data rate automatically	Auto

Transmission Power

Setting	Description	Factory Default
3 dBm to 20 dBm	The device adjusts the transmission Rate	10 dBm

Fragmentation threshold

Setting	Description	Factory Default
256 to 2346	Specifies the maximum size of a data packet before splitting and creating another new packet	2346

RTSreshold

Setting	Description	Factory Default
256 to 2346	Determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication	2346

WMM

Setting	Description	Factory Default
Enable/ Disable	WMM is a QoS standard for WLAN traffic. Voice and video data will be given priority bandwidth when enabled with WMM supported wireless clients.	Enable

Turbo Roaming

Setting	Description	Factory Default
Enable/ Disable	Moxa's Turbo Roaming can enable rapid handover when the device, as a client, roams among a group of APs.	Disable

AP Alive Check

AP alive check will check if the AP connection is still available. When this function is enabled, a check will be done every 10 ms.

Scan Channels

You can set up Scan channels for the APs among which this client is going to roam. There are three Scan channels available.

Note that the Scan channels may need to be modified when the RF type is changed. (For example, channel 36 is not available in B, G, or B/G Mix mode.)

Network Port Usage

The ioLogik 2500 uses the following network ports:

Usage	Type	Port	User-Defined
Serial Tunnel Client	TCP	1	✓
FTP Client	TCP	21	✓
FTP Server	TCP	21	✓
Web Console	TCP	80	
SNMP Server	TCP	161	
SNMP Client	TCP	162	
Modbus Communication	TCP	502	
SMTP	TCP	587	✓
Serial Tunnel Server	TCP	4001	✓
Auto Search Function	UDP	4800	
TCP/UDP Message	TCP	9000	✓
	UDP	9000	✓
Remote Action Function	TCP	9010	
Peer-to-peer Function	TCP	9300	✓
IOxpress	TCP	10124	
AOPC Protocol*	TCP	9200	
	TCP	9300	
	TCP	9500	
	TCP	9900	✓

*The ioLogik 2500 series only supports MX-AOPC UA server.

- NOTE**
- Client refers to when the ioLogik 2500 is acting as a client to connect other services.
 - Server refers to when the ioLogik 2500 is acting as a server to provide services to other devices.