WE-2100T Series User’s Manual

Third Edition, June 2008

www.moxa.com/product

© 2008 Moxa Inc., all rights reserved.
Reproduction without permission is prohibited.

WE-2100T 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

Copyright © 2008 Moxa Inc.
All rights reserved.
Reproduction without permission is prohibited.

Trademarks

MOXA 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 China (Shanghai office):
Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-10-6872-3958

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

Moxa Asia-Pacific:
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Table of Contents

1

Introduction

The WE-2100T is a small embedded serial-to-WLAN module that gives your serial device the ability to connect to a wireless network. It comes with built-in TCP/IP and wireless security/authentication protocols for fast integration, saving you time and energy on programming.

The following topics are covered in this chapter:

- ❑ **Overview**
- ❑ **Package Checklist**
- ❑ **Product Features**
- ❑ **Product Specifications**

Overview

The WE-2100T is a very compact module that installs in a serial device to connect it to a wireless LAN. With such a small size, around half the size of a credit card., it can be installed into almost any kind of serial device. The WE-2100T also comes with a built-in TCP/IP stack for fast integration with your serial devices. This means that your engineers can spend less time with the TCP/IP and wireless details, and more time on developing major features, shortening your product's time to market. The reliable TCP/IP communication firmware can be configured easily using a Windows utility, a web browser, serial console, or Telnet console. In addition, a Windows-based NECI (Network Enabler Configuration Interface) library is available to help you develop your own Windows utilities.

An integration kit and a complete development kit are both available for evaluation and development use. The development kit contains a development board, documents, sample code, cables, and accessories.

Package Checklist

- 1 WE-2100T Series module (depending on which model you order)
- 1 WE-2100T-ST (the evaluation board)
- WE-2100T Series Documentation & Software CD
- 1 power adaptor
- 1 null modem cable
- 1 cross-over Ethernet cable
- Product Warranty Booklet
- Quick Installation Guide

NOTE: Notify your sales representative if any of the above items is missing or damaged.

Product Features

The WE-2100T has the following features:

- 802.11 a/b/g compliance
- Auto-sensing TTL to 10/100 Mbps Ethernet interface
- Compact size and ready-to-go design
- Ready-to-use TCP/IP firmware for fast integration
- TCP Server, TCP Client, UDP, Real COM, RFC2217 operation modes
- Serial Command Mode for configuration through the data port
- Easy configuration by web console, serial console, Windows utility, or Telnet console
- 9 GPIOs for user-developed applications
- Software reset function

Product Specifications

WLAN	
Spread Spectrum Technology	DSSS,CCK,OFDM
Standards Compliance	802.11 a/b/g
Tx Power	5.15~5.25 GHz: 15 dBm@6 Mbps; 12 dBm@54 Mbps 5.725~5.825 GHz: 15 dBm@6 Mbps; 12 dBm@54 Mbps 2.412~2.483 GHz: 17 dBm@6 Mbps; 15 dBm@54 Mbps 2.412~2.472 GHz: 18 dBm@1~11 Mbps
Transmission Distance	Up to 100 meters (in open areas)
Security	AES, WEP 64/128-bit, WPA, WPA2, 802.11i
Network Modes	Infrastructure for 802.11 a/b/g Ad-Hoc for 802.11 b/g
Authentication	PEAP, EAP-TLS, EAP-TTLS, PEAP/MSCHAPv2, PEAP/TLS, PEAP/GTC, PEAP/MD5, EAP-TTLS/ EAP-MD5, EAP-TTLS/EAP-GTC, EAPTTLS, EAP-TTLS/EAP-MSCHAPv2, EAP-TTLS/EAP-TLS, EAP-TTLS/ MSCHAPv2, EAP-TTLS/MSCHAP
Security	AES, WEP 64/128-bit, WPA, WPA2, 802.11i
LAN	
Ethernet	10/100 Mbps
Serial	
Interface	TTL
Digital I/O	
Channels	9
Serial Communication Parameters	
Parity	None, Even, Odd, Space, Mark
Data Bits	5, 6, 7, 8
Stop Bit	1, 1.5, 2
Flow Control	RTS/CTS, XON/XOFF, DTR/DSR
Transmission Speed	50 to 921.6K bps (standard baudrates), 250K and 500K bps (nonstandard baudrates)
Software Features	
Protocols	ICMP, IP, TCP, UDP, DHCP, Telnet, DNS, SNMP, HTTP, SSH, HTTPS
Operating Modes	TCP Server, TCP Client, UDP, Real COM, RFC2217
Utilities	Configuration utility supported by Windows 98, ME, 2000, XP, 2003, Vista
COM Driver	Windows Real COM drivers for Windows 95, 98, ME, NT, 2000, XP, 2003, XPx64, 2003x64, Vista Linux Real TTY driver UNIX Fixed TTY driver for SCO Unix, SCO OpenServer 5, UnixWare 7, UnixWare 2.1.x, SVR4.2, QNX

Configuration	Web console, serial console, Telnet console, Windows utility, serial command
Power Requirements	
Power Input	3.3V ± 5% VDC
Power Consumption	950 mA @ 3.3 VDC (max.)
Environmental	
Operating Temperature	0 to 55 °C (32 to 131 °F), 5 to 95% RH
Storage Temperature	-20 to 85 °C (-4 to 185 °F), 5 to 95% RH
Regulatory Approvals	
EMC	CE EN550022 Class A FCC Part 15, Subpart B, Class A Safety: EN60950, CUL, TUV
Wireless	CE ETSI EN 301 489-17 CE ETSI EN 301 489-1 FCC Part 15, Subpart B, Class A FCC Part 17 Subpart B, Class A
Warranty	5 years

2

Panel Layout and Pin Assignments

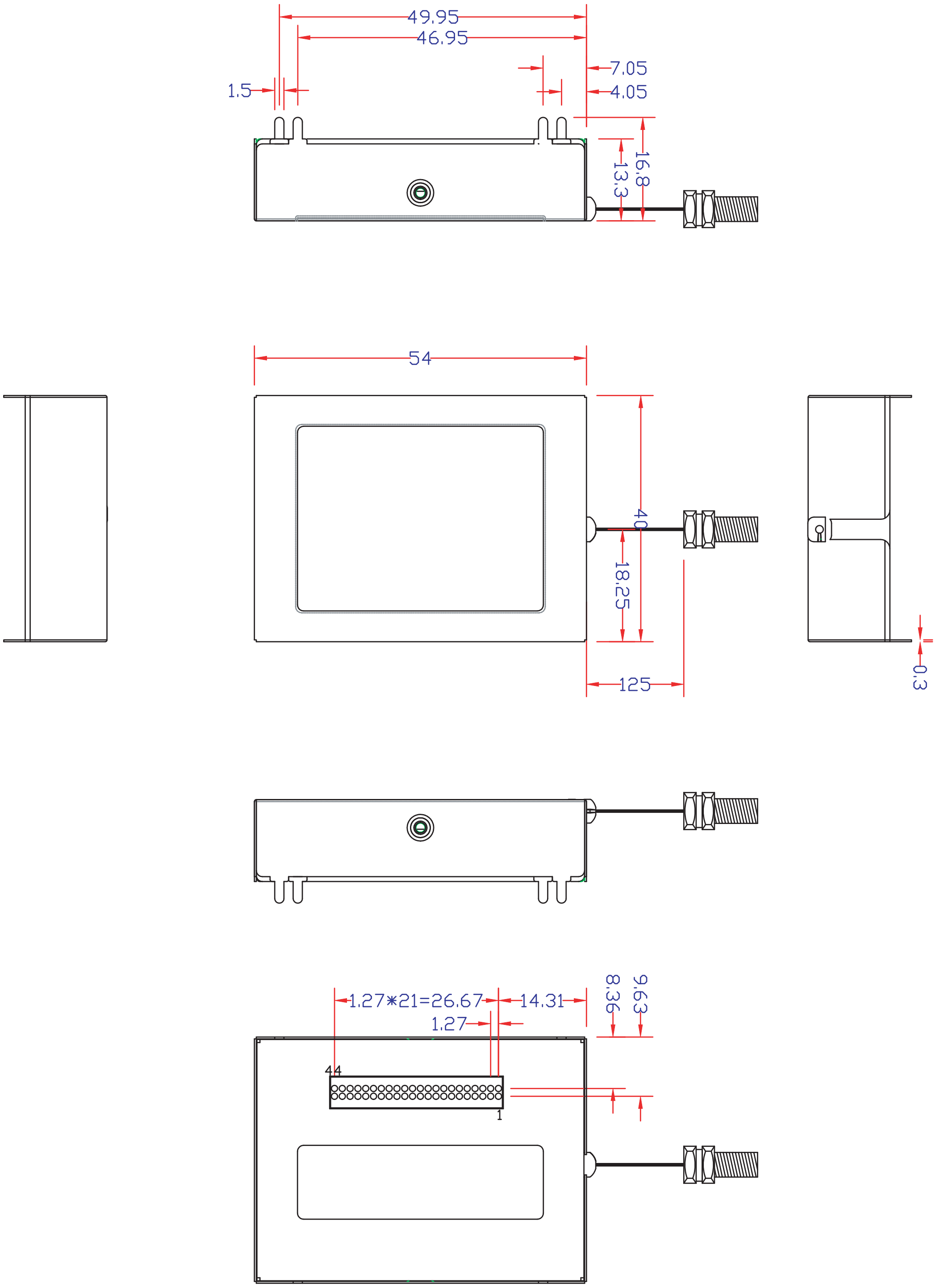
This chapter includes information about the panel layouts and pin assignments for WE-2100T. The layouts and reference circuit diagrams for the evaluation boards are also covered. The evaluation boards are used for evaluation and development of applications for WE-2100T.

The following topics are covered in this chapter:

- ❑ **Dimensions**
  - ➢ WE-2100T
  - ➢ WE-2100T-ST
- ❑ **Pin Assignments**
- ❑ **WE-2100-ST LED Indicators**

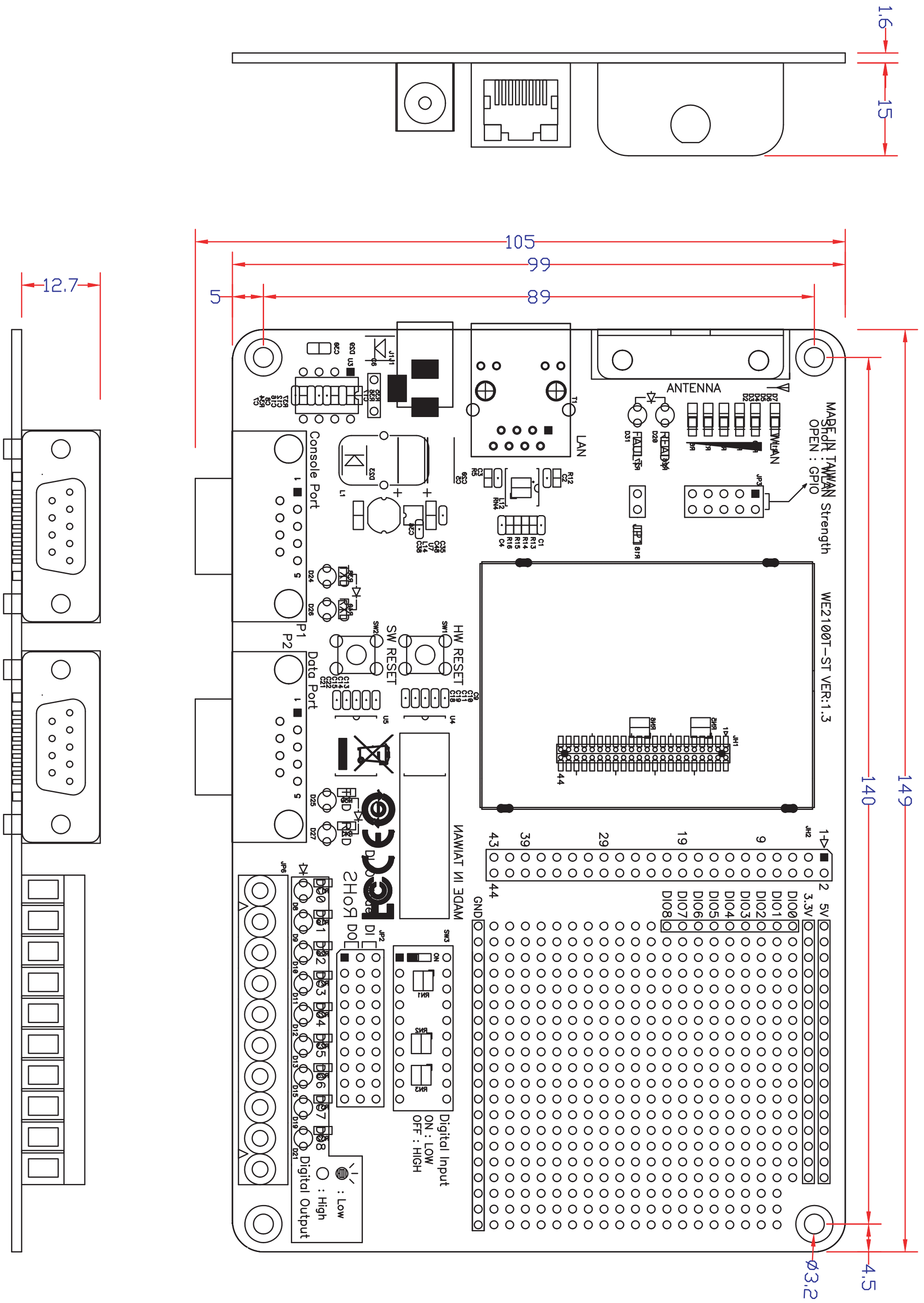
Dimensions

WE-2100T



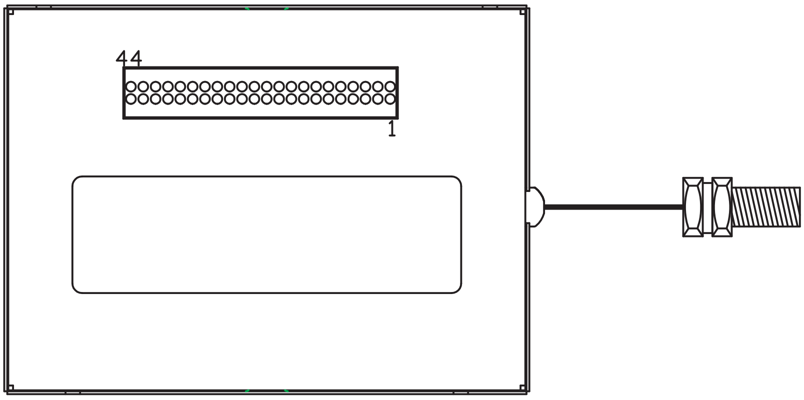
Unit: mm

WE-2100T-ST



Unit: mm

Pin Assignments



Pin	Function	Pin	Function
1	3.3V	2	GND
3	3.3V	4	GND
5	3.3V	6	GND
7	Console_TxD	8	Console_RxD
9	Console_RTS	10	Console_CTS
11	Console_DTR	12	Console_DSR
13	PIO0	14	Console_DCD
15	PIO1	16	PIO4 (WLAN strength 1)
17	PIO2	18	PIO5 (WLAN strength 2)
19	PIO3	20	PIO6 (WLAN strength 3)
21	Data_TxD	22	PIO7 (WLAN strength 4)
23	Data_RTS	24	Data_RxD
25	Data_DTR	26	Data_CTS
27	Ready_LED	28	Data_DSR
29	Fault_LED	30	Data_DCD
31	Eth_Tx+	32	WLAN_Act_LED
33	Eth_Tx-	34	SW_RESET
35	Eth_Center_TAP	36	HW_RESET
37	Eth_Center_TAP	38	Eth_100M_LED
39	Eth_Rx+	40	Eth_10M_LED
41	Eth_Rx-	42	Reserved
43	PIO8 (WLAN strength 0)	44	Reserved

WE-2100-ST LED Indicators

Type	Color	Status	Meaning
Ready	Off	Off	Power is off.
			Unit is booting or rebooting.
			IP error condition occurs.
	Green	Steady On	Unit is functioning normally.
		Blinking	Unit is responding to software Locate function.
			Reset button is being held down.
Fault	Off	Off	Power is off.
			Unit is functioning normally.
	Red	Steady On	Unit is booting or rebooting.
		Blinking	IP conflict, DHCP or BOOTP server did not respond properly.
WLAN	Off	Off	Unit was booted with Ethernet cable plugged.
	Green	Steady On	Wireless LAN is activated. (Unit was booted with Ethernet cable unplugged.)
WLAN Strength	Off	Off	JP3 is opened.
	Green/Off	Steady On/Off	JP3 is shorted, each LED corresponds to 20% WLAN signal strength.
Ethernet	Off	Off	Ethernet cable is unplugged.
	Orange	Steady On	10M Ethernet connected.
	Green	Steady On	100M Ethernet connected.
Serial TXD	Off	Off	No data is being transmitted from unit.
	Green	On	Data is being transmitted from unit.
Serial RXD	Off	Off	No data is being transmitted to unit.
	Yellow	On	Data is being transmitted to unit.
DO0~DO8	Off	Off	GPIO mode is input
			JP2 DO is opened.
			GPIO mode is output, and state is high.
	Green	Steady On	JP2 DO is shorted, GPIO mode is output, and state is low.

3

Getting Started

This chapter includes information about installing WE-2100T.

The following topics are covered in this chapter:

- ❑ **Wiring Requirements**
- ❑ **Installing onto the WE-2100T-ST Evaluation Board**
  - ➢ Circuit Pad
- ❑ **Connecting to the Network**
- ❑ **Connecting the Power**
- ❑ **Connecting to a Serial Device**
- ❑ **DI/O Test Settings**
  - ➢ LED Circuit Diagram

Wiring Requirements

ATTENTION

Before connecting the hardware, follow these important wiring safety precautions:

Disconnect power source
Do not install or wire this unit or any attached devices with the power connected. Disconnect the power before installation by removing the power cord before installing and/or wiring your unit.

Follow maximum current ratings
Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.

If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.

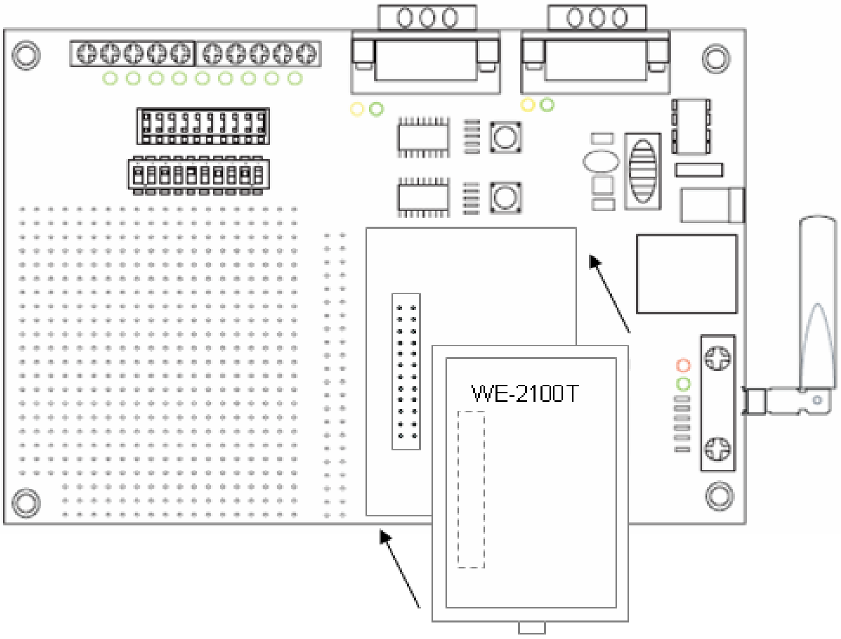
Use caution - unit may get hot
The unit will generate heat during operation, and the casing may feel hot to the touch. Take care when handling unit. Be sure to leave adequate space for ventilation.

The following guidelines will help ensure trouble-free signal communication:

- Use separate paths to route wiring for power and devices to avoid interference. Do not run signal or communication wiring and power wiring in the same wire conduit. The rule of thumb is that wiring that shares similar electrical characteristics can be bundled together.
- If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.
- Keep input wiring and output wiring separate.
- Label all wiring to each device in the system for easier testing and troubleshooting

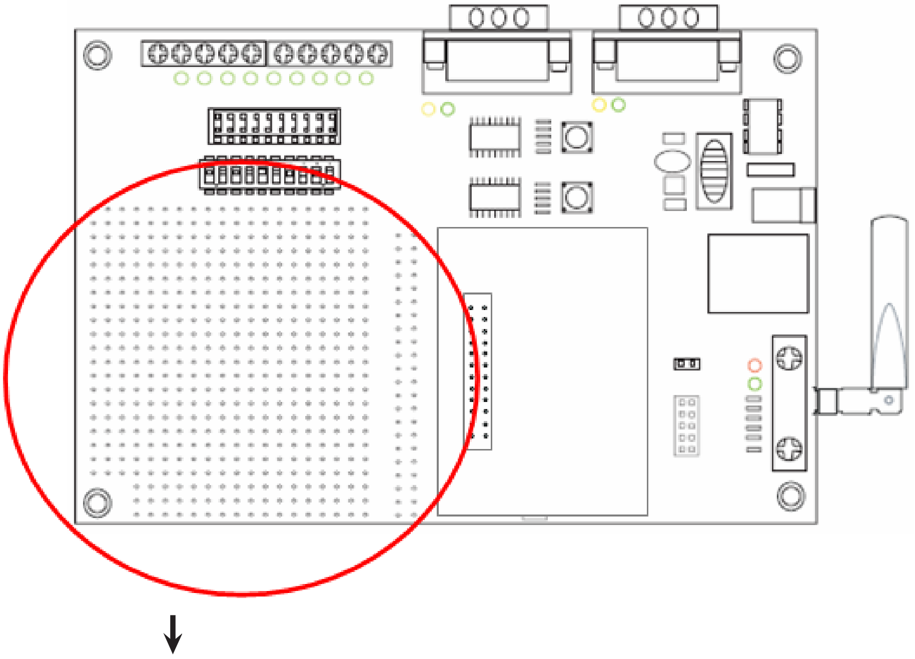
Installing onto the WE-2100T-ST Evaluation Board

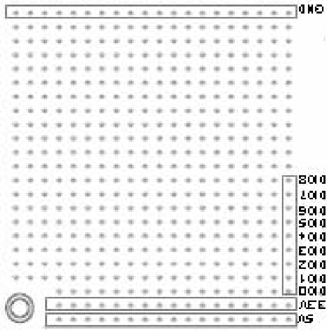
The WE-2100T-ST evaluation board is a tool to help you develop your WE-2100T application. The module must first be installed on the board before the power supply, network, and serial device are connected. Align the sockets on the WE-2100T module with the pins on the WE-2100T-ST board, as shown in the following figure.



Circuit Pad

The circuit pad on the evaluation board can be used to develop additional application circuits.





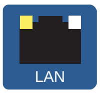
The bottom row of pins is for connecting a 5V power supply; the next row up is for connecting a 3.3V power supply. Digital I/O pins are located on the right side. The top row of pins is for grounding.

Connecting to the Network

When developing your application, you may wish to use Ethernet to configure the WE-2100T, especially if your wireless LAN is not functional yet. You may connect to the network using the evaluation board's RJ45 Ethernet port. In order to use the LAN connection, make sure the network cable is already plugged in before the unit is powered on.

After power is connected in the next step, the RJ45 connector will indicate a valid connection to the Ethernet as follows:

A green LED indicator indicates a valid 100 Mbps Ethernet network connection and will flicker as data is being transmitted.



A yellow LED indicator indicates a valid 10 Mbps Ethernet network connection and will flicker as data is being transmitted.

Connecting the Power

Connect the 12 to 48 VDC power line to the power jack on the evaluation board.

Connecting to a Serial Device

Use a serial cable to connect the serial device to the data port, P2, on the evaluation board. (P1 is the console port, which is used for the serial console.)

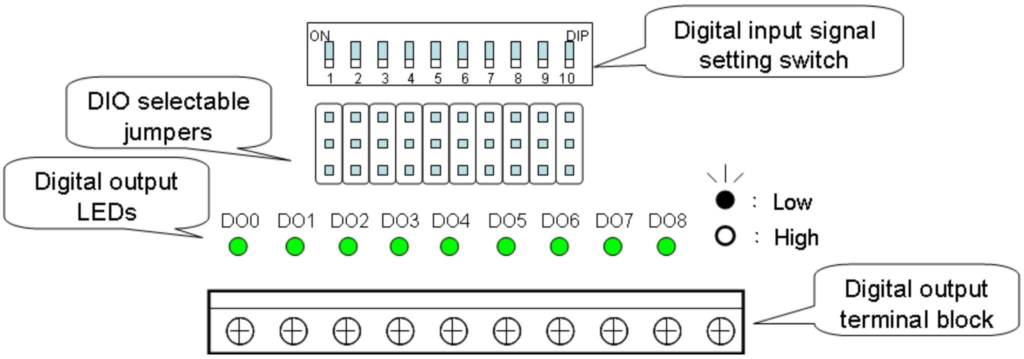
DI/O Test Settings

The WE-2100T includes 9 digital I/O channels. Each digital I/O channel is a GPIO (General Purpose I/O) channel that can be set to "digital output" or "digital input" mode by software. When developing your own applications, be aware of the voltage limits. The output current is 1 mA.

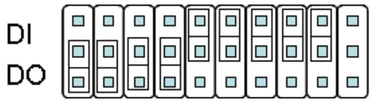
		Min.	Max.	Unit	Conditions
Low-level input voltage	Maximum voltage when DI is set to "Low" status.	-----	0.8	V	
High-level input voltage	Minimum voltage when DI is set to "High" status.	2	-----	V	
Low-level input voltage	Maximum voltage when DO is set to "Low" status.	-----	0.4	V	
High-level input voltage	Minimum voltage when DO is set to "High" status	2.4	-----	V	

The output current for each digital output channel carries only 1 mA.

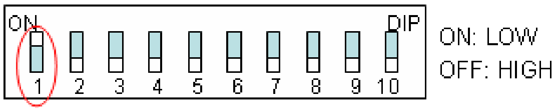
On the evaluation board, the DIO mode jumper selects whether a digital channel will be connected to the DIP switch for input testing, or to the LED for output testing. If DIO1 is set to digital input mode on the WE-2100T, you can use a jumper setting on the evaluation board to connect DIO1 to the DIP switch. Digit one on the DIP switch will then be the input device for DIO1. When you flip the switch on or off, you can see the status of DIO1 change on the web console or in the Windows utility.


ON
DIP
1 2 3 4 5 6 7 8 9 10
Digital input signal setting switch
DIO selectable jumpers
Digital output LEDs
DO0 DO1 DO2 DO3 DO4 DO5 DO6 DO7 DO8
● : Low
○ : High
Digital output terminal block

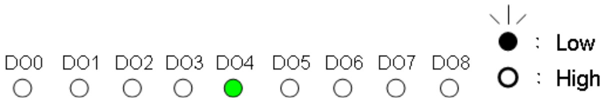
1. First, position the jumpers so they correspond with the input/output mode of each digital I/O channel. In the example below, channels 0 through 3 are output (DO) channels and channels 4 through 8 are input (DI) channels.



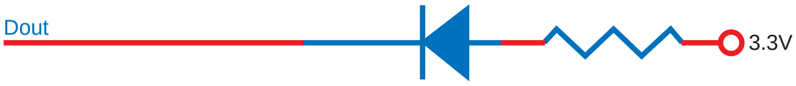
2. After setting the jumpers, use the DIP switches to set the status for input channels 0 through 3. You can set the status to either low (on) or high (off). In the example below, channel 0 is set to low, and channels 1 through 3 are set to high. Note that channel 0 corresponds to switch 1.



3. Use the web console to set the status of output channels. If you set channel 4's status to "Low" and the others to "High," the DO4 LED will glow and the other LEDs will remain dark. Please refer to Chapter 9 for more configuration details.



LED Circuit Diagram



The digital output LEDs is a sink circuit, as shown in the circuit diagram.

4

Selecting an Operation Mode

In this section, we describe the available operation modes for the WE-2100T. There is a mode that relies on a driver installed on the host computer, and other modes that rely on TCP/IP socket programming concepts. After determining the proper operation mode for your application, please refer to Chapter 8 for instructions on configuring that mode.

- ❑ **Overview**
- ❑ **TCP Server Mode**
- ❑ **TCP Client Mode**
- ❑ **UDP Mode**
- ❑ **Real COM Mode**

Overview

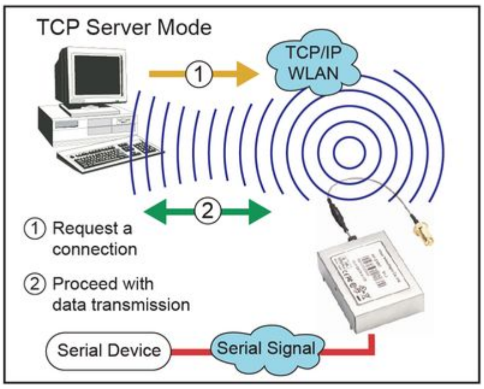
The WE-2100T connects serial devices to the wireless LAN. It has a built-in TCP/IP stack that saves you the effort of programming networking protocols. Simply select the proper operating mode to allow your computer to access, manage, and configure your serial device over the Internet.

Traditional SCADA and data collection systems collect data from various instruments over serial connections (RS-232/422/485). Since WE-2100T is designed to convert between serial and Ethernet signals, both local and remote devices can be connected to a standard TCP/IP network and made accessible to SCADA and data collection systems.

Real COM and **RFC2217** modes allow serial-based software to access the module's serial port as if it were a local serial port on a PC. These modes are appropriate when your application relies on Windows or Linux software that was originally designed for locally attached COM or TTY devices. With these modes, you can access your devices from the network using your existing COM/TTY-based software, without investing in additional software.

Three different socket modes are available for user-developed socket programs: **TCP Server**, **TCP Client**, and **UDP Server/Client**. For TCP applications, the appropriate mode depends on whether the connection will be hosted or initiated from the module's serial port or from the network. The main difference between the TCP and UDP protocols is that TCP guarantees delivery of data by requiring the recipient to send an acknowledgement to the sender. UDP does not require this type of verification, making it possible to offer speedier delivery. UDP also allows multi-unicasting of data to groups of IP addresses and would be suitable for streaming media or non-critical messaging applications such as LED message boards.

TCP Server Mode

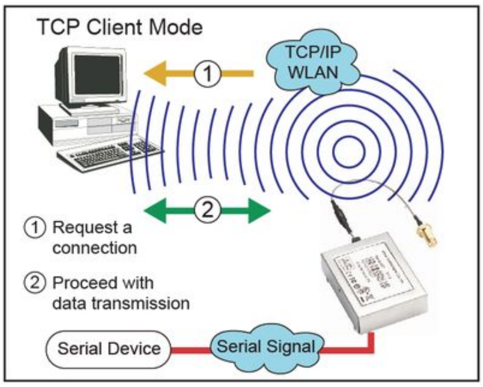


In **TCP Server** mode, the module's serial port is assigned an IP:port address that is unique on your TCP/IP network. It waits for the host computer to establish a connection to the attached serial device. This operation mode also supports up to four simultaneous connections, so multiple hosts can collect data from the attached device at the same time.

Data transmission proceeds as follows:

1. A host requests a connection to the module's serial port.
2. Once the connection is established, data can be transmitted in both directions—from the host to the device, and from the device to the host.

TCP Client Mode

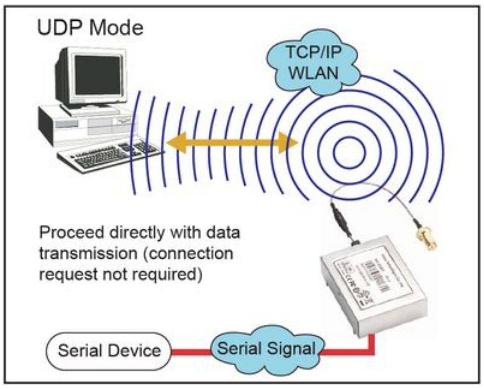


In **TCP Client** mode, the module actively establishes a TCP connection to a specific network host when data is received from the attached serial device. After the data has been transferred, the module can automatically disconnect from the host computer through the **Inactivity time** settings. Please refer to Chapter 8 for details on these parameters.

Data transmission proceeds as follows:

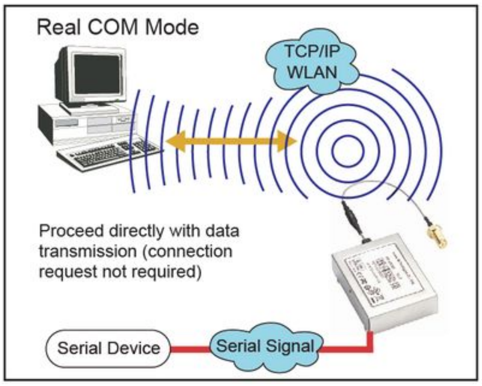
1. The module requests a connection from the host.
2. The connection is established and data can be transmitted in both directions between the host and device.

UDP Mode


UDP Mode
TCP/IP WLAN
Proceed directly with data transmission (connection request not required)
Serial Device
Serial Signal

UDP is similar to TCP but is faster and more efficient. Data can be broadcast to or received from multiple network hosts. However, UDP does not support verification of data and would not be suitable for applications where data integrity is critical. It is ideal for message display applications.

Real COM Mode


Real COM Mode
TCP/IP WLAN
Proceed directly with data transmission (connection request not required)
Serial Device
Serial Signal

Real COM mode is designed to work with drivers that are installed on a network host. COM drivers are provided for Windows systems, and TTY drivers are provided for Linux and UNIX systems. The driver establishes a transparent connection to the attached serial device by mapping a local serial port to the module's serial port. Real COM mode supports up to four simultaneous connections, so multiple hosts can collect data from the attached device at the same time.

ATTENTION

Real COM drivers are installed and configured through the included Windows utility.

Real COM mode allows you to continue using your serial communications software to access devices that are now attached to the WE-2100T module. On the host, the Real COM driver automatically intercepts data sent to the COM port, packs it into a TCP/IP packet, and redirects it to the network. At the other end of the connection, the WE-2100T accepts the Ethernet frame, unpacks the TCP/IP packet, and sends the serial data to the appropriate device.

ATTENTION

In Real COM mode, several hosts can have simultaneous access control over the serial port on the module. If necessary, you can limit access by using the Accessible IP settings. Please refer to Chapter 9 for additional information on Accessible IP settings.

5

Initial IP Address Configuration

When setting up your WE-2100T module for the first time, the first thing you should do is configure the IP address. This chapter introduces the methods that can be used to configure the WE-2100T's IP address. For more details about network settings, please refer to Chapter 7.

This chapter includes the following sections:

- ❑ **Selecting an IP Address or Configuration**
- ❑ **Assigning IP Address with Network Enabler Administration Suite**
- ❑ **Assigning IP Address with ARP**
- ❑ **Assigning IP Address with Telnet Console**
- ❑ **Assigning IP Address with Serial Console**

Selecting an IP Address or Configuration

For most applications, you will assign a fixed IP address to the module, which means that you set the IP address directly. However, for certain network environments, your module’s IP address will need to be assigned by a DHCP or BOOTP server. In this case, instead of directly assigning the module’s IP address, you will need to configure the module to receive its IP address from the appropriate DHCP or BOOTP server.

If you are not sure whether you need to configure your module for a dynamic or static IP address, consult the administrator who set up the LAN. You will also need to consult the network administrator if you wish to use a fixed IP address in a DHCP or BOOTP environment.

Factory Default IP Address

Network Interface	IP Configuration	IP Address
LAN	Static	192.168.126.254
WLAN	Static	192.168.127.254

If the module is configured to obtain its IP settings from a DHCP or BOOTP server but is unable to get a response, it will use the factory default IP address and netmask.

The 192.168.xxx.xxx set of addresses are private IP addresses, since they cannot be directly accessed from a public network. You cannot ping a device with a 192.168.xxx.xxx address from an outside Internet connection. If your application requires sending data over a public network, such as the Internet, you will need to assign a valid public IP address, which can be leased from a local ISP.

Assigning IP Address with Network Enabler Administration Suite

Please refer to Chapter 12 for instructions on using Network Enabler Administrator to configure and manage your WE-2100T embedded module.

Assigning IP Address with ARP

The ARP (Address Resolution Protocol) command can be used to assign an IP address to the module. The ARP command tells your computer to associate the module’s MAC address with the specified IP address. You must then use Telnet to access the module, at which point the module’s IP address will be reconfigured. This method only works when the module is configured with default IP settings.

ATTENTION

When using ARP to set the module’s IP address, be aware of the following items:

- Your computer and your module must be connected to the same LAN or WLAN. You may use a cross-over Ethernet cable to connect the module directly to your computer’s Ethernet port.
- Your module must be configured with the factory default IP address before executing the ARP command. When connected to a LAN, the default IP is 192.168.126.254. When connected to a WLAN, the default IP is 192.168.127.254.

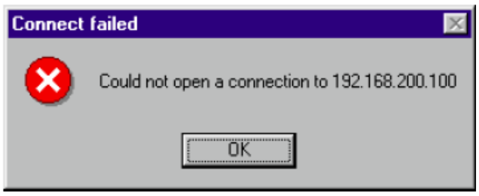
1. Select a valid IP address for your WE-2100T module. Consult with your network administrator if necessary.
2. Obtain the module's MAC address from the label on the module.
3. From the DOS prompt, execute the **arp -s** command with the desired IP address and the module's MAC address, as in the following example:

   arp -s 192.168.200.100 00-90-E8-xx-xx-xx

   In this example 192.168.200.100 is the new IP address that you wish to assign to the module, and 00-90-E8-xx-xx-xx is the module's MAC address.
4. From the DOS prompt, execute a special Telnet command using port 6000, as in the following example:

   telnet 192.168.200.100 6000

   In this example, 192.168.200.100 is the new IP address that is being assigned to the module.
5. You should see a message indicating that the connection failed.



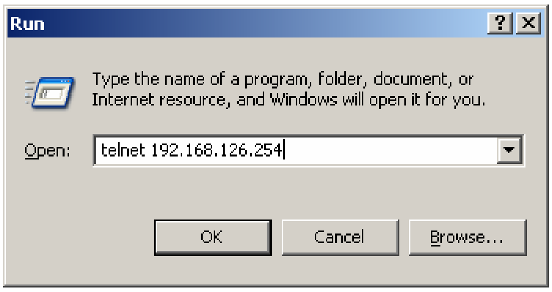
Could not open a connection to 192.168.200.100

6. The module will automatically reboot with the new IP address. You can verify that the configuration was successful by connecting to the new IP address with Telnet, ping, or another method.

Assigning IP Address with Telnet Console

Depending on how your computer and network are configured, you may find it convenient to use network access to set up your WE-2100T module's IP address. This can be done using the Telnet program.

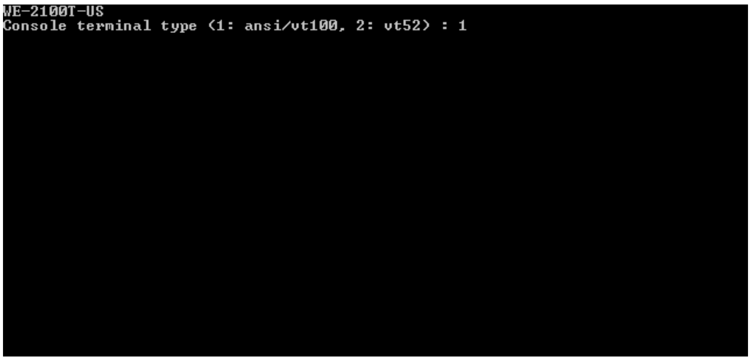
1. Select **Run…** from the Windows Start menu.
2. Enter the **telnet** command using your module's current IP address and click **OK**.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

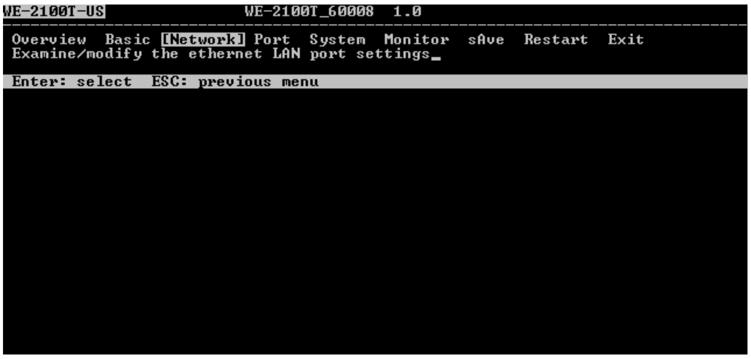
Open: telnet 192.168.126.254

3. Select the terminal type and press **ENTER.**



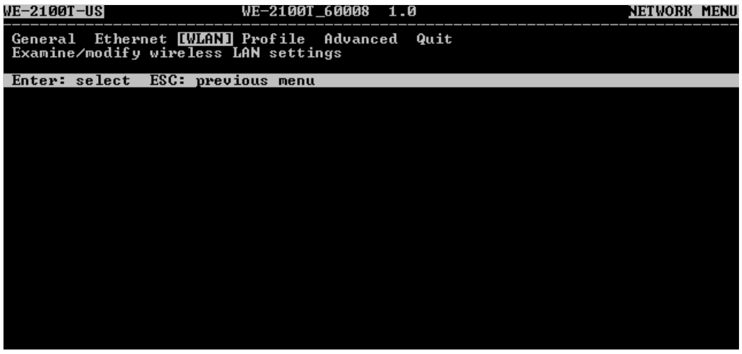
```
WE-2100T-US
Console terminal type (1: ansi/vt100, 2: vt52) : 1
```

4. Select **Network** by pressing **N** or by using the cursor keys. Press **ENTER** after making the selection.



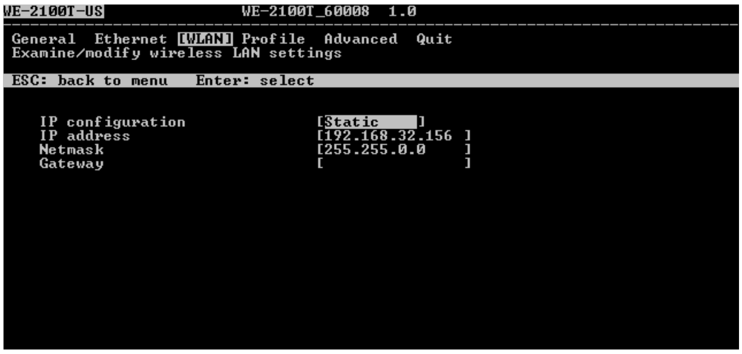
```
WE-2100T-US                WE-2100T_60008  1.0
--------------------------------------------------------------------------------
 Overview  Basic [Network] Port  System  Monitor  sAve  Restart  Exit
 Examine/modify the ethernet LAN port settings_

 Enter: select  ESC: previous menu
```

5. Select **Ethernet** or **WLAN** and press **ENTER**.



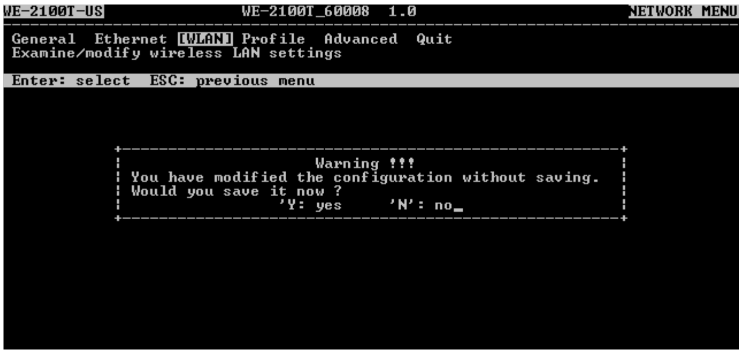
```
WE-2100T-US                WE-2100T_60008  1.0                       NETWORK MENU
--------------------------------------------------------------------------------
 General  Ethernet [WLAN] Profile  Advanced  Quit
 Examine/modify wireless LAN settings

 Enter: select  ESC: previous menu
```

6. Use the cursor keys to navigate between the different fields. For **IP address**, **Netmask**, and **Gateway**, enter the desired values directly. For **IP configuration** and **LAN speed**, press **ENTER** to open a submenu and select between the available options.



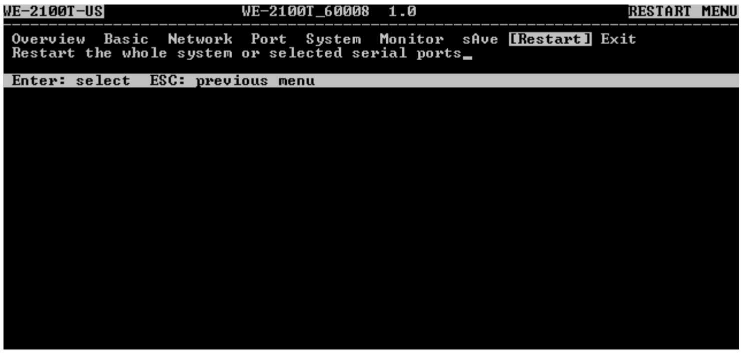
```
WE-2100T-US              WE-2100T_60008  1.0
--------------------------------------------------------------------------------
 General  Ethernet [WLAN] Profile  Advanced  Quit
 Examine/modify wireless LAN settings
 ESC: back to menu   Enter: select

    IP configuration              [Static     ]
    IP address                    [192.168.32.156 ]
    Netmask                       [255.255.0.0    ]
    Gateway                       [               ]
```

7. Press **ESC** to return to the menu. Press **ESC** again to return to the main menu. When prompted, press **Y** to save the configuration changes.



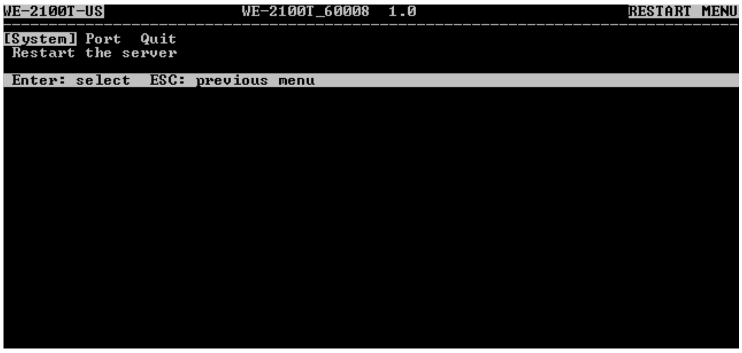
```
WE-2100T-US              WE-2100T_60008  1.0                        NETWORK MENU
--------------------------------------------------------------------------------
 General  Ethernet [WLAN] Profile  Advanced  Quit
 Examine/modify wireless LAN settings
 Enter: select  ESC: previous menu


            +-------------------------------------------------------+
            |                     Warning !!!                       |
            | You have modified the configuration without saving.   |
            | Would you save it now ?                               |
            |                  'Y': yes      'N': no_               |
            +-------------------------------------------------------+
```

8. Select **Restart** and then press **ENTER**.



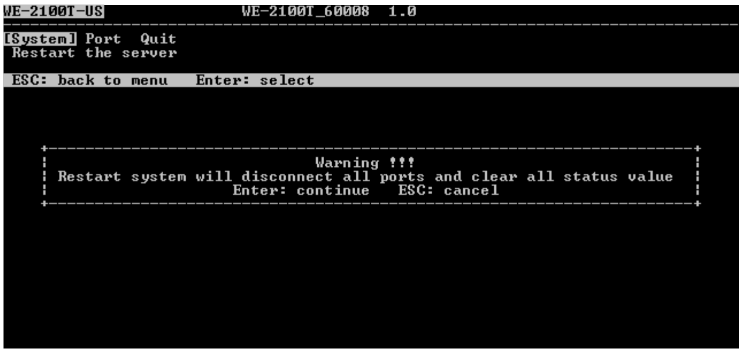
```
WE-2100T-US              WE-2100T_60008  1.0                        RESTART MENU
--------------------------------------------------------------------------------
 Overview  Basic  Network  Port  System  Monitor  sAve [Restart] Exit
 Restart the whole system or selected serial ports_
 Enter: select  ESC: previous menu
```

9. Select **System** and then press **ENTER**.



```
WE-2100T-US                 WE-2100T_60008  1.0                    RESTART MENU
-------------------------------------------------------------------------------
[System] Port  Quit
 Restart the server

 Enter: select  ESC: previous menu
```

10. Press **Enter** to restart the module. It will reboot with the new IP settings.

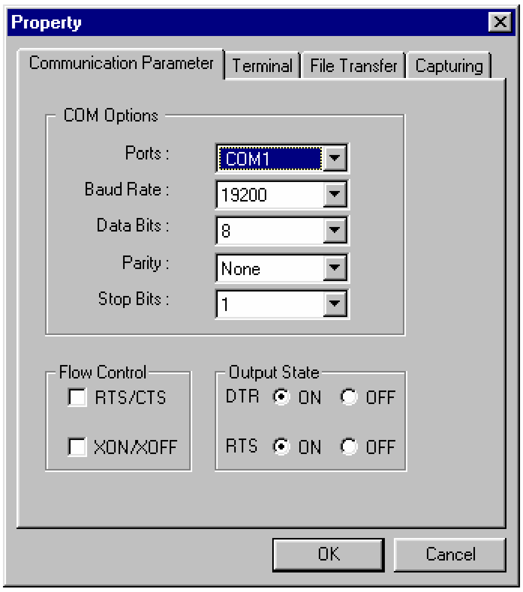


```
WE-2100T-US                 WE-2100T_60008  1.0
-------------------------------------------------------------------------------
[System] Port  Quit
 Restart the server

 ESC: back to menu   Enter: select


    +-----------------------------------------------------------------------+
    |                              Warning !!!                              |
    | Restart system will disconnect all ports and clear all status value   |
    |                    Enter: continue    ESC: cancel                      |
    +-----------------------------------------------------------------------+
```

Assigning IP Address with Serial Console

You may use the module's console port to configure the IP address. As soon as the connection is open, you will be presented with a text menu identical to the Telnet console.

1. Connect your PC's serial port to the module's console port. On the evaluation board, the console port is P1.
2. Open your terminal emulator program, such as Windows HyperTerminal. We recommend using PComm Terminal Emulator, which can be downloaded for free at www.moxa.com.
3. In your terminal emulator program, configure the communication parameters for the serial port on the PC. The parameters should be set to **19200** for baud rate, **8** for data bits, **None** for parity, and **1** for stop bits.



COM Options

Ports : COM1

Baud Rate : 19200

Data Bits : 8

Parity : None

Stop Bits : 1

Flow Control

□ RTS/CTS

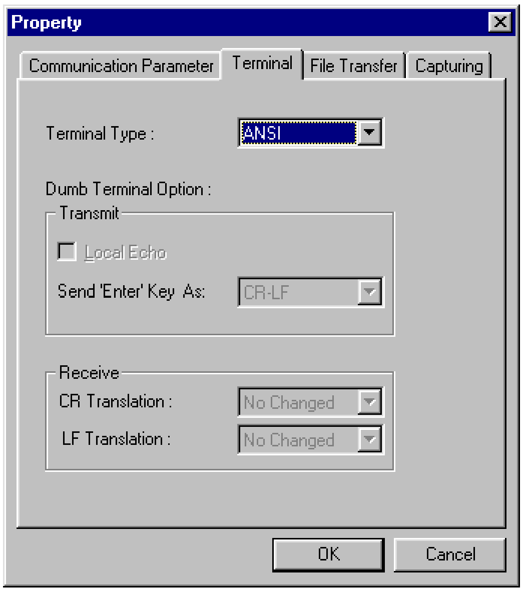
□ XON/XOFF

Output State

DTR ● ON ○ OFF

RTS ● ON ○ OFF

4. In your terminal emulator program, set the terminal type to **ANSI** or **VT100**. If you select **Dumb Terminal** as the terminal type, some of the console functions may not work properly.



Terminal Type : ANSI

Dumb Terminal Option :

Transmit

□ Local Echo

Send 'Enter' Key As: CR-LF

Receive

CR Translation : No Changed

LF Translation : No Changed

5. After setting the terminal options, enter any character. The serial console will open and will be functionally identical to the Telnet console. Please refer to the Telnet console section for instructions on how to navigate the console and configure the IP settings.

6

Web Console: Basic Settings

The web console is the most user-friendly method available to configure the module. With a standard web browser, you have easy and intuitive access to all settings and options. In this chapter, we introduce the web console and go through the basic configuration options. The same configuration options are also available through the Telnet and serial console.

This chapter covers the following topics:

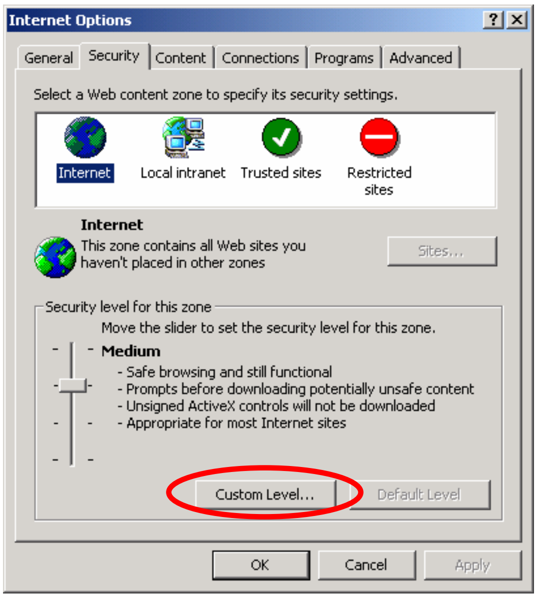
- ❑ **Overview**
  - ➢ Web Browser Settings
  - ➢ Navigating the Web Console
- ❑ **Basic Settings**
  - ➢ Server Name
  - ➢ Server Location
  - ➢ Time Zone
  - ➢ Local TimeTime Server

Overview

Web Browser Settings

In order to use the web console, you will need to have cookies enabled for your browser. Please note that the web console uses cookies only for password transmission.

For Internet Explorer, cookies can be enabled by right-clicking the Internet Explorer icon on your desktop and selecting Properties from the context menu. On the Security tab, click "Custom Level…"



Select a Web content zone to specify its security settings.

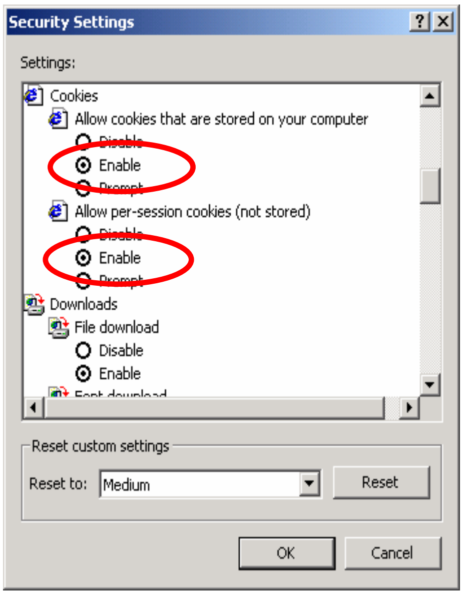
Internet
This zone contains all Web sites you haven't placed in other zones

Security level for this zone
Move the slider to set the security level for this zone.

Medium
- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

Enable these two items:

- Allow cookies that are stored on your computer
- Allow per-session cookies (not stored)



Settings:

Cookies
Allow cookies that are stored on your computer
○ Disable
● Enable
○ Prompt
Allow per-session cookies (not stored)
○ Disable
● Enable
○ Prompt
Downloads
File download
○ Disable
● Enable
Font download

Reset custom settings
Reset to: Medium

ATTENTION

If you are not using Internet Explorer, cookies are usually enabled through a web browser setting such as "allow cookies that are stored on your computer" or "allow per-session cookies." Cookies are used for password transmission only.

Navigating the Web Console

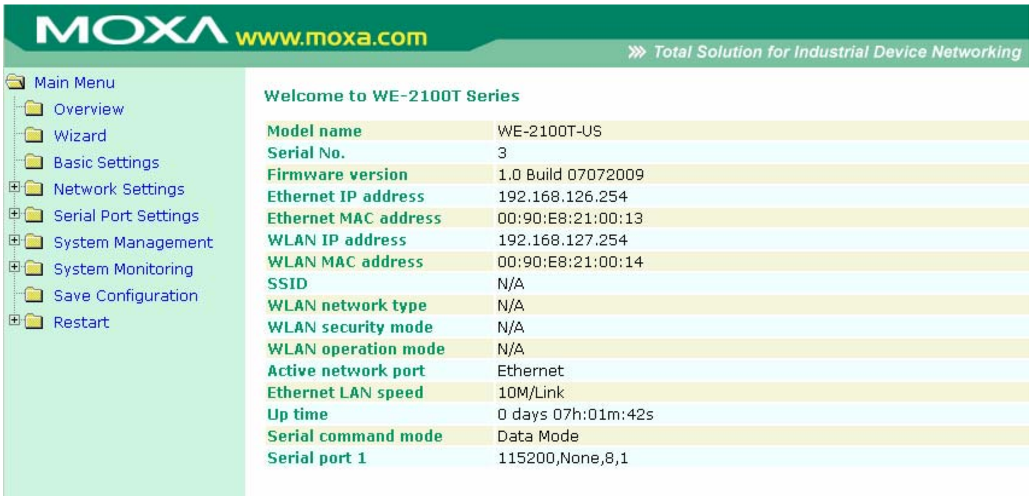
To open the web console, enter your module's IP address in the website address line. If you are configuring the unit for the first time over an Ethernet cable, you will use the default LAN IP address, **192.168.126.254**. Please refer to Chapter 5 for instructions on assigning the IP address.

If prompted, enter the console password. You will only be prompted for a password if you have enabled password protection on the module. The password will be transmitted with MD5 encryption over the Ethernet.

ATTENTION

If you have forgotten the password, you can use the reset button to load factory defaults. This will erase all previous configuration information.

The web console will appear as shown below.



Welcome to WE-2100T Series

Model name	WE-2100T-US
Serial No.	3
Firmware version	1.0 Build 07072009
Ethernet IP address	192.168.126.254
Ethernet MAC address	00:90:E8:21:00:13
WLAN IP address	192.168.127.254
WLAN MAC address	00:90:E8:21:00:14
SSID	N/A
WLAN network type	N/A
WLAN security mode	N/A
WLAN operation mode	N/A
Active network port	Ethernet
Ethernet LAN speed	10M/Link
Up time	0 days 07h:01m:42s
Serial command mode	Data Mode
Serial port 1	115200,None,8,1

Settings are presented on pages that are organized by folder. Pages are selected in the left navigation panel. For example, if you click **Basic Settings** in the navigation panel, the main window will show a page of basic settings that you can configure. Certain folders can be expanded by clicking the adjacent "+" symbol.

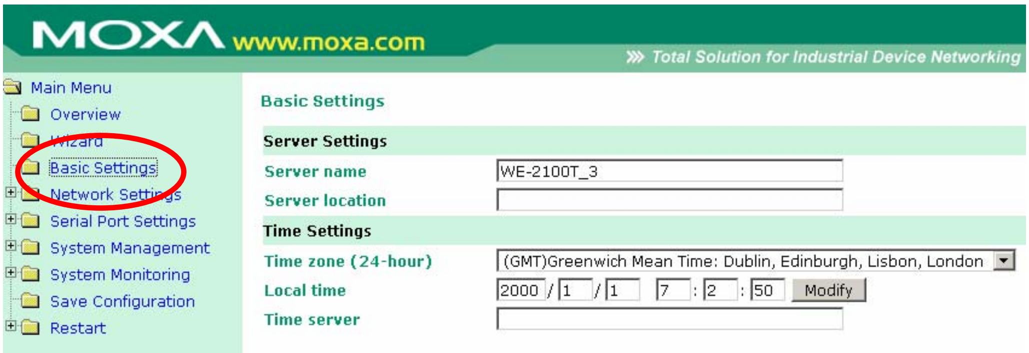
After you have made changes on a page, you must click **Submit** in the main window before jumping to another page. Your changes will be lost if you do not click **Submit**.

After you have finished modifying the desired pages, you must save and restart the module for the new settings to take effect. You may complete this in one step by clicking **Save/Restart** after you submit a change. Changes will not take effect until they are saved and the unit is restarted. If you restart the module without saving your configuration, all configuration changes will be lost.

ATTENTION

You may use Network Enabler Administrator to export the configuration file when you have finished configuring the module. This way, you can restore your settings if you need to reset the module. Please refer to Chapter 12 for additional information about using the Export and Import functions.

Basic Settings



Basic Settings

Server Settings

Server name: WE-2100T_3

Server location:

Time Settings

Time zone (24-hour): (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

Local time: 2000 / 1 / 1 7 : 2 : 50

Time server:

On the **Basic Settings** page, you can configure **Server name**, **Server location, Time zone**, **Local time**, and **Time server**.

Server Name

Default	
Options	free text (e.g., “Server 1”)
Description	This is an optional free text field to help you differentiate one module from another. It does not affect operation of the module.

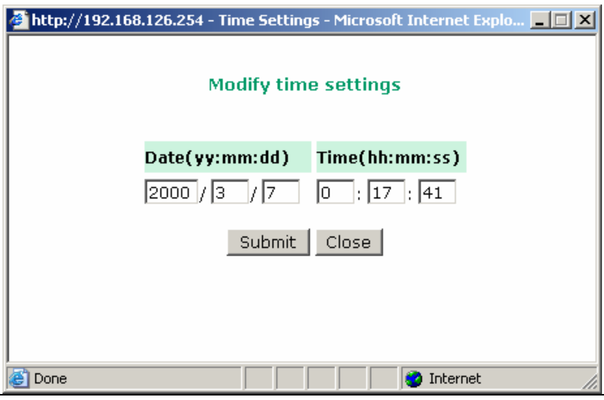
Server Location

Default	
Options	free text (e.g., “Building 4, Level 2”)
Description	This is an optional free text field to help you differentiate one module from another. It does not affect operation of the module.

Time Zone

Default	(GMT)Greenwich Mean Time
Options	(GMT)Greenwich Mean Time (GMT-01:00)Azores, Cape Verde Is. (GMT-02:00)Mid-Atlantic etc.
Description	This field shows the currently selected time zone and allows you to select a different time zone.

Local Time

Default	
Options	Date (yy:mm:dd), Time (hh:mm:ss)
Description	The module has a built-in real-time clock that allows you to add time information to functions such as the automatic warning e-mail or SNMP trap. This field shows the current time according to the module's built-in real-time clock. This is not a live field, so you will need to refresh the browser to get an updated reading. Click **Modify** to adjust the real-time clock. Make sure that you first select the correct time zone. The real-time clock will be updated immediately, with no need to restart the module.  http://192.168.126.254 - Time Settings - Microsoft Internet Explo... Modify time settings Date(yy:mm:dd) 2000 / 3 / 7 Time(hh:mm:ss) 0 : 17 : 41

ATTENTION

When modifying the local time, select the time zone first. The time display will be updated to reflect the specified time zone.

ATTENTION

There is a risk of explosion if the real-time clock battery is replaced incorrectly!
The real time clock is powered by a lithium battery. We strongly recommend that you obtain assistance from a Moxa support engineer before replacing the battery. Please contact the Moxa RMA service team if you need to change the battery.

Time Server

Default	
Options	IP address or domain name (e.g., "192.168.1.1" or "time.nist.gov")
Description	This optional field specifies your time server's IP address or domain name, if a time server is used in your network. The module supports SNTP (RFC-1769) for automatic time calibration. The module will request time information from the specified time server every 10 minutes.

7

Web Console: Network Settings

The web console is the most user-friendly method available to configure the module. With a standard web browser, you have easy and intuitive access to all settings and options. In this chapter, we introduce the web console and go through the basic configuration options. The same configuration options are also available through the Telnet and serial console.

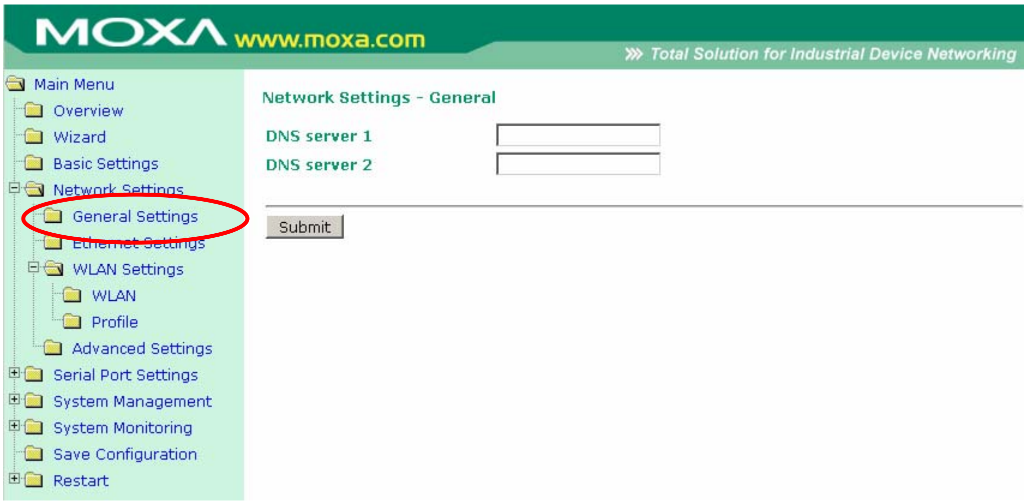
This chapter covers the following topics:

- ❑ **Overview**
- ❑ **Network Settings> General Settings**
- ❑ **Network Settings> Ethernet Settings**
- ❑ **Network Settings> WLAN Settings> WLAN**
- ❑ **Network Settings> WLAN Settings> Profile**
- ❑ **General Settings for WLAN Profile**
- ❑ **Security Settings for WLAN Profile**
- ❑ **Security Settings for WEP Encryption**
- ❑ **Security Settings for WPA, WPA2**
- ❑ **Network Settings> Advanced Settings**

Overview

This chapter explains how to configure all settings located under the **Network Settings** folder in the web console.

Network Settings> General Settings



Network Settings - General

DNS server 1

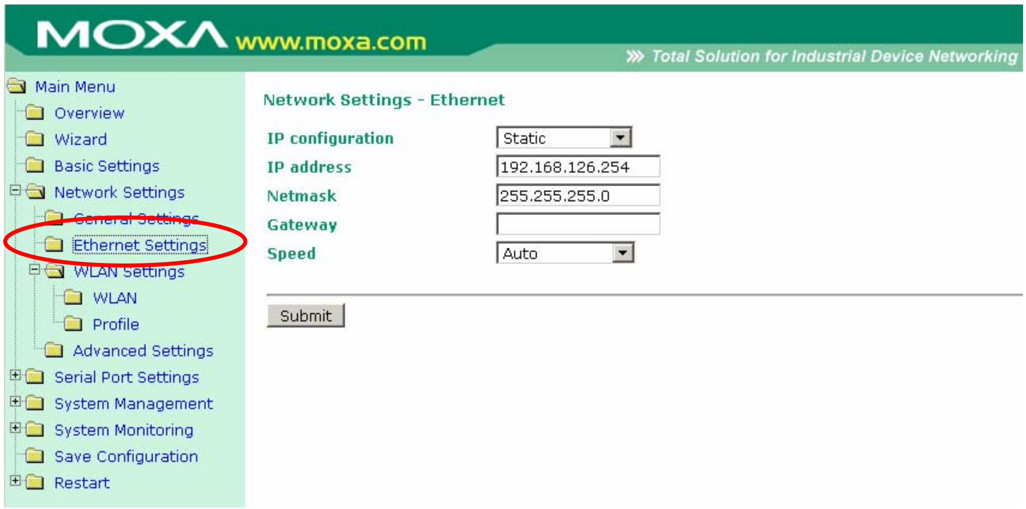
DNS server 2

On the **General Settings** page in the **Network Settings** folder, you can modify **DNS server 1** and **2**.

DNS Server 1 and 2

Default	
Options	IP address (e.g., "192.168.1.1")
Description	This field is for the DNS server's IP address, if applicable. With the DNS server configured, the WE-2100T module can use domain names instead of IP addresses to access hosts. Domain Name System (DNS) is how Internet domain names are identified and translated into IP addresses. A domain name is an alphanumeric name, such as www.moxa.com, that it is usually easier to remember than the numeric IP address. A DNS server is a host that translates a text-based domain name into an IP address in order to establish a TCP/IP connection. When the user wants to visit a particular website, the user's computer sends the domain name (e.g., www.moxa.com) to a DNS server to request that website's numeric IP address. When the IP address is received from the DNS server, the user's computer uses that information to connect to the website's web server. The WE-2100T will play the role of a DNS client, actively querying the DNS server for the IP address associated with a particular domain name.

Network Settings> Ethernet Settings



Network Settings - Ethernet

IP configuration	Static
IP address	192.168.126.254
Netmask	255.255.255.0
Gateway	
Speed	Auto

On the **Ethernet Settings** page in the **Network Settings** folder, you can modify **IP configuration**, **IP address**, **Netmask**, **Gateway**, and **Speed**.

You must assign a valid IP address to the WE-2100T before it will work in your network environment. Your network system administrator should provide you with an IP address and related settings for your network. The IP address must be unique within the network; otherwise the WE-2100T will not have a valid connection to the network. First-time users should refer to Chapter 5 for more information.

IP Configuration

Default	Static
Options	Static, DHCP, DHCP/BOOTP, BOOTP
Description	This field determines how the WE-2100T's IP address will be assigned. Static: IP address, netmask, and gateway are user-defined. DHCP: IP address, netmask, gateway, DNS, and time server are assigned by DHCP server. DHCP/BOOTP: IP address, netmask, gateway, DNS, and time server are assigned by DHCP server. IP address is assigned by BOOTP server if DHCP server does not respond. BOOTP: IP address is assigned by BOOTP server.

IP Address

Default	192.168.126.254
Options	IP address (e.g., "192.168.1.1")
Description	This field is for the IP address that will be assigned to your WE-2100T module. An IP address is a number assigned to a network device (such as a computer) as a permanent address on the network. Computers use the IP address to identify and talk to each other over the network. Choose a proper IP address that is unique and valid in your network environment. If your module will be assigned a dynamic IP address, set the "IP configuration" parameter appropriately.

Netmask

Default	255.255.255.0
Options	Netmask setting (e.g., "255.255.0.0")
Description	This field is for the subnet mask. A subnet mask represents all of the network hosts at one geographic location, in one building, or on the same local area network. When a packet is sent out over the network, the WE-2100T module will use the subnet mask to check whether the desired TCP/IP host specified in the packet is on the local network segment. If the address is on the same network segment as the module, a connection is established directly from the module. Otherwise, the connection is established through the gateway as specified in the "Gateway" parameter.

Gateway

Default	
Options	IP address (e.g., "192.168.1.1")
Description	This field is for the IP address of the gateway, if applicable. A gateway is a network computer that acts as an entrance to another network. Usually, the computers that control traffic within the network or at the local Internet service provider are gateway nodes. The WE-2100T module needs to know the IP address of the default gateway computer in order to communicate with the hosts outside the local network environment. Consult your network administrator if you do not know how to set this parameter.

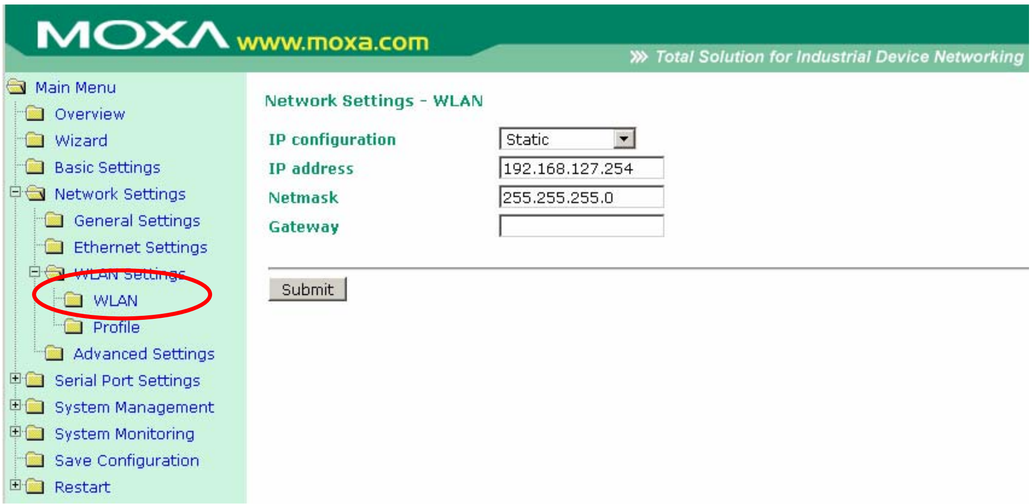
Speed

Default	Auto
Options	Auto, 10Mbps Half, 10Mbps Full, 100Mbps Half, 100Mbps Full
Description	This field specifies the network speed for the built-in Ethernet connection. IEEE802.3 Ethernet supports auto negotiation of transfer speed. However, some switches/hubs require that the communication speed be fixed at 100Mbps or 10Mbps.

ATTENTION

In dynamic IP environments, the WE-2100T will send 3 requests every 30 seconds to the DHCP or BOOTP server until the network settings have successfully been assigned. The first request will time out after one second; the second request will time out after three seconds, and the third request will timeout after five second. If the DHCP or BOOTP server is unavailable, the WE-2100T will use the factory default network settings.

Network Settings> WLAN Settings> WLAN



Network Settings - WLAN

IP configuration	Static
IP address	192.168.127.254
Netmask	255.255.255.0
Gateway	

The **WLAN** page is located under **WLAN Settings** in the **Network Settings** folder. You can modify **IP configuration**, **IP address**, **Netmask**, and **Gateway** for your WLAN.

The WE-2100T supports IEEE 802.11a/b/g wireless network interfaces. The supported IP configurations are static and dynamic (BOOTP , DHCP, or BOOTP+DHCP). Users can set up the IP configuration with the serial console, or the Web/Telnet consoles through the WE-2100T's Ethernet interface.

IP Configuration

Default	Static
Options	Static, DHCP, DHCP/BOOTP, BOOTP
Description	This field determines how the WE-2100T's IP address will be assigned. Static: IP address, netmask, and gateway are user-defined. DHCP: IP address, netmask, gateway, DNS, and time server are assigned by DHCP server. DHCP/BOOTP: IP address, netmask, gateway, DNS, and time server are assigned by DHCP server. IP address is assigned by BOOTP server if DHCP server does not respond. BOOTP: IP address is assigned by BOOTP server.

IP Address

Default	192.168.127.254
Options	IP address (e.g., "192.168.1.1")
Description	This field is for the IP address that will be assigned to your WE-2100T module. An IP address is a number assigned to a network device (such as a computer) as a permanent address on the network. Computers use the IP address to identify and talk to each other over the network. Choose a proper IP address that is unique and valid in your WLAN environment. If your module will be assigned a dynamic IP address, set the "IP configuration" parameter appropriately.

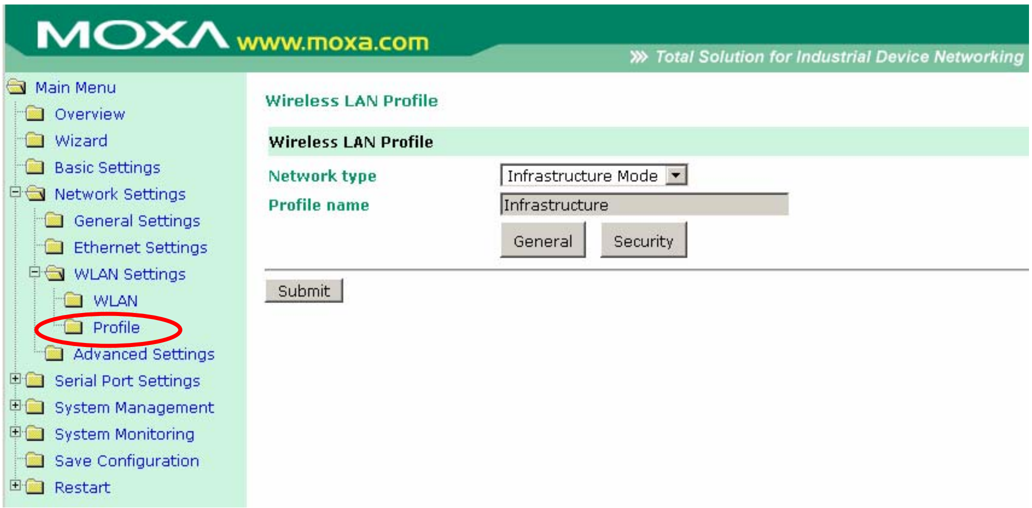
Netmask

Default	255.255.255.0
Options	Netmask setting (e.g., "255.255.0.0")
Description	This field is for the subnet mask. A subnet mask represents all of the network hosts at one geographic location, in one building, or on the same local area network. When a packet is sent out over the network, the WE-2100T module will use the subnet mask to check whether the desired TCP/IP host specified in the packet is on the local network segment. If the address is on the same network segment as the module, a connection is established directly from the module. Otherwise, the connection is established through the gateway as specified in the "Gateway" parameter.

Gateway

Default	
Options	IP address (e.g., "192.168.1.1")
Description	This field is for the IP address of the gateway, if applicable. A gateway is a network computer that acts as an entrance to another network. Usually, the computers that control traffic within the network or at the local Internet service provider are gateway nodes. The WE-2100T module needs to know the IP address of the default gateway computer in order to communicate with the hosts outside the local network environment. Consult your network administrator if you do not know how to set this parameter.

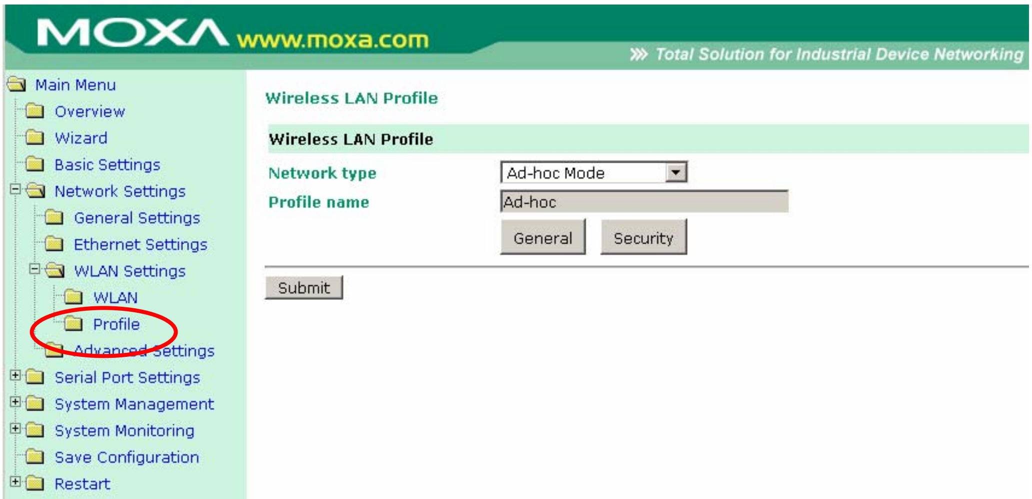
Network Settings> WLAN Settings> Profile



Wireless LAN Profile

Wireless LAN Profile

Network type	Infrastructure Mode
Profile name	Infrastructure



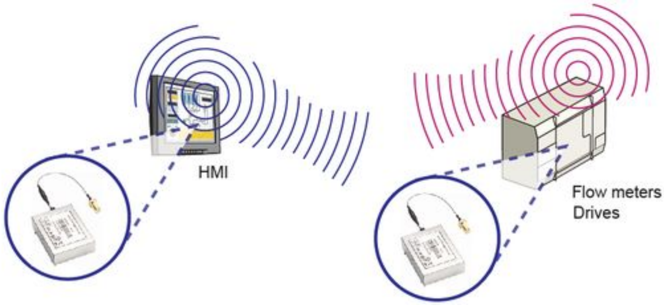
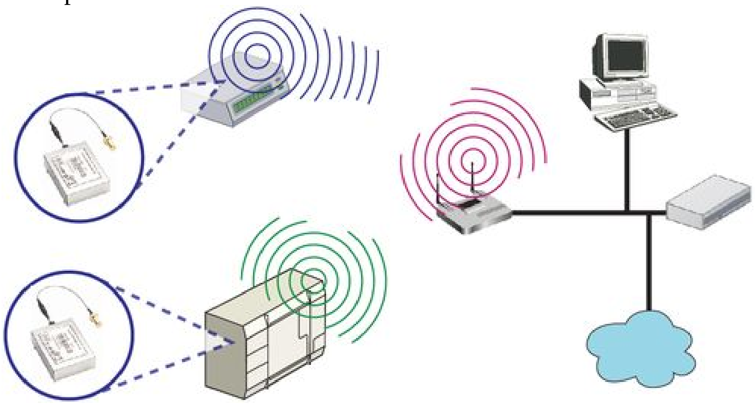
Wireless LAN Profile

Wireless LAN Profile

Network type	Ad-hoc Mode
Profile name	Ad-hoc

The **Profile** page is located under **WLAN Settings** in the **Network Settings** folder. This is where you configure the WE-2100T for Ad-hoc or Infrastructure operation. Different settings are available depending on whether you select Ad-hoc Mode or Infrastructure Mode.

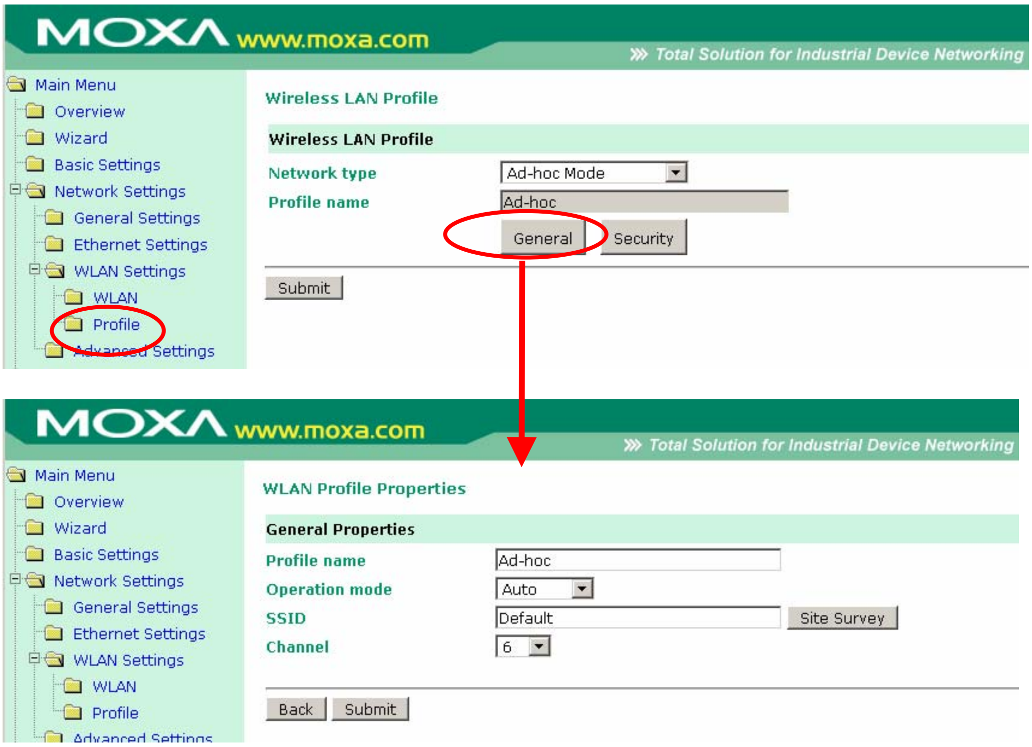
Network Type

Default	Infrastructure Mode
Options	Infrastructure Mode, Ad-hoc Mode
Description	This field specifies whether the WE-2100T will operate in Ad-hoc or Infrastructure Mode. For all wireless networking devices, there are two possible modes for communication with another wireless device. Devices that are configured for Ad-hoc Mode automatically detect and communicate directly with each other and do not require a wireless access point (AP) or gateway. Wireless devices that are configured for Infrastructure Mode do not communicate directly with each other, but through a wireless access point (AP). Devices can only communicate with devices operating in the same mode. Devices in Ad-Hoc Mode cannot communicate with devices in Infrastructure Mode. Example of Ad-Hoc Mode  Example of Infrastructure Mode  After setting the **Network type**, you will need to adjust the **General** and **Security** settings for the profile. In Ad-hoc Mode, only one profile is available. In Infrastructure Mode, three profiles can be defined.

General Settings for WLAN Profile

The **General** page is opened through the **Profile** page, under **WLAN Settings** in the **Network Settings** folder. After selecting Ad-hoc or Infrastructure Mode, click **General** to view or modify the general properties for that profile.

In Ad-hoc Mode



Wireless LAN Profile

Wireless LAN Profile

Network type: Ad-hoc Mode

Profile name: Ad-hoc

WLAN Profile Properties

General Properties

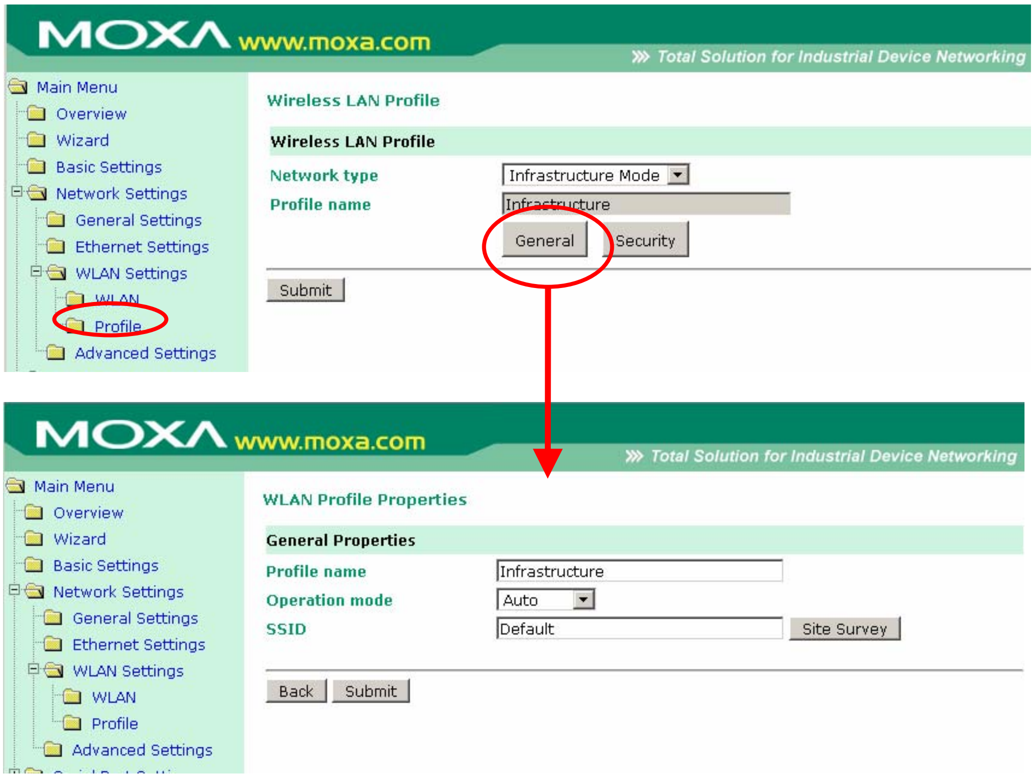
Profile name: Ad-hoc

Operation mode: Auto

SSID: Default

Channel: 6

In Infrastructure Mode



Wireless LAN Profile

Wireless LAN Profile

Network type: Infrastructure Mode

Profile name: Infrastructure

WLAN Profile Properties

General Properties

Profile name: Infrastructure

Operation mode: Auto

SSID: Default

On the General page, you can configure **Profile name**, **Operation mode**, and **SSID**. Additional settings are also available depending on whether you select Ad-hoc Mode or Infrastructure Mode.

Profile Name

Default	Ad-hoc (in Ad-hoc Mode) Profile1, Profile2, or Profile 3 (in Infrastructure Mode)
Options	free text (e.g., "Primary Connection")
Description	This is a free text field to help you differentiate one profile from another. It does not affect operation of the WE-2100T.

Operation Mode

Default	Auto
Options	Auto, 802.11a, 802.11b, 802.11g
Description	This field determines which wireless standard will be used by the selected profile. 802.11a, 802.11b, and 802.11g are supported. Auto: In Ad-hoc Mode, the WE-2100T will scan the 2.4G wireless band and will automatically select the appropriate wireless standard for communication with any other wireless devices that are detected. In Infrastructure Mode, the WE-2100T will automatically select between 802.11a, 802.11b and 802.11g according to the settings of the AP. 802.11a: This setting is only available in Infrastructure Mode. The Unlicensed National Information Infrastructure (UNII) 5 GHz band is used for communication, which is different from the RF band used by 802.11b and 802.11g. Consequently, 802.11a devices will not be able to communicate with 802.11b or 802.11g devices. (Multi-mode 802.11a/b/g APs or client adapters can be used to resolve this.) Transmission rates up to 54Mbps are supported. 802.11b: This is the well-known "Wi-Fi" standard, also referred to as "802.11 High-Rate (HR)". Wireless communication is in the 2.4 GHz ISM band, using the DSSS spread spectrum transmission scheme. 802.11b supports data rates of 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps. 802.11g: This is currently the most widely used standard for wireless LANS and is sometimes referred to as "54g™". Communication is in the 2.4 GHz ISM band and uses Orthogonal Frequency Division Multiplexing (OFDM). Data rates up to 54 Mbps are supported.

SSID

Default	Default
Options	free text (e.g., "Coffeeshop WLAN")
Description	This field specifies the SSID, or name, of the wireless network (SSID) that will be used by the WE-2100T. Wireless devices must use the same SSID in order to communicate with each other.

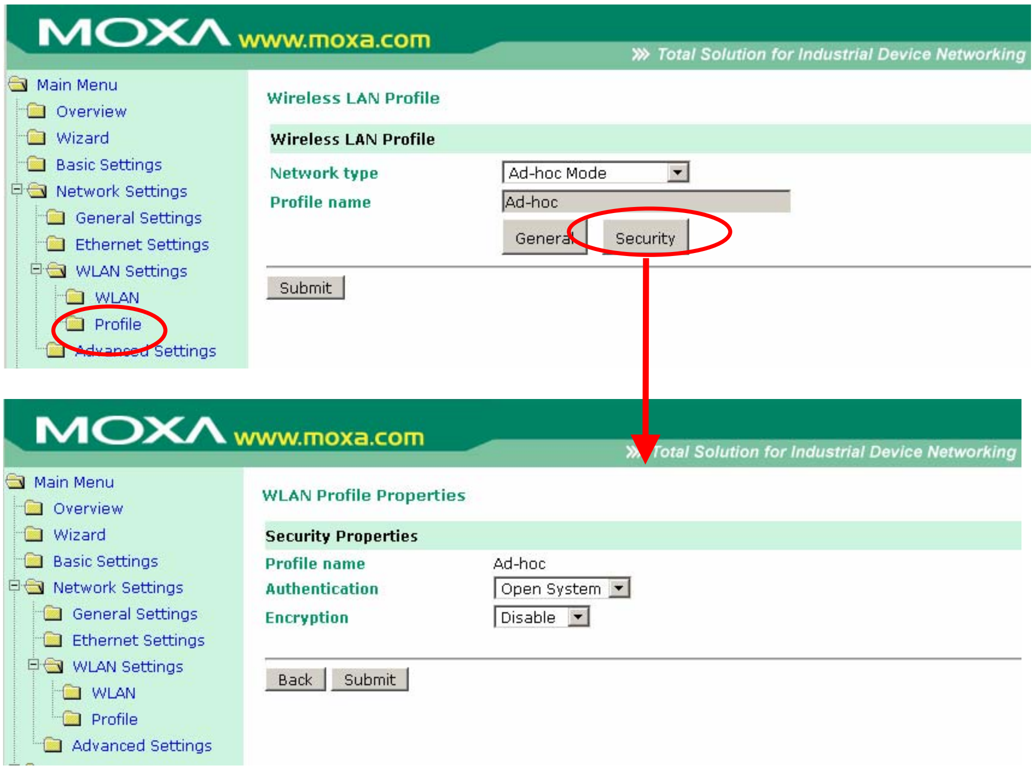
Channel

Default	6
Options	1 through 11 (USA models) 1 through 13 (Europe models) 1 through 14 (Japan models)
Description	This field is for Ad-Hoc Mode only and specifies the radio channel to use for the wireless network. In Infrastructure Mode, the AP specifies the channel automatically.

Security Settings for WLAN Profile

The **Security** page is opened through the **Profile** page, under **WLAN Settings** in the **Network Settings** folder. After selecting Ad-hoc or Infrastructure Mode, click **Security** to open the Security page for that profile.

In Ad-hoc Mode



Wireless LAN Profile

Wireless LAN Profile

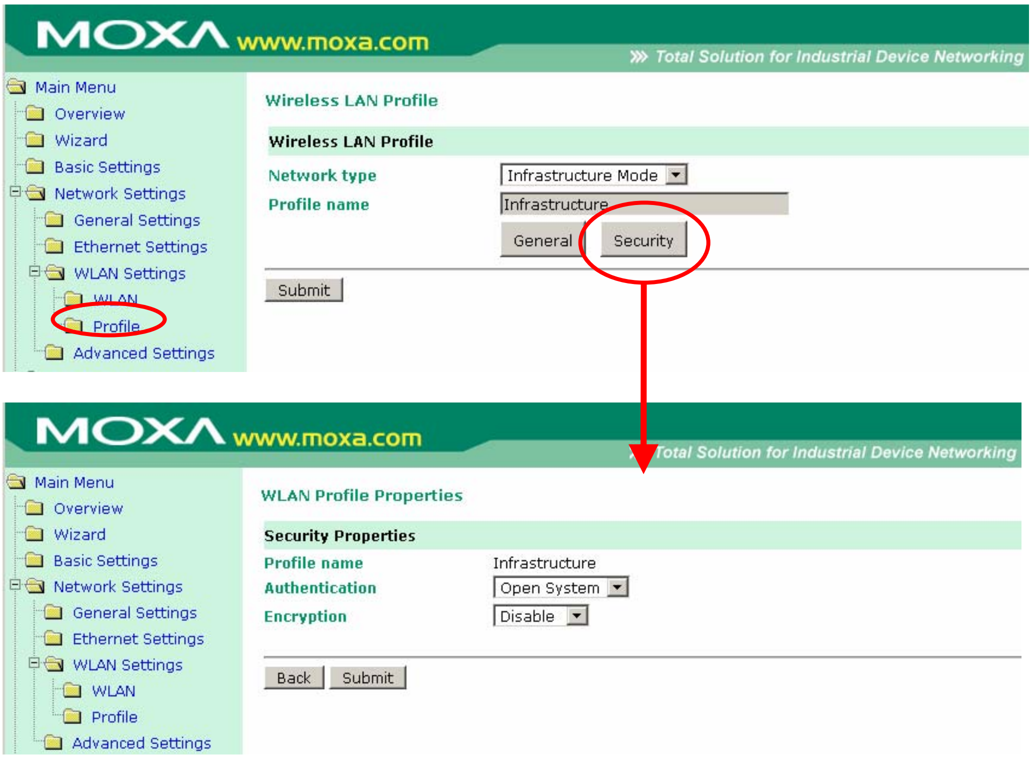
Network type	Ad-hoc Mode
Profile name	Ad-hoc

WLAN Profile Properties

Security Properties

Profile name	Ad-hoc
Authentication	Open System
Encryption	Disable

In Infrastructure Mode



Wireless LAN Profile

Wireless LAN Profile

Network type: Infrastructure Mode

Profile name: Infrastructure

WLAN Profile Properties

Security Properties

Profile name: Infrastructure

Authentication: Open System

Encryption: Disable

You will need to configure **Authentication** and **Encryption**. These settings must match the settings on the wireless device at the other end of the connection (such as the AP). Different settings and options are available depending on how **Authentication** and **Encryption** are configured.

Authentication

Default	Open System
Options	Open System, Shared Key, WPA, WPA-PSK, WPA2, WPA2-PSK
Description	This field specifies how wireless devices will be authenticated. Only authenticated devices will be allowed to communicate with the WE-2100T. If a RADIUS server is used, this setting must match the setting on the RADIUS server. Open System: The WE-2100T will simply announce a desire to associate with another station or access point. No authentication is required. For Ad-hoc Mode, this is the only option for authentication, since Ad-hoc Mode was designed for open communication. Shared Key: This option is only available in Infrastructure Mode. Authentication involves a more rigorous exchange of frames to ensure that the requesting station is authentic. WEP encryption is required. WPA: This is a managed authentication option that is only available in Infrastructure Mode. WPA was created by the Wi-Fi Alliance, the industry trade group that owns the Wi-Fi trademark and certifies devices with the Wi-Fi name. It is based on Draft 3 of the IEEE 802.11i standard. Each user uses a unique key for authentication, distributed from an IEEE 802.1X authentication server, also known as a RADIUS server. This option is also referred to as WPA Enterprise Mode, since it is intended to meet rigorous enterprise security requirements. Tunneled authentication is supported, depending on the EAP method selected. WPA-PSK: This is an unmanaged authentication option that is only available in Infrastructure Mode. Instead of a unique key for each user, a pre-shared key (PSK) is manually entered on the access point to generate an encryption key that is shared among all users. Consequently, this method does not scale well for enterprise. A PSK that uses a mix of letters, numbers and non-alphanumeric characters is recommended. This option is also referred to as WPA Personal Mode, since it is designed for the needs and capabilities of small home and office WLANs. WPA2: This is a managed authentication option that is only available in Infrastructure Mode. WPA2 implements the mandatory elements of 802.11i. Supported encryption algorithms include TKIP, Michael, and AES-based CCMP, which is considered fully secure. Since March 13, 2006, WPA2 has been mandatory for all Wi-Fi-certified devices. This option may also be referred to as WPA Enterprise Mode. Tunneled authentication is supported, depending on the EAP method selected. WPA2-PSK: This is an unmanaged authentication option that is only available in Infrastructure Mode. It employs WP2 encryption algorithms but relies on a PSK for authentication. A PSK that uses a mix of letters, numbers and non-alphanumeric characters is recommended. This option can also be referred to as WPA Personal Mode.

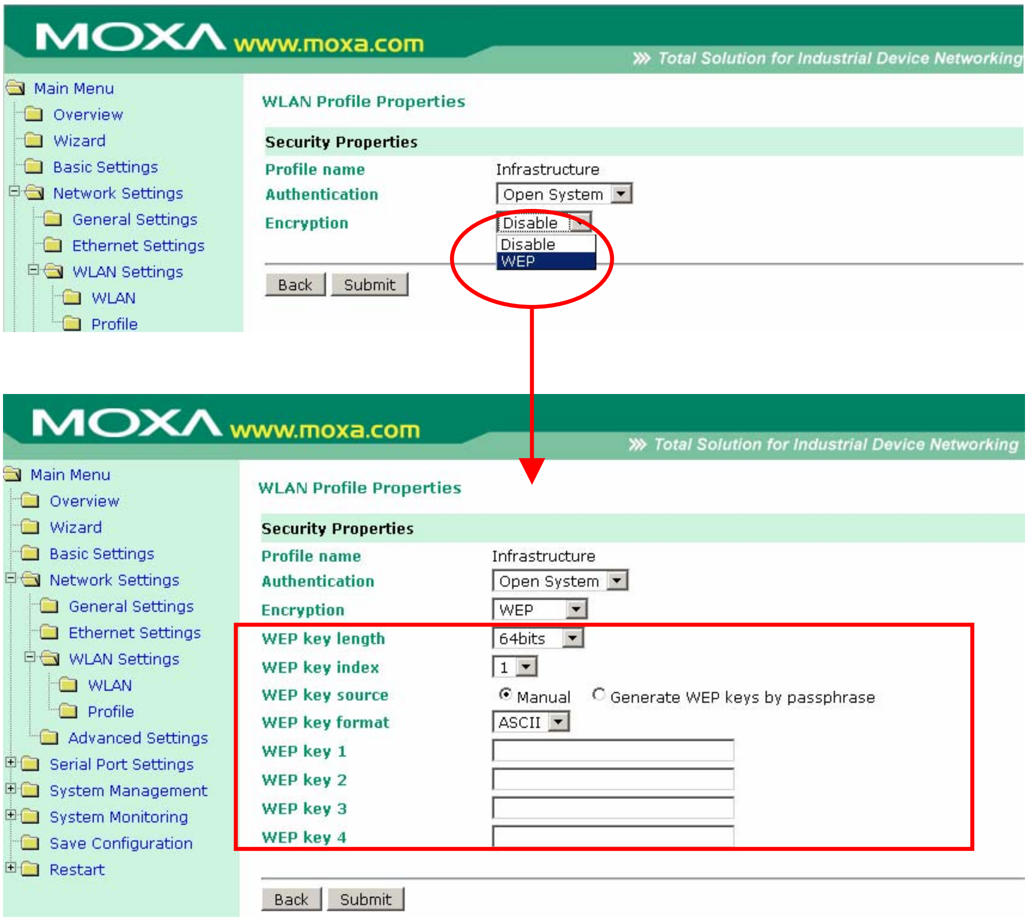
Encryption

Default	Disable
Options	Disable, WEP, TKIP, AES-CCMP
Description	This field specifies the type of encryption to use during wireless communication. Different encryption methods are available depending on the Authentication setting. Also, each encryption method has its own set of parameters that may also require configuration. Disable: No encryption is applied to the data during wireless communication. WEP: Wired Equivalent Privacy (WEP) is only available for Open System and Shared Key authentication methods. Data is encrypted according to a key. The WE-2100T supports both 64 and 128-bit keys. This method may deter casual snooping but is not considered very secure. TKIP: Temporal Key Integrity Protocol (TKIP) is only available for WPA, WPA2, WPA-PSK, and WPA2-PSK authentication methods. TKIP is part of a draft standard from the IEEE 802.11i working group and utilizes the RC4 stream cipher with 128-bit keys for encryption and 64-bit keys for authentication. TKIP improves on WEP by adding a per-packet key mixing function to de-correlate the public initialization vectors (IVs) from weak keys. AES-CCMP: This is a powerful encryption method that is only available for WPA, WPA2, WPA-PSK, and WPA2-PSK authentication methods. Advanced Encryption Standard (AES) is the block cipher system used by the Robust Secure Network (RSN) protocol and is equivalent to the RC4 algorithm used by WPA. CCMP is the security protocol used by AES, equivalent to TKIP for WPA. Data undergoes a Message Integrity Check (MIC) using a well-known and proven technique called Cipher Block Chaining Message Authentication Code (CBC-MAC). The technique ensures that even a one-bit alteration in a message produces a dramatically different result. Master keys are not used directly but are used to derive other keys, each of which expire after a certain amount of time. Messages are encrypted using a secret 128-bit key and a 128-bit block of data. The encryption process is complex, but the administrator does not need to be aware of the intricacies of the computations. The end result is encryption that is much harder to break than even WPA.

PSK Passphrase

Default	
Options	free text (e.g., "This is the WLAN passphrase")
Description	This field is only available for WPA-PSK and WPA2-PSK authentication methods. If the WE-2100T's passphrase does not match the AP's passphrase, the connection will be denied. A PSK of sufficient strength—one that uses a mix of letters, numbers and non-alphanumeric characters—is recommended.

Security Settings for WEP Encryption



WLAN Profile Properties

Security Properties

Profile name: Infrastructure
Authentication: Open System
Encryption: Disable (Disable, WEP)

WLAN Profile Properties

Security Properties

Profile name: Infrastructure
Authentication: Open System
Encryption: WEP
WEP key length: 64bits
WEP key index: 1
WEP key source: ● Manual ○ Generate WEP keys by passphrase
WEP key format: ASCII
WEP key 1:
WEP key 2:
WEP key 3:
WEP key 4:

When **Encryption** is set to WEP on the **Security** page for the WLAN profile, you will be able to configure **WEP key length**, **WEP key index**, and **WEP key source**. Other settings will be displayed depending on how **WEP key source** is configured.

WEP Key Length

Default	64bits
Options	64bits, 128bits
Description	This field specifies the length of the WEP key. 64bits is the industry standard for WEP, but 128bits provides better protection.

WEP Key Index

Default	1
Options	1 through 4
Description	This field specifies the primary WEP key to use for the WLAN.

WEP Key Source

Default	Manual
Options	Manual, Generate WEP keys by passphrase
Description	This field specifies whether the WEP key will be generated manually or through a user-specified passphrase. A passphrase is equivalent to a free-text password that will be used to generate the WEP key. A passphrase is typically easier to remember and enter than a long and complicated WEP key.

WEP Passphrase

Default	
Options	free text (e.g., "This is the WEP passphrase")
Description	This field is only available if **WEP key source** is set to "Generate WEP keys by passphrase". A standard hexadecimal password will be generated using the supplied passphrase. For example, if "404tech" is entered, the WEP key will be "DB971608E942FC39BD89FC4ADB".

WEP Key Format

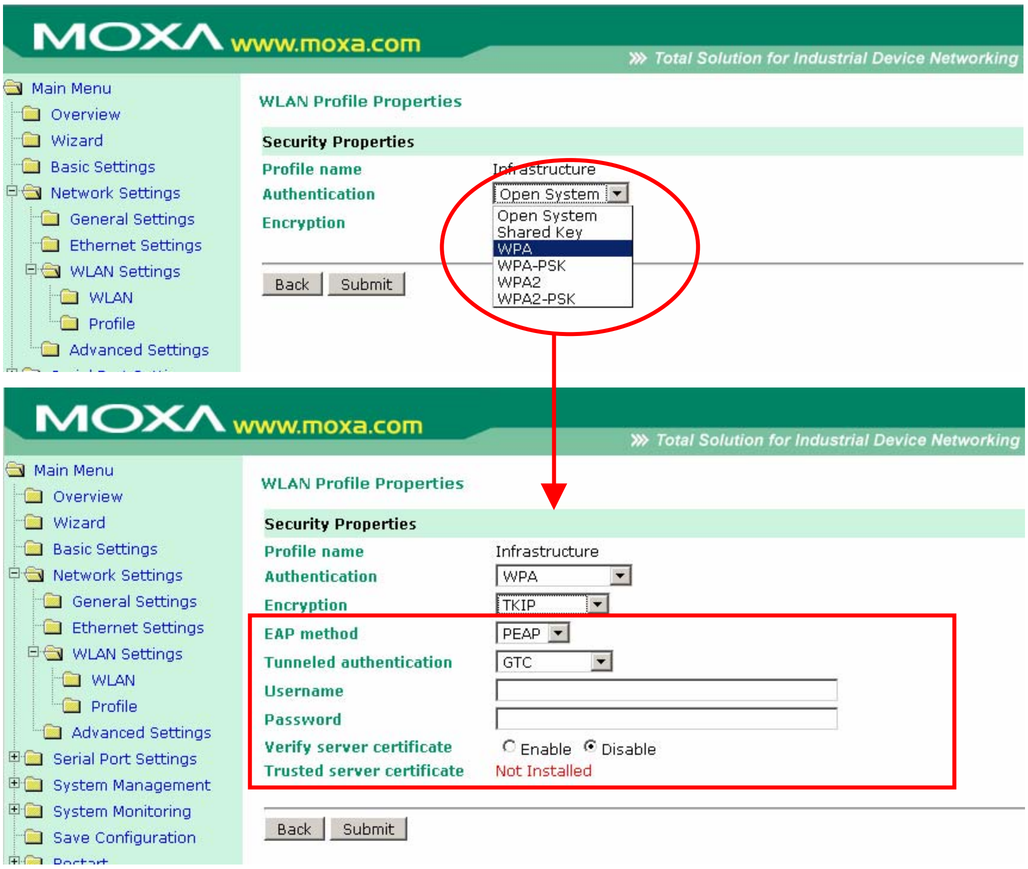
Default	ASCII
Options	ASCII, HEX
Description	This field is only available if **WEP key source** is set to "Manual". It specifies the format you will use to enter the WEP key.

WEP Key 1 Through 4

Default	
Options	free text in ASCII or HEX
Description	These fields are only available if **WEP key source** is set to "Manual". Enter each WEP key in ASCII or HEX as specified in **WEP key format**. The number of characters required for each key depends on **WEP key length** and **WEP key format**.

WEP Key Length	WEP Key Format	Key Length
64bits	ASCII	5 characters
	HEX	10 characters
128bits	ASCII	13 characters
	HEX	26 characters

Security Settings for WPA, WPA2



WLAN Profile Properties

Security Properties

Profile name	Infrastructure
Authentication	Open System
Encryption	

WLAN Profile Properties

Security Properties

Profile name	Infrastructure
Authentication	WPA
Encryption	TKIP
EAP method	PEAP
Tunneled authentication	GTC
Username	
Password	
Verify server certificate	○ Enable ● Disable
Trusted server certificate	Not Installed

When WPA or WPA2 is used for authentication, you will also need to configure **EAP method** in the **Security** settings for the WLAN profile. Other settings will also be displayed depending on how **EAP method** is configured.

There are two parts to WPA and WPA2 security, authentication and data encryption.

- Authentication occurs before access is granted to a WLAN. Wireless clients such as the WE-2100T are first authenticated by the AP according to the authentication protocol used by the RADIUS server. Depending on the WLAN security settings, an EAP tunnel can be used to scramble the username and password that is submitted for authentication purposes.
- Encryption occurs after WLAN access has been granted. For all wireless devices, data is first encrypted before wireless transmission, using mutually agreed-upon encryption protocols.

EAP Method

Default	PEAP
Options	TLS, PEAP, TTLS, LEAP
Description	This field specifies the EAP method to use for authentication. Four methods are supported. TLS: Transport Layer Security (TLS) was created by Microsoft and accepted by the IETF as RFC 2716: PPP EAP TLS Authentication Protocol. Passwords and tunneled authentication are not used. A user certificate and user private key are used to identify the WE-2100T. The WE-2100T's user certificate and user private key must already be installed on the RADIUS server. PEAP: Protected Extensible Authentication Protocol (PEAP) is a proprietary protocol which was developed by Microsoft, Cisco and RSA Security. TTLS: Tunneled Transport Layer Security (TTLS) is a proprietary protocol which was developed by Funk Software and Certicom, and is supported by Agere Systems, Proxim, and Avaya. TTLS is being considered by the IETF as a new standard. For more information on TTLS, read the draft RFC EAP Tunneled TLS Authentication Protocol. LEAP: Lightweight Extensible Authentication Protocol (LEAP) is a proprietary protocol which was developed by Cisco. LEAP doesn't check certificate during the authentication process.

Tunneled Authentication

Default	PAP (when using TTLS) GTC (when using PEAP)
Options	GTC, MD5, MSCHAP V2 (when using PEAP) PAP, CHAP, MSCHAP, MSCHAP V2, EAP-MSCHAP V2, EAP-GTC, EAP-MD5 (when using TTLS)
Description	This field specifies the encryption method to use during the authentication process. Different encryption methods are available depending on the **EAP method**.

Username

Default	
Options	free text (e.g., "Smith_John")
Description	This field specifies the username that will be used to gain access to the WLAN. The correct username and password must be provided for access to be granted.

Password

Default	
Options	free text (e.g., "Password123")
Description	This field specifies the password that will be used to gain access to the WLAN. The correct username and password must be provided for access to be granted.

Anonymous Username

Default	
Options	free text (e.g., “Anyuser”)
Description	This field specifies the anonymous username to use when initiating authentication. After the RADIUS server has been verified by certificate, the true username and password will be used to complete the authentication process.

Verify Server Certificate

Default	Disable
Options	Disable, Enable
Description	Disable: The certificate from the RADIUS server will be ignored. Enable: The certificate from the RADIUS server will be used to authenticate access to the WLAN. The RADIUS server’s trusted server certificate must already be installed on the WE-2100T. To install a trusted server certificate, visit the corresponding page in the **System Management> Certificate** folder.

Trusted Server Certificate

Default	---
Options	---
Description	This field is available for PEAP, TLS, and TTLS EAP methods only. It displays information on the trusted server certificate that is installed on the WE-2100T. To install a trusted server certificate, visit the corresponding page in the **System Management> Certificate** folder.

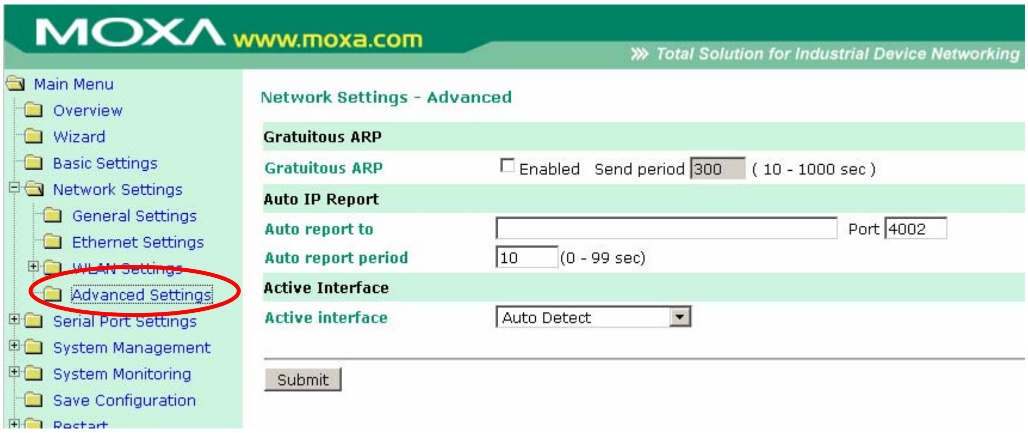
User Certificate

Default	---
Options	---
Description	This field is available only when **EAP method** has been set to TLS. It displays information on the user certificate that is installed on the WE-2100T. To install a user certificate, visit the corresponding page in the **System Management> Certificate** folder.

User Private Key

Default	---
Options	---
Description	This field is available only when **EAP method** has been set to TLS. It displays information on the user private key on the WE-2100T.

Network Settings> Advanced Settings



Network Settings - Advanced

Gratuitous ARP

Gratuitous ARP □ Enabled Send period 300 (10 - 1000 sec)

Auto IP Report

Auto report to Port 4002

Auto report period 10 (0 - 99 sec)

Active Interface

Active interface Auto Detect

On the **Advanced Settings** page in the **Network Settings** folder, you can modify **Gratuitous ARP**, **Auto report to**, **Auto report period**, and **Active interface**.

Gratuitous ARP

Default	Disabled
Options	Disabled, Enabled, 10 to 1000 sec
Description	This field specifies how often the WE-2100T sends broadcast packets to update the ARP table. This may be required for certain applications. Disabled: The WE-2100T will not send broadcast packets to update the ARP table. Enabled: The WE-2100T will send periodically send broadcast packets at the time interval as specified in **Send period**.

Auto Report To

Default	
Options	IP address and port (e.g., “192.168.64.64” and “4002”)
Description	This optional field specifies the destination IP address for the module’s IP address report. Regular IP address reports are sent to the specified IP address and port when the module’s IP address is configured by DHCP or BOOTP. These IP address reports are used to notify a network host of the module’s current IP address. The destination for the IP address report should be one of the following : ● a network host running the IP Address Report function in Network Enabler Administrator ● a network host running a user-developed application that uses the IP report protocol Please refer to Chapter 12 for details on receiving IP address reports in Network Enabler Administrator. Please refer to Appendix E for details on the IP report protocol.

Auto Report Period

Default	10
Options	0 to 99
Description	This field specifies how often the WE-2100T sends IP address reports.

Active Interface

Default	Auto Detect
Options	Auto Detect, Select by DI8, Force Wired Ethernet, Force Wireless LAN
Description	This field specifies how the WE-2100T will select whether to use the wired LAN connection or the wireless (WLAN) connection. Auto Detect: The LAN connection will be used if a valid connection is detected when the module is powered on. Otherwise, the module will use the WLAN connection. Select by DI8: The network connection will be determined by the signal from DIO channel 8. This channel must be set to DI mode. When the signal is low, the module will use the LAN connection. When the signal is high, the module will use the WLAN connection. Force Wired Ethernet: The module will only use the LAN connection. The WLAN connection will be ignored. Force Wireless LAN: The module will only use the WLAN connection. The LAN connection will be ignored.

8
Web Console: Serial Port Settings

The web console is the most user-friendly method available to configure the module. With a standard web browser, you have easy and intuitive access to all settings and options. In this chapter, we introduce the web console and go through the basic configuration options. The same configuration options are also available through the Telnet and serial console.

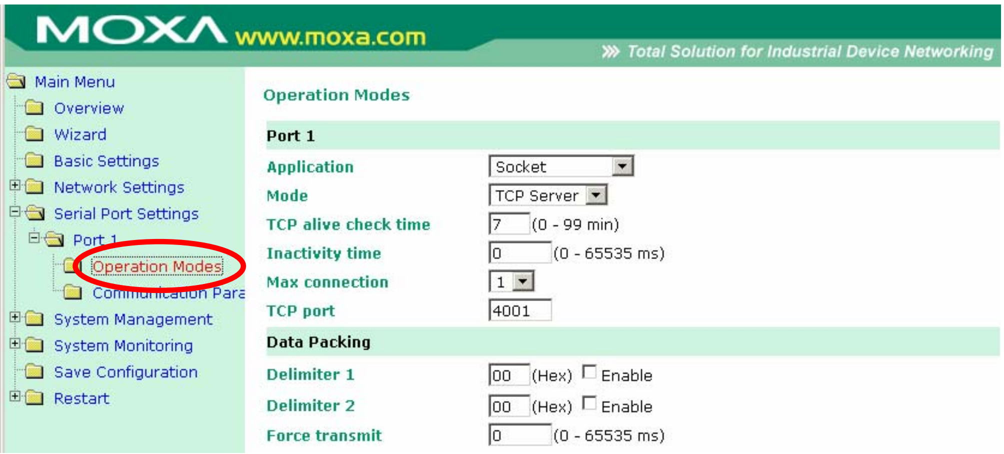
This chapter covers the following topics:

- ❑ **Overview**
- ❑ **Serial Port Settings> Port 1> Operation Modes**
- ❑ **Settings for RealCOM Mode**
- ❑ **Settings for RFC2217 Mode**
- ❑ **Settings for TCP Server Mode**
- ❑ **Settings for TCP Client Mode**
- ❑ **Settings for UDP Mode**
- ❑ **Serial Port Settings> Port 1> Communication Parameters**

Overview

This chapter explains how to configure all settings located under the **Serial Port Settings** folder in the web console.

Serial Port Settings> Port 1> Operation Modes



Operation Modes

Port 1	
Application	Socket
Mode	TCP Server
TCP alive check time	7 (0 - 99 min)
Inactivity time	0 (0 - 65535 ms)
Max connection	1
TCP port	4001
Data Packing	
Delimiter 1	00 (Hex) □ Enable
Delimiter 2	00 (Hex) □ Enable
Force transmit	0 (0 - 65535 ms)

The **Operation Modes** page is where you configure the serial port's operation mode and related settings. For an introduction to the different operation modes, please refer to Chapter 4.

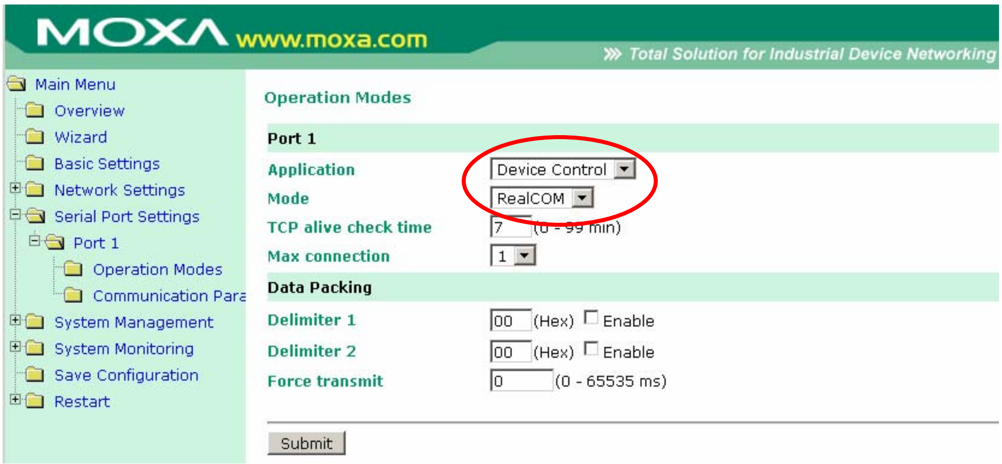
Application

Default	Socket
Options	Socket, Device Control
Description	This field specifies what kind application you will be using for this serial port. Depending on the application, different operation modes and related settings will be displayed. For an introduction to the different operation modes, please refer to Chapter 4. Device Control: The serial port will be used to control a device using legacy software installed on a Windows, Linux, or UNIX system. Drivers will need to be installed that will allow your software to communicate with the device as if it were physically attached to a local COM or TTY port. You may select between RealCOM and RFC2217 operation modes. Socket: This serial port will be used for a TCP or UDP socket-based application. You may select between TCP Client, TCP Server, and UDP operation modes.

Mode

Default	(depends on Application)
Options	RealCOM, RFC2217, TCP Server, TCP Client, UDP
Description	Along with **Application**, this field specifies the serial port's operation mode, or how it will interact with network devices. Depending on how **Application** is configured, different options are available for Mode. Depending on how Mode is configured, additional settings will be available for configuration. For an introduction to the different operation modes, please refer to Chapter 4. RealCOM: This serial port will operate in RealCOM mode. RFC2217: This serial port will operate in RFC2217 mode. TCP Server: This serial port will operate in TCP Server mode. TCP Client: This serial port will operate in TCP Client mode. UDP: This serial port will operate in UDP mode.

Settings for RealCOM Mode



Operation Modes

Port 1

Application: Device Control

Mode: RealCOM

TCP alive check time: 7 (0 - 99 min)

Max connection: 1

Data Packing

Delimiter 1: 00 (Hex) □ Enable

Delimiter 2: 00 (Hex) □ Enable

Force transmit: 0 (0 - 65535 ms)

When **Mode** is set to RealCOM on the **Operation Modes** page, you will be able to configure additional settings such as **TCP alive check time**, **Max connection**, and **Delimiter 1 and 2**.

TCP Alive Check Time

Default	7 min
Options	0 to 99 min
Description	This field specifies how long the module will wait for a response to “keep alive” packets before closing the TCP connection. The module checks connection status by sending periodic “keep alive” packets. 0: The TCP connection will remain open even if there is no response to the “keep alive” packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the module will force the existing TCP connection to close.

Max Connection

Default	1
Options	1 to 4
Description	This field specifies the maximum number of connections that will be accepted by the serial port. 1: Only one specific host can access this serial port, and the Real COM driver on that host will have full control over the port. 2 to 4: This serial port will allow the specified number of connections to be opened simultaneously. With simultaneous connections, the Real COM driver will only provide a pure data tunnel with no control ability. The serial communication will be determined by the module rather than by your application program. Application software that is based on the Real COM driver will receive a driver response of “success” when using any of the Win32 API functions. The module will send data only to the Real COM driver on the host. Data received from hosts will be sent to the attached serial device on a first-in-first-out basis.

⚠ ATTENTION

When **Max connection** is 2 or greater, the serial port’s communication settings (i.e., baudrate, parity, data bits, etc.) will be determined by the module. Any host that opens the COM port connection must use identical serial communication settings.

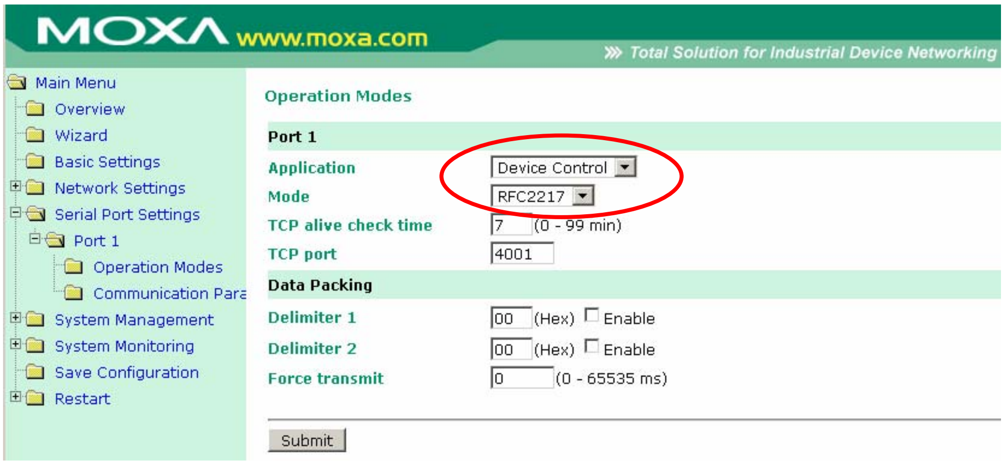
Delimiter 1 and 2

Default	Disabled
Options	Disabled, Enabled, 00 to FF
Description	These fields are used to define special delimiter character(s) for data packing. Enable **Delimiter 1** to control data packing with a single character; enable both **Delimiter 1 and 2** to control data packing with two characters received in sequence. When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Delimiters must be incorporated into the data stream at the software or device level.

Force Transmit

Default	0 ms
Options	0 to 65535
Description	This field controls data packing by the amount of time that elapses between bits of data. 0: If serial data is not received, the module will wait indefinitely for additional data. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.

Settings for RFC2217 Mode



Operation Modes

Port 1

Application	Device Control
Mode	RFC2217
TCP alive check time	7 (0 - 99 min)
TCP port	4001
Data Packing	
Delimiter 1	00 (Hex) □ Enable
Delimiter 2	00 (Hex) □ Enable
Force transmit	0 (0 - 65535 ms)

When **Mode** is set to RFC2217 on the **Operation Modes** page, you will be able to configure additional settings such as **TCP alive check time**, **TCP port**, and **Delimiter 1 and 2**.

TCP Alive Check Time

Default	7 min
Options	0 to 99 min
Description	This field specifies how long the module will wait for a response to "keep alive" packets before closing the TCP connection. The module checks connection status by sending periodic "keep alive" packets. 0: The TCP connection will remain open even if there is no response to the "keep alive" packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the module will force the existing TCP connection to close.

TCP Port

Default	4001
Options	0 to 9999
Description	This field specifies the TCP port number that the serial port will use to listen to connections, and that other devices must use to contact the serial port.

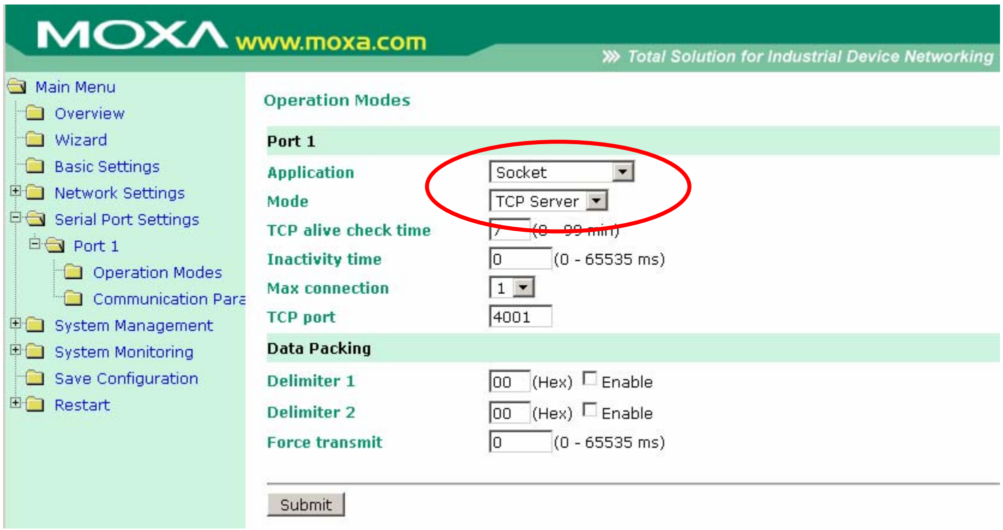
Delimiter 1 and 2

Default	Disabled
Options	Disabled, Enabled, 00 to FF
Description	These fields are used to define special delimiter character(s) for data packing. Enable **Delimiter 1** to control data packing with a single character; enable both **Delimiter 1 and 2** to control data packing with two characters received in sequence. When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Delimiters must be incorporated into the data stream at the software or device level.

Force Transmit

Default	0 ms
Options	0 to 65535
Description	This field controls data packing by the amount of time that elapses between bits of data. 0: If serial data is not received, the module will wait indefinitely for additional data. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.

Settings for TCP Server Mode



Operation Modes

Port 1

Application	Socket
Mode	TCP Server
TCP alive check time	7 (0 - 99 min)
Inactivity time	0 (0 - 65535 ms)
Max connection	1
TCP port	4001

Data Packing

Delimiter 1	00 (Hex) □ Enable
Delimiter 2	00 (Hex) □ Enable
Force transmit	0 (0 - 65535 ms)

When **Mode** is set to **TCP Server** on the **Operation Modes** page, you will be able to configure additional settings such as **TCP alive check time**, **Inactivity time**, and **Max connection**.

TCP Alive Check Time

Default	7 min
Options	0 to 99 min
Description	This field specifies how long the module will wait for a response to "keep alive" packets before closing the TCP connection. The module checks connection status by sending periodic "keep alive" packets. 0: The TCP connection will remain open even if there is no response to the "keep alive" packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the module will force the existing TCP connection to close.

Inactivity Time

Default	0 ms
Options	0 to 65535 ms
Description	This field specifies the time limit for keeping the connection open if no data flows to or from the serial device. 0: The connection will remain open even if data is never received. For many applications, the serial device may be idle for long periods of time, so 0 is an appropriate setting. 1 to 65535: If there is no activity for the specified time, the connection will be closed. When adjusting this field, make sure that it is greater than the **Force transmit** time. Otherwise, the TCP connection may be closed before data in the buffer can be transmitted.

Max Connection

Default	1
Options	1 to 4
Description	This field specifies the maximum number of connections that will be accepted by the serial port. 1: Only a single host may open the TCP connection to the serial port. 2 to 4: This serial port will allow the specified number of connections to be opened simultaneously. When multiple connections are established, serial data will be duplicated and sent to all connected hosts. Data from hosts will be sent to the attached serial device on a first-in-first-out basis.

TCP Port

Default	4001
Options	0 to 9999
Description	This field specifies the TCP port number that the serial port will use to listen to connections, and that other devices must use to contact the serial port.

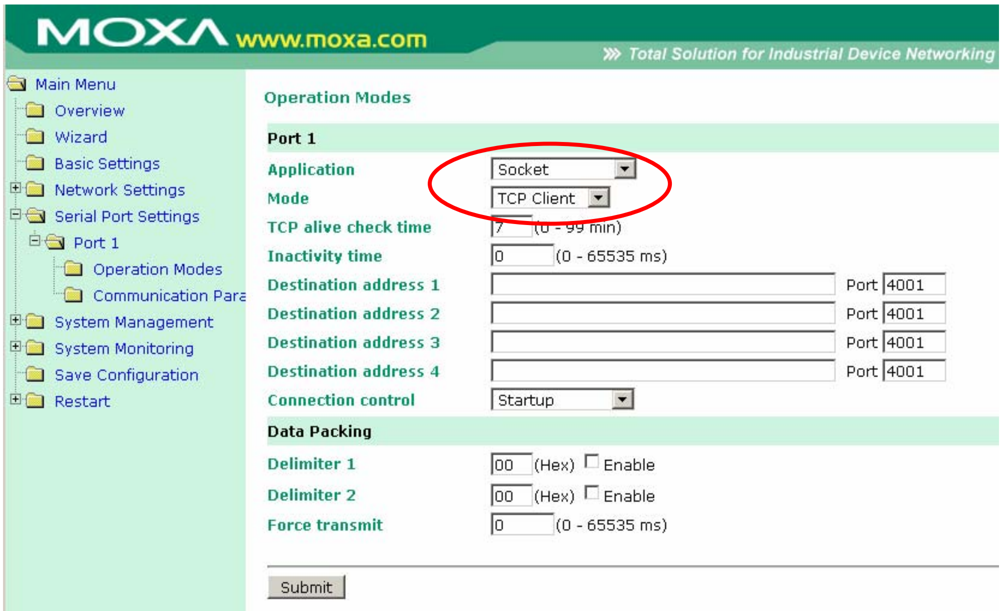
Delimiter 1 and 2

Default	Disabled
Options	Disabled, Enabled, 00 to FF
Description	These fields are used to define special delimiter character(s) for data packing. Enable **Delimiter 1** to control data packing with a single character; enable both **Delimiter 1 and 2** to control data packing with two characters received in sequence. When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Delimiters must be incorporated into the data stream at the software or device level.

Force Transmit

Default	0 ms
Options	0 to 65535
Description	This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that **Inactivity time** is disabled or set to a larger value. Otherwise the connection may be closed before the data in the buffer can be transmitted. 0: If serial data is not received, the module will wait indefinitely for additional data. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.

Settings for TCP Client Mode



Operation Modes

Port 1

Application	Socket		
Mode	TCP Client		
TCP alive check time	7 (0 - 99 min)		
Inactivity time	0 (0 - 65535 ms)		
Destination address 1		Port	4001
Destination address 2		Port	4001
Destination address 3		Port	4001
Destination address 4		Port	4001
Connection control	Startup		

Data Packing

Delimiter 1	00 (Hex) □ Enable
Delimiter 2	00 (Hex) □ Enable
Force transmit	0 (0 - 65535 ms)

When **Mode** is set to **TCP Client** on the **Operation Modes** page, you will be able to configure additional settings such as **TCP alive check time**, **Inactivity time**, and **Connection control**.

TCP Alive Check Time

Default	7 min
Options	0 to 99 min
Description	This field specifies how long the module will wait for a response to "keep alive" packets before closing the TCP connection. The module checks connection status by sending periodic "keep alive" packets. 0: The TCP connection will remain open even if there is no response to the "keep alive" packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the module will force the existing TCP connection to close.

Inactivity Time

Default	0 ms
Options	0 to 65535 ms
Description	This field specifies the time limit for keeping the connection open if no data flows to or from the serial device. 0: The TCP connection will be kept active until a connection close request is received, even if data is never received. For many applications, the serial device may be idle for long periods of time, so 0 is an appropriate setting. 1 to 65535: If there is no activity for the specified time, the connection will be closed. When adjusting this field, make sure that it is greater than the Force transmit time. Otherwise, the TCP connection may be closed before data in the buffer can be transmitted. **Connection control** must be set to "Any character" for this setting to have effect.

Destination Address 1 to 4

Default	
Options	IP address and port (e.g., "192.168.1.1" and "4001")
Description	This field specifies the remote host(s) that will access the attached device. At least one destination must be provided. This field supports the use of domain names and names defined in the host table.

ATTENTION

In TCP Client mode, up to 4 connections can be established between the serial port and TCP hosts. The connection speed or throughput may be low if any one of the four connections is slow, since the one slow connection will slow down the other 3 connections.

Connection Control

Default	Startup
Options	Startup, Any Character
Description	This field specifies how connections to the device are established and closed. Startup: The connection will be opened as the module starts up. Any Character: The connection will be opened as soon as a character is received from the attached device.

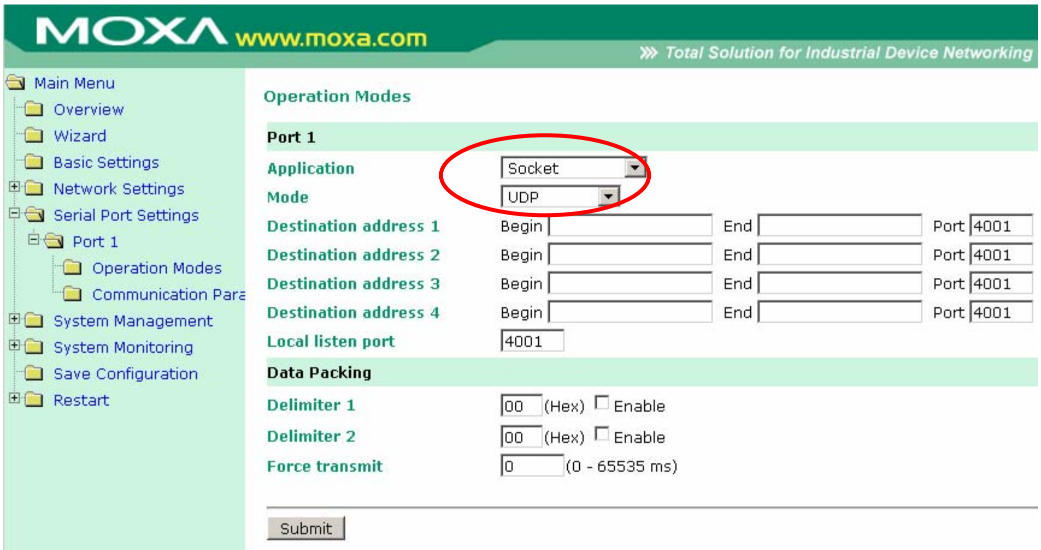
Delimiter 1 and 2

Default	Disabled
Options	Disabled, Enabled, 00 to FF
Description	These fields are used to define special delimiter character(s) for data packing. Enable **Delimiter 1** to control data packing with a single character; enable both **Delimiter 1 and 2** to control data packing with two characters received in sequence. When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Delimiters must be incorporated into the data stream at the software or device level.

Force Transmit

Default	0 ms
Options	0 to 65535
Description	This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that **Inactivity time** is disabled or set to a larger value. Otherwise the connection may be closed before the data in the buffer can be transmitted. 0: If serial data is not received, the module will wait indefinitely for additional data. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.

Settings for UDP Mode



Operation Modes

Port 1			
Application	Socket		
Mode	UDP		
Destination address 1	Begin	End	Port 4001
Destination address 2	Begin	End	Port 4001
Destination address 3	Begin	End	Port 4001
Destination address 4	Begin	End	Port 4001
Local listen port	4001		
Data Packing			
Delimiter 1	00 (Hex) □ Enable		
Delimiter 2	00 (Hex) □ Enable		
Force transmit	0 (0 - 65535 ms)		

When **Mode** is set to **UDP** on the **Operation Modes** page, you will be able to configure additional settings such as **Destination address 1** through **4**, **Local listen port**, and **Delimiter 1 and 2**.

Destination Address 1 to 4

Default	
Options	IP address range and port (e.g., "192.168.1.1" to "192.168.1.64" and "4001")
Description	In UDP mode, you may specify up to 4 ranges of IP addresses for the serial port to connect to. At least one destination range must be provided. The maximum selectable IP address range is 64 addresses. However, you can enter multi-unicast addresses in the Begin field, in the form xxx.xxx.xxx.255. For example, enter "192.127.168.255" to allow the module to broadcast UDP packets to all hosts with IP addresses between 192.127.168.1 and 192.127.168.254.

Local Listen Port

Default	4001
Options	0 to 9999
Description	This field specifies the UDP port that the module listens to and that other devices must use to contact the attached serial device.

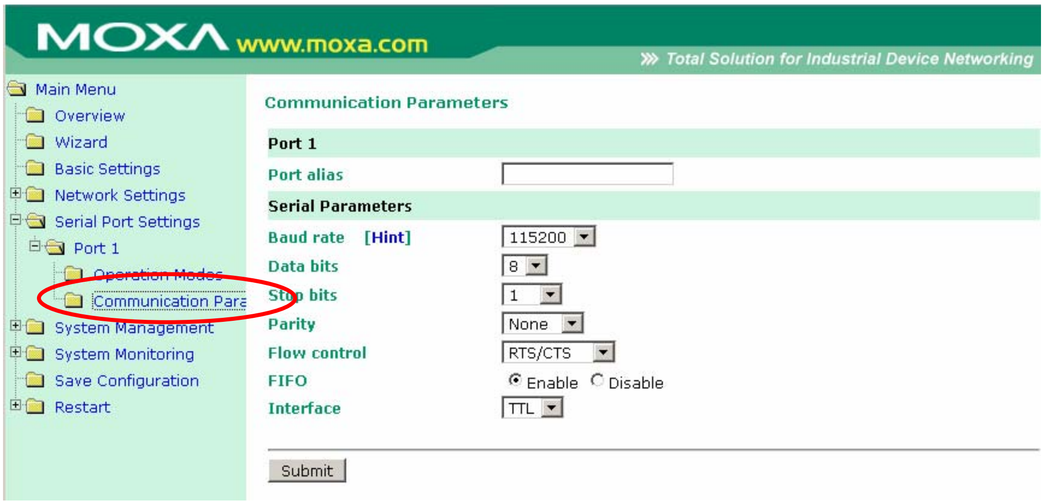
Delimiter 1 and 2

Default	Disabled
Options	Disabled, Enabled, 00 to FF
Description	These fields are used to define special delimiter character(s) for data packing. Enable **Delimiter 1** to control data packing with a single character; enable both **Delimiter 1 and 2** to control data packing with two characters received in sequence. When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Delimiters must be incorporated into the data stream at the software or device level.

Force Transmit

Default	0 ms
Options	0 to 65535
Description	This field controls data packing by the amount of time that elapses between bits of data. 0: If serial data is not received, the module will wait indefinitely for additional data. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.

Serial Port Settings> Port 1> Communication Parameters



Communication Parameters

Port 1

Port alias	
Serial Parameters	
Baud rate [Hint]	115200
Data bits	8
Stop bits	1
Parity	None
Flow control	RTS/CTS
FIFO	● Enable ○ Disable
Interface	TTL

The **Communication Parameters** page is where serial communication settings are specified, such as **Baud rate**, **Data bits**, and **Stop bits**.

Port Alias

Default	
Options	free text (e.g., “Secondary console connection”)
Description	This is an optional free text field to help you differentiate one serial port from another. It does not affect operation of the module.

ATTENTION

Serial communication settings should match the attached serial device. Check the communication settings in the user’s manual for your serial device.

Baud Rate

Default	115200
Options	50, 75, 110, 134, 150, 300, 600, 1200, 1800, 2400, 4800, 7200, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600
Description	This field specifies the baudrate for the serial port.

Data Bits

Default	8
Options	5, 6, 7, 8
Description	This field specifies the number of data bits used to encode each character of data.

Stop Bits

Default	1
Options	1, 1.5, 2
Description	This field specifies the number of stop bits used for each character frame.

Parity

Default	None
Options	None, Odd, Even, Space, Mark
Description	This field specifies the type of parity bit used for each character frame.

Flow Control

Default	RTS/CTS
Options	None, RTS/CTS, XON/XOFF, DTR/DSR
Description	This field specifies the type of flow control used by the serial port.

FIFO

Default	Enable
Options	Enable, Disable
Description	This field specifies whether the serial port will use the built-in FIFO. A 128-byte FIFO is provided to each serial port for both Tx and Rx directions. To prevent data loss during serial communication, this should be set to Disabled if the attached serial device does not have a FIFO.

Interface

Default	TTL
Options	TTL
Description	This field specifies the type of interface the serial port will use. The WE-2100T supports TTL only.

9

Web Console: System Management

The web console is the most user-friendly method available to configure the module. With a standard web browser, you have easy and intuitive access to all settings and options. In this chapter, we introduce the web console and go through the basic configuration options. The same configuration options are also available through the Telnet and serial console.

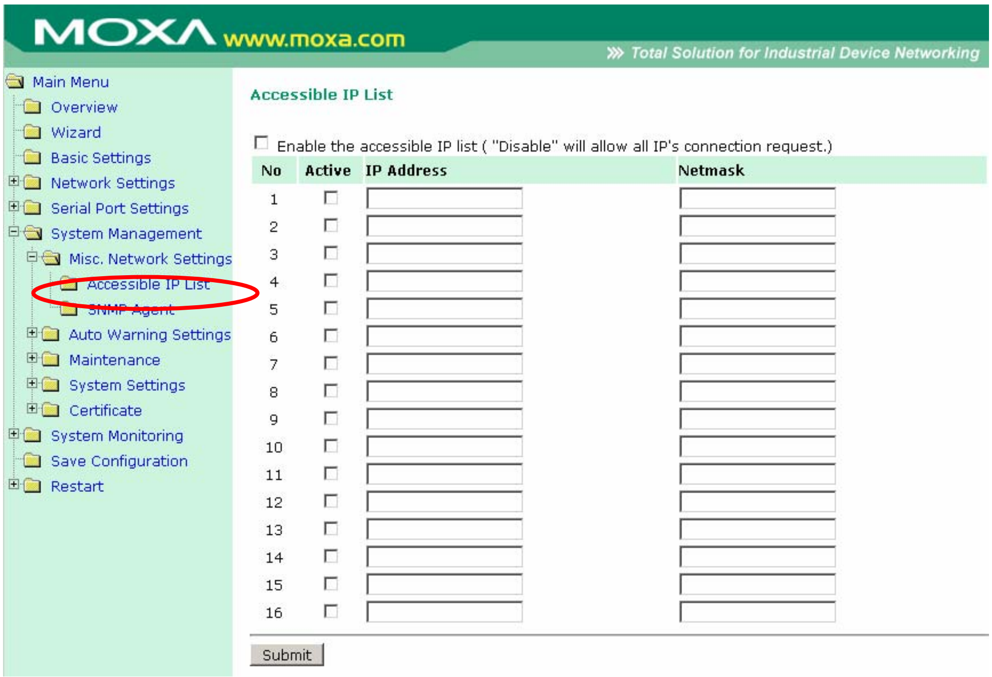
This chapter covers the following topics:

- ❑ **Overview**
- ❑ **System Management> Misc. Network Settings> Accessible IP List**
- ❑ **System Management> Misc. Network Settings> SNMP Agent Settings**
- ❑ **System Management> Auto Warning Settings> Event Settings**
- ❑ **System Management> Auto Warning Settings> Serial Event Settings**
- ❑ **System Management> Auto Warning Settings> E-mail Alert**
- ❑ **System Management> Auto Warning Settings> SNMP Trap**
- ❑ **System Management> Maintenance> Console Settings**
- ❑ **System Management> Maintenance> Ping**
- ❑ **System Management> Maintenance> Firmware Upgrade**
- ❑ **System Management> Maintenance> Configuration Import**
- ❑ **System Management> Maintenance> Configuration Export**
- ❑ **System Management> Maintenance> Load Factory Default**
- ❑ **System Management> Maintenance> Change Password**
- ❑ **System Management> System Settings> Serial Command Mode**
- ❑ **System Management> System Settings> Digital IO**
- ❑ **System Management> Certificate> Ethernet SSL Certificate Import**
- ❑ **System Management> Certificate> WLAN SSL Certificate Import**
- ❑ **System Management> Certificate> WPA Server Certificate Import**
- ❑ **System Management> Certificate> WPA User Certificate Import**
- ❑ **System Management> Certificate> WPA User Key Import**
- ❑ **System Management> Certificate> Certificate/Key Delete**

Overview

This chapter explains how to configure all settings located under the **System Management** folder in the web console.

System Management> Misc. Network Settings> Accessible IP List



Accessible IP List

□ Enable the accessible IP list ("Disable" will allow all IP's connection request.)

No	Active	IP Address	Netmask
1	□		
2	□		
3	□		
4	□		
5	□		
6	□		
7	□		
8	□		
9	□		
10	□		
11	□		
12	□		
13	□		
14	□		
15	□		
16	□		

Submit

The **Accessible IP List** page is located under **Misc. Network Settings** in the **System Management** folder. This page is used this restrict access to the module by IP address. Only IP addresses on the list will be allowed access to the module. You may add a specific address or range of addresses by using a combination of IP address and netmask, as follows:

To allow access to a specific IP address
Enter the IP address in the corresponding field; enter 255.255.255.255 for the netmask.

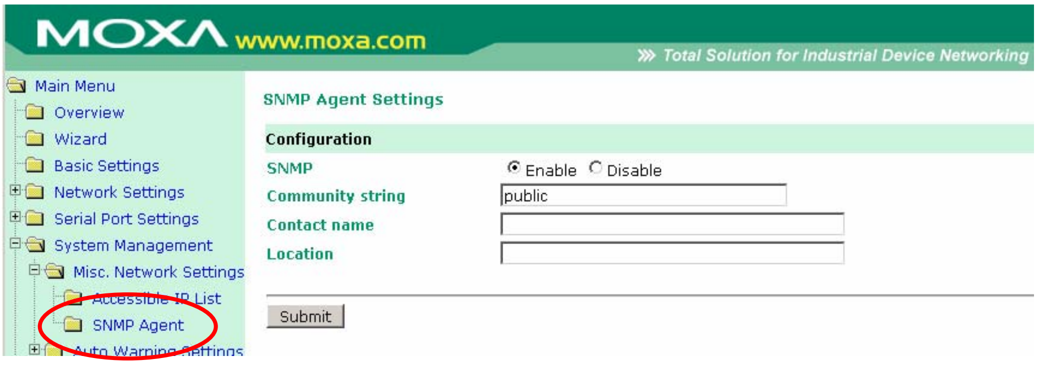
To allow access to hosts on a specific subnet
For both the IP address and netmask, use 0 for the last digit (e.g., "192.168.1.0" and "255.255.255.0").

To allow access to all IP addresses
Make sure that **Enable the accessible IP list** is not checked.

Additional configuration examples are shown in the following table:

Desired IP Range	IP Address Field	Netmask Field
Any host	Disable	Disable
192.168.1.120	192.168.1.120	255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0	255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0	255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0	255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128	255.255.255.128

System Management> Misc. Network Settings> SNMP Agent Settings



SNMP Agent Settings

Configuration

SNMP ● Enable ○ Disable

Community string: public

Contact name:

Location:

The **SNMP Agent** page is located under **Misc. Network Settings** in the **System Management** folder. This page is used to configure the SNMP Agent on the WE-2100T.

SNMP

Default	Enable
Options	Enable, Disable
Description	This field enables or disables the SNMP Agent. If enabled, you will need to configure other SNMP Agent settings. You will need to enter a community name under **Community string**.

Community String

Default	public
Options	free text (e.g., "public community")
Description	This field specifies the community string used for the SNMP Agent. This is a text password mechanism that is used to weakly authenticate queries to agents of managed network devices.

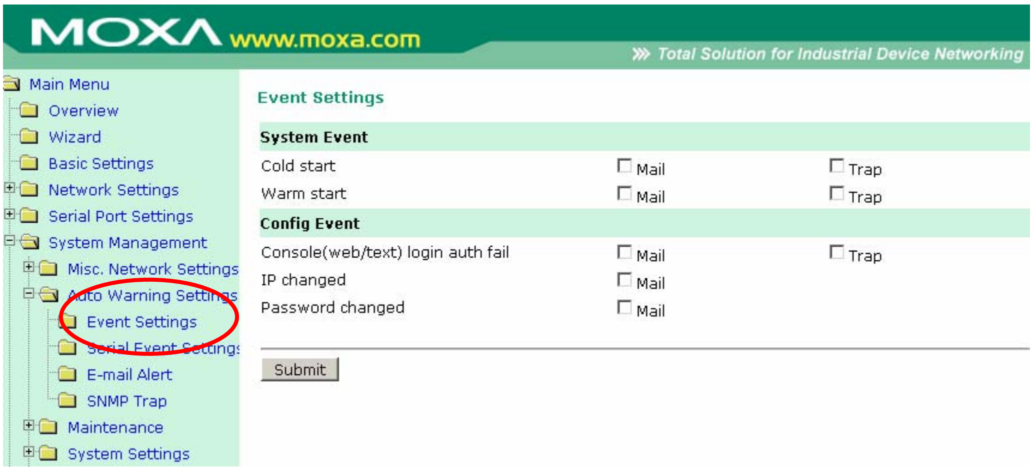
Contact Name

Default	
Options	free text (e.g., "J Smith")
Description	This is an optional free text field that can be used to specify the SNMP emergency contact name, telephone, or pager number.

Location

Default	
Options	free text (e.g., "Building XYZ")
Description	This is an optional free text field that can be used to specify the location for SNMP agents such as the module.

System Management> Auto Warning Settings> Event Settings



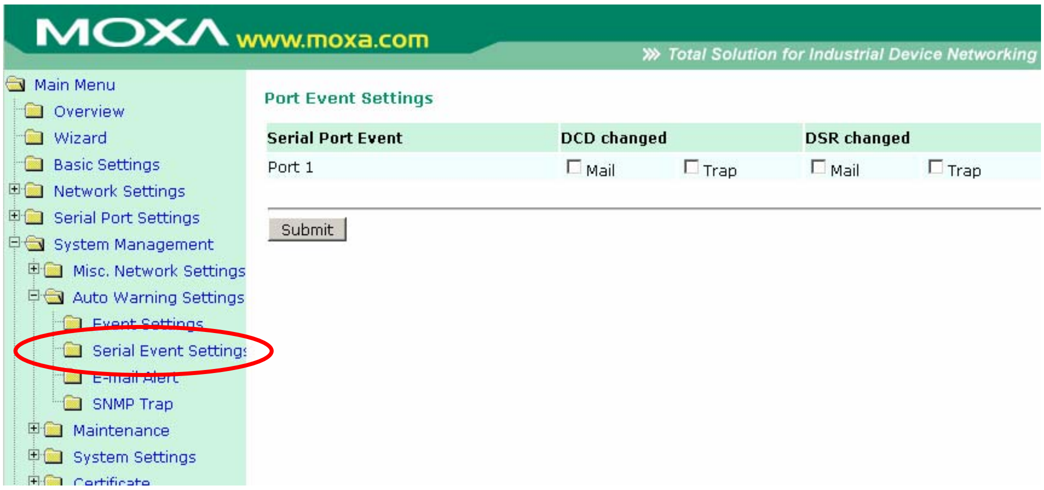
Event Settings

System Event		
Cold start	□ Mail	□ Trap
Warm start	□ Mail	□ Trap
Config Event		
Console(web/text) login auth fail	□ Mail	□ Trap
IP changed	□ Mail	
Password changed	□ Mail	

The **Event Settings** page is located under **Auto Warning Settings** in the **System Management** folder. This is where you specify how the WE-2100T will notify you of system and configuration events. Depending on the event, different options for notification are available, as shown above. **Mail** refers to sending an e-mail to a specified address. **Trap** refers to sending an SNMP trap.

Event	Description
Cold start	The module was powered on, or was restarted after a firmware upgrade.
Warm start	The module restarted without powering off.
Console login auth fail	An attempt has been made to open the web, Telnet, or serial console, but the password was incorrect.
IP changed	The IP address has been changed.
Password changed	The password to the console has been changed.

System Management> Auto Warning Settings> Serial Event Settings



Port Event Settings

Serial Port Event	DCD changed		DSR changed	
Port 1	□ Mail	□ Trap	□ Mail	□ Trap

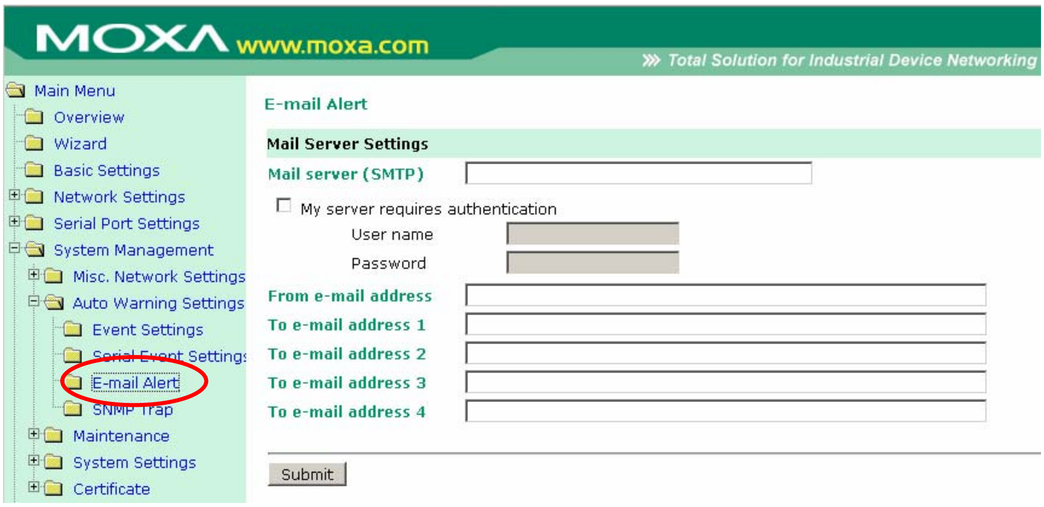
The **Serial Event Settings** page is located under **Auto Warning Settings** in the **System Management** folder. This is where you specify how the WE-2100T will notify you of DCD and DSR events for each serial port. **Mail** refers to sending an e-mail to a specified address. **Trap** refers to sending an SNMP trap.

A change in the DCD (Data Carrier Detect) signal indicates that the modem connection status has changed. If the DCD signal changes to low, it indicates that the connection line is down. A change in the DSR (Data Set Ready) signal indicates that the data communication equipment is powered off. If the DSR signal changes to low, it indicates that the data communication equipment is powered down.

ATTENTION

SNMP indicates a change in DCD or DSR signals but does not differentiate between the two. A change in either signal from “–” to “+” is indicated by “link up” and a change in either signal from “+” to “–” is indicated by “link down.”

System Management> Auto Warning Settings> E-mail Alert



E-mail Alert

Mail Server Settings

Mail server (SMTP)

□ My server requires authentication

User name

Password

From e-mail address

To e-mail address 1

To e-mail address 2

To e-mail address 3

To e-mail address 4

The **E-mail Alert** page is located under **Auto Warning Settings** in the **System Management** folder. This is where you specify how and where e-mail is sent for automatic notification of system and serial port events.

ATTENTION

Consult your network administrator or ISP for the mail server settings to use for your network. If these settings are not configured correctly, e-mail notification may not work properly.

Mail Server

Default	
Options	free text (e.g., "192.168.3.3")
Description	This field specifies the IP address of the mail server that will be used when sending automatic warning e-mails. If the mail server requires authentication, select "My server requires authentication" and enter the username and password.

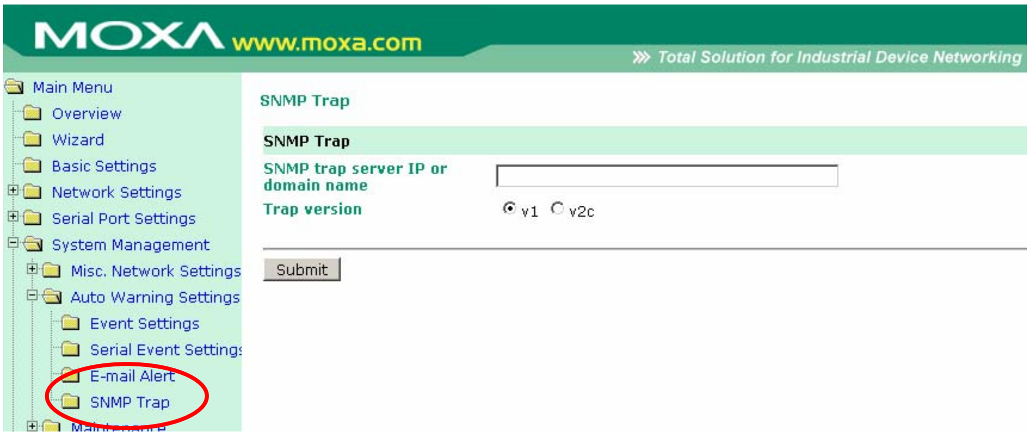
From E-mail Address

Default	
Options	free text (e.g., "jsmith@xyz.com")
Description	This field specifies the e-mail address that will be listed in the e-mail's "From" field.

To E-mail Address 1 to 4

Default	
Options	free text (e.g., "admin@abc.com")
Description	These fields specify the destination e-mail address(es) for the automatic e-mail warnings.

System Management> Auto Warning Settings> SNMP Trap



SNMP Trap

SNMP Trap

SNMP trap server IP or domain name

Trap version ● v1 ○ v2c

The **SNMP Trap** page is located under **Auto Warning Settings** in the **System Management** folder. This is where you specify the SNMP trap settings to use for automatic notification of system and serial port events.

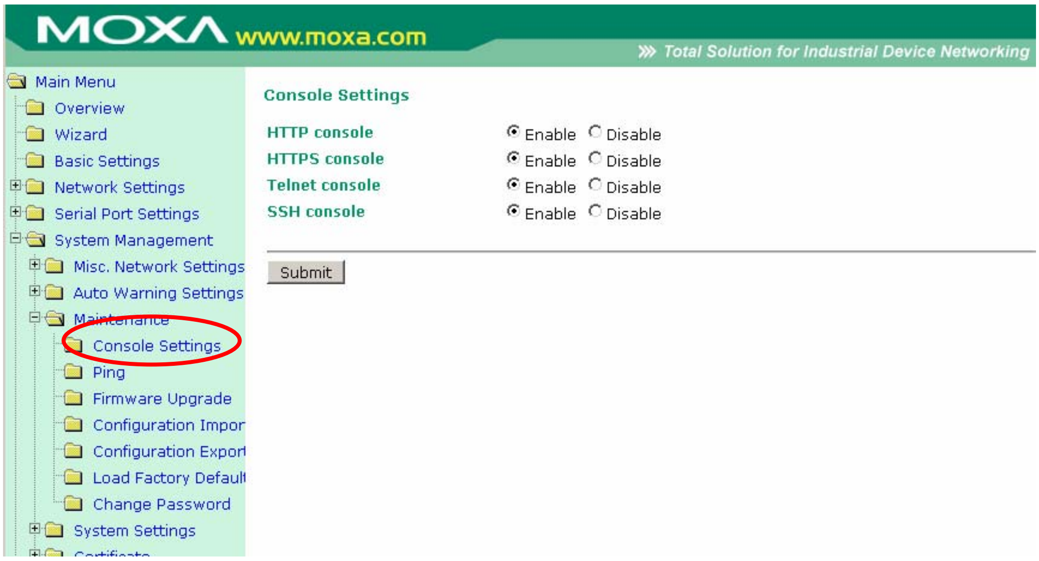
SNMP Trap Server IP or Domain Name

Default	
Options	IP address (e.g., "192.168.5.5") or domain name (e.g., "Trapserver 1")
Description	This field specifies the IP address or domain name of the SNMP trap server that will receive SNMP traps.

Trap Version

Default	v1
Options	v1, v2c
Description	This field specifies the SNMP trap version to use.

System Management> Maintenance> Console Settings



Console Settings

HTTP console	● Enable ○ Disable
HTTPS console	● Enable ○ Disable
Telnet console	● Enable ○ Disable
SSH console	● Enable ○ Disable

The **Console Settings** page is located under **Maintenance** in the **System Management** folder. This is where you enable or disable access to the various module configuration consoles. You may modify **HTTP console**, **HTTPS console**, **Telnet console**, and **SSH console**.

HTTP Console

Default	Enable
Options	Enable, Disable
Description	This field enables or disables access to the HTTP (web) console.

HTTPS Console

Default	Enable
Options	Enable, Disable
Description	This field enables or disables access to the HTTPS (web) console.

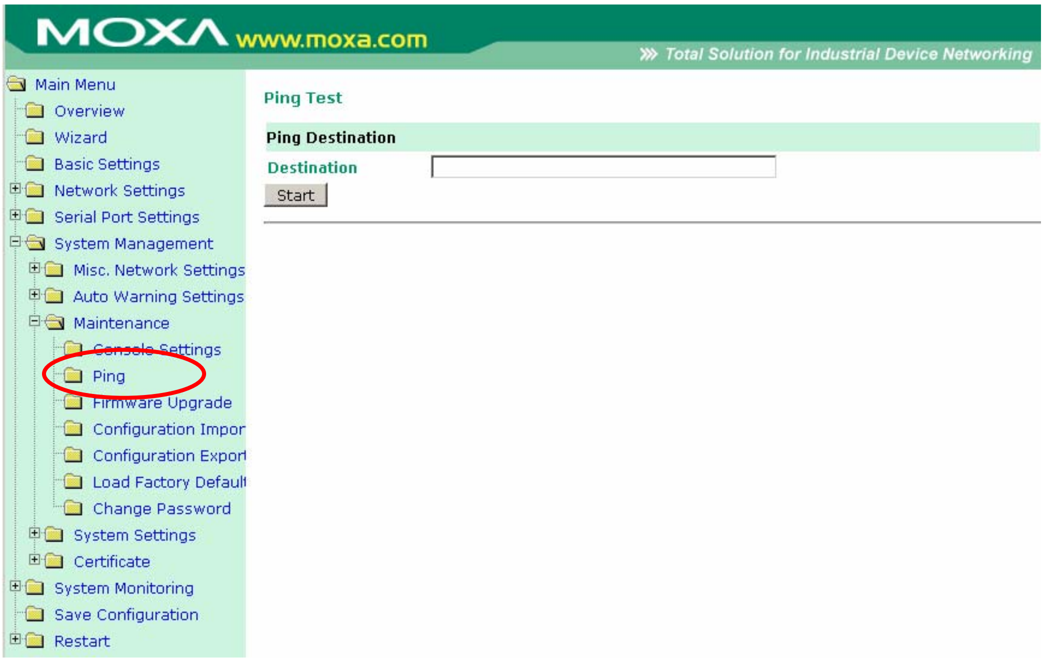
Telnet Console

Default	Enable
Options	Enable, Disable
Description	This field enables or disables access to the Telnet console.

SSH Console

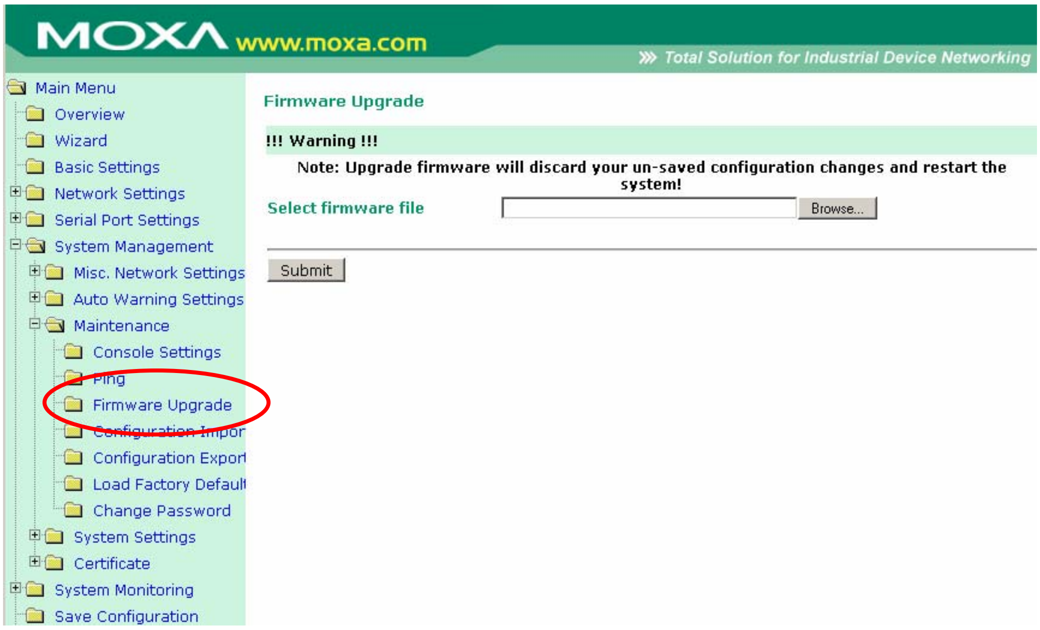
Default	Enable
Options	Enable, Disable
Description	This field enables or disables access to the SSH console.

System Management> Maintenance> Ping



The **Ping** page is located under **Maintenance** in the **System Management** folder. It provides a convenient way to test an Ethernet connection or verify an IP address. Enter the IP address or domain name in the **Destination** field and click **Start**. The results will be displayed immediately.

System Management> Maintenance> Firmware Upgrade



Firmware Upgrade

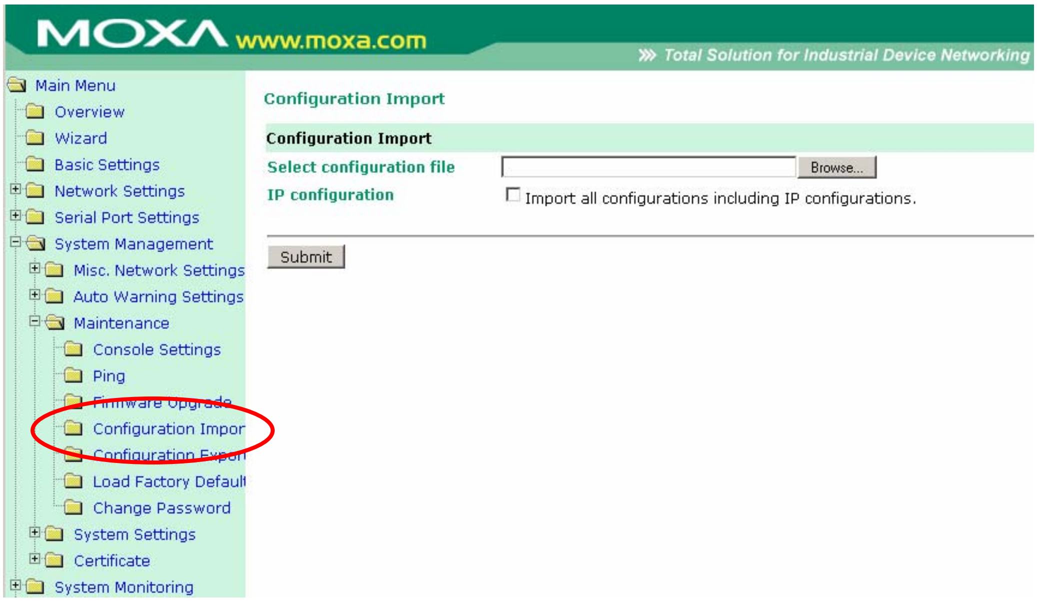
!!! Warning !!!

Note: Upgrade firmware will discard your un-saved configuration changes and restart the system!

Select firmware file

The **Firmware Upgrade** page is located under **Maintenance** in the **System Management** folder. This is where you can update the WE-2100T's firmware. After obtaining the latest firmware from www.moxa.com, select or browse for the firmware file in the **Select firmware file** field. Before clicking **Submit**, it is a good idea to save the configuration using the **Configuration Export** page, since the firmware upgrade process may cause all settings to revert to factory defaults.

System Management> Maintenance> Configuration Import



Configuration Import

Configuration Import

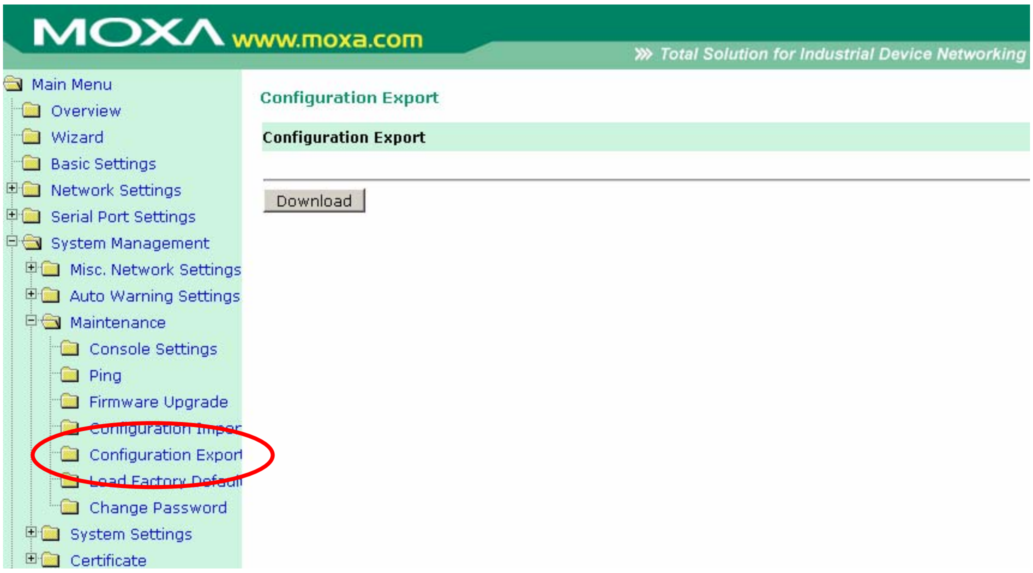
Select configuration file [ ] Browse...

IP configuration □ Import all configurations including IP configurations.

Submit

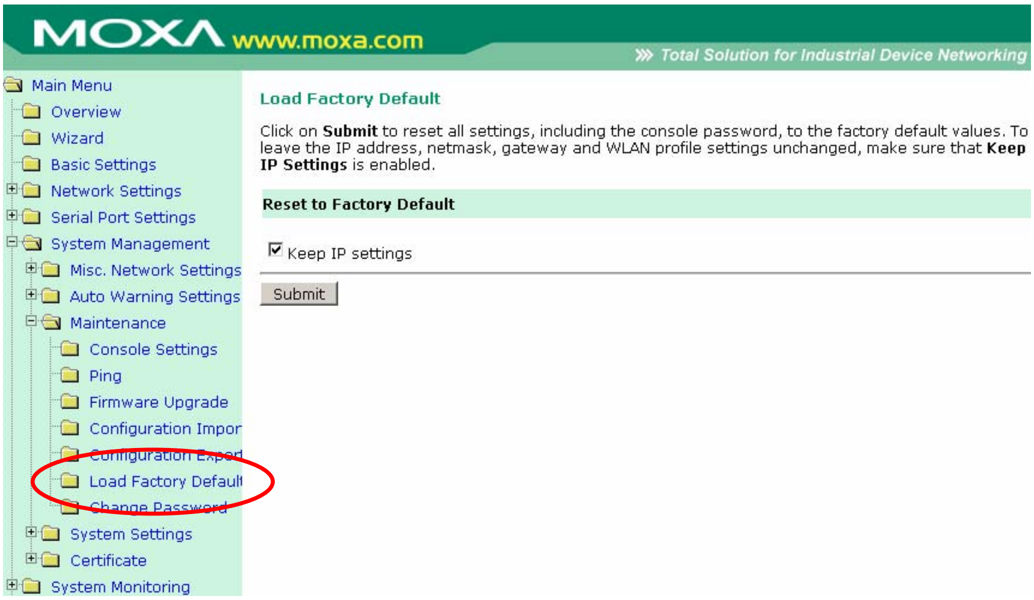
The **Configuration Import** page is located under **Maintenance** in the **System Management** folder. This is where you can load a previously saved or exported configuration. Select or browse for the configuration file in the **Select configuration file** field. If you also wish to import the IP configuration (i.e., IP address, netmask, and gateway), make sure that **Import all configurations including IP configurations** is checked.

System Management> Maintenance> Configuration Export



The **Configuration Export** page is located under **Maintenance** in the **System Management** folder. This is where you can save the module's current configuration to a file on the local host. Click **Download** to begin the process. A window should appear asking you to open or save the configuration text file.

System Management> Maintenance> Load Factory Default



Load Factory Default

Click on **Submit** to reset all settings, including the console password, to the factory default values. To leave the IP address, netmask, gateway and WLAN profile settings unchanged, make sure that **Keep IP Settings** is enabled.

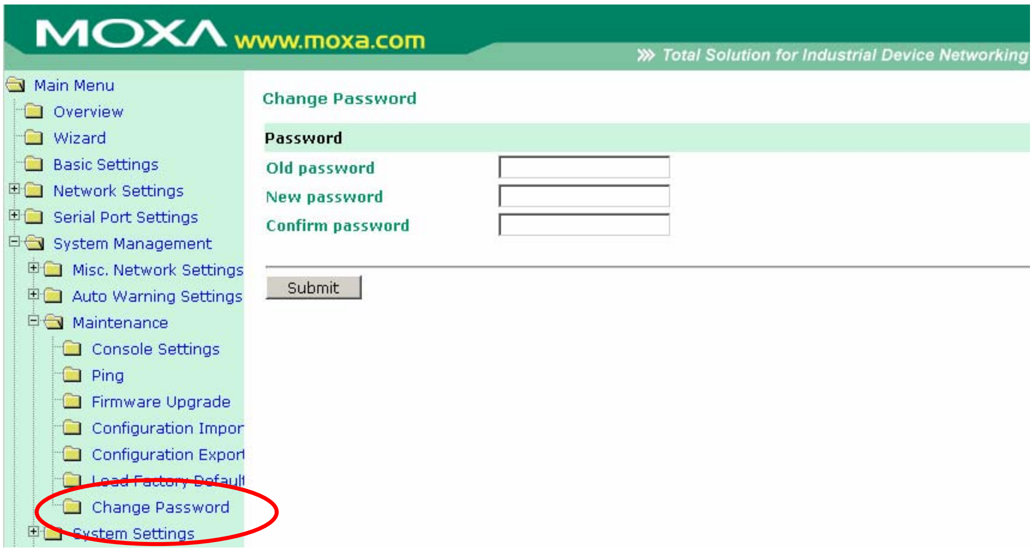
Reset to Factory Default

☑ Keep IP settings

Submit

The **Load Factory Default** page is located under **Maintenance** in the **System Management** folder. Click **Submit** to reset all settings to the factory defaults. You can preserve the module's existing IP settings (i.e., IP address, netmask, gateway, WLAN profile, and all certificates) by making sure **Keep IP settings** is checked before clicking **Submit**.

System Management> Maintenance> Change Password



Change Password

Password	
Old password	
New password	
Confirm password	

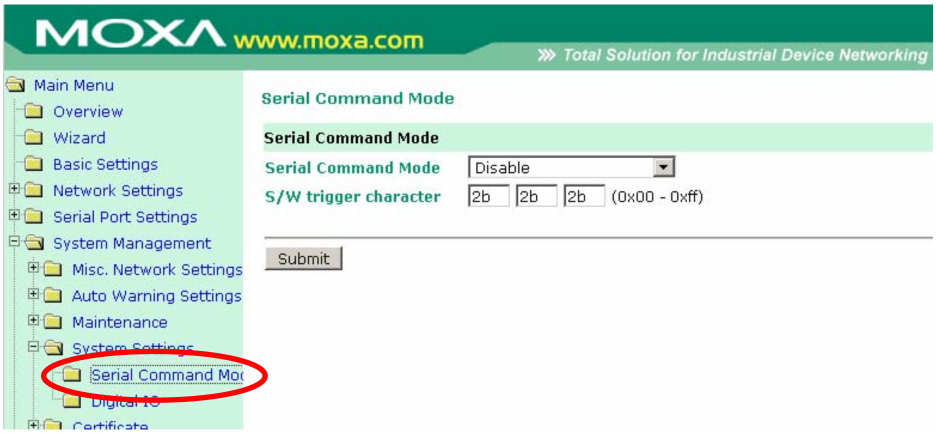
The **Change Password** page is located under **Maintenance** in the **System Management** folder. To change the password, first enter the old password in the **Old password** field. Leave this blank if the module is not currently password-protected. Enter the new password twice, once in the **New password** field and once in the **Confirm password** field. Leave these fields blank to remove password protection.

ATTENTION

If you forget the password, the ONLY way to configure the module is by loading the factory defaults with the reset button on the evaluation board. All settings will be lost.

Before setting the password, you may want to first export the configuration to a file. Your configuration can then be easily imported back into the module if necessary.

System Management> System Settings> Serial Command Mode



Serial Command Mode

Serial Command Mode

Serial Command Mode: Disable

S/W trigger character: 2b 2b 2b (0x00 - 0xff)

The **Serial Command Mode** page is located under **System Settings** in the **System Management** folder. This is where you specify how Serial Command Mode will be enabled. For details on Serial Command Mode, please refer to Chapter 13.

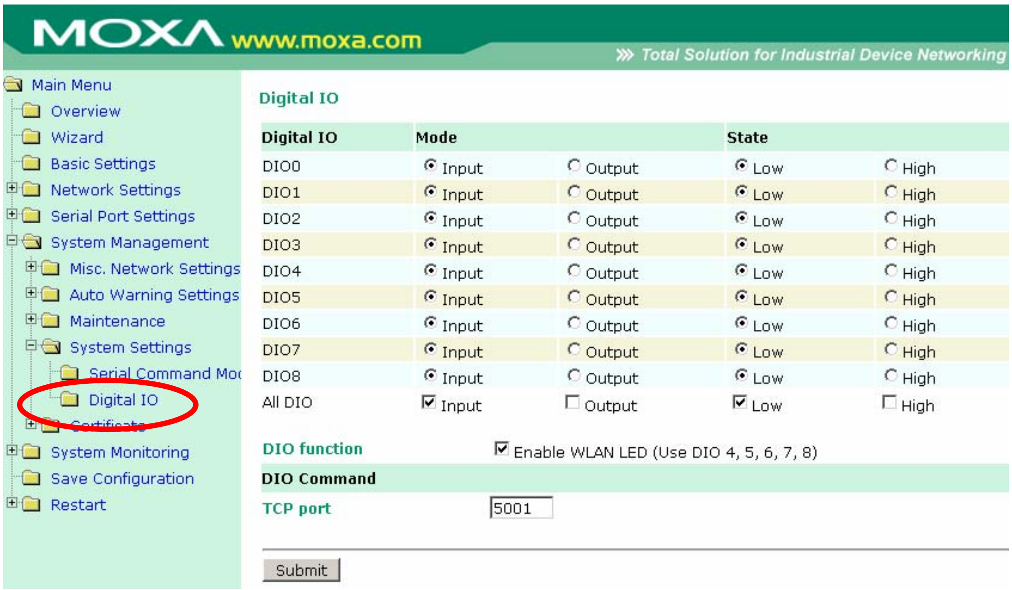
Serial Command Mode

Default	Disable
Options	Disable, H/W control pin (DIO0), Activate by characters
Description	This field specifies how to enter Serial Command Mode on the module. Disable: Serial Command Mode will be disabled on the module. H/W control pin (DIO0): Serial Command Mode will be activated according to the signal received on DIO channel 0. This is used to set up a hardware trigger through a switch connected to DIO 0. When the signal from DIO0 is low for at least 200 ms, the WE-2100T will enter Serial Command Mode. Make sure that DIO 0 is set to "DI" mode and an input device is properly connected. Activate by characters: Serial Command Mode will be entered when three trigger characters are received in rapid sequence (within 20 ms of each other). The trigger characters are specified by **S/W trigger character**.

S/W Trigger Character

Default	2b 2b 2b
Options	00 to ff (hex)
Description	This field specifies the three characters that will activate Serial Command Mode if received in rapid sequence (within 20 ms of each other). **Serial Command Mode** must be set to "Activate by characters".

System Management> System Settings> Digital IO



Digital IO

Digital IO	Mode		State	
DIO0	● Input	○ Output	● Low	○ High
DIO1	● Input	○ Output	● Low	○ High
DIO2	● Input	○ Output	● Low	○ High
DIO3	● Input	○ Output	● Low	○ High
DIO4	● Input	○ Output	● Low	○ High
DIO5	● Input	○ Output	● Low	○ High
DIO6	● Input	○ Output	● Low	○ High
DIO7	● Input	○ Output	● Low	○ High
DIO8	● Input	○ Output	● Low	○ High
All DIO	☑ Input	□ Output	☑ Low	□ High

DIO function ☑ Enable WLAN LED (Use DIO 4, 5, 6, 7, 8)

DIO Command

TCP port 5001

The **Digital IO** page is located under **System Settings** in the **System Management** folder. This is where you configure the 9 built-in DIO channels.

DIO0 through DIO8

Default	Input (Mode), Low (State)
Options	Input, Output (for Mode) Low, High (for State)
Description	This field specifies the mode and state of the DIO channel. In "Input" mode, the DIO channel will operate as a digital input (DI) channel, and the State setting will be disregarded. The channel state will be controlled by the digital input device that is connected to the channel, such as a switch or a button. In "Output" mode, the DIO channel will operate as a digital output (DO) channel. The State setting will control the channel's state, allowing on/off control of a connected device such as an LED or alarm.

All DIO

Default	Input (Mode), Low (State)
Options	Input, Output (for Mode) Low, High (for State)
Description	This field specifies the mode and state of all DIO channels, if desired. Any setting that is selected will be applied to all DIO channels at once.

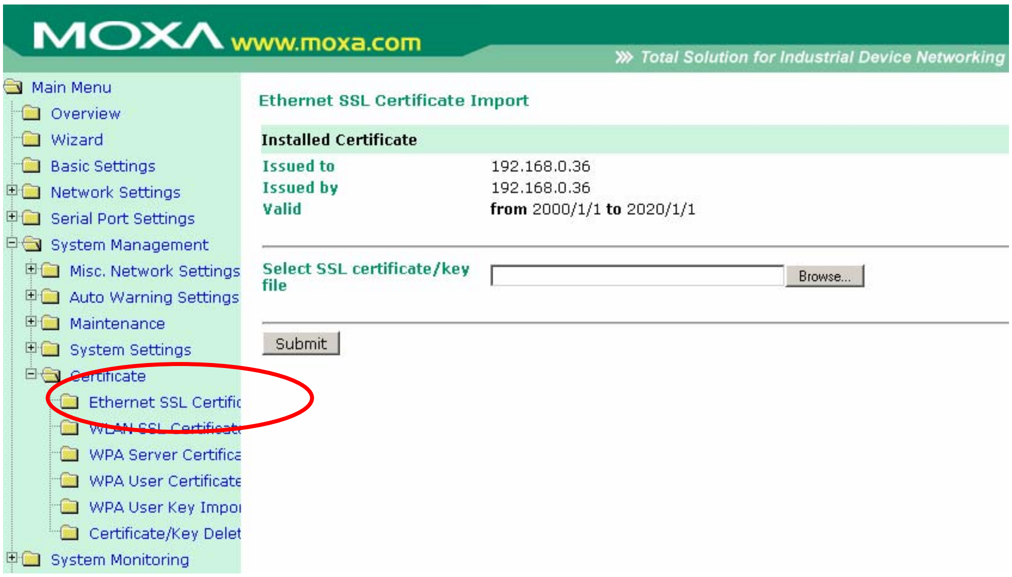
DIO Function

Default	Enable WLAN LED
Options	Enable/Disable WLAN LED
Description	This specifies whether the WLAN LEDs will be used. If enabled, DIO 4 through 8 will be reserved for use as WLAN LEDs. Manual settings for those DIO channels will thus be ignored.

TCP Port

Default	5001
Options	0 to 9999
Description	This specifies the TCP port number that will be reserved for DIO commands. DIO commands may be used to control and obtain data from the module's DIO channels. Please refer to Appendix C for additional information on DIO commands.

System Management> Certificate> Ethernet SSL Certificate Import



Ethernet SSL Certificate Import

Installed Certificate

Issued to 192.168.0.36

Issued by 192.168.0.36

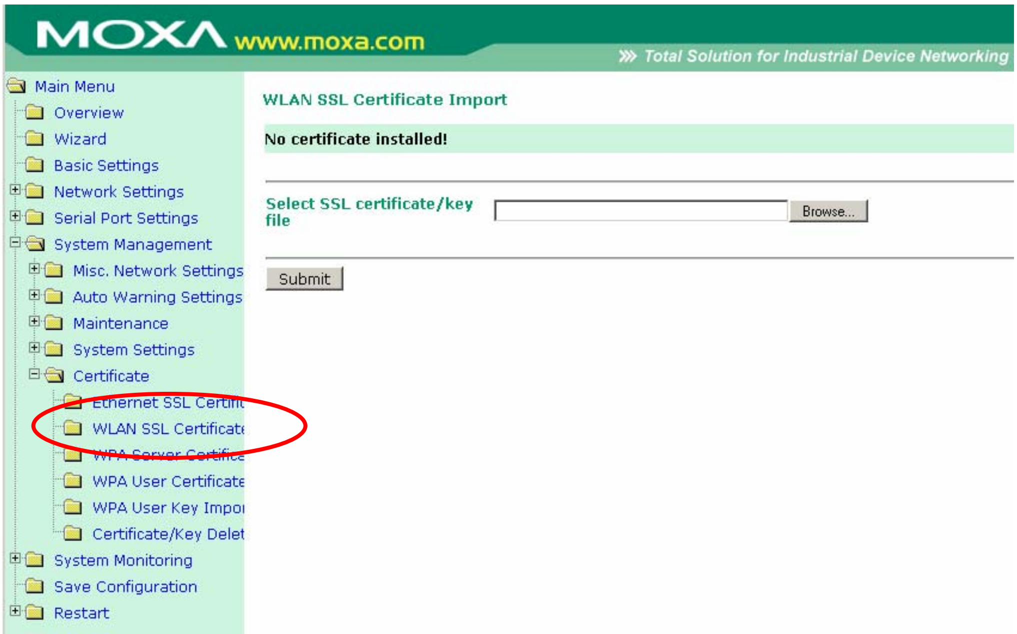
Valid **from** 2000/1/1 **to** 2020/1/1

Select SSL certificate/key file [ ] Browse...

Submit

The **Ethernet SSL Certificate Import** page is located under **Certificate** in the **System Management** folder. This is where you can load the Ethernet SSL certificate. Select or browse for the certificate file in the **Select SSL certificate/key file** field.

System Management> Certificate> WLAN SSL Certificate Import



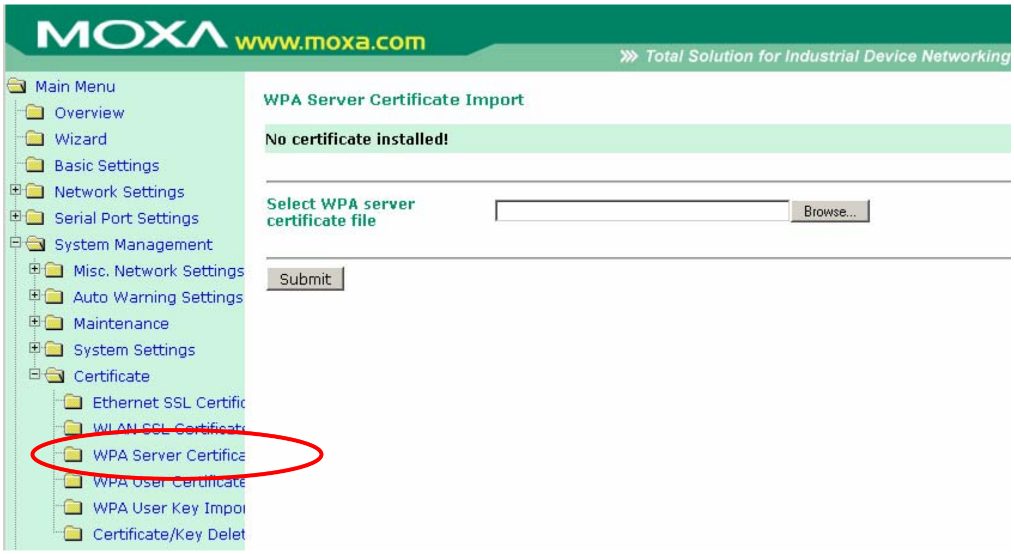
WLAN SSL Certificate Import

No certificate installed!

Select SSL certificate/key file

The **WLAN SSL Certificate Import** page is located under **Certificate** in the **System Management** folder. By default, the WLAN SSL certificate is automatically generated by the WE-2100T based on the IP address of the wireless interface. You can also import a certificate. Select or browse for the certificate file in the **Select SSL certificate/key file** field.

System Management> Certificate> WPA Server Certificate Import



WPA Server Certificate Import

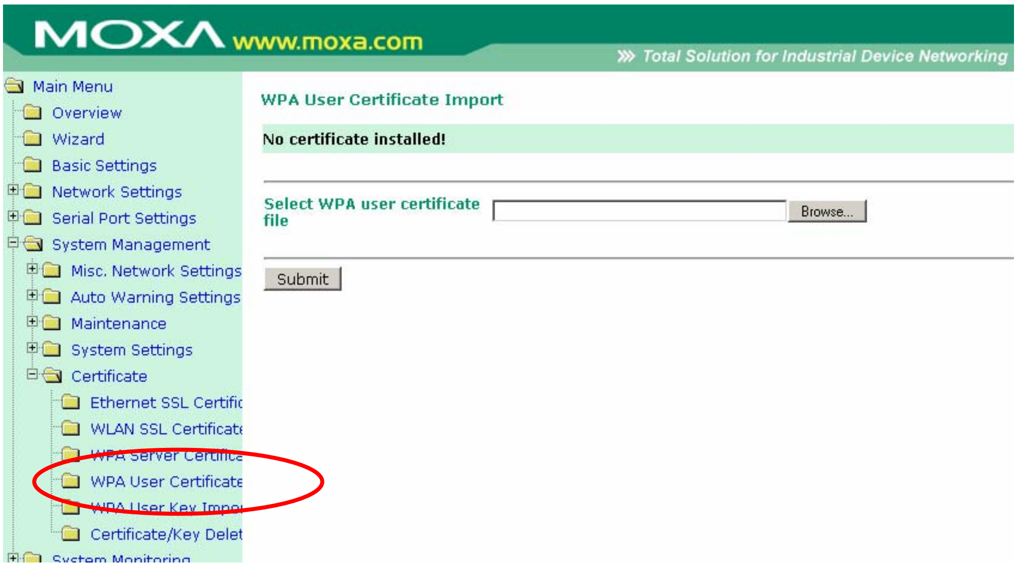
No certificate installed!

Select WPA server certificate file

The **WPA Server Certificate Import** page is located under **Certificate** in the **System Management** folder. This is where you can load the WPA server certificate. Select or browse for the certificate file in the **Select WPA server certificate file** field.

You must install the trusted server certificate from the RADIUS server in order to enable **Verify server certificate** in the WLAN **Security** settings. This certificate will then be used by the WE-2100T to authenticate the RADIUS server.

System Management> Certificate> WPA User Certificate Import



WPA User Certificate Import

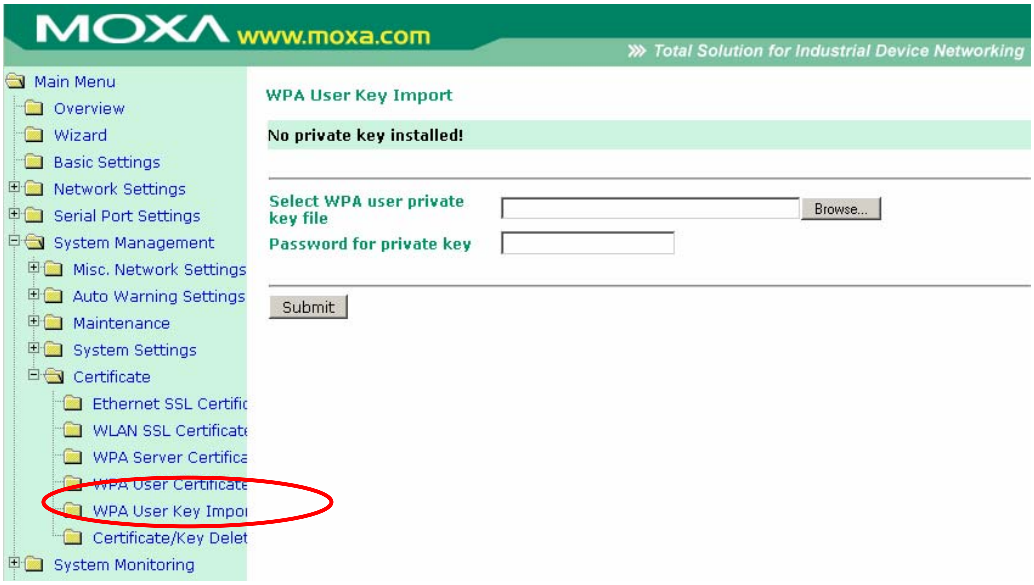
No certificate installed!

Select WPA user certificate file

The **WPA User Certificate Import** page is located under **Certificate** in the **System Management** folder. This is where you can load the WPA user certificate. Select or browse for the certificate file in the **Select WPA user certificate file** field.

The user certificate of the WE-2100T must be installed in the RADIUS server when the WE-2100T uses WPA (WPA2)/TLS. The trusted server certificate of the RADIUS server must also be installed in the WE-2100T.

System Management> Certificate> WPA User Key Import



WPA User Key Import

No private key installed!

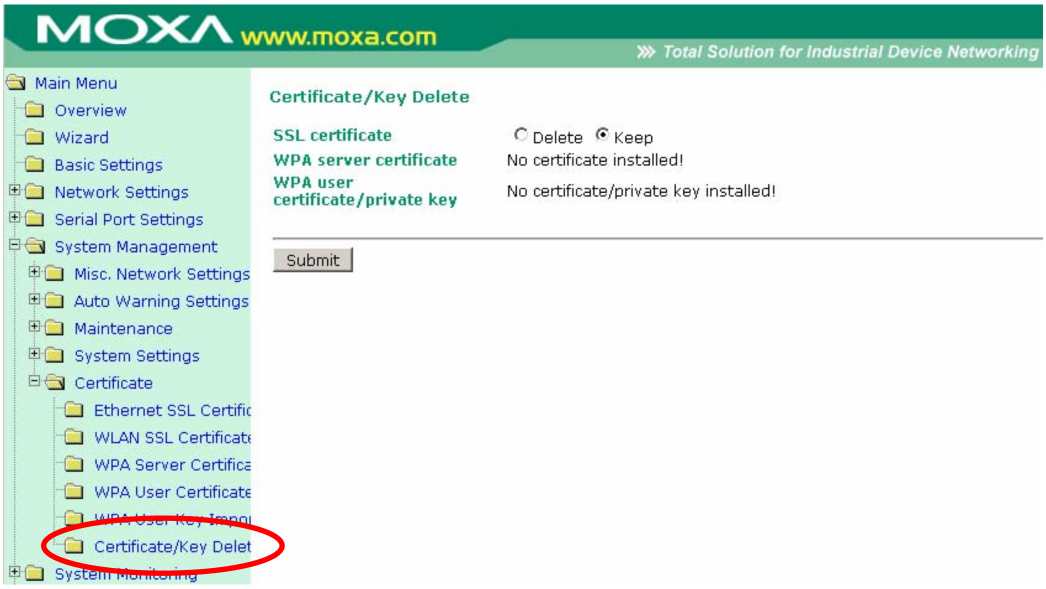
Select WPA user private key file

Password for private key

The **WPA User Key Import** page is located under **Certificate** in the **System Management** folder. This is where you can load the WPA user key. Select or browse for the user private key file in the **Select WPA user privacy key file** field and enter the **Password for the private key**.

The user private key of the WE-2100T must be installed in the RADIUS server when the WE-2100T uses WPA(WPA2)//TLS. The trusted server certificate of RADIUS server must also be installed on the WE-2100T.

System Management> Certificate> Certificate/Key Delete



Certificate/Key Delete

SSL certificate	○ Delete ● Keep
WPA server certificate	No certificate installed!
WPA user certificate/private key	No certificate/private key installed!

The **Certificate/Key Delete** page is located under **Certificate** in the **System Management** folder. This page is where you can delete certificates or WPA keys that have been installed on the

WE-2100T. When you click **Submit**, any certificate or key that has been set to "Delete" will be deleted from the module.

10

Web Console: System Monitoring

The web console is the most user-friendly method available to configure the module. With a standard web browser, you have easy and intuitive access to all settings and options. In this chapter, we introduce the web console and go through the basic configuration options. The same configuration options are also available through the Telnet and serial console.

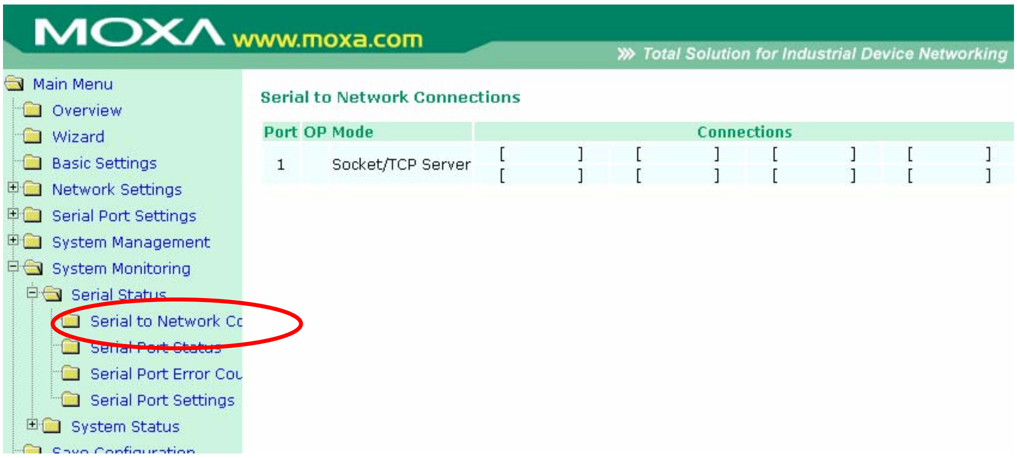
This chapter covers the following topics:

- ❑ **Overview**
- ❑ **System Monitoring> Serial Status> Serial to Network Connections**
- ❑ **System Monitoring> Serial Status> Serial Port Status**
- ❑ **System Monitoring> Serial Status> Serial Port Error Count**
- ❑ **System Monitoring> Serial Status> Serial Port Settings**
- ❑ **System Monitoring> System Status> Network Connections**
- ❑ **System Monitoring> System Status> Network Statistics**
- ❑ **System Monitoring> System Status> WLAN Status**
- ❑ **System Monitoring> System Status> WLAN Site Survey**
- ❑ **System Monitoring> System Status> Digital IO State**

Overview

This chapter explains how to use the **System Monitoring** functions on the web console. These functions allow you to monitor many different aspects of operation.

System Monitoring> Serial Status> Serial to Network Connections

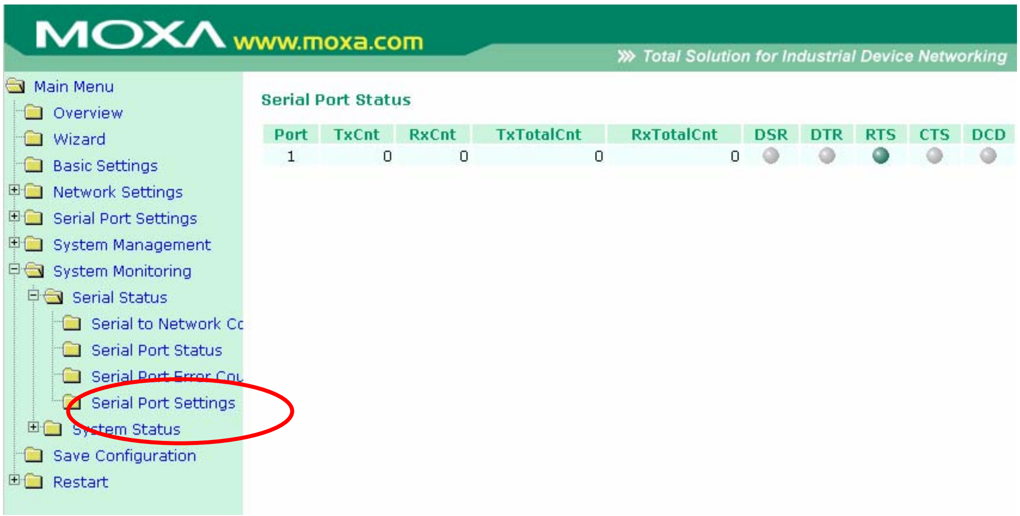


Serial to Network Connections

Port	OP Mode	Connections			
1	Socket/TCP Server	[ ] [ ]	[ ] [ ]	[ ] [ ]	[ ] [ ]

The **Serial to Network Connections** page is located under **Serial Status** in the **System Monitoring** folder. On this page, you can monitor the serial port's operation mode and host connection status.

System Monitoring> Serial Status> Serial Port Status



Serial Port Status

Port	TxCnt	RxCnt	TxTotalCnt	RxTotalCnt	DSR	DTR	RTS	CTS	DCD
1	0	0	0	0	○	○	●	○	○

The **Serial Port Status** page is located under **Serial Status** in the **System Monitoring** folder. On this page, you can monitor the serial signal and data transmission status.

TxCnt: number of Tx packets (to device) for the current connection

RxCnt: number of Rx packets (from device) for the current connection

TxTotalCnt: number of Tx packets since the module was powered on

RxTotalCnt: number of Rx packets since the module was powered on

DSR: status of DSR signal

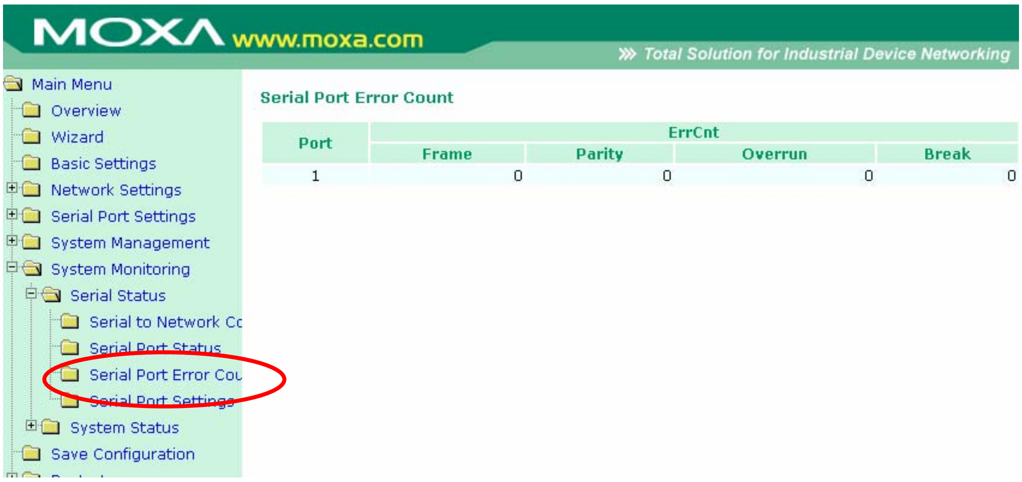
DTR: status of DTR signal

RTS: status of RTS signal

CTS: status of CTS signal

DCD: status of DCD signal

System Monitoring> Serial Status> Serial Port Error Count

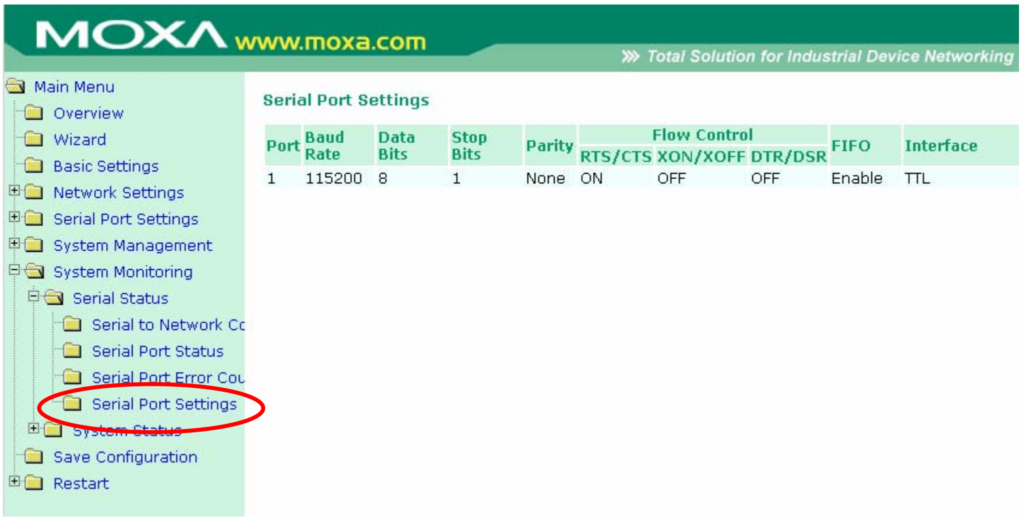


Serial Port Error Count

Port	ErrCnt			
	Frame	Parity	Overrun	Break
1	0	0	0	0

The **Serial Port Error Count** page is located under **Serial Status** in the **System Monitoring** folder. On this page, you can view the current number of frame, parity, overrun and break errors.

System Monitoring> Serial Status> Serial Port Settings

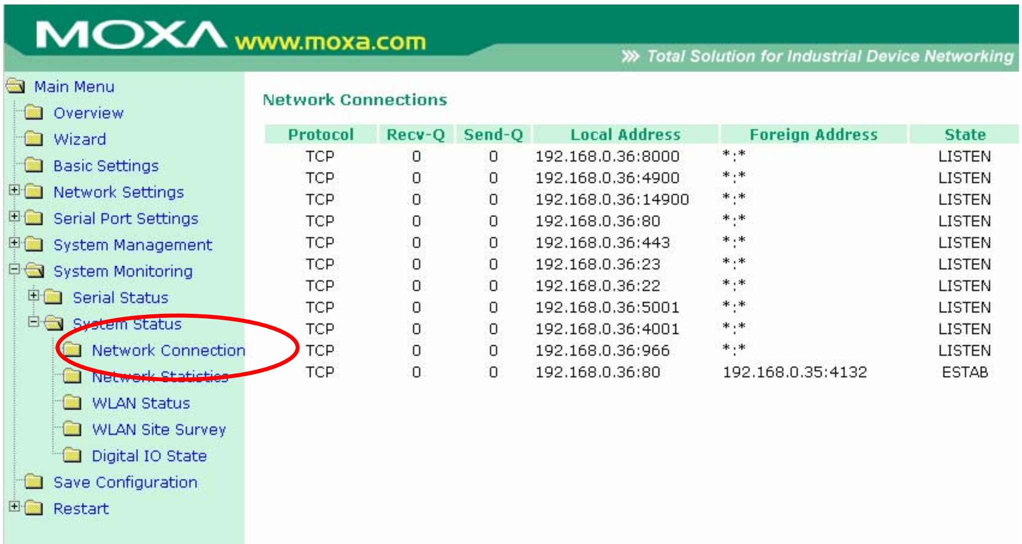


Serial Port Settings

Port	Baud Rate	Data Bits	Stop Bits	Parity	Flow Control			FIFO	Interface
					RTS/CTS	XON/XOFF	DTR/DSR		
1	115200	8	1	None	ON	OFF	OFF	Enable	TTL

The **Serial Port Settings** page is located under **Serial Status** in the **System Monitoring** folder. On this page, you can view the current serial communication settings.

System Monitoring> System Status> Network Connections

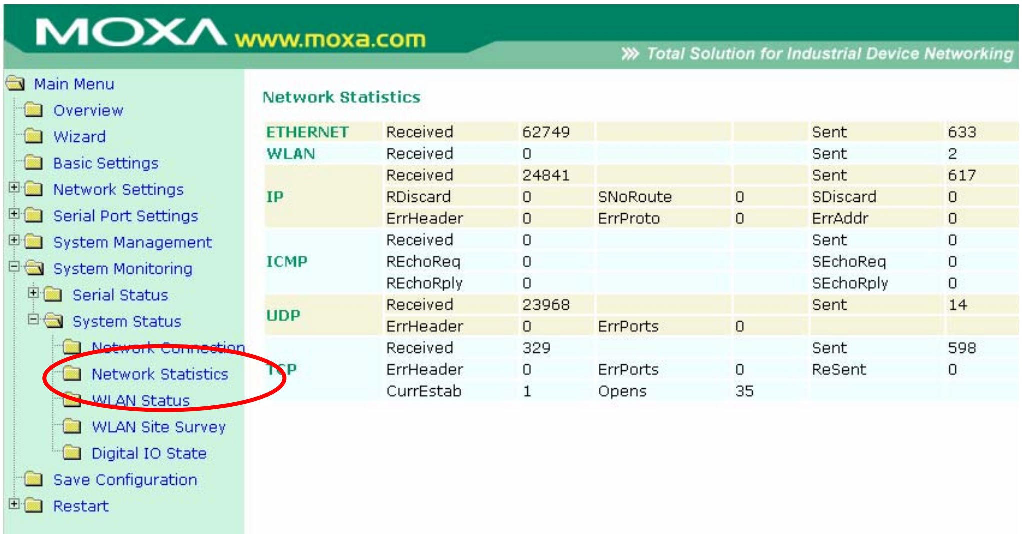


Network Connections

Protocol	Recv-Q	Send-Q	Local Address	Foreign Address	State
TCP	0	0	192.168.0.36:8000	*:*	LISTEN
TCP	0	0	192.168.0.36:4900	*:*	LISTEN
TCP	0	0	192.168.0.36:14900	*:*	LISTEN
TCP	0	0	192.168.0.36:80	*:*	LISTEN
TCP	0	0	192.168.0.36:443	*:*	LISTEN
TCP	0	0	192.168.0.36:23	*:*	LISTEN
TCP	0	0	192.168.0.36:22	*:*	LISTEN
TCP	0	0	192.168.0.36:5001	*:*	LISTEN
TCP	0	0	192.168.0.36:4001	*:*	LISTEN
TCP	0	0	192.168.0.36:966	*:*	LISTEN
TCP	0	0	192.168.0.36:80	192.168.0.35:4132	ESTAB

The **Network Connections** page is located under **System Status** in the **System Monitoring** folder. On this page, you can view the current status of any network connection to the WE-2100T.

System Monitoring> System Status> Network Statistics

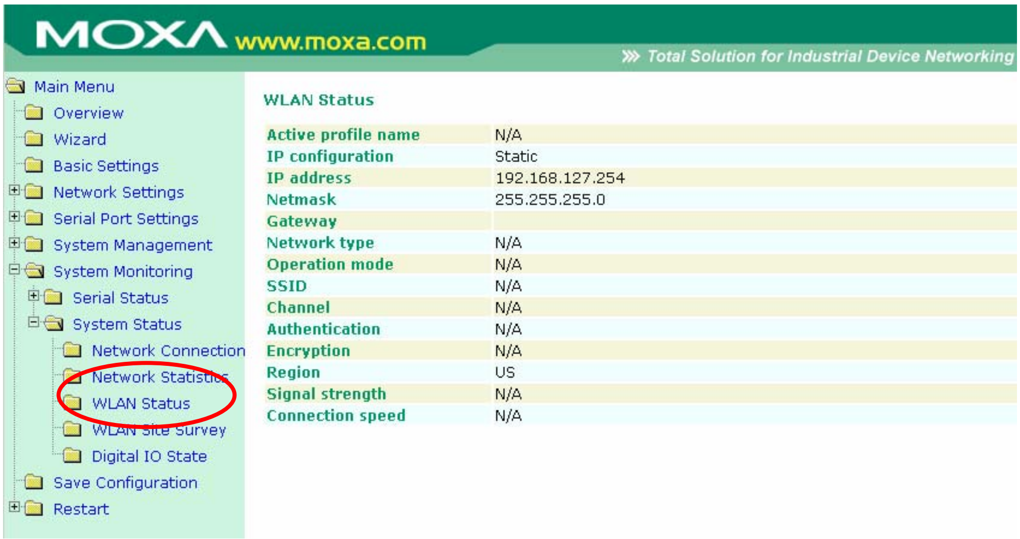


Network Statistics

ETHERNET	Received	62749			Sent	633
WLAN	Received	0			Sent	2
IP	Received	24841			Sent	617
	RDiscard	0	SNoRoute	0	SDiscard	0
	ErrHeader	0	ErrProto	0	ErrAddr	0
ICMP	Received	0			Sent	0
	REchoReq	0			SEchoReq	0
	REchoRply	0			SEchoRply	0
UDP	Received	23968			Sent	14
	ErrHeader	0	ErrPorts	0		
TCP	Received	329			Sent	598
	ErrHeader	0	ErrPorts	0	ReSent	0
	CurrEstab	1	Opens	35		

The **Network Statistics** page is located under **System Status** in the **System Monitoring** folder. On this page, you can view current network transmission statistics.

System Monitoring> System Status> WLAN Status

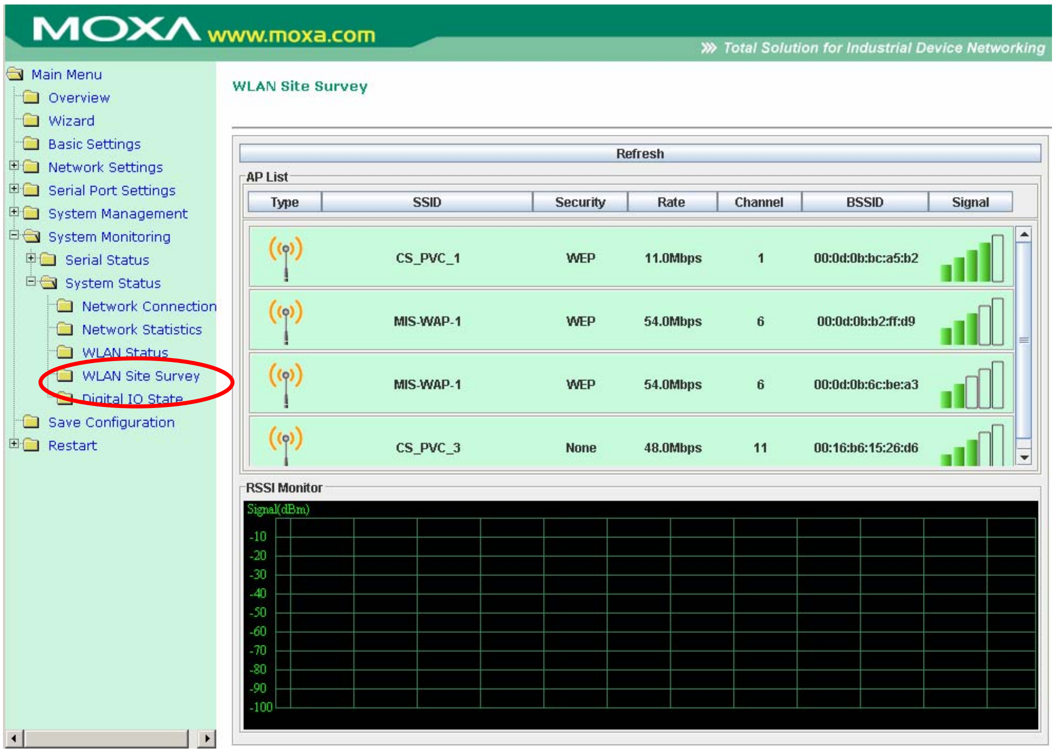


WLAN Status

Active profile name	N/A
IP configuration	Static
IP address	192.168.127.254
Netmask	255.255.255.0
Gateway	
Network type	N/A
Operation mode	N/A
SSID	N/A
Channel	N/A
Authentication	N/A
Encryption	N/A
Region	US
Signal strength	N/A
Connection speed	N/A

The **WLAN Status** page is located under **System Status** in the **System Monitoring** folder. This is where you can view the current WLAN settings and status.

System Monitoring> System Status> WLAN Site Survey



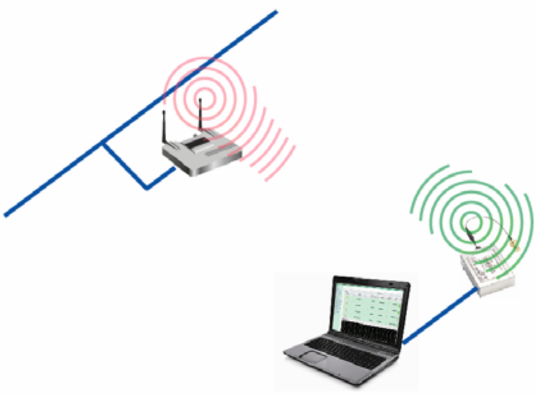
WLAN Site Survey

AP List

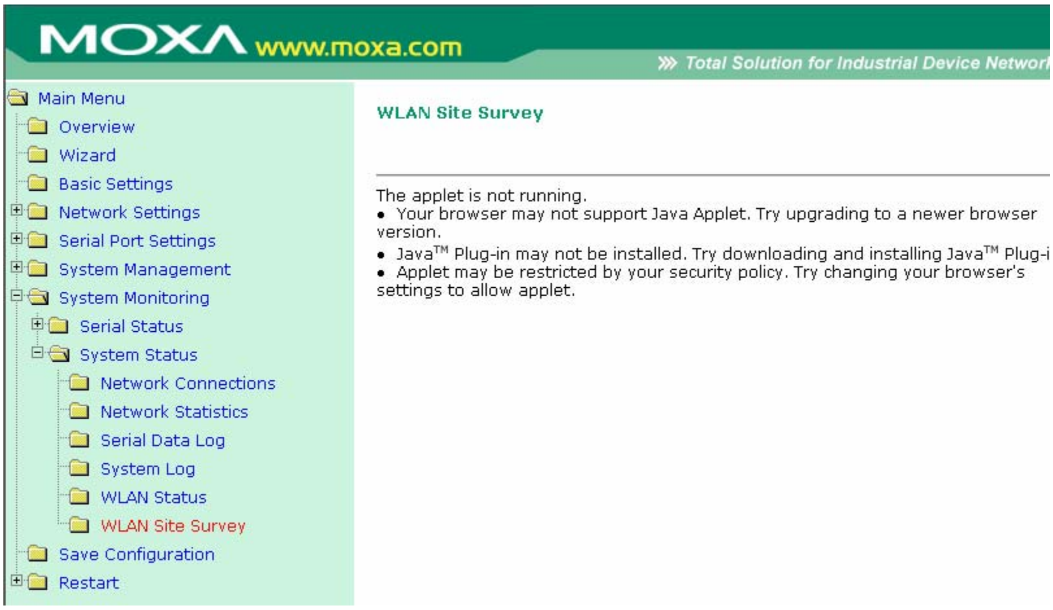
Type	SSID	Security	Rate	Channel	BSSID	Signal
	CS_PVC_1	WEP	11.0Mbps	1	00:0d:0b:bc:a5:b2	
	MIS-WAP-1	WEP	54.0Mbps	6	00:0d:0b:b2:ff:d9	
	MIS-WAP-1	WEP	54.0Mbps	6	00:0d:0b:6c:be:a3	
	CS_PVC_3	None	48.0Mbps	11	00:16:b6:15:26:d6	

The **WLAN Site Survey** page is located under **System Status** in the **System Monitoring** folder. This is where you can view live data on wireless signal strength and characteristics. It is a useful tool to help you complete a wireless site survey without installing additional software.

The goal of a WLAN site survey is to determine the number and placement of access points to provide enough coverage to the facility. For most implementations, "enough coverage" means that the data rate at all locations does not fall below a certain threshold. For most wireless sites, it is necessary to perform a WLAN site survey before access point installation in order to determine the behavior of radio waves at the site.

Typical WLAN Site Survey 	Procedure 1. Download/install site survey software. 2. Run software on laptop. 3. Measure AP signal strength using software on laptop. Weakness • Signal strength is read from the laptop NIC rather than from the module
WLAN Site Survey with WE-2100T 	Procedure 1. Open web browser 2. Measure AP signal from web console. Advantages • Signal strength is read from module • Additional software not required

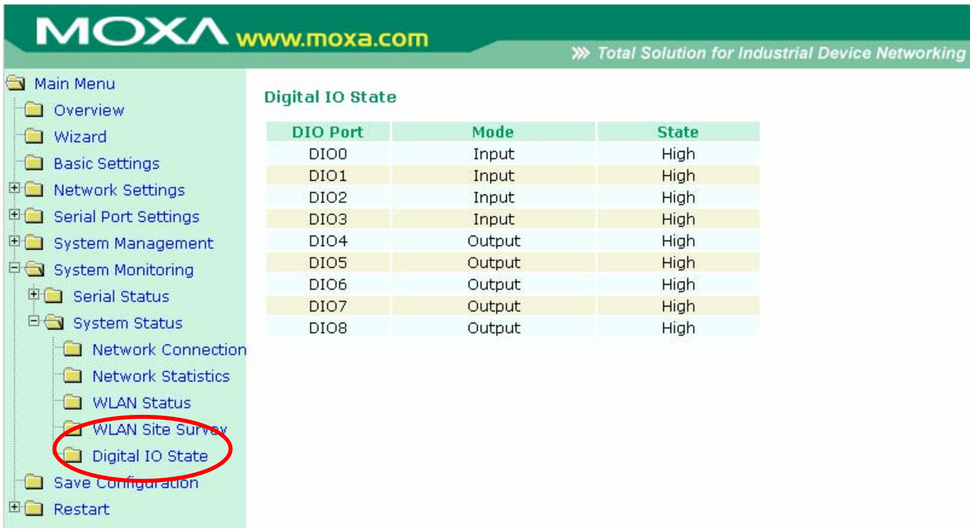
Please note that Java must be enabled in your web browser for the **WLAN Site Survey** page to display properly.



WLAN Site Survey

The applet is not running.
- Your browser may not support Java Applet. Try upgrading to a newer browser version.
- Java^{TM} Plug-in may not be installed. Try downloading and installing Java^{TM} Plug-i
- Applet may be restricted by your security policy. Try changing your browser's settings to allow applet.

System Monitoring> System Status> Digital IO State



Digital IO State

DIO Port	Mode	State
DIO0	Input	High
DIO1	Input	High
DIO2	Input	High
DIO3	Input	High
DIO4	Output	High
DIO5	Output	High
DIO6	Output	High
DIO7	Output	High
DIO8	Output	High

The **Digital IO State** page is located under **System Status** in the **System Monitoring** folder. This is where you can view the current settings and status for all DIO channels.

11

Web Console: Save and Restart

The web console is the most user-friendly method available to configure the module. With a standard web browser, you have easy and intuitive access to all settings and options. In this chapter, we introduce the web console and go through the basic configuration options. The same configuration options are also available through the Telnet and serial console.

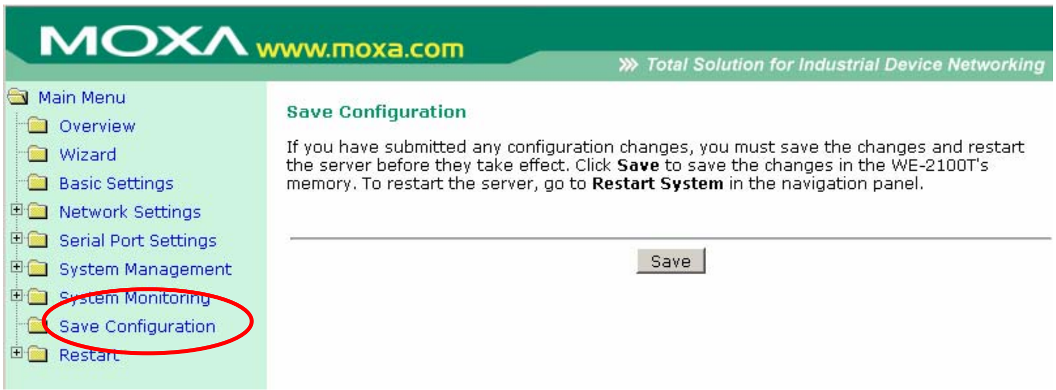
This chapter covers the following topics:

- ❑ **Overview**
- ❑ **Save Configuration**
- ❑ **Restart> Restart System**
- ❑ **Restart> Restart Ports**

Overview

This chapter explains how to use save your configuration changes and restart the WE-2100T using the web console. Configuration changes will not be effective until they are saved and the WE-2100T is rebooted.

Save Configuration

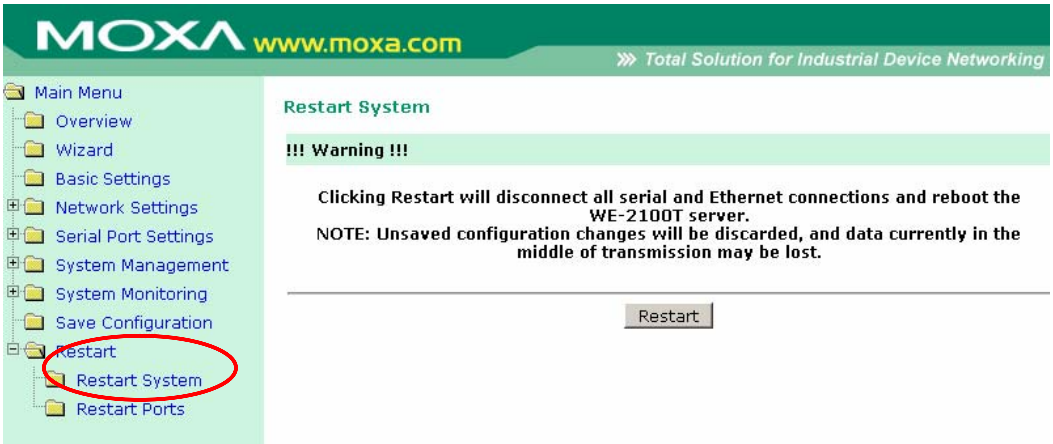


Save Configuration

If you have submitted any configuration changes, you must save the changes and restart the server before they take effect. Click **Save** to save the changes in the WE-2100T's memory. To restart the server, go to **Restart System** in the navigation panel.

Go to the **Save Configuration** page in order to save all configuration changes to the WE-2100T. The new settings will be effective when the WE-2100T is restarted. If you restart or power off the module without saving the configuration, any changes will be discarded.

Restart> Restart System



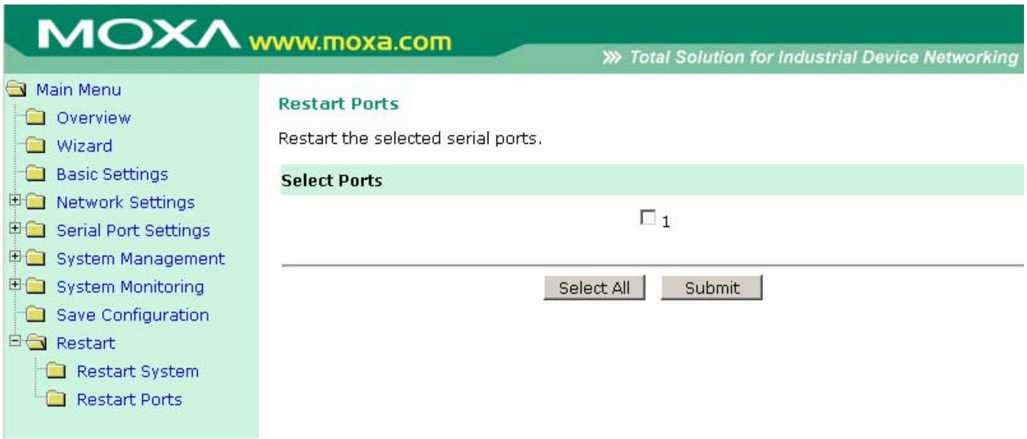
Restart System

!!! Warning !!!

Clicking Restart will disconnect all serial and Ethernet connections and reboot the WE-2100T server.
NOTE: Unsaved configuration changes will be discarded, and data currently in the middle of transmission may be lost.

The **Restart System** page is located in the **Restart** folder. Click **Restart** to restart the WE-2100T. Before restarting, be sure to save the configuration so the new settings will take effect upon restart. Configuration changes that have not been saved will be discarded when the WE-2100T is restarted.

Restart> Restart Ports



Restart Ports

Restart the selected serial ports.

Select Ports

□ 1

The **Restart Ports** page is located in the **Restart** folder. Select port 1 and click **Submit** to restart the serial port.

12

Using Network Enabler Administrator

Network Enabler Administrator is a useful Windows utility that can be used to configure your WE-2100T. In this chapter, we will discuss how to use Network Enabler Administrator.

This chapter includes the following sections:

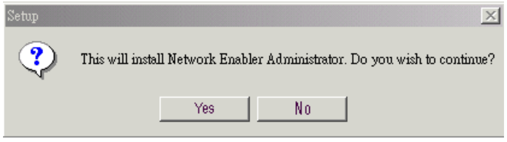
- ❑ **Overview**
  - ➢ Installation
  - ➢ Navigation
- ❑ **Configuration**
- ❑ **Monitor**
- ❑ **Port Monitor**
- ❑ **COM Mapping**
- ❑ **IP Address Report**

Overview

Network Enabler Administrator provides everything you need to remotely manage, monitor, and modify your WE-2100T—hassle free.

Installation

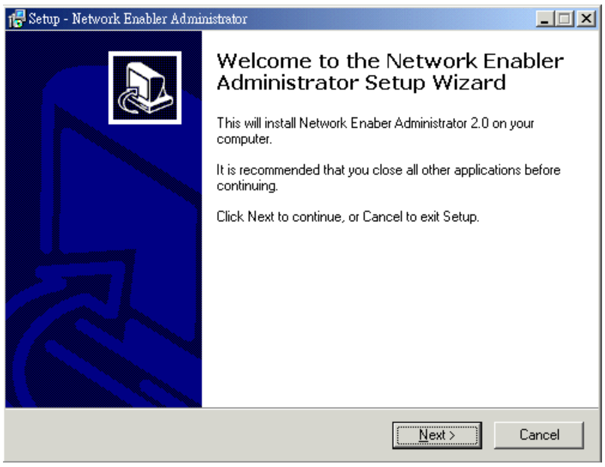
1. Open the setup program and click **Yes** to proceed.



Setup

This will install Network Enabler Administrator. Do you wish to continue?

2. A **Welcome** message will appear. Click **Next** to proceed.



Setup - Network Enabler Administrator

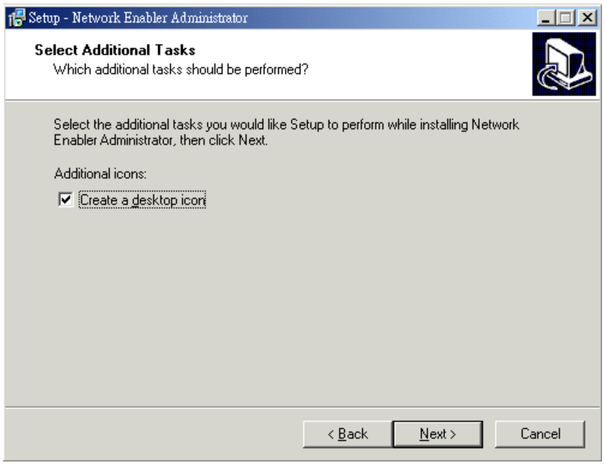
Welcome to the Network Enabler Administrator Setup Wizard

This will install Network Enaber Administrator 2.0 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

3. Select the desired additional tasks and click **Next** to proceed.



Setup - Network Enabler Administrator

Select Additional Tasks

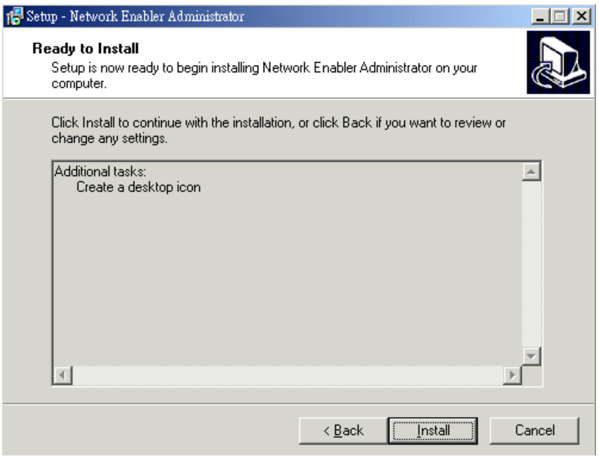
Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing Network Enabler Administrator, then click Next.

Additional icons:

☑ Create a desktop icon

4. Verify that you are ready to install and click **Install** to proceed.



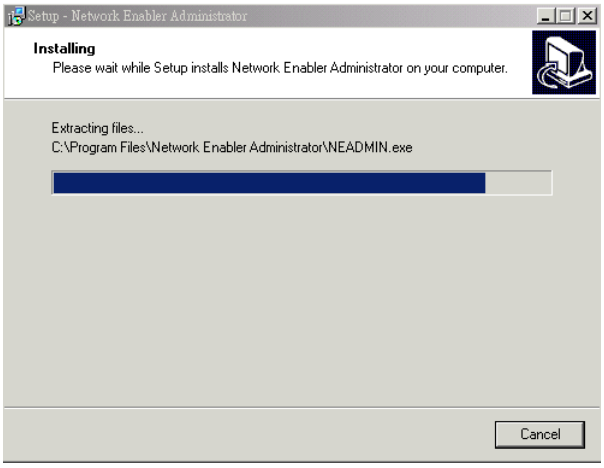
Ready to Install

Setup is now ready to begin installing Network Enabler Administrator on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

Additional tasks:
Create a desktop icon

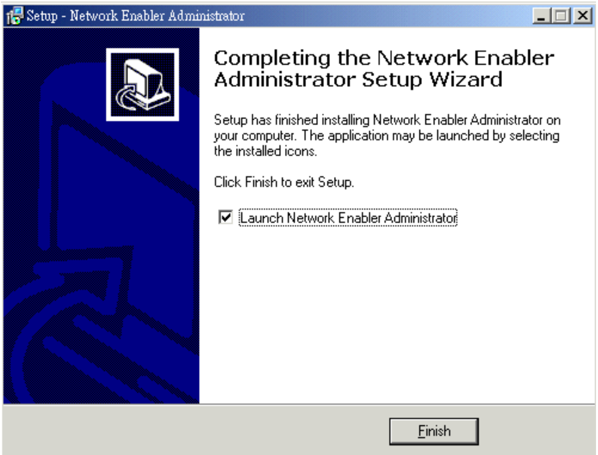
5. When the installation is complete, click **Finish** to exit the wizard.



Installing

Please wait while Setup installs Network Enabler Administrator on your computer.

Extracting files...
C:\Program Files\Network Enabler Administrator\NEADMIN.exe



Completing the Network Enabler Administrator Setup Wizard

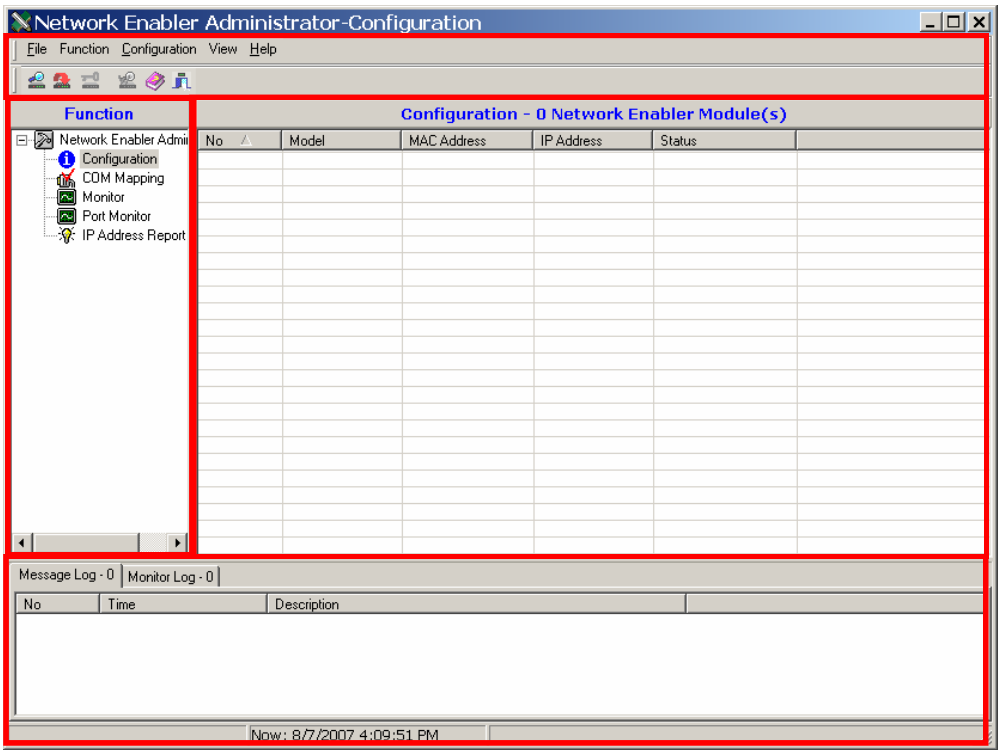
Setup has finished installing Network Enabler Administrator on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

☑ Launch Network Enabler Administrator

Navigation

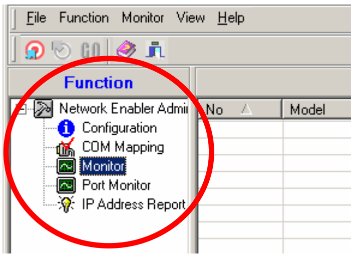
Network Enabler Administrator is designed to make it easy to configure, monitor, or manage any WE-2100T module on your network. The interface is organized into four areas as follows:

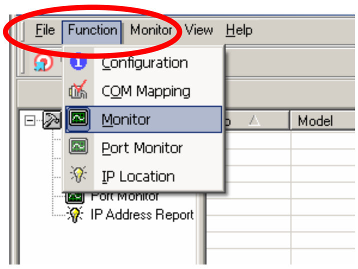


- The top section is the menu area. Functions and commands can be selected here.
- The left panel is the Function panel. Functions can be selected here.
- The right panel is the list of modules that are available for the selected function. Target modules for specific commands are selected from this list.
- The bottom section is the log area, which shows a record of status and processing messages.

Selecting a Function

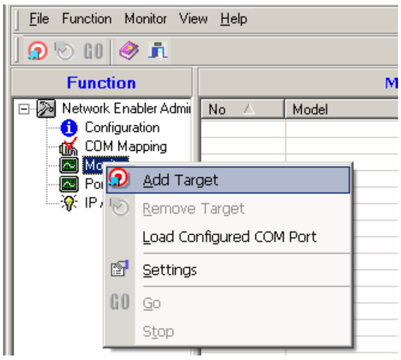
Functions, such as Monitor, are selected in the Function panel or from the Function menu. Five functions are available: Configuration, COM Mapping, Monitor, Port Monitor, and IP Address Report.

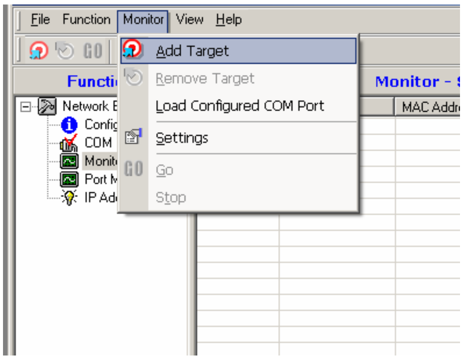




Opening the Function Context Menu

Each function has its own function context menu where specific commands are selected. A function's context menu is opened by right-clicking the function in the function panel or by right-clicking the target module in the module list. It can also be opened through the menu bar.



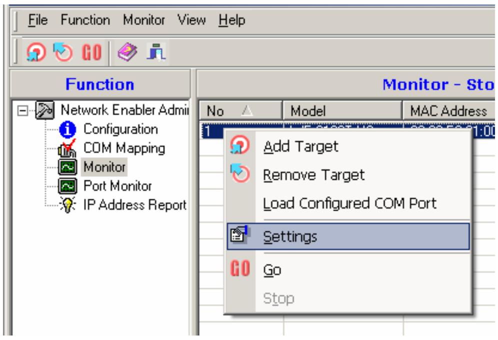


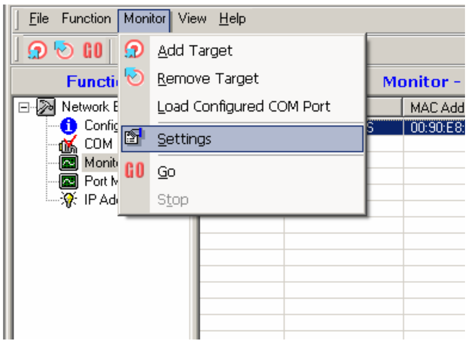
Using the Target Module List

For each function, target modules for specific commands are selected from the list in the right panel. This list will initially be empty, so you will need to add your module to this list when selecting a function for the first time. To add modules to the list, open the function context menu and select the appropriate command, such as "Search" or "Add Target". Note that different lists are maintained for each function.

Applying a Command to a Module

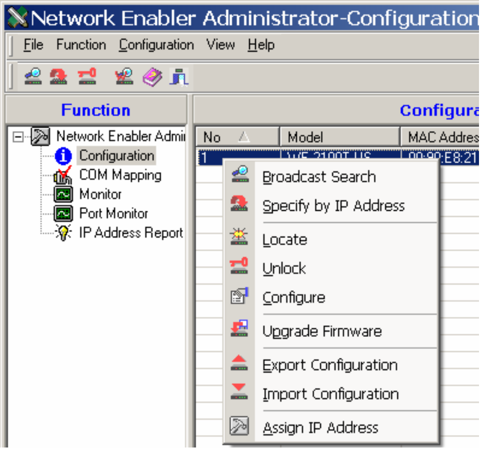
Specific commands are applied by right-clicking the target module in the module list. This will open the function context menu, and you may select the desired command. You may also select the module and then open the function context menu from the menu bar.



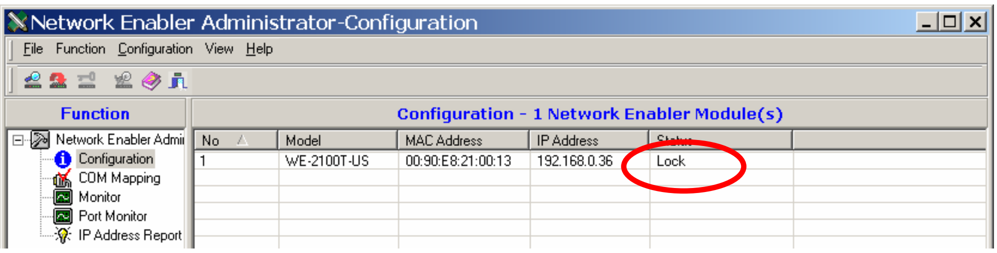


Configuration

Within the **Configuration** function are commands to configure your module, import and export its configuration, and update its firmware. The Configuration context menu is shown below:



Modules may be password-protected to prevent unauthorized configuration changes. A module's password status will be shown in the target module list.


Network Enabler Administrator-Configuration
File Function Configuration View Help
Function
Configuration - 1 Network Enabler Module(s)
Network Enabler Admi
Configuration
COM Mapping
Monitor
Port Monitor
IP Address Report

No	Model	MAC Address	IP Address	Status
1	WE-2100T-US	00:90:E8:21:00:13	192.168.0.36	Lock

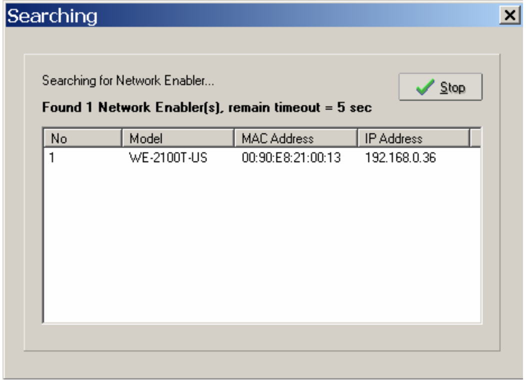
Password Status		
Modules found with "Broadcast Search"	Modules found with "Specify By IP Address"	Description
(none)	Fixed	Module has no password protection
Lock	Lock Fixed	Module requires password entry
Unlock	Unlock Fixed	Module has received correct password

When a module's password status is **Lock** or **Lock Fixed**, you will need to use the **Unlock** command before you can change any of the module's settings.

Broadcast Search

Description

This identifies all modules on the LAN and places them in the target module list for the Configuration function. Since this search is based on MAC address, rather than IP address, it will be able to find units that are not on the same subnet as your PC. You may click **Stop** as soon as your module is found.



Searching for Network Enabler...

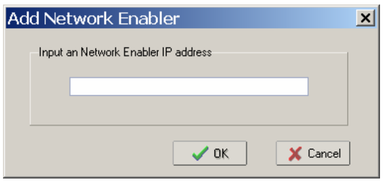
Found 1 Network Enabler(s), remain timeout = 5 sec

No	Model	MAC Address	IP Address
1	WE-2100T-US	00:90:E8:21:00:13	192.168.0.36

Specify by IP Address

Description

This allows you to add a module to the target module list by entering its IP address.

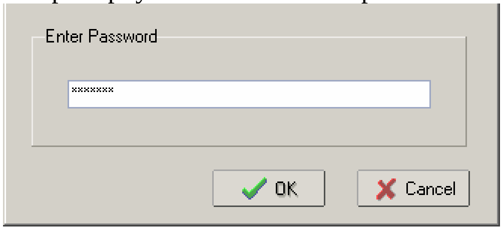


Input an Network Enabler IP address

Unlock

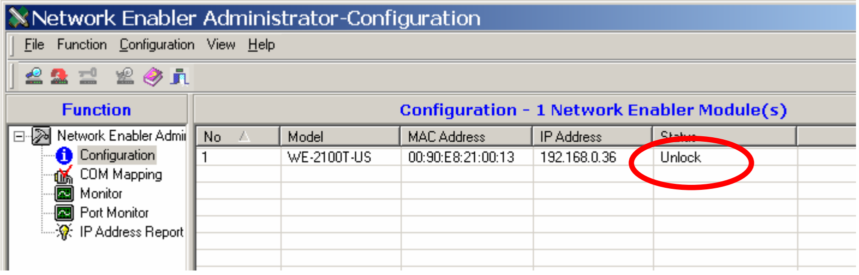
Description

This allows you to gain access to a module that is protected by a password. It will prompt you for the module's password.



Enter Password: ********

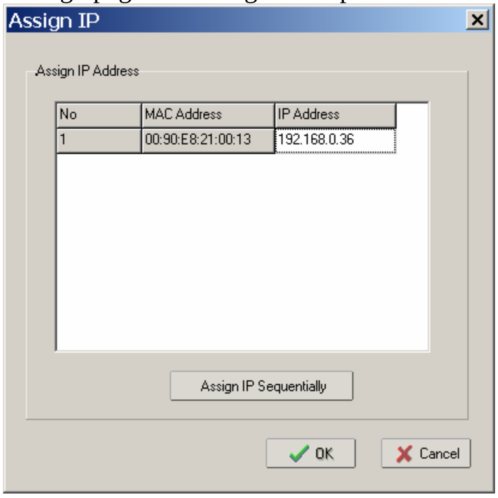
If the correct password is provided, the module's status will be updated to "Unlock".



Configuration - 1 Network Enabler Module(s)

No	Model	MAC Address	IP Address	Status
1	WE-2100T-US	00:90:E8:21:00:13	192.168.0.36	Unlock

Assign IP Address

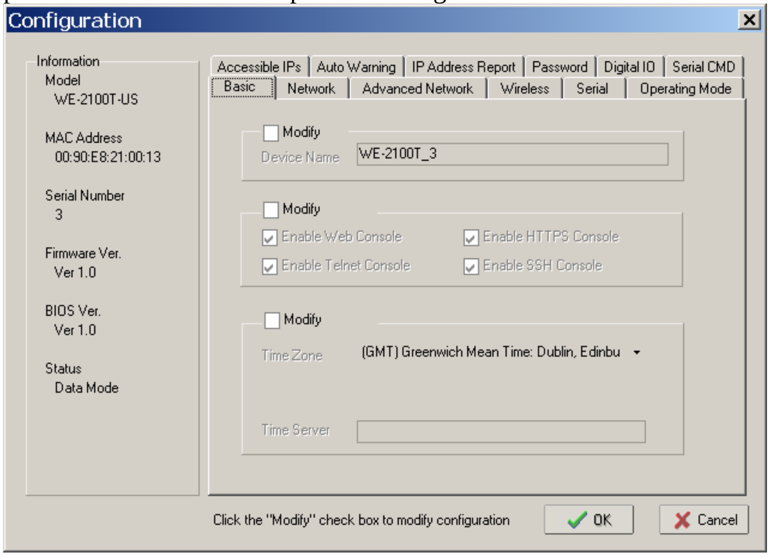
Description	This allows you to set the target module's IP address quickly, instead of digging through pages of configuration parameters. 

Assign IP

Assign IP Address

No	MAC Address	IP Address
1	00:90:E8:21:00:13	192.168.0.36

Configure

Description	This opens the target module's configuration window. In the configuration window, tabs are used to navigate between the different settings. Please refer to Chapters 6 through 10 for a description of the various settings on the WE-2100T. Click a **Modify** checkbox to enable changes to the associated parameter. Click **OK** to implement changes. 

Configuration

Information
Model
WE-2100T-US
MAC Address
00:90:E8:21:00:13
Serial Number
3
Firmware Ver.
Ver 1.0
BIOS Ver.
Ver 1.0
Status
Data Mode

Accessible IPs | Auto Warning | IP Address Report | Password | Digital IO | Serial CMD
Basic | Network | Advanced Network | Wireless | Serial | Operating Mode

□ Modify
Device Name: WE-2100T_3

□ Modify
☑ Enable Web Console ☑ Enable HTTPS Console
☑ Enable Telnet Console ☑ Enable SSH Console

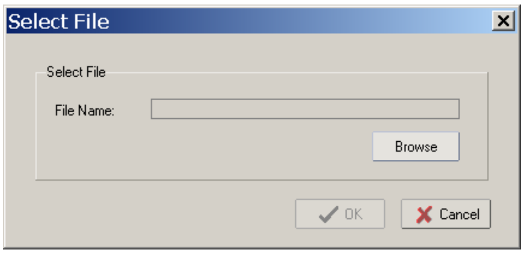
□ Modify
Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinbu
Time Server:

Click the "Modify" check box to modify configuration

ATTENTION

You can configure multiple units simultaneously if the units are all the same model. Simply hold down the **CTRL** or **SHIFT** key when selecting the target modules.

Upgrade Firmware

Description	This allows you to upload new firmware to the target module. You will be prompted to indicate where the firmware file is located. Firmware updates can be downloaded from www.moxa.com.  Select File Select File File Name: Browse OK Cancel It will take a few moments for the module's firmware to be updated. Do not disconnect the network, the module, or your PC at any time during the update.

ATTENTION

You can update the firmware of multiple units simultaneously if the units are all the same model. Simply hold down the **CTRL** or **SHIFT** key when selecting the target modules.

Import and Export Configuration

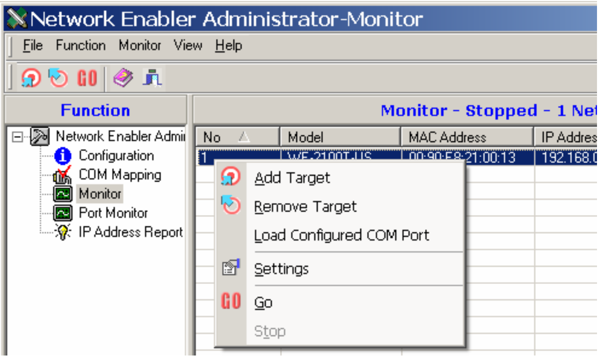
Description	These commands are used to save or restore the target module's configuration. All configuration settings can be stored on a file to be restored later, from anywhere on the network. Follow the onscreen instructions to save or restore the target unit's configuration.

ATTENTION

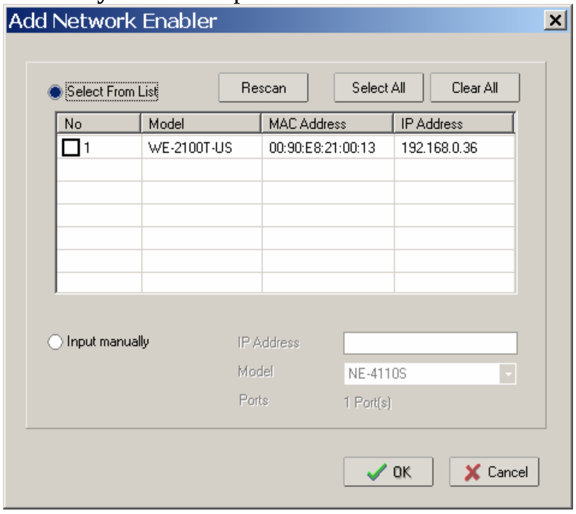
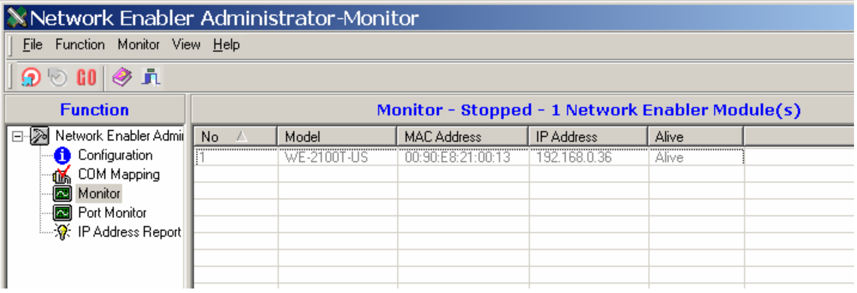
You can import the configuration of multiple units simultaneously if the units are all the same model. Simply hold down the **CTRL** or **SHIFT** key when selecting the target modules.

Monitor

The **Monitor** function is used for live monitoring of your module over the network. Different parameters and events may be monitored, and you can receive pop-up warnings for certain events. The Monitor context menu is shown below:



Add Target

Description	This places modules on the module list for monitoring. You may need to click **Rescan** to search the network for available modules. You can also select **Input manually** to enter a specific IP address and model.  Add Network Enabler ● Select From List Rescan Select All Clear All ○ Input manually IP Address Model Ports OK Cancel No | Model | MAC Address | IP Address □ 1 | WE-2100T-US | 00:90:E8:21:00:13 | 192.168.0.36 Model: NE-4110S Ports: 1 Port(s) Any module that is added to the list will be monitored when the **Go** command is selected.  Network Enabler Administrator-Monitor File Function Monitor View Help GO Function Monitor - Stopped - 1 Network Enabler Module(s) Network Enabler Admi Configuration COM Mapping Monitor Port Monitor IP Address Report No | Model | MAC Address | IP Address | Alive 1 | WE-2100T-US | 00:90:E8:21:00:13 | 192.168.0.36 | Alive

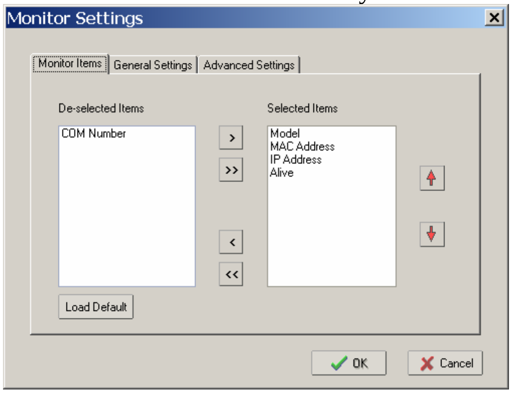
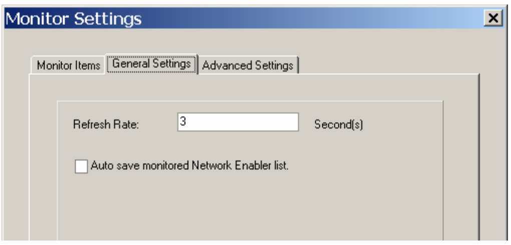
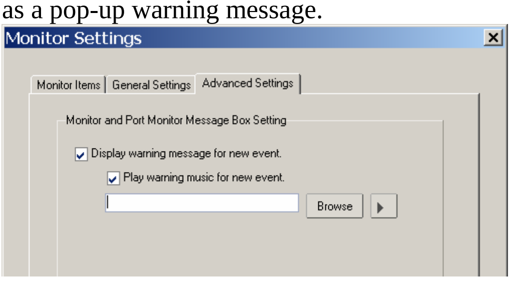
Remove Target

Description	This removes a module from the Monitor list.

Load Configured COM Port

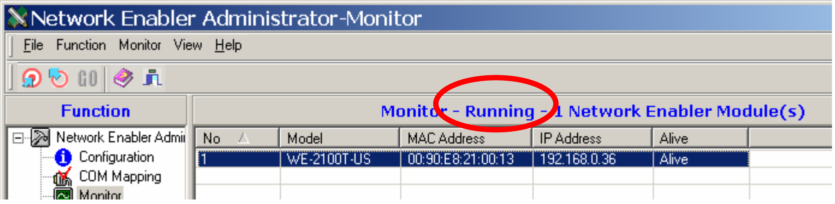
Description	If any COM ports are being mapped to modules over the network, this command will add those modules to the Monitor list. (COM ports can be mapped over the network to a serial port on the WE-2100T that is operating in RealCOM mode.)

Settings

Description	This specifies which items of information will be monitored, how often the information is refreshed, and how notification of events will occur. The **Monitor Items** tab is where you select the items to be monitored.  Monitor Settings Monitor Items General Settings Advanced Settings > >> < << Load Default OK Cancel De-selected Items: COM Number Selected Items: Model, MAC Address, IP Address, Alive The **General Settings** tab is where you specify how often the status of each module will be checked. The default is 3 seconds.  Monitor Settings Monitor Items General Settings Advanced Settings Refresh Rate: 3 Second(s) □ Auto save monitored Network Enabler list. The **Advanced Settings** tab is where you specify alarm behavior. The alarm notifies you if a connection is off-line. You may choose an audio alarm as well as a pop-up warning message.  Monitor Settings Monitor Items General Settings Advanced Settings Browse Monitor and Port Monitor Message Box Setting ☑ Display warning message for new event. ☑ Play warning music for new event.

Go

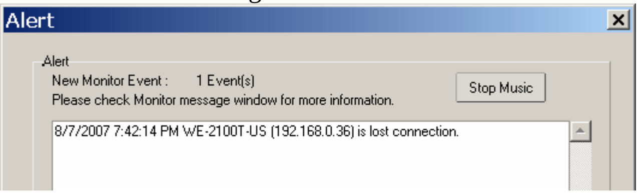
<table>
<tr>
<td><b>Description</b></td>
<td>
This activates live monitoring. All modules on the Monitor list will be monitored live, as indicated by "Running" in the header.


Network Enabler Administrator-Monitor
File Function Monitor View Help
Function
Network Enabler Admi
Configuration
COM Mapping
Monitor

Monitor - Running - 1 Network Enabler Module(s)

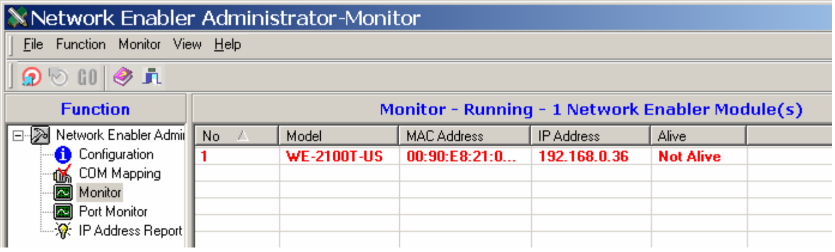
<table>
<tr><th>No</th><th>Model</th><th>MAC Address</th><th>IP Address</th><th>Alive</th></tr>
<tr><td>1</td><td>WE-2100T-US</td><td>00:90:E8:21:00:13</td><td>192.168.0.36</td><td>Alive</td></tr>
</table>

If alarms are enabled through the <b>Setting</b> command, a notification will appear when a monitored unit goes off-line.



New Monitor Event : 1 Event(s)
Please check Monitor message window for more information.
8/7/2007 7:42:14 PM WE-2100T-US (192.168.0.36) is lost connection.

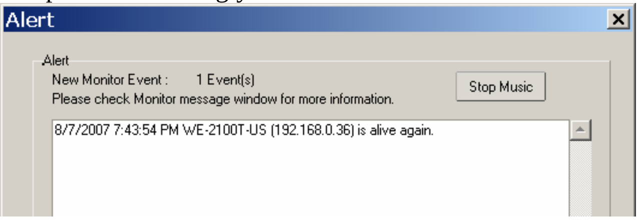
Modules that go off-line will be also displayed in red in the Monitor list.



Monitor - Running - 1 Network Enabler Module(s)

<table>
<tr><th>No</th><th>Model</th><th>MAC Address</th><th>IP Address</th><th>Alive</th></tr>
<tr><td>1</td><td>WE-2100T-US</td><td>00:90:E8:21:0...</td><td>192.168.0.36</td><td>Not Alive</td></tr>
</table>

If the module is able to re-establish the connection, another notification will appear indicating that the module is now "Alive". The Monitor list will be also be updated accordingly.



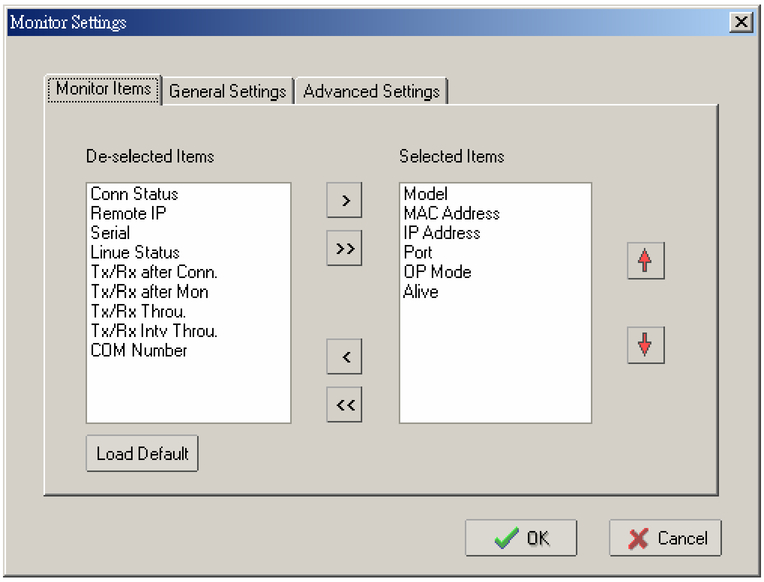
New Monitor Event : 1 Event(s)
Please check Monitor message window for more information.
8/7/2007 7:43:54 PM WE-2100T-US (192.168.0.36) is alive again.
</td>
</tr>
</table>

Stop

Description	This suspends live monitoring.

Port Monitor

The **Port Monitor** function is identical to the **Monitor** function, but with many additional items that can be monitored, as shown below.



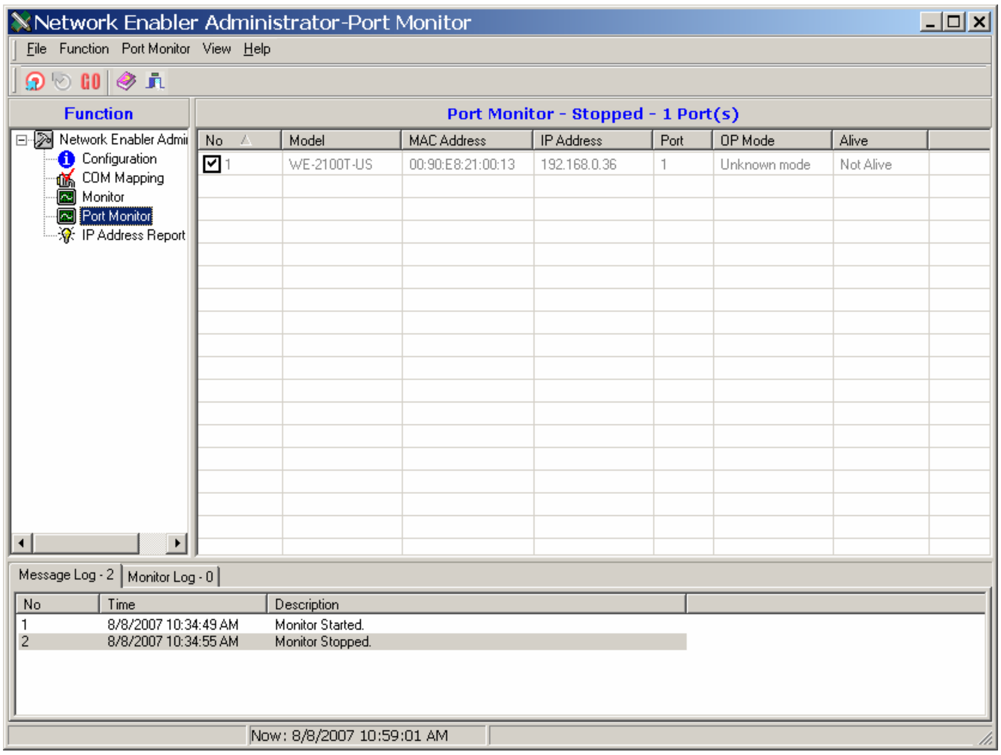
De-selected Items

- Conn Status
- Remote IP
- Serial
- Linue Status
- Tx/Rx after Conn.
- Tx/Rx after Mon
- Tx/Rx Throu.
- Tx/Rx Intv Throu.
- COM Number

Selected Items

- Model
- MAC Address
- IP Address
- Port
- OP Mode
- Alive

In addition, each serial port will be listed as a separate item on the Port Monitor list and can be selected or deselected for monitoring. Modules that have more than one serial port will be listed twice, once for each port.



Port Monitor - Stopped - 1 Port(s)

No	Model	MAC Address	IP Address	Port	OP Mode	Alive
☑ 1	WE-2100T-US	00:90:E8:21:00:13	192.168.0.36	1	Unknown mode	Not Alive

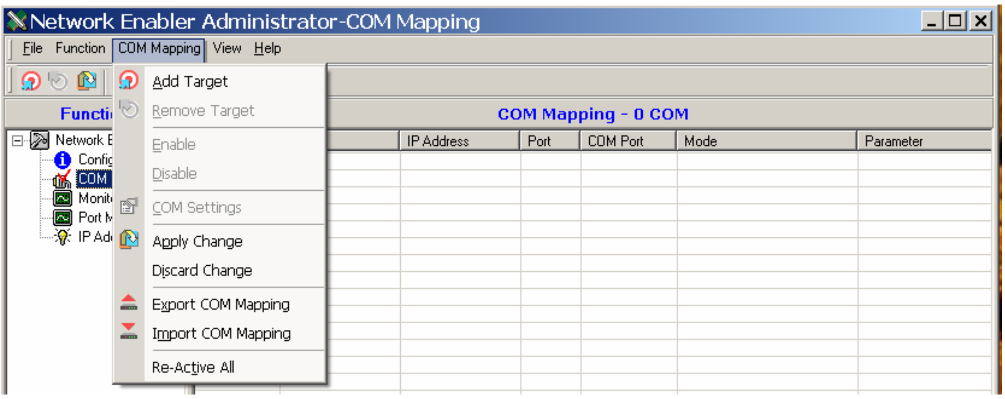
No	Time	Description
1	8/8/2007 10:34:49 AM	Monitor Started.
2	8/8/2007 10:34:55 AM	Monitor Stopped.

Now: 8/8/2007 10:59:01 AM

COM Mapping

The **COM Mapping** function is used to configure the Real COM drivers, which are automatically installed with Network Enabler Administrator. The Real COM drivers map COM ports over the network to serial ports on WE-2100T modules. This allows a local application to use COM5, for example, to communicate with a device attached to the module.

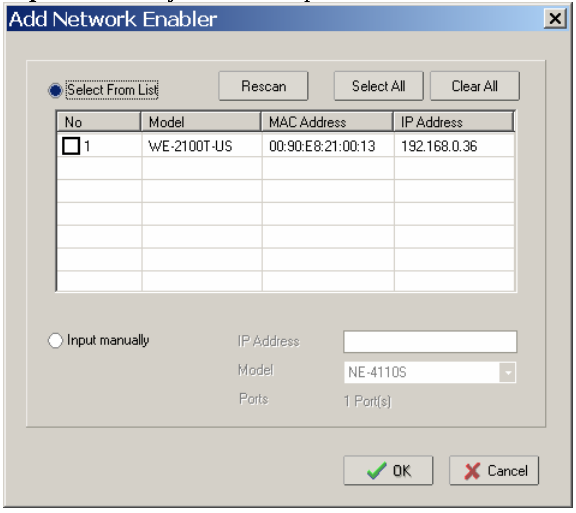
The Real COM drivers operate transparently and rely on Network Enabler Administrator only for initial configuration or adjustment. The COM Mapping context menu is shown below:



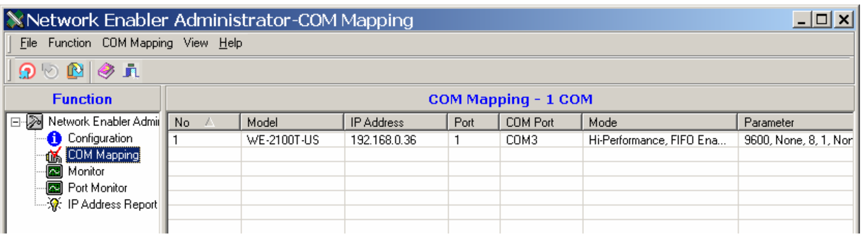
ATTENTION

The WE-2100T's serial port must be operating in Real COM mode in order to be used for COM mapping.

Add Target

<table>
<tr><td><b>Description</b></td><td>This places modules on the module list for COM mapping. You may need to click <b>Rescan</b> to search the network for available modules. You can also select <b>Input manually</b> to enter a specific IP address and model.


Add Network Enabler
Rescan
Select All
Clear All
OK
Cancel

● Select From List
<table><tr><th>No</th><th>Model</th><th>MAC Address</th><th>IP Address</th></tr><tr><td>□ 1</td><td>WE-2100T-US</td><td>00:90:E8:21:00:13</td><td>192.168.0.36</td></tr></table>
○ Input manually
IP Address:
Model: NE-4110S
Ports: 1 Port(s)
Each item on the COM Mapping list refers to a single serial port on a WE-2100T module.


Network Enabler Administrator-COM Mapping
File Function COM Mapping View Help
Function
Network Enabler Admii
Configuration
COM Mapping
Monitor
Port Monitor
IP Address Report

COM Mapping - 1 COM
<table><tr><th>No</th><th>Model</th><th>IP Address</th><th>Port</th><th>COM Port</th><th>Mode</th><th>Parameter</th></tr><tr><td>1</td><td>WE-2100T-US</td><td>192.168.0.36</td><td>1</td><td>COM3</td><td>Hi-Performance, FIFO Ena...</td><td>9600, None, 8, 1, Nor</td></tr></table></td></tr>
</table>

Remove Target

Description	This removes an item from the COM Mapping list.

ATTENTION

You can configure COM mapping even if your module is off-line (not connected). When using the **Add Target** command, simply select the "Input manually" option and enter the IP address and model. This is a useful option for certain field installations where COM mapping must be set up before the module is physically installed.

COM Settings

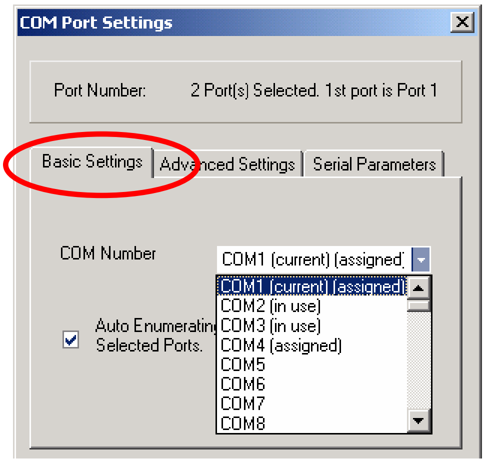
Description	This specifies which COM port will be mapped to the selected serial port, along with other settings.

ATTENTION

You can map multiple COM ports in one step by holding down the **CTRL** or **SHIFT** key when selecting the target serial ports.

Basic Settings

In the **Basic Settings** tab, the **COM Number** parameter selects the COM port that will be mapped to the device port. The drop-down list shows available COM ports with status.

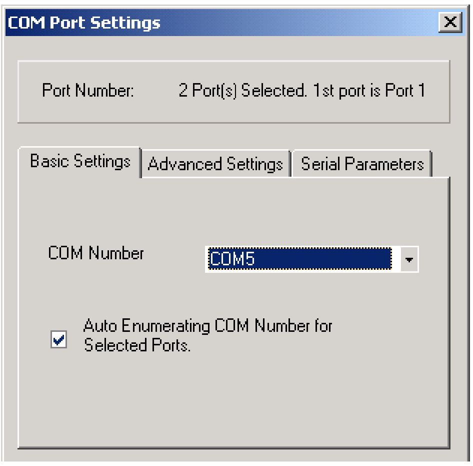


Port Number: 2 Port(s) Selected. 1st port is Port 1

COM Number: COM1 (current) (assigned)

COM1 (current) (assigned)
COM2 (in use)
COM3 (in use)
COM4 (assigned)
COM5
COM6
COM7
COM8

☑ Auto Enumerating COM Number for Selected Ports.



Port Number: 2 Port(s) Selected. 1st port is Port 1

COM Number: COM5

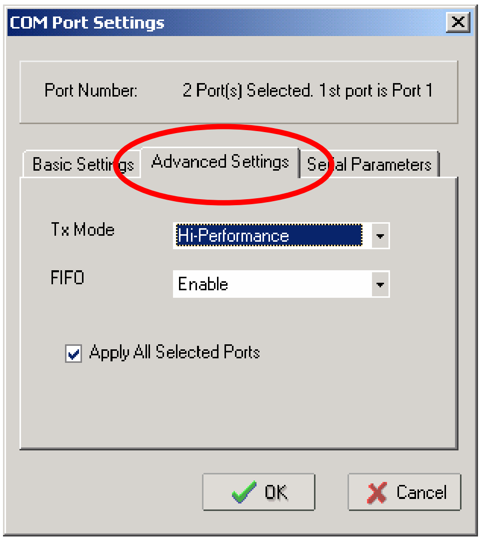
☑ Auto Enumerating COM Number for Selected Ports.

Status	Description
in use	The COM number is already being used by the system or being mapped to a module.
assigned	The COM number has been tentatively mapped to one of the serial ports on the COM Mapping list.
current + in use	The COM number is currently being mapped by the Real COM driver to the selected serial port.
current + assigned	The COM number has been tentatively mapped to the selected serial port, but the Real COM driver has not been updated yet.

The "Auto Enumerating" parameter can be used when mapping multiple COM ports at the same time. When the parameter is checked, this option automatically assigns available COM numbers sequentially. If not checked, you will need to assign each COM number separately.

Advanced Settings

In the **Advanced Settings** tab, you may configure how serial data is transmitted from the PC to the WE-2100T.



Port Number: 2 Port(s) Selected. 1st port is Port 1

Tx Mode: Hi-Performance

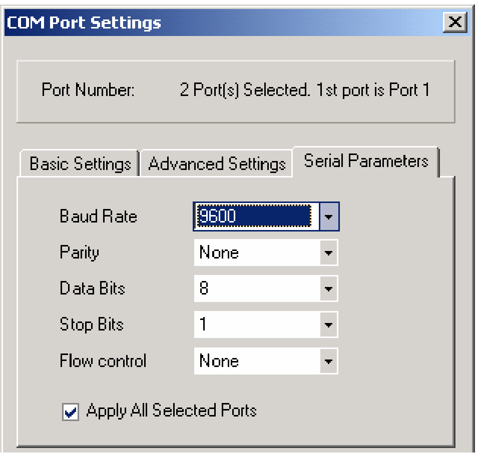
FIFO: Enable

☑ Apply All Selected Ports

Tx Mode	Hi-Performance is the default for Tx mode. After the driver sends data to the module, the driver immediately issues a "Tx Empty" response to the program. Under Classical mode, the driver will not send the "Tx Empty" response until after confirmation is received from the module. This causes lower throughput. Classical mode is recommended if you want to ensure that all data is sent out before further processing.
FIFO	When "FIFO" is disabled, the selected serial port will send one byte each time the Tx FIFO becomes empty, and an Rx interrupt will be generated for each incoming byte. This will cause a faster response time but lower throughput.

Serial Parameters

In the **Serial Parameters** tab, the COM port's serial communication parameters are defined.



Port Number: 2 Port(s) Selected. 1st port is Port 1

Baud Rate: 9600

Parity: None

Data Bits: 8

Stop Bits: 1

Flow control: None

☑ Apply All Selected Ports

Apply and Discard Change

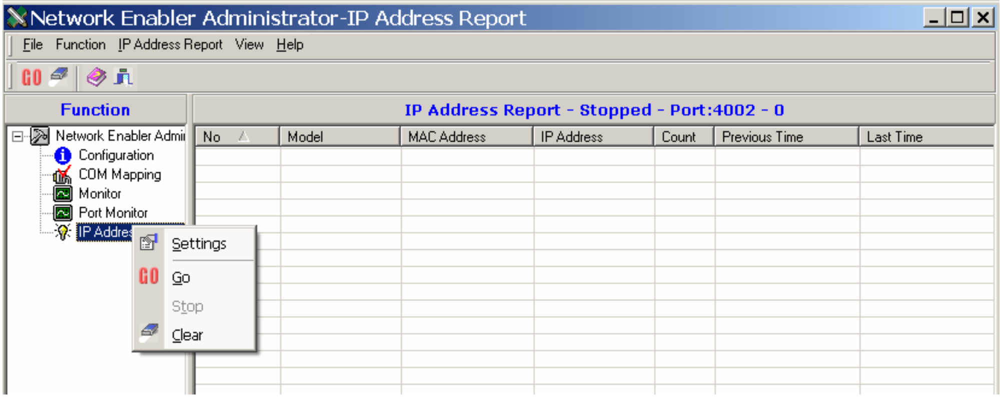
Description	This specifies whether or not to update the Real COM drivers with the changes made through the **COM Settings** command. If changes are discarded, the Real COM drivers will retain their original settings. If the changes are applied, the Real COM drivers will be updated with the new settings and mappings.

Import and Export COM Mapping

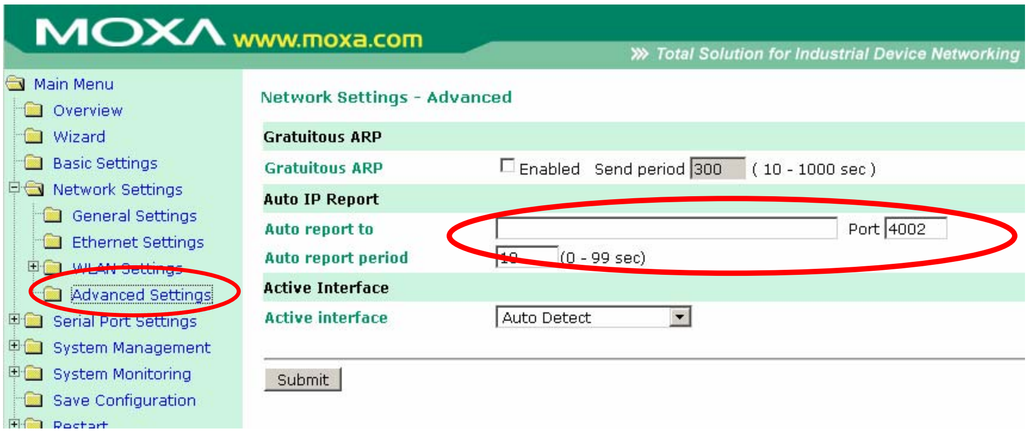
Description	This allows Real COM settings to be saved or loaded from a text file. Use the **Export COM Mapping** command to save the current COM mapping settings. Use the **Import COM Mapping** command to load COM mapping settings from a previously saved file.

IP Address Report

The **IP Address Report** function is used to receive automatic IP reports from appropriately configured WE-2100T modules. The IP Address Report context menu is shown below:



To configure a module to send IP address reports, enter the destination IP address in the **Auto report to** parameter. On the web console, this parameter is on the **Advanced Settings** page in the the **Network Settings** folder. The destination IP address should be the address of the PC that is running Network Enabler Administrator.



Network Settings - Advanced

Gratuitous ARP

Gratuitous ARP □ Enabled Send period 300 (10 - 1000 sec)

Auto IP Report

Auto report to Port 4002

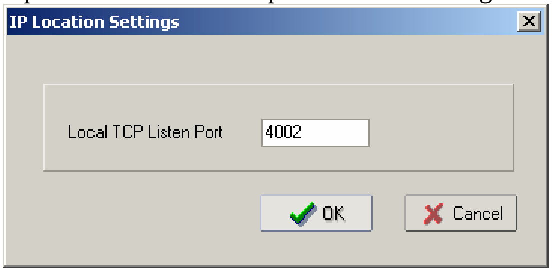
Auto report period 10 (0 - 99 sec)

Active Interface

Active interface Auto Detect

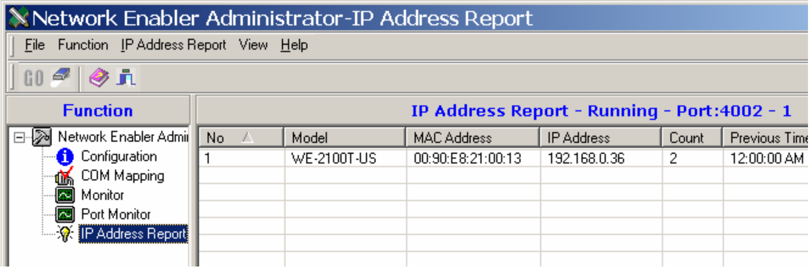
Please refer to Chapter 7 for information on configuring the module to send automatic IP reports. Please refer to Appendix E for information on the IP report protocol.

Settings

<table>
<tr><td><b>Description</b></td><td>This designates the TCP port number that the module is using to send IP address reports. This must correspond with the settings on the module.


Local TCP Listen Port: 4002</td></tr>
</table>

Go

<table>
<tr><td><b>Description</b></td><td>This activates monitoring for IP address reports. Network Enabler Administrator will begin listening for reports using the port number specified by the <b>Settings</b> command. As IP address reports are received, the information will be displayed in the right panel.


Network Enabler Administrator-IP Address Report
File Function IP Address Report View Help
GO
Function
Network Enabler Admi
Configuration
COM Mapping
Monitor
Port Monitor
IP Address Report

IP Address Report - Running - Port:4002 - 1
<table><tr><th>No</th><th>Model</th><th>MAC Address</th><th>IP Address</th><th>Count</th><th>Previous Time</th></tr><tr><td>1</td><td>WE-2100T-US</td><td>00:90:E8:21:00:13</td><td>192.168.0.36</td><td>2</td><td>12:00:00 AM</td></tr></table></td></tr>
</table>

Stop

Description	This suspends monitoring for IP address reports.

Clear

Description	This clears the current display of address reports in the right panel.

13
Serial Command Mode

Serial Command Mode allows configuration of the module through serial commands received directly through the serial port.

This chapter includes the following sections:

- ❑ **Overview**
- ❑ **Serial Command Format**
  - ➢ Command Structure
  - ➢ Reply Structure
- ❑ **Command Set**
- ❑ **Operation Flow Chart**
- ❑ **Configuring Trigger Type**
- ❑ **Entering Serial Command Mode**
- ❑ **Determining the Active Mode**
- ❑ **Serial Command Examples**
  - ➢ Example 1: Use Hardware Trigger
  - ➢ Example 2: Use Hardware Trigger
  - ➢ Example 3: Use Software Trigger, Get IP Mode
  - ➢ Example 4: Use SW Trigger, Change TCP Port Number

Overview

In Serial Command Mode, the module’s parameters are retrieved or configured using specially parsed commands that are sent through the serial port. Device manufacturers can take advantage of Serial Command Mode to add local configuration capability to their products. For example, a card reader’s number pad could be used to configure the card reader's IP address, netmask, and baudrate. Using Serial Command Mode, a device can be configured on-site without requiring a laptop or other additional equipment.

Serial Command Format

Each command and reply is a sequence of case-sensitive ASCII characters transmitted in the following order: head, command code, OP code, parameter, and tail.

ATTENTION

The **carriage return** character is used as the last byte or tail for each data frame; an additional **line feed** character is not required. For most systems, the **ENTER** key typically sends both a carriage return character and a line feed character. Most terminal emulators refer to the carriage return character as **CR** and to the line feed character as **LF**. In hex, **CR** is 0x0D and **LF** is 0x0A. In C language, “\r” refers to **CR**, whereas “\n” refers to **CR** + **LF**.

Command Structure

Descriptor	Bytes	Character	Description
Head	1	“>”	fixed value (0x3E)
Command Code	1	“R”, “W”	R: get module parameter W: set module parameter
OP Code	2	(varies)	
Parameter	varies	(varies)	
Tail	1	CR	carriage return character, no line feed

For example, if you wanted to change the TCP server port number to 4001, you would send "**>WTL4001**" followed by **CR** (carriage return). Available OP codes and parameters are described in detail later in this chapter.

Reply Structure

Descriptor	Bytes	Character	Comments
Head	1	“<”	<: fixed value (0x3C)
Reply Code	1	“Y”, “1” to “5”, “E’	Y: command was executed successfully 1: command not supported 2: OP code not supported 3: invalid command encapsulation 4: invalid parameter 5: invalid return value E: enter Serial Command Mode
OP Code	2	(varies)	
Parameter	varies	(varies)	

Descriptor	Bytes	Character	Comments
Tail	1	CR	carriage return character, no line feed

For example, to indicate that the TCP server port number has been written successfully, the module would return "**<YTL**" followed by **CR**. Available OP codes and parameters are described in the next section.

Command Set

Basic Commands

OP Code	Parameter	Comments
BS	(read only)	serial number
BV	(read only)	firmware version
BN	(alphanumeric, max. 15 bytes)	server name
BW	0: disable 1: enable	web console
BT	0: disable 1: enable	Telnet console
BP	(alphanumeric, max. 10 bytes)	password
BR	1: restart only 2: save & restart (write only)	save and restart
NC	0: static 1: DHCP	IP configuration
NP	xxx.xxx.xxx.xxx (e.g., 192.168.127.254)	IP address
NM	xxx.xxx.xxx.xxx (e.g., 255.255.0.0)	netmask
NG	xxx.xxx.xxx.xxx (e.g., 192.168.1.254)	gateway
NA	(read only) (e.g., 00:90:e8:09:44:fe)	MAC address

Accessible IP Commands

OP Code	Parameter	Comments
AS	0: disable 1: enable	accessible IP list filtering
AA	xxx.xxx.xxx.xxx (e.g., 192.168.127.1)	accessible IP address 01
AB	xxx.xxx.xxx.xxx (e.g., 192.168.127.1)	accessible IP address 02
AC	xxx.xxx.xxx.xxx (e.g., 192.168.127.1)	accessible IP address 03
AD	xxx.xxx.xxx.xxx (e.g., 192.168.127.1)	accessible IP address 04

OP Code	Parameter	Comments
AE	xxx.xxx.xxx.xxx (e.g., 192.168.127.1)	accessible IP address 05
AF	xxx.xxx.xxx.xxx (e.g., 192.168.127.1)	accessible IP address 06
AG	xxx.xxx.xxx.xxx (e.g., 192.168.127.1)	accessible IP address 07
AH	xxx.xxx.xxx.xxx (e.g., 192.168.127.1)	accessible IP address 08
AI	xxx.xxx.xxx.xxx (e.g., 192.168.127.1)	accessible IP address 09
AJ	xxx.xxx.xxx.xxx (e.g., 192.168.127.1)	accessible IP address 10
AK	xxx.xxx.xxx.xxx (e.g., 192.168.127.1)	accessible IP address 11
AL	xxx.xxx.xxx.xxx (e.g., 192.168.127.1)	accessible IP address 12
AM	xxx.xxx.xxx.xxx (e.g., 192.168.127.1)	accessible IP address 13
AN	xxx.xxx.xxx.xxx (e.g., 192.168.127.1)	accessible IP address 14
AO	xxx.xxx.xxx.xxx (e.g., 192.168.127.1)	accessible IP address 15
AP	xxx.xxx.xxx.xxx (e.g., 192.168.127.1)	accessible IP address 16
Aa	xxx.xxx.xxx.xxx (e.g., 255.255.255.0)	accessible IP netmask 01
Ab	xxx.xxx.xxx.xxx (e.g., 255.255.255.0)	accessible IP netmask 02
Ac	xxx.xxx.xxx.xxx (e.g., 255.255.255.0)	accessible IP netmask 03
Ad	xxx.xxx.xxx.xxx (e.g., 255.255.255.0)	accessible IP netmask 04
Ae	xxx.xxx.xxx.xxx (e.g., 255.255.255.0)	accessible IP netmask 05
Af	xxx.xxx.xxx.xxx (e.g., 255.255.255.0)	accessible IP netmask 06
Ag	xxx.xxx.xxx.xxx (e.g., 255.255.255.0)	accessible IP netmask 07
Ah	xxx.xxx.xxx.xxx (e.g., 255.255.255.0)	accessible IP netmask 08
Ai	xxx.xxx.xxx.xxx (e.g., 255.255.255.0)	accessible IP netmask 09
Aj	xxx.xxx.xxx.xxx (e.g., 255.255.255.0)	accessible IP netmask 10

OP Code	Parameter	Comments
Ak	xxx.xxx.xxx.xxx (e.g., 255.255.255.0)	accessible IP netmask 11
Al	xxx.xxx.xxx.xxx (e.g., 255.255.255.0)	accessible IP netmask 12
Am	xxx.xxx.xxx.xxx (e.g., 255.255.255.0)	accessible IP netmask 13
An	xxx.xxx.xxx.xxx (e.g., 255.255.255.0)	accessible IP netmask 14
Ao	xxx.xxx.xxx.xxx (e.g., 255.255.255.0)	accessible IP netmask 15
Ap	xxx.xxx.xxx.xxx (e.g., 255.255.255.0)	accessible IP netmask 16

Operation Mode Commands

OP Code	Parameter	Comments
OM	0: Real COM 1: TCP server 2: TCP client 3: UDP mode	operation mode

TCP Server Mode Commands

OP Code	Parameter	Comments
TM	1 – 4	max. number of connections
TL	0 – 65535	local TCP port
TT	0 – 99 (minutes)	TCP alive check time
TI	0 – 65535 (ms)	inactivity time
TX	0: no delimiter 1: enable 1-character delimiter 2: enable 2 character delimiter	number of characters to use as delimiter
TY	ASCII character in hex code (i.e., "A1" for character 0xA1)	character to use for delimiter 1
TZ	ASCII character in hex code (i.e., "A1" for character 0xA1)	character to use for delimiter 2
TF	0 – 65535 (ms)	force transmit time

Real COM Mode Commands

OP Code	Parameter	Comments
RM	1 – 4	max. number of connections
RT	0 – 99 (minutes)	TCP alive check time
RX	0: no delimiter 1: enable 1-character delimiter 2: enable 2 character delimiter	number of characters to use as delimiter
RY	ASCII character in hex code (i.e., “A1” for character 0xA1)	character to use for delimiter 1
RZ	ASCII character in hex code (i.e., “A1” for character 0xA1)	character to use for delimiter 2
RF	0 – 65535 (ms)	force transmit time

TCP Client Mode Commands

OP Code	Parameter	Comments
CM	0: startup 1: any character	TCP connect on
CA	xxx.xxx.xxx.xxx (e.g., 192.168.1.1)	destination IP address 1
CB	xxx.xxx.xxx.xxx (e.g., 192.168.1.1)	destination IP address 2
CC	xxx.xxx.xxx.xxx (e.g., 192.168.1.1)	destination IP address 3
CD	xxx.xxx.xxx.xxx (e.g., 192.168.1.1)	destination IP address 4
C1	0 – 65535	destination port 1
C2	0 – 65535	destination port 2
C3	0 – 65535	destination port 3
C4	0 – 65535	destination port 4
CT	0 – 99 (minutes)	TCP alive check time
CI	0 – 65535	inactivity time
CX	0: no delimiter 1: enable 1-character delimiter 2: enable 2 character delimiter	number of characters to use as delimiter
CY	ASCII character in hex code (i.e., “A1” for character 0xA1)	character to use for delimiter 1
CZ	ASCII character in hex code (i.e., “A1” for character 0xA1)	character to use for delimiter 2
CF	0 – 65535 (ms)	force transmit time

UDP Mode Commands

OP Code	Parameter	Comments
UL	0 – 65535	local listen port
UA	xxx.xxx.xxx.xxx (e.g., 192.168.1.1)	destination IP address 1, begin range
UB	xxx.xxx.xxx.xxx (e.g., 192.168.1.1)	destination IP address 2, begin range
UC	xxx.xxx.xxx.xxx (e.g., 192.168.1.1)	destination IP address 3, begin range
UD	xxx.xxx.xxx.xxx (e.g., 192.168.1.1)	destination IP address 4, begin range
Ua	xxx.xxx.xxx.xxx (e.g., 192.168.1.1)	destination IP address 1, end range
Ub	xxx.xxx.xxx.xxx (e.g., 192.168.1.1)	destination IP address 2, end range
Uc	xxx.xxx.xxx.xxx (e.g., 192.168.1.1)	destination IP address 3, end range
Ud	xxx.xxx.xxx.xxx (e.g., 192.168.1.1)	destination IP address 4, end range
U1	0 – 65535	destination IP address 1, port
U2	0 – 65535	destination IP address 2, port
U3	0 – 65535	destination IP address 3, port
U4	0 – 65535	destination IP address 4, port
UX	0: no delimiter 1: enable 1-character delimiter 2: enable 2 character delimiter	number of characters to use as delimiter
UY	ASCII character in hex code (i.e., "A1" for character 0xA1)	character to use for delimiter 1
UZ	ASCII character in hex code (i.e., "A1" for character 0xA1)	character to use for delimiter 2
UF	0 – 65535 (ms)	force transmit time

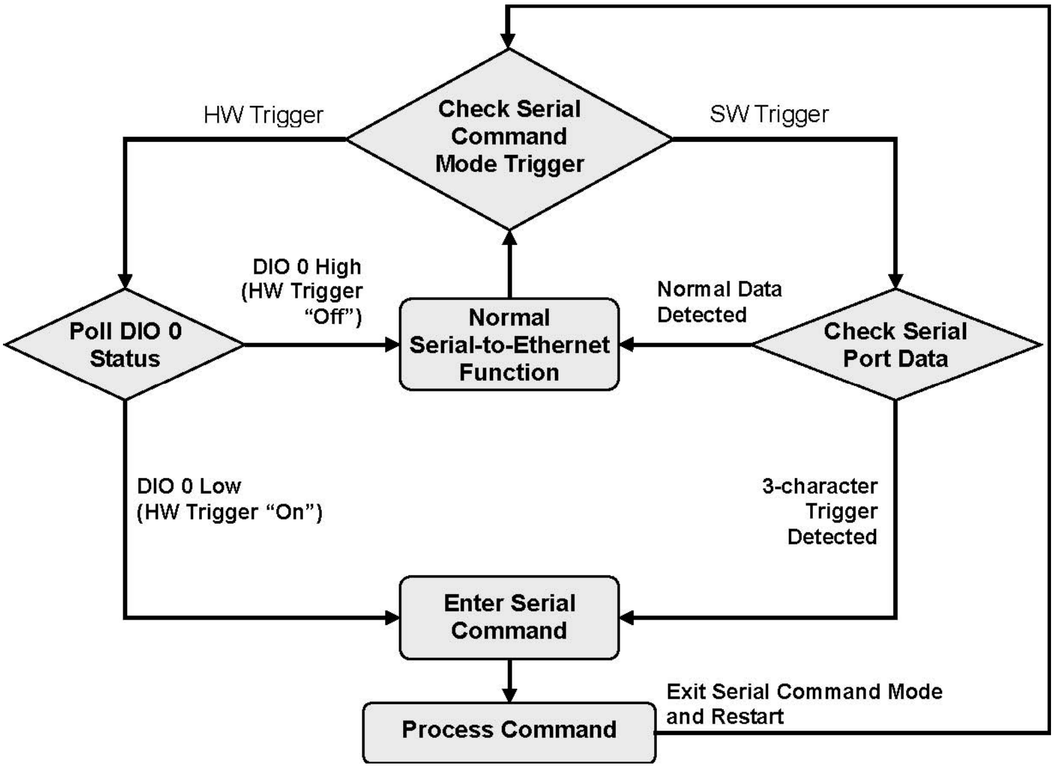
Digital IO Commands

OP Code	Parameter	Comments
DM	bytes 1 and 2 (DIO #) 00: DIO 0 00: DIO 1 00: DIO 2 03: DIO 3 byte 3 (DIO mode) 0: input 1: output	set DIO mode (e.g., "000" sets DIO 0 to input mode)
DS	bytes 1 and 2 (DIO #) 00: DIO 0 00: DIO 1 00: DIO 2 03: DIO 3 byte 3 (DIO status) 0: low 1: high	set DIO status (e.g., "011" sets DIO 1 to high)

Serial Command Mode Commands

OP Code	Parameter	Comments
ES	0: disable 1: enable HW trigger 2: enable SW trigger	enable Serial Command Mode
EC	three ASCII characters in hex code (i.e., "A1A2A3" for ASCII characters 0xA1, 0xA2, 0xA3)	SW trigger characters

Operation Flow Chart


Check Serial Command Mode Trigger
HW Trigger
SW Trigger
Poll DIO 0 Status
DIO 0 High (HW Trigger "Off")
Normal Serial-to-Ethernet Function
Normal Data Detected
Check Serial Port Data
DIO 0 Low (HW Trigger "On")
3-character Trigger Detected
Enter Serial Command
Process Command
Exit Serial Command Mode and Restart

ATTENTION

This flowchart represents a continual process. You can start trace out a logical flow by starting anywhere on the chart.

Diamonds represent decision points. Only one path leading out of any diamond can be followed.

Configuring Trigger Type

Serial Command Mode may be triggered by either software or hardware. You can set the trigger type using Network Enabler Administrator, the Telnet console, the web console, or the serial console.

With a hardware trigger, a signal received through DIO 0 will trigger the module to enter Serial Command Mode. This is the default setting.

With a software trigger, a three-character sequence received through the serial port will trigger the module to enter Serial Command Mode. When the software trigger is used, the highest achievable data transmission rate will be 55000 bps. This is because all data received through the serial port will be parsed. In other words, the system must continuously check the serial port data for the trigger characters.

Disabling the trigger will disable Serial Command Mode.

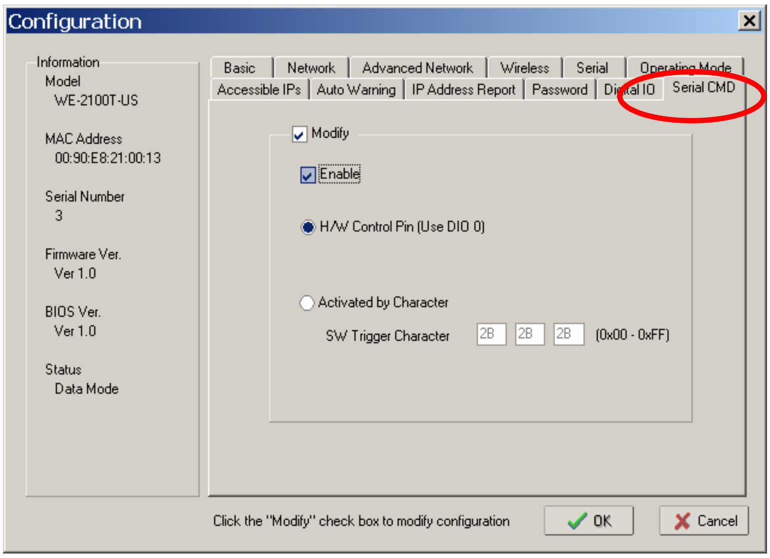
ATTENTION

The default trigger type is hardware (DIO 0). Only one type of trigger may be active at a time; hardware and software trigger may not be used at the same time.

Using Network Enabler Administrator

To use Network Enabler Administrator to configure the trigger type, you will need to find the module and open its configuration window. Please refer to Chapter 12 for additional details.

The trigger type will be configured under the **Serial CMD** tab. Check the **Modify** and **Enable** boxes to configure the trigger type.



Configuration

Information
Model
WE-2100T-US
MAC Address
00:90:E8:21:00:13
Serial Number
3
Firmware Ver.
Ver 1.0
BIOS Ver.
Ver 1.0
Status
Data Mode

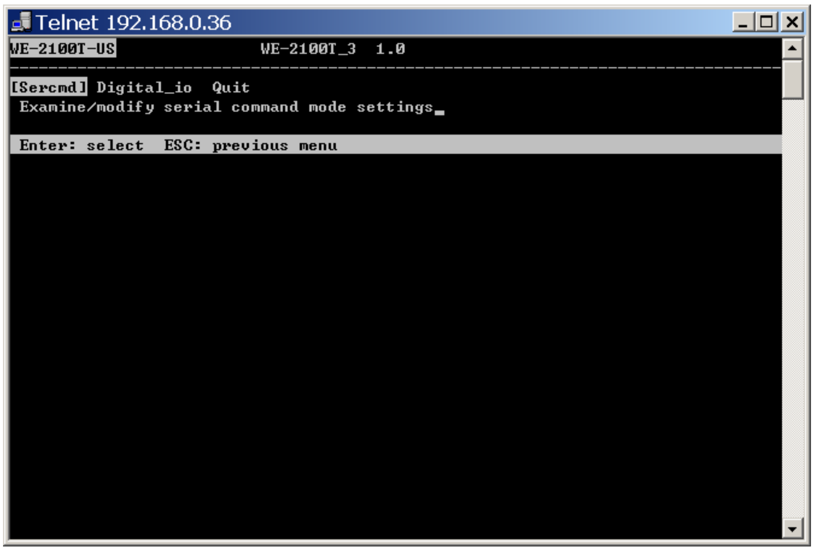
☑ Modify
☑ Enable
● H/W Control Pin (Use DIO 0)
○ Activated by Character
SW Trigger Character 2B 2B 2B (0x00 - 0xFF)

Click the "Modify" check box to modify configuration

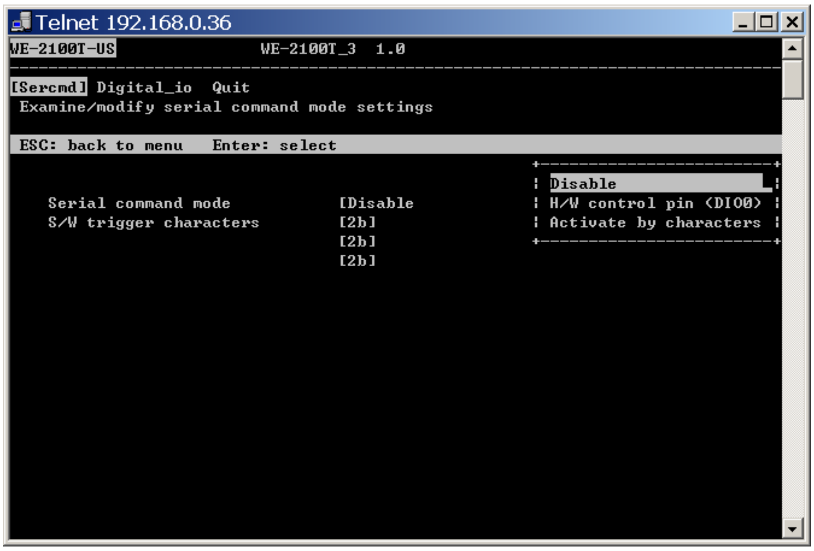
When the trigger has been configured, click **OK** to save and restart the module with the new settings.

Using Telnet Console

Please refer to Chapter 5 for information on opening the Telnet console. The Serial Command Mode trigger is configured under **System** > **System** > **Sercmd**.



```
WE-2100T-US                  WE-2100T_3   1.0
--------------------------------------------------------------------------------
[Sercmd] Digital_io  Quit
 Examine/modify serial command mode settings_

 Enter: select   ESC: previous menu
```

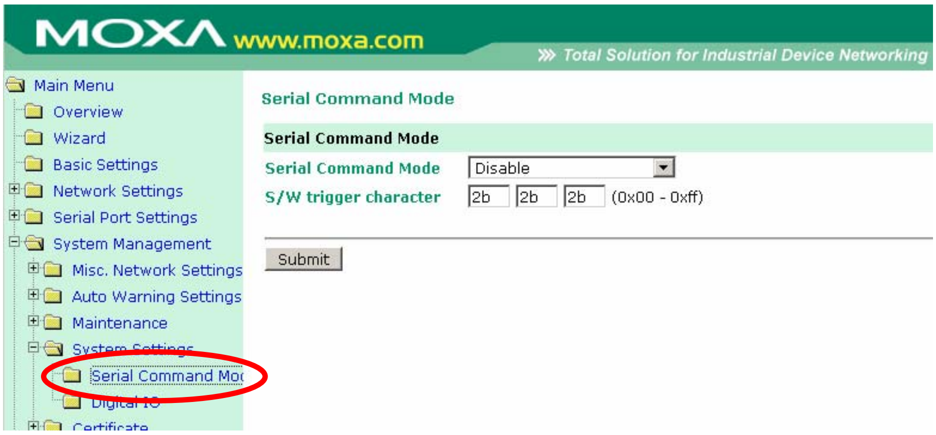


```
WE-2100T-US                  WE-2100T_3   1.0
--------------------------------------------------------------------------------
[Sercmd] Digital_io  Quit
 Examine/modify serial command mode settings

 ESC: back to menu    Enter: select
                                                       +------------------------+
                                                       | Disable                |
    Serial command mode            [Disable            | H/W control pin (DIO0) |
    S/W trigger characters         [2b]                | Activate by characters |
                                   [2b]                +------------------------+
                                   [2b]
```

For the changes to take effect, you will need to go back to the main menu, save the configuration, and restart the module. If you quit without saving, any changes you made to the configuration will be lost.

Using Web Console

Please refer to Chapter 6 for information on opening the web console. The **Serial Command Mode** page is located under **System Settings** in the **System Management** folder.



Serial Command Mode

Serial Command Mode	
Serial Command Mode	Disable
S/W trigger character	2b 2b 2b (0x00 - 0xff)

Modify the settings as needed, and then click **Submit.** Remember that you will need to save the configuration and restart the module for any changes to effect.

Using Serial Console

To access the serial console, connect the module's serial console port (P1) to your PC's serial port, and then use a terminal emulator program to enter the serial console. Please refer to the Serial Console section in Chapter 5 for details on how to open the serial console. Once the serial console is open, it functions exactly the same as if connecting by Telnet console.

Entering Serial Command Mode

The module can enter Serial Command Mode through either a hardware trigger or a software trigger, depending on how it has been configured. Please refer to the previous section for details on how to configure the trigger type.

Hardware Trigger

- Connect a hardware trigger such as a button or a switch to DIO 0.
- Use the trigger to pull DIO 0 to **low** in order to enter Serial Command Mode. Low state must be maintained for at least 200 ms to qualify as a valid trigger.

Software Trigger

- Send the 3 software trigger characters to the serial port in rapid sequence (less than 20 ms between characters).

When first entering Serial Command Mode, the module will respond with the string "**<E**" followed by **CR**. All data communication will cease when the device is in Serial Command Mode.

- Any open TCP connection will be closed, for both the client and the server.
- No new TCP connections will be allowed.
- UDP data communication will be disabled.

For testing purposes, you will likely use a terminal emulator to send and receive data frames for Serial Command Mode. You will need to match the serial communication settings on the module, which can be obtained using Network Enabler Administrator, the web console, or the Telnet console.

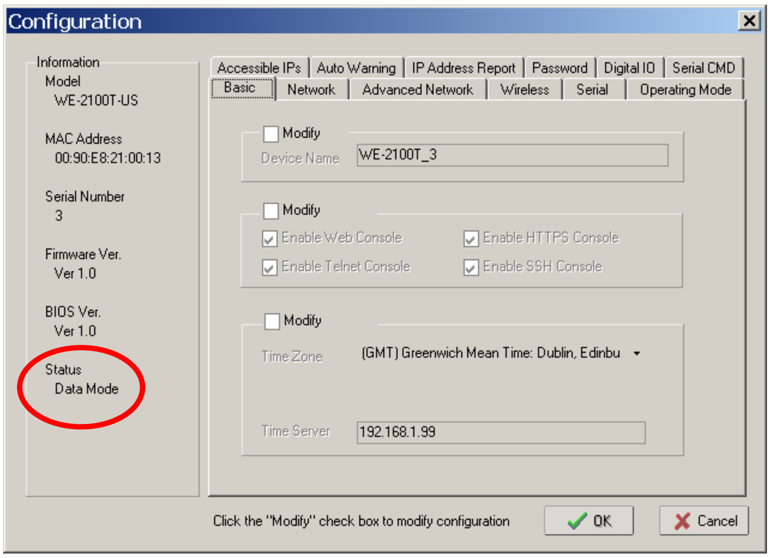
Exiting Serial Command Mode

After the module has entered Serial Command Mode, there are three ways to exit.

- **Power Off:** If the module is powered off without saving the configuration, all changes will be lost when the module is powered on again.
- **Exit by Command (OP Code: BR):** There are two options when manually exiting by serial command. **Save & Restart** must be selected if you want to save any of the changes that were made during the Serial Command Mode session. **Restart** will restart the module without saving any of the changes.
- **Auto Restart:** If 5 minutes elapses without inputting a valid command, then the module will automatically restart without saving the configuration.

Determining the Active Mode

If you need to verify whether or not the module is operating in Serial Command Mode, there are two methods available: by Network Enabler Administrator or by serial console. In Network Enabler Administrator, you may open a module's configuration window and determine if it is in Serial Command Mode in the Information panel.


Configuration

Information
Model
WE-2100T-US
MAC Address
00:90:E8:21:00:13
Serial Number
3
Firmware Ver.
Ver 1.0
BIOS Ver.
Ver 1.0
Status
Data Mode

☐ Modify
Device Name WE-2100T_3

☐ Modify
☑ Enable Web Console ☑ Enable HTTPS Console
☑ Enable Telnet Console ☑ Enable SSH Console

☐ Modify
Time Zone (GMT) Greenwich Mean Time: Dublin, Edinbu
Time Server 192.168.1.99

Click the "Modify" check box to modify configuration

In the example above, the status is **Data Mode,** which indicates normal data transmission. For Serial Command Mode, the status would be **Command Mode.**

You may also verify if the module is in Serial Command Mode by attaching a serial console to the serial port (P0). If the module is in Serial Command Mode, it will respond with a sequence of characters after receiving the serial command end character **CR**, as shown below.

Command sent by serial device	**Module's reply**
CR	"<E" + CR (0x3C, 0x45, 0x0D)
CR + LF (0x0D, 0x0A)	"<E" + CR (0x3C, 0x45, 0x0D)
Error command	"<3" + CR (0x3C, 0x33, 0x0D)

Simply send **CR** to the module. If it is in Serial Command Mode, it should respond with "**<E**" followed by **CR**.

Serial Command Examples

For the following examples, the module should be installed onto the evaluation board, and the evaluation board's serial port (P0) should be connected to a COM port on your PC.

ATTENTION

When using a terminal emulator program such as PComm Terminal, make sure that the **ENTER** key is configured to send **CR** only, rather than **CR + LF**.

Example 1: Use Hardware Trigger, Get Model Name

STEP 1: Verify that the hardware trigger is enabled for Serial Command Mode.

STEP 2: Check the module's serial port settings.

STEP 3: Start Windows HyperTerminal and make sure that the PC's serial port settings match the module's settings.

STEP 4: Pull DIO 0 to "Low" to enter Serial Command Mode. DIP switch 0 on the evaluation board may be used to control DIO 0's state. Please refer to Chapter 3 for information on configuring the DIP switches for use with DIO channels.

STEP 5: HyperTerminal displays **"<E",** indicating that the module is in serial command mode.

STEP 6: Type **">RBN"** in HyperTerminal and press **ENTER**, which requests the module's model name.

STEP 7: HyperTerminal displays **"<YBNNE-4100T",** indicating that the module's model name is "NE-4100T".

STEP 8: Type **">WBR1"** in HyperTerminal and press **ENTER**, which exits serial command mode.

Example 2: Use Hardware Trigger, Change IP Address

STEP 1: Verify that the hardware trigger is enabled for Serial Command Mode.

STEP 2: Check the module's serial port settings.

STEP 3: Start Windows HyperTerminal and make sure that the PC's serial port settings match the module's settings.

STEP 4: Pull DIO 0 to "Low" to enter Serial Command Mode. DIP switch 0 on the evaluation board may be used to control DIO 0's state. Please refer to Chapter 3 for information on configuring the DIP switches for use with DIO channels.

STEP 5: HyperTerminal displays **"<E",** indicating that the module is in serial command mode.

STEP 6: Type **">WNP192.168.127.253"** in HyperTerminal and press **ENTER**, which sets the module's IP address to 192.168.127.253.

STEP 7: HyperTerminal displays **"<YNP",** indicating that the IP address command was executed successfully.

STEP 8: Type **">WBR2"** in HyperTerminal and press **ENTER**, which saves changes and restarts the module.

STEP 9: Repeat STEP 1 to STEP 5 to re-enter Serial Command Mode.

STEP 10: Type **">RNP"** in HyperTerminal and press **ENTER**, which requests the module's IP address.

STEP 11: HyperTerminal displays **"<YNP192.168.127.253",** indicating that the module's IP address is 192.168.127.253.

STEP 12: Type **">WBR1"** in HyperTerminal and press **ENTER**, which exits serial command mode.

Example 3: Use Software Trigger, Get IP Mode

STEP 1: Verify that the software trigger is enabled for Serial Command Mode, and check the three trigger characters. For this example, assume the trigger is "2B 2B 2B".

STEP 2: Check the module's serial port settings.

STEP 3: Start Windows HyperTerminal and make sure that the PC's serial port settings match the module's settings.

STEP 4: Type the three trigger characters used to enter Serial Command Mode; "2B 2B 2B" in this example.

STEP 5: HyperTerminal displays **"<E",** indicating that the module is in serial command mode.

STEP 6: Type **">RNC"** in HyperTerminal and press **ENTER**, which requests the module's IP mode.

STEP 7: HyperTerminal displays **"<YNC1",** indicating that the module's IP mode is DHCP.

STEP 8: Type **">WBR1"** in HyperTerminal and press **ENTER**, which exits serial command mode.

Example 4: Use SW Trigger, Change TCP Port Number

STEP 1: Verify that the software trigger is enabled for Serial Command Mode, and check the three trigger characters. For this example, assume the trigger is "2B 2B 2B".

STEP 2: Check the module's serial port settings.

STEP 3: Start Windows HyperTerminal and make sure that the PC's serial port settings match the module's settings.

STEP 4: Type the three trigger characters used to enter Serial Command Mode; "2B 2B 2B" in this example.

STEP 5: HyperTerminal displays **"<E",** indicating that the module is in serial command mode.

STEP 6: Type **">WTL4001"** in HyperTerminal and press **ENTER**, which sets the TCP server port number to 4001.

STEP 7: HyperTerminal displays **"<YTL",** indicating that the TCP server port command was executed successfully.

STEP 8: Type **">WBR2"** in HyperTerminal and press **ENTER**, which saves all changes and restarts the module.

STEP 9: Repeat STEP 1 to STEP 5 to re-enter Serial Command Mode.

STEP 10: Type **">RTL"** in HyperTerminal and press **ENTER**, which requests the TCP server's TCP port number.

STEP 11: HyperTerminal displays **"<YTL4001",** indicating that the TCP server's TCP port number is 4001.

STEP 12: Type **">WBR1"** in HyperTerminal and press **ENTER**, which exits serial command mode.

A

Well Known Port Numbers

This appendix is included for your reference. Listed below are Well Known Port Numbers that may cause network problems if you configure WE-2100T for the same port. Refer to RFC 1700 for Well Know Port Numbers or refer to the following introduction from IANA.

The port numbers are divided into three ranges: the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports.

- The Well Known Ports are those from 0 through 1023.
- The Registered Ports are those from 1024 through 49151.
- The Dynamic and/or Private Ports are those from 49152 through 65535.

The Well Known Ports are assigned by IANA, and on most systems, can only be used by system processes or by programs executed by privileged users. Some of the most widely used ports are shown below. For more details, please visit the IANA website at http://www.iana.org/assignments/port-numbers.

TCP Socket	Application Service
0	reserved
1	TCP Port Service Multiplexor
2	Management Utility
7	Echo
9	Discard
11	Active Users (systat)
13	Daytime
15	Netstat
20	FTP data port
21	FTP CONTROL port
23	Telnet
25	SMTP (Simple Mail Transfer Protocol)
37	Time (Time Server)
42	Host name server (names server)

TCP Socket	Application Service
43	Whois (nickname)
49	(Login Host Protocol) (Login)
53	Domain Name Server (domain)
79	Finger protocol (Finger)
TCP Socket	Application Service
80	World Wibe Web HTTP
119	Netword news Transfer Protocol (NNTP)
123	Network Time Protocol
213	IPX
160 – 223	Reserved for future use

UDP Socket	Application Service
0	reserved
2	Management Utility
7	Echo
9	Discard
11	Active Users (systat)
13	Daytime
35	Any private printer server
39	Resource Location Protocol
42	Host name server (names server)
43	Whois (nickname)
49	(Login Host Protocol) (Login)
53	Domain Name Server (domain)
69	Trivial Transfer Protocol (TETP)
70	Gopher Protocol
79	Finger Protocol
80	World Wide Web HTTP
107	Remote Telnet Service
111	Sun Remote Procedure Call (Sunrpc)
119	Network news Tcanster Protocol (NNTP)
123	Network Time protocol (nnp)
161	SNMP (Simple Network Mail Protocol)
162	SNMP Traps
213	IPX (Used for IP Tunneling)

B
NECI Library

The NECI (Network Enabler Configuration Interface) library is a set of APIs that run in Windows to search, locate, and configure the WE-2100T over the network. The library supports Windows 95, 98, ME, NT, 2000, XP, and Vista. You can find the library on the Document and Software CD in the **\NECI_ LIB** folder. For additional information, please refer to the **NECI.chm** file in that folder. Examples will be located in the **.\NECI_LIB\VC\ConsoleExample** folder.

C
DIO Commands

In this appendix, we present the DIO commands used to access the Digital I/O status of the WE-2100T from an Ethernet network. The Digital I/O status can be accessed by a specific TCP port (default 5001) on the WE-2100T.

Command Packet Format

Length (Bytes)	4	1 – 255
Format	*Header	Data

Send the Command packet to the WE-2100T. The “Data” field is command specific.

ACK Packet Format

Length (Bytes)	4	1 -255
Format	*Header	Data

The WE-2100T returns by ACK packet. You can determine a DIO channel's status and mode by checking the “Data” field of the packet.

*Header Format

Length (Bytes)	1	1	1	1
Format	Command	Version (must be 2)	Command Status	Length (for data)

Check the “Command Status” to obtain the result after sending a Command packet.

Command: This field specifies the command code. For example, 1 (hex) represents “read single D I/O.” Command codes are listed later in this appendix.

Command Status: This field returns the status of the command.

0 – OK
1 – Command error; may be unknown
2 – Version error; not supported by this version
3 – Length error; the length member does not match the attached data
4 – Operation error; you cannot set the DIO mode to input mode, and set the DO status at the same time
5 – “Packet too short” error
6 – DIO number error; might not support request DIO number
0xFF – other unknown error

Data Structure Definition:

C code example:

```
//define DIO Header format
typedef struct _DIO_Header_Struct {
     char   command;
     char   version;      /* This specification is version 2 */
     char   status;
     char   length;
} DIOHeaderStruct, *pDIOHeaderStruct;

//define DIO Packet format
//Used for Command and ACK packet
typedef struct _DIO_Packet_Struct {
     DIOHeaderStruct header;
     char   data[255];
} DIOPacketStruct, *pDIOPacketStruct;
```

Command Code Usage

1. Reading Single DIO

Parameters:

Command code: 1(hex)

Version: 2(hex)

Command Status: doesn't matter

Length of data: 1(hex), represents one byte.

data[0]: Fill in the number of the DIO you wish to access. The DIO number starts from 0(hex).

Return:

Command Status: Check the Command Status code on the previous page.

Length of data: 3(hex). Must be 3 bytes of return code in this mode.

data[0]: The number of the DIO you wish to access.

data[1]: DIO mode(hex), 0 for IN, 1 for OUT

data[2]: DIO status(hex), 0 for LOW, 1 for HIGH

C code example:

```
BOOL   ReadSingleDIO(int port, int *mode, int *status)
{
          DIOPacketStruct packet;

          packet.header.command = 1;        // read single DIO command
          packet.header.version = 2;          // DIO protocol version
          packet.header.length = 1;         // data length
          packet.data[0] = (char)port;         // Number of the DIO
          send(SocketFd, (char *)&packet, sizeof(DIOHeaderStruct)+1, 0); //Send TCP Packet
         // Process the returned data here.
          return TRUE;
 }
```

2. Writing a Single DIO

Parameters:

Command code: 2(hex)

Version: 2(hex)

Command Status: doesn't matter
Length of data: 3(hex); represents three bytes.
data[0]: The number of the DIO you wish to access.
data[1]: DIO mode(hex), 0 for IN, 1 for OUT
data[2]: DIO status(hex), 0 for LOW, 1 for HIGH

Return:
Command Status: Check the Command Status code on the previous page.
Length of data: 3(hex). Must be 3 bytes of return code in this mode.
data[0]: The number of the DIO you wish to access.
data[1]: DIO mode(hex), 0 for IN, 1 for OUT
data[2]: DIO status(hex), 0 for LOW, 1 for HIGH

C code example:

```
void    WriteSingleDIO(int port, int mode, int status)
{
        DIOPacketStruct packet;

        packet.header.command = 2;      // write single DIO command
        packet.header.version = 2;      // DIO protocol version
        packet.header.length = 3;       // data length
        packet.data[0] = (char)port;    // number of the DIO
        packet.data[1] = (char)mode;    // DIO mode
        packet.data[2] = (char)status;  // DIO status;
        send(SocketFd, (char *)&packet, sizeof(DIOHeaderStruct)+3, 0); //Send TCP packet
      //Process the returned data here
}
```

3. Reading Multiple DIOs

Parameter:
Command code: 5(hex)
Version: 2(hex)
Command status: doesn't matter
Length of data: 2(hex); represents two bytes.
data[0]: Number of the DIO you wish to access first.
data[1]: The last number of the DIO you wish to access.

Return:
Command Status : Check the Command Status code on the previous page.
Length of data: (end-start+1)*2
data[0]: mode of start DIO
data[1]: status of start DIO
data[2]: mode of (start+1) DIO
data[3]: status of (start+1) DIO
….
data[(end-start)*2]: mode of end DIO
data[(end-start)*2+1]: status of end DIO

C code example:

```
BOOL     ReadMultipleDIO(int start, int end, int *mode, int *status)
{
        DIOPacketStruct packet;
```

```
            packet.header.command = 5;        // Read Multiple DIO Commands
            packet.header.version = 2;         // DIO protocol command version
            packet.header.length = 2;          // data length
            packet.data[0] = start;            // start of the DIO number
            packet.data[1] = end;              // end of the DIO number
            send(SocketFd, (char *)&packet, sizeof(DIOHeaderStruct)+2, 0); //Send TCP packet
              //Process the returned data here
              return TRUE;
    }
```

4. Writing Multiple DIOs

Parameters:

Command code: 6(hex)
Version: 2(hex)
Command status: doesn't matter
Length of data: (end-start+1)*2 + 2
data[0]: Number of the DIO you wish to access first.
data[1]: The last number of the DIO you wish to access
data[2]: mode of start DIO
data[3]: status of start DIO
data[4]: mode of (start+1) DIO
data[5]: status of (start+1) DIO
….
data[(end-start)*2+2]: mode of end DIO
data[(end-start)*2+3]: status of end DIO

Return:

Command Status: Check the Command Status code on the previous page.
Length of data : (end-start+1)*2
data[0]: mode of start DIO
data[1]: status of start DIO
data[2]: mode of (start+1) DIO
data[3]: status of (start+1) DIO
….
data[(end-start)*2]: mode of end DIO
data[(end-start)*2+1]: status of end DIO

C code example:

```
void      WriteMultipleDIO(int start, int end, int* mode, int* status)
{
          DIOPacketStruct packet;

          packet.header.command = 6;                  // Write Multiple DIO Command Codes
          packet.header.version = 2;                  // DIO protocol version
          packet.header.length = (end-start+1)*2+2;   // data length
          packet.data[0] = start;                     // start DIO number
          packet.data[1] = end;                       // end DIO number
          int       i, len;
          for ( i=0; i<(end-start+1);i++ ) {
                    packet.data[i+2] = mode[i];
                    packet.data[i+3] = status[i];
          }
send(SocketFd, )(char*)&packet,( end-start+1)*2+2+sizeof(DIOHeaderStruct), 0); //Send TCP
packet
```

```
//Process the returned data here
}
```

A utility for testing DIO access commands is provided on the Document and Software CD-ROM.

D

SNMP Agent with MIB II & RS-232 Like Group

The WE-2100T has built-in SNMP (Simple Network Management Protocol) agent software. It supports SNMP Trap, RFC1317 RS-232-like groups, and RFC 1213 MIB-II. The following table lists the standard MIB-II groups, as well as the variable implementations for WE-2100T.

RFC1213 MIB-II supported SNMP variables

System MIB	Interfaces MIB	IP MIB	ICMP MIB
SysDescr	itNumber	ipForwarding	IcmpInMsgs
SysObjectID	ifIndex	ipDefaultTTL	IcmpInErrors
SysUpTime	ifDescr	ipInreceives	IcmpInDestUnreachs
SysContact	ifType	ipInHdrErrors	IcmpInTimeExcds
SysName	ifMtu	ipInAddrErrors	IcmpInParmProbs
SysLocation	ifSpeed	ipForwDatagrams	IcmpInSrcQuenchs
SysServices	ifPhysAddress	ipInUnknownProtos	IcmpInRedirects
	ifAdminStatus	ipInDiscards	IcmpInEchos
	ifOperStatus	ipInDelivers	IcmpInEchoReps
	ifLastChange	ipOutRequests	IcmpInTimestamps
	ifInOctets	ipOutDiscards	IcmpTimestampReps
	ifInUcastPkts	ipOutNoRoutes	IcmpInAddrMasks
	ifInNUcastPkts	ipReasmTimeout	IcmpOutMsgs
	ifInDiscards	ipReasmReqds	IcmpOutErrors
	ifInErrors	ipReasmOKs	IcmpOutDestUnreachs
	ifInUnknownProtos	ipReasmFails	IcmpOutTimeExcds
	ifOutOctets	ipFragOKs	IcmpOutParmProbs
	ifOutUcastPkts	ipFragFails	IcmpOutSrcQuenchs
	ifOutNUcastPkts	ipFragCreates	IcmpOutRedirects
	ifOutDiscards	ipAdEntAddr	IcmpOutEchos

System MIB	Interfaces MIB	IP MIB	ICMP MIB
	ifOutErrors	ipAdEntIfIndex	IcmpOutEchoReps
	ifOutQLen	ipAdEntNetMask	IcmpOutTimestamps
	ifSpecific	ipAdEntBcastAddr	IcmpOutTimestampReps
		ipAdEntReasmMaxSize	IcmpOutAddrMasks
		IpNetToMediaIfIndex	IcmpOutAddrMaskReps
		IpNetToMediaPhysAddress	
		IpNetToMediaNetAddress	
		IpNetToMediaType	
		IpRoutingDiscards	

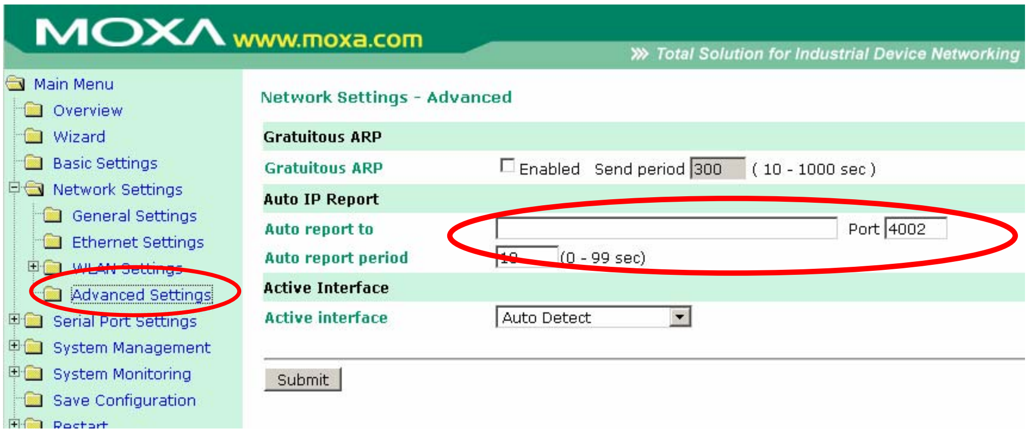
UDP MIB	TCP MIB	SNMP MIB
UdpInDatagrams	tcpRtoAlgorithm	snmpInPkts
UdpNoPorts	tcpRtoMin	snmpOutPkts
UdpInErrors	tcpRtoMax	snmpInBadVersions
UdpOutDatagrams	tcpMaxConn	snmpInBadCommunityNames
UdpLocalAddress	tcpActiveOpens	snmpInASNParseErrs
UdpLocalPort	tcpPassiveOpens	snmpInTooBigs
	tcpAttempFails	snmpInNoSuchNames
Address Translation MIB	tcpEstabResets	snmpInBadValues
AtIfIndex	tcpCurrEstab	snmpInReadOnlys
AtPhysAddress	tcpInSegs	snmpInGenErrs
AtNetAddress	tcpOutSegs	snmpInTotalReqVars

E

IP Address Report Protocol

When the WE-2100T module is configured to obtain its IP address automatically as a DHCP client, it sends a DHCP request over the network to find the DHCP server. The DHCP server will then send an available IP address to the module with an expiration time. The module will use this IP address until the expiration time has been reached. When the expiration time has been reached, the process will repeat, and module will send another DHCP request to the DHCP server. Therefore, a module may end up using more than one IP address while it is connected to the network.

To address this, the module has been designed to report its IP data to a specific IP address and port number when it is not using a static or fixed IP address. The IP address report parameters may be configured in the web console as shown below. In the **Auto report to** field, enter the IP address of the PC that will receive the IP address reports.



Network Settings - Advanced

Gratuitous ARP

Gratuitous ARP □ Enabled Send period 300 (10 - 1000 sec)

Auto IP Report

Auto report to Port 4002

Auto report period 10 (0 - 99 sec)

Active Interface

Active interface Auto Detect

IP Address Report Structure

The first 4 bytes of the module’s IP address report are the characters “Moxa”. The rest of the report is composed of 9 items, with each item preceded by a 2-byte header indicating the item ID and item length.

Header (Item ID)	Header (Item Length)	Item
(none)	(none)	“Moxa” (text string)

Header (Item ID)	Header (Item Length)	Item
1	(varies)	server name (text string)
2	2	hardware ID (little endian, see table below)
3	6	MAC address (00-90-E8-01-02-03 would be sent in sequence as 0x00, 0x90, 0xE8, 0x01, 0x02, 0x03)
4	4	serial number (little endian DWORD)
5	4	IP address
6	4	netmask
7	4	default gateway
8	4	firmware version (little endian DWORD, Version 4.3.1= 0x04030 100)
9	4	AP ID (little endian DWORD, see table below)

Hardware and AP ID

Each model is assigned a Hardware ID and AP ID as shown below:

Product	Hardware ID	AP ID
NE-4110S	0x4119	0x80004100
NE-4120S	0x4129	0x80004100
NE-4100T	0x4109	0x80004100
NE-4110A	0x4118	0x80004100
NE-4120A	0x4128	0x80004100

Example

The following example shows the first 22 bytes of a typical IP address report:

	report header "Moxa"				item ID	item Length	server name "TEST"				item ID	item Length	hardware ID 0x4119		item ID	item Length	MAC address 00-90-E8-01 -02-03					
HEX	4D	4F	58	41	01	04	54	45	53	54	02	02	19	41	03	06	00	90	E8	01	02	03
ASCII	"M"	"O"	"X"	"A"			"T"	"E"	"S"	"T"												