



IMG-111 Series Industrial M2M Gateway User Manual

Version 2.0 July, 2014

www.oring-networking.com

ORing industrial Networking Corp.



COPYRIGHT NOTICE

Copyright © 2014 ORing Industrial Networking Corp. All rights reserved.

No part of this publication may be reproduced in any form without the prior written consent of ORing Industrial Networking Corp.

TRADEMARKS

ORing is a registered trademark of ORing Industrial Networking Corp. All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

WARRANTY

ORing warrants that all ORing products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). ORing will repair or replace products found by ORing to be defective within this warranty period, with shipment expenses apportioned by ORing and the distributor. This warranty does not cover product modifications or repairs done by persons other than ORing-approved personnel, and this warranty does not apply to ORing products that are misused, abused, improperly installed, or damaged by accidents.

Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

DISCLAIMER

Information in this publication is intended to be accurate. ORing shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ORing reserves the right to revise the contents of this publication without notice.

CONTACT INFORMATION

ORing Industrial Networking Corp.

3F., No.542-2, Zhongzheng Rd., Xindian Dist., New Taipei City 23148, Taiwan (R.O.C.) Tel: +886-2-2218-1066 // Fax: +886-2-2218-1014

Website: <u>www.oring-networking.com</u>

Technical Support

E-mail: support@oring-networking.com

Sales Contact

E-mail: <u>sales@oring-networking.com</u> (Headquarters) <u>sales@oring-networking.com.cn</u> (China)



Tables of Contents

Getting	Started 1
1.1	About the IMG-111 Series1
1.2	Software Features1
1.3	Hardware Features1
Hardwa	re Overview2
2.1	Front Panel2
2.2	Front Panel LED
Hardwa	re Installation4
3.1	DIN-Rail Installation
3.2	Wall Mounting
3.3	SIM Card Installation
Cables a	and Antenna6
4.1	Ethernet Cables
4.2	Wireless Antenna
Manage	ment
5.1	Network Connection
5.2	Configuration
5.2.1	Basic Setting
W	'AN9
L	AN
D	HCP11
IP	Allocation
5.2.2	Serial Setting
Re	emote management
Se	erial Configuration
Po	ort Configuration
Se	ervice Mode15
Т	CP Server Mode
Т	CP Client Mode
U	DP Client Mode
5.2.3	Advanced Settings
N.	AT Setting
Se	ecurity Setting
V	PN Setting
Ro	outing Protocol
Μ	Tiscellaneous
5.2.4	System Tools



Date & Time
System Event
Login Setting
M2M Gateway Restart
Firmware Upgrade
Save/Restore Configurations
Remote Management
Miscellaneous (Ping)
5.2.5 System Status
System Info
System Log
Traffic Statistics
5.3 DS-tool
5.3.1 General settings
5.3.2 Security
5.3.3 Network Setting
5.3.4 Upgrade Firmware
5.3.5 Reboot Device
5.3.6 Serial Settings
5.3.7 Service Mode
Virtual COM Mode
TCP Server Mode45
TCP Client Mode
UDP Mode
Technical Specifications 49



Getting Started

1.1 About the IMG-111 Series

The IMG-111 series M2M Gateway is designed to operate in industrial environment, allowing devices to communicate with the Internet rapidly and efficiently over the LAN. The series consists of the IMG-111 and IMG-111-2G models to meet customers' different needs. The series comes with a RS-232 interface which enables users to access RS-232 data via 3.5G/2G connections. With built-in WAN connections, the series can be



mounted in harsh environment easily to provide Internet access anytime and anywhere. The device also provides VPN capability to create encrypted virtual tunnels through the Internet, ensuring remote or mobile users safe connections to office networks.

1.2 Software Features

- 2G GSM/GPRS or 3.5G HSUDPA modem included
- Supports Open VPN, PPTP VPN
- Update DNS hostname: DDNS
- Versatile modes & event alarm by e-mail.
- Event warning by Syslog, Email, SNMP Trap, Relay output
- Redundant multiple host devices:
- 5 host devices: Virtual COM, TCP Server, TCP Client mode; UDP
- 4 IP Ranges: UDP

1.3 Hardware Features

- 1 x 10/100Base-T(X) Ethernet ports for LAN connection
- 1 x RS-232 Interface
- 1 x SIM card slot
- Power Inputs: 12~48 VDC
- Casing: IP-30
- Din-Rail and panel mounting enabled.
- Operating Temperature: -10 to 60°C
- Storage Temperature: -40 to 85°C
- Operating Humidity: 5% to 95%, non-condensing



Hardware Overview

2.1 Front Panel

The device provides the following ports on the front panel.

Port	Description
Ethernet port	1 x 10/100Base-T(X) copper ports
RS-232 port	1 x RS-232 Serial port
Reset button	Press the button for 3-5 seconds to reset the device.
SIM card slot	1 x SIM card slot
Antenna connector	1 x antenna connector



- 1. Fault LED. .
- 2. Status LED
- 3. Power LED
- 4. WAN LED
- 5. Serial transmission LED
- 6. RS-232 Serial port
- 7. 10/100Base-T(X) RJ45 fast Ethernet port



- 8. Reset button
- 9. GSM/DCS/UMT antenna for internal modem
- 10. SIM card slot

2.2 Front Panel LED

LED	Color	Status	Description
PWR	Green	On Power On.	
Statua	Green	On	Device is ready
Sialus		Blinking	Booting up
Fault	Amber	On	WAN connection fails (enable event
			through web)
\A/A NI	Croon	On	Modem is ready
VVAIN	Green	Blinking	Checking modem status
сти	Amber	On	Port speed at 10Mbps
	Green	On	Port speed at 100Mbps



Hardware Installation

3.1 DIN-Rail Installation

The device comes with a DIN-Rail kit in the package. The DIN-Rail kit allows you to fasten the device to a DIN-Rail.

Installing the device on the DIN-rail is easy. First, screw the Din-rail kit onto the back of the device, right in the middle of the back panel. Then slide the device onto a DIN-rail from the Din-rail kit and make sure the device clicks into the rail firmly.



3.2 Wall Mounting

Besides Din-rail, the device can be fixed to the wall via a wall mount panel, which can be found in the package.

Follow the steps below to install the device to a rack.

Step 1: Install the L-shape mounting kits provided in the package to the left and right of the device.

Step 2: With front brackets orientated in front of the rack, mount the device in the rack with four rack-mounting screws.





3.3 SIM Card Installation

After disconnecting the power of the device:

- 1. Un-fasten the screws.
- 2. Remove the cover

Note: only remove the cover for SIM card installation. DO NOT remove the cover in normal operation.

- 3. Insert the SIM card into the slot.
- 4. Put the cover back
- 5. Fasten the screws.

Note: Make sure the power is off before you install the SIM card.



Cables and Antenna

4.1 Ethernet Cables

The device has standard Ethernet ports. According to the link type, the device uses CAT 3, 4, 5,5e UTP cables to connect to any other network devices (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications:

Cable	Туре	Max. Length	Connector
10Base-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ45
100Base-T(X)	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ45

With 10/100Base-T(X) cables, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

10/100 Base-T(X) RJ-45 Port Pin Assignments:

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

The device supports auto MDI/MDI-X operation. You can use a cable to connect the switch to a PC. The table below shows the 10/100Base-T(X) MDI and MDI-X port pin outs.

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used

10/100 Base-T(X) MDI/MDI-X Pin Assignments:



5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.

4.2 Wireless Antenna

A GSM/DCS/UMT antenna is used for the built-in modem. You can also use an external RF cable and antenna for this connector.



Cellular Antenna



<u>Management</u>

5.1 Network Connection

Before installing the device, you need to be able to access the device via a computer equipped with an Ethernet card or wireless LAN interface. To simplify the connection, it is recommended to use an Ethernet card to connect to a LAN.



Step 1: Select power source. The device can be powered by +12~48V DC power input. **Step 2**: Connect a computer to the device. Use either a straight-through Ethernet cable or cross-over cable to connect the device to a computer. Once the LED of the LAN port lights up, which indicates the connection is established, the computer will initiate a DHCP request to retrieve an IP address from the device.

Step 3: Configure the device on a web-based management utility. Open a web browser on your computer and type http://192.168.10.1 (default gateway IP of the device) in the address box to access the webpage. A login window will pop up where you can enter the default login name admin and password admin. For security reasons, we strongly recommend you to change the password. Click on **System Tools** > **Login Setting** after logging in to change the password.



Address 실 192, 168, 10,	1			🖌 🄁 Co
	Connect to 192.1	68.10.1	? 🔀	
		G		
	Login			
	<u>U</u> ser name:	S	×	
	<u>P</u> assword:			
		Remember my password		
		ОК	Cancel	

After you log in successfully, a Web interface will appear, as shown below. On the left hand side of the interface is a list of functions where you can configure the settings. The details of the configurations will be shown on the right screen.

ORING	M2M 1 Port Serial Gateway	
	Firmware Ver: 1.0e Wan IP: Uptime: 01:22:51	www.oring-networking.com
B Home	Home	
Basic Setting Serial Setting Advanced Setting System Tools System Status	Welcome to M2M 1 Port Serial Gateway configuration page.	

5.2 Configuration

On top of the Home screen shows information about the firmware version, uptime, and WAN

IP address.

Label	Description
Firmware	Shows the current firmware version
Uptime	Shows the elapsed time since the AP device is started
Wan IP	Shows WAN IP address

5.2.1 Basic Setting

This section will guide you through the general settings for the device.

WAN

This page allows you to configure WAN settings. Different WAN connection types will have different settings.



Basic Setting> WAN	
WAN Settings.	
Phone Number:	
APN:	
User Name:	
Password:	
Baud Rate:	460800 💌
PIN:	Enable PIN check before dialing
	PIN Code:
Auto Connect :	✓ Enable
Reconnect on Failure:	✓ Enable
Fast Mode:	Enable
Device Status :	Ready.
Operations :	Connect Disconnect
Link Status :	Disconnected
Modem Status:	Operator:
	RadioType:
	Signal Quality:
Auto recheck:	00h:00m:00s 🗖
Save Refresh	Cancel

Label	Description
Phone Number	Telephone number provided by your ISP
APN	Enter the APN value (optional)
User Name	Enter the user name provided by your ISP
Password	Enter the password provided by your ISP
PIN	Enter the PIN code if PIN check is required
Auto Connect	If this option is enabled, the connection will be called up when
	M2M Gateway boots up
Device Status	Show the status of built-in modem device.
Operations	Click "Connect" to call up the built-in modem.
	Click "Disconnect" to shut down the connection
Link Status	Show the status of connection, up, down or connecting
Auto recheck	Enable auto refresh modem status per 28 sec

LAN

These are the IP settings of the LAN interface for the IMG-111 M2M Gateway. The LAN IP address is privately for your internal network and cannot be exposed on the Internet.



Basic Setting> LAN	
LAN Side settings.	
Router Name:	IR71001210F
IP Address:	192.168.10.1
Subnet Mask:	255.255.0

Label	Description
Router Name	Enter the name of your device
IP Address	The IP address of the LAN. The default value is 192.168.10.1
Subnet Mask	The subnet mask of the LAN. The default value is 255.255.255.0

DHCP

DHCP stands for Dynamic Host Control Protocol. The IMG-111 was built-in DHCP server. The internal DHCP server will assign an IP address to the computers (DHCP client) on the LAN automatically.

Set your computers to be DHCP clients by setting their TCP/IP settings to obtain an IP address automatically. The DHCP server will allocate an unused IP address from the IP address pool to the requesting computer automatically.

Basic Setting> DHCP -> DHCP Server			
Set DHCP Server.			
DHCP Server:	⊙Enabled ○Disabled		
Starting IP:	192.168.10.2		
Ending IP:	192.168.10.100		
Lease Time:	48 Hours		
Local Domain Name:	(optional)		
Current DHCP Client Information			
# HostName	Mac	IP	Expires In
Static IP Allocation Setup			

Label	Description
DHCP Server	Enables or disables the DHCP server function. The default setting
	is Enabled .
Starting IP	The starting IP address of the IP range assigned by the DHCP
	server
Ending IP	The ending IP address of the IP range assigned by the DHCP
	server



Lease Time	The period of time for the IP address to be leased. During the lease	
	time, the DHCP server cannot assign that IP address to any other	
	clients. Enter a number in the field. The default setting is 48 hours.	
Local Domain Name	Enter the local domain name of a private network (optional)	
Current DHCP	List of the computers on your network that are assigned an IP	
Client Information	address by internal DHCP server.	

IP Allocation

IP allocation provides one-to-one mapping of MAC address to IP address. When computers with the MAC address requesting an IP from IMG-111, it will be assigned with the IP address according to the mapping. You can choose one from the client list and add it to the mapping relationship.

Basic Setting> DHCP -> IP Allocation		
Allocate IP Address Manually.		
Choose a Client to Edit 💌 Copy to		
MAC Address	IP Address	
MAC Address	IP Address	Add Clear
MAC Address Static DHCP Client List:	IP Address	Add Clear

Label	Description	
Choose a Client to Edit	The list shows the MAC addresses and IP addresses that are	
	already assigned by IMG-111. Choose one from the list and click	
	Copy to button for editing.	
MAC Address	The MAC addresses of the computer.	
IP Address	The IP address to be related to the MAC address.	
Static DHCP Client List	Shows the IP addresses locked to specific MAC addresses	

5.2.2 Serial Setting

Remote management

The remote management setting allows user to enable the WAN access of the DS-tool management and serial port access.



Ser2net Setting>Remote management		
Set the Remote Management enable DS-tool to access from WAN.		
Remote management:	○ Enable ⊙ Disable	
Port External Access:		
Port1:	○Enable ⊙Disable	
Apply Cancel		

Label		Description
Remote		Enable to managed IMG-111 by DS-tool through WAN access
Managem	ent	
Port	External	Enable to allow using of serial data port and control port through
Access		WAN access I

Serial Configuration

This page allows you to configure serial port parameters.

Ser2net Setting>	Serial Configuration
------------------	----------------------

	Port1
Port Alias	Port1
Interface	RS232 💌
Baud Rate	38400 💌
Data Bits	8 🛩
Stop Bits	1 💌
Parity	None 💌
Flow Control	None 💌
Force TX Interval Time	0 ms
Performance	Throughput O Latency
Apply Cancel	



Label	Description
Port Alias	Remark the port to hint the connected device
Interface	RS422 / RS485(2-wires) / RS485(4-wires)
Boud roto	110bps/300bps/1200bps/2400bps/4800bps/9600bps/19200bps/
Baud rate	38400bps/57600bps/115200bps
Data Bits	5, 6, 7, 8
Stop Bits	1, 2 (1.5)
Parity	No, Even, Odd, Mark, Space
Flow Control	No, XON/XOFF
	Force TX interval time is to specify the timeout when no data has
Force TV Interval Time	been transmitted. When the timeout is reached or TX buffer is full
Force 1X Interval Time	(4K Bytes), the queued data will be sent. 0 means disable.
	Factory default value is 0
Performance	Throughput: This mode is optimized for the highest transmission
	speed.
	Latency: This mode is optimized for the shortest response time.

Port Configuration

Ser2net Setting> Port Configuration	
	Port1
Local TCP Port	4008
Command Port	4009
Mode	Serial to Ethernet
Flush Data Buffer After	0 ms
Delimiter(Hex 0~ff)	1: 00 2: 00 3: 00 4: 00
Mode	Ethernet to Serial
Flush Data Buffer After	0 ms
Delimiter(Hex 0~ff)	1: 00 2: 00 3: 00 4: 00
Apply Cancel	

Label	Description
Serial to Ethernet	Flush Data Buffer After:
	The received data will be queued in the buffer until all the delimiters are
	matched. When the buffer is full (4K Bytes) or after "flush S2E data
	buffer" timeout, the data will also be sent. You can set the time from 0
	to 65535 second.

	Delimiter:
	You can define max. 4 delimiters (00~FF, Hex) for each way. The data
	will be hold until the delimiters are received or the option "Flush Serial to
	Ethernet data buffer" times out. ${f 0}$ means disable. Factory default is ${f 0}$
	Flush Data Buffer After:
Ethernet to serial	The received data will be queued in the buffer until all the delimiters are
	matched. When the buffer is full (4K Bytes) or after "flush E2S data
	buffer" timeout, the data will also be sent. You can set the time from 0 to
	65535 seconds.
	Delimiter:
	You can define max. 4 delimiters (00~FF, Hex) for each way. The data
	will be hold until the delimiters are received or the option "Flush Ethernet
	to Serial data buffer" times out. ${f 0}$ means disable. Factory default is ${f 0}$

Service Mode Virtual COM Mode

In Virtual COM mode, the driver establishes a transparent connection between host and serial device by mapping the port of the serial server serial port to a local COM port on the host computer. The Virtual COM mode also supports up to 5 simultaneous connections, so that multiple hosts can send or receive data by the same serial device at the same time.

Serzhet Setting> Service Mode	
	Port1
Data Encryption	○ Enable ④ Disable
Service Mode	Virtual COM Mode 💌
Idle Timeout	10 (0~65535)seconds
Alive Check	20 (0~65535)seconds
Max Connection	1 v max. connection (1~5)
Apply Cancel	

Label	Description
Data Encryption	Use SSL to encrypt data.
Idle Timeout	When serial port stops data transmission for a defined period of
	time (Idle Timeout), the connection will be closed and the port will
	be freed and try to connect with other hosts. 0 indicate disable
	this function. Factory default value is 0 . If Multilink is configured,
	only the first host connection is effective for this setting.
Alive Check	The serial device will send TCP alive-check package in each

ORing Industrial Networking Corp.

	defined time interval (Alive Check) to remote host to check the
	TCP connection. If the TCP connection is not alive, the
	connection will be closed and the port will be freed. ${\bf 0}$ indicate
	disable this function. Factory default is 0.
Max Connection	The number of maximum connections can be supported. The
	maximum value is 5 , default values is 1 .

*Not allowed to mapping Virtual COM from web

TCP Server Mode

In TCP Server mode, IMG is configured with a unique port combination on a TCP/IP network. In this case, IMG waits passively to be contacted by the device. After the device establishes a connection with the serial device, it can then proceed with data transmission. The TCP Server mode also supports up to 5 simultaneous connections, so that multiple device can receive data from the same serial device at the same time.

Ser2net Set	ting>	Service	Mode
-------------	-------	---------	------

	Port1
Data Encryption	○ Enable
Service Mode	TCP Server Mode 💌
TCP Server Port	4008
Idle Timeout	10 (0~65535)seconds
Alive Check	20 (0~65535)seconds
Max Connection	1 v max. connection(1~5)
Apply Cancel	

Label	Description
Data Encryption	Use SSL to encrypt data.
TCP Server Port	Set the port number for data transmission.
Idle Timeout	When serial port stops data transmission for a defined period of
	time (Idle Timeout), the connection will be closed and the port will
	be freed and try to connect with other hosts. ${\boldsymbol 0}$ indicate disable this
	function. Factory default value is 0. If Multilink is configured,
	only the first host connection is effective for this setting.
Alive Check	The serial device will send TCP alive-check package in each
	defined time interval (Alive Check) to remote host to check the
	TCP connection. If the TCP connection is not alive, the



	connection will be closed and the port will be freed. 0 indicate
	disable this function. Factory default is 0 .
Max Connection	The number of maximum connections can be supported. The
	maximum value is 5 , default values is 1 .

TCP Client Mode

In TCP Client mode, the device can establish a TCP connection with a server by the method you set (Startup or any character). After the data has been transferred, device can disconnect automatically from the server by using the TCP alive check time or Idle timeout settings.

Ser2net Setting> Service Mode	
	Port1
Data Encryption	◯ Enable ④ Disable
Service Mode	TCP Client Mode
Destination Host	0.0.0.0 : 4008
Idle Timeout	10 (0~65535)seconds
Alive Check	20 (0~65535)seconds
Connect on	Startup ○ Any Character
Destination Host	Port
1.	65535
2.	65535
3.	65535
4.	65535
Apply Cancel	

Label	Description
Data Encryption	Use SSL to encrypt data.
Destination Host	Set the IP address of host and the port number of data port
	When serial port stops data transmission for a defined period of
	time (Idle Timeout), the connection will be closed and the port will
Idle Timeout	be freed and try to connect with other hosts. ${\boldsymbol 0}$ indicate disable this
	function. Factory default value is ${f 0}$. If Multilink is configured, only
	the first host connection is effective for this setting.
	The serial device will send TCP alive-check package in each
Alive Check	defined time interval (Alive Check) to remote host to check the
	TCP connection. If the TCP connection is not alive, the
	connection will be closed and the port will be freed. 0 indicate



	disable this function. Factory default is 0.			
Connact on Startun	The TCP Client will build TCP connections once the connected			
Connect on Startup	serial device is started.			
Connect on Any	The TCP Client will build TCP connections once the connected			
Character	serial device starts to send data.			

UDP Client Mode

Compared to TCP communications, UDP is faster and more efficient. In UDP mode, you can Uni-cast or Multi-cast data from the serial device server to host computers, and the serial device can also receive data from one or multiple host

Ser2net Setting> Service Mod	Ser2net Setting> Service Mode					
	Port1	Port1				
Service Mode	UDP Mode					
Listen Port	4008					
Host start IP	Host end IP	Send Port				
1.		65535				
2.		65535				
3.		65535				
4.		65535				
Apply Cancel						

5.2.3 Advanced Settings

NAT Setting

Virtual Server

Virtual Server is used for setting up public services on the LAN, such as DNS, FTP and Email. Virtual Server is defined as a Local Port to the LAN servers, and all requests from Internet to this Local port will be redirected to the computer specified by the Local IP.

Any PC that was used for a virtual server must have static or reserved IP Address because its IP address may change when requesting IP by DHCP



Advanced S	etting> NAT Se	tting -> Virtua	al Server					
Virtual serve	er settings.							
Virtual Serve	er:	🔿 Enable 💿	Disable					
Description:								
Public IP:		💿 All _O Spe	cify					
Public Port:								
Protocol:			P 🔿 Both					
Local IP:								
Local Port:								
Enable Now	:	💿 Yes 🔵 No						
		Add Can	cel					
Virtual serve	er list:							
#	Description	Public IP	Public Port	Protocol	Local IP	Local Port	Enabled	Ops

Label	Description
Virtual Server	Enable or disable Virtual Server
Description	Enter the description of the entry. Acceptable characters consist of
	'0-9', 'a-z', 'A-Z'. This field accepts null value.
Public IP	Enter a public IP allowed to access the virtual service. If not specified,
	choose All.
Public Port	The port number on the WAN (Wide Area Network) side that will be
	used to access the virtual service.
Protocol	The protocol used for the virtual service
Local IP	The IP address of the computer that will provide virtual service
Local Port	The port number of the service used by the private IP computer
Enable Now	Enables the virtual server entry after adding it
Virtual server list	Click Edit to edit the virtual service entry and Del to delete the entry.

Port Trigger

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT M2M Gateway. Port Trigger is used for some of the applications that can work with an NAT M2M Gateway



Advanced Setting> NAT 9	Setting ->	Port Trigger					
Port Trigger settings.							
Port Trigger:	🔿 Enal	ole 💿 Disable					
Description:							
Trigger Port:							
Trigger Protocol:	🔿 ТСР	⊖ UDP ⊖ Bo	th				
Incoming Port:							
Incoming Protocol:	🔿 ТСР	⊖ UDP ⊖ Bo	th				
Enable:	🔵 Yes	🔿 No					
	Add	Cancel					
Port Trigger List:							
# Description		Trigger Protocol	Trigger Port	Incoming Protocol	Incoming Port	Enable	Ops

Label	Description
Port Trigger	Enable or disable Port Trigger
Description	Enter the description for the entry
Trigger Port	This is the port used to trigger the application.
Trigger Protocol	This is the protocol used to trigger the application.
Incoming Port This is the port number on the WAN side that will be used to acce	
	the application.
Incoming Protocol	This is the protocol used for incoming port.
Enable Now	Enable the rule after adding the entry
Port Trigger List	Click Edit to edit the entry, click Del to delete the entry

DMZ

DMZ (Demilitarized Zone) allows a computer to be exposed to the Internet without passing through the security settings and therefore is unsecured. This feature is useful for special purposes such as gaming.

To use this function, you need to set an internal computer as the DMZ host by entering its IP address. Adding a client to the DMZ may expose your local network to a variety of security risks, so use this function carefully.



Advanced Setting> NAT S	etting -> DMZ				
DMZ settings.					
DMZ:	🔿 Enable 💿 Disable				
Description:]			
DMZ Host IP:					

Label	Description
DMZ	Enables or disables DMZ
Description	Enter a description for the DMZ host entry
DMZ Host IP	Enter the IP address of the computer to act as the DMZ host

UPnP

The UPnP (Universal Plug and Play) feature allows Internet devices to access local host resources or devices as needed. UPnP-enabled devices can be automatically discovered by the UPnP service application on the LAN.

Advanced Setting> N	NAT Setting -> UPnP				
UPnP settings.					
UPnP:	 Enabled O Disabled Enable NAT-PMP 				
UPnP List:					
#	Application	Ext Port	Protocol	Int Port	IP Address

Label	Description				
UPnP	Enable or disable UPnP.				
Enable NAT-PMP	NAT-PMP allows a computer in a private network (behind a NAT				
	router) to automatically configure the device to allow parties				
	outside the private network to contact with each other. NAT-PMP				
	operates with UDP. It essentially automates the process of port				
	forwarding. Check the box to enable NAT-PMP.				
UPnP List	P List This table lists the current auto port forwarding information.				
	Application: The application that generates this port forwarding.				
	Ext Port: The port opened on WAN				
	Protocol: The protocol type				
	Int Port: The port redirected to the local computer				
	IP Address: The IP address of local computer to be redirected to				



Security Setting

IP Filter

IP filters enable you to control the forwarding of incoming and outgoing data between your LAN and the Internet and within your LAN. This control is implemented via IP filter rules which are defined to block attempts by certain computers on your LAN to access certain types of data or Internet locations. You can also block incoming access to computers on your LAN.

ID filter cottings							
IP filter settings.							
IP Filter:	🔿 Enable 💿 D	isable					
Description:							
Rule:	DROP 💌						
Direction:	LAN->WAN 🔽						
IP Address:	Source IP:						
	Destination IP:						
Protocol:	⊖ All						
	○ ICMP						
	Specify prote	col number:					
	TCP	Specify po	ort:				
	O UDP	Specify po	ort:				
Enable Now:	💿 Yes 🔿 No						
	Add Cance	el					
IP filter list:							
# Description	Rule Direction	Source IP	Destination IP	Protocol	Port	Enabled	Operations

Label	Description
IP Filter	Enables or disables the IP Filter
Description	Enter description for the entry.
Rule	Configures the rules to be applied to the IP filter. Available options include
	DROP, ACCEPT, and REJECT.
Direction	Specif the direction of data flow to be filtered
IP Address	Enter the IP address of the source and destination computer
Protocol	Choose which protocol to be filtered.
Enable Now	Enable the entry after adding it
IP Filter List	Click edit for editing the entry, click Del to delete the entry.

MAC Filter

This page enables you to deny or allow LAN computers to access the Internet based on their MAC addresses.

ORing Industrial Networking Corp.



Advanced Setting> Security Setting -> MAC Filter					
MAC Filter set	tings.				
MAC Filter:	🔿 Enat	ble 💿 Disable			
Description:					
Rule:	DROP	V			
MAC Address:		(e.x. 00:11)	22:aa:bb:cc)		
Enable Now:	Yes	O No			
	Add	Cancel			
MAC filter list:					
#	Description	Rule	MAC Address	Enabled	Operations

Label	Description	
MAC Filter	Enables or disables the MAC Filter	
Description	Enter description for the entry	
Rule	Configures the rules to be applied to the MAC filter. Available	
	options include DROP, ACCEPT, and REJECT.	
MAC Address	Enter the MAC address to be filtered	
Enable Now	Click Yes to enable the entry after adding it	
MAC Filter List	Shows the information of all MAC filters.	

VPN Setting Open VPN

Open VPN is a full-functioned SSL VPN solution which can accommodates a wide range of configurations including remote access, site-to-site VPNs, WiFi security, and enterprise-scale remote access solutions with load balancing, failover, and fine-grained access-controls.



Advanced Setting> V	Advanced Setting> Vpn Setting -> Openvpn	
Openvpn settings.		
Server settings.		
Openvpn Server:	○ Enable ⊙ Disable	
Tunnel Protocol:	UDP 💌	
Port:	1194	
LZO Compression:	💿 Enable 🔿 Disable	
Keys Setting:	Auto 🔽	
Diagnosis		
Client settings.		
Openvpn Client:	🔿 Enable 💿 Disable	
Server IP :		
Tunnel Protocol:	UDP 💽	
Port:	1194	
LZO Compression:	⊙ Enable ○ Disable	
Keys Setting:	Auto 🔽	
Diagnosis		

The following topology shows the common use of VPN connection from WAN side



1: Open VPN Server

Connection to Open VPN Server

Before connecting to the Open VPN server of IMG-111 M2M Gateway, please install Open VPN client software for your windows PC. It can be downloaded from http://Open



VPN.net/download.html#stablel. The current version of Open VPN used in IMG-111 is version 2.0.9. The corresponding software for client should be installed

Label	Description	
Open VPN Server	Enables or disables the function of Open VPN server	
Tunnel Protocol	Select UDP or TCP protocol depending on your needs. TCP is	
	more reliable than UDP, but UDP performs better than TCP. It is	
	recommended to use UDP if the distance between VPN server	
	and client is short; otherwise, use TCP.	
Port	The number of the port (default is 1194).	
LZO Compression	Enables or disables the function of LZO Compression	
Keys Setting	Select Auto to use preset certificates or Manual to use your	
	certificates. Please install openvpn client software to generate	
	your certificates and paste them here. For more information,	
	please visit openvpn website.	

2: Open VPN Client

Two M2M Gateways are needed for creating site-to-site VPN connection using this mode

Label	Description	
Open VPN Client	Enables or disables the function of Open VPN client.	
Server IP/Host Name	Enter the Open VPN server IP address	
Tunnel Protocol	Select UDP or TCP protocol depending on your needs. TCP is	
	more reliable than UDP, but UDP performs better than TCP. It is	
	recommended to use UDP if the distance between VPN server	
	and client is short; otherwise, use TCP.	
Port	The number of the port (default is 1194).	
LZO Compression	Enables or disables the LZO Compression	
Keys Setting	Select Auto to use preset certificates or Manual to use your	
	certificates. Please install openvpn client software to generate	
	your certificates and paste them here. For more information,	
	please visit openvpn website.	



3: Open VPN Server VS Client



Open VPN Server and Client Connection

The chart above displays the connection of Open VPN Server and Client. The Server IP and Client IP address should configure with the same network domain.

PPTP VPN

PPTP (Point to Point Tunneling Protocol) VPN allows PCs connected to the router through WAN ports to act as PCs in the same LAN.





To create a PPTP connection to the router, you must create a new network connection on your Windows PC by right clicking **Network > Property > Create a new connection > Connect to my work space (VPN) > Use VPN to Internet**, and then enter the user name and password set in the page.

After setting up a new connection, you can make configurations in the following page.

Advanced Setting> Vpn Setting -> PPTP Vpn	
PPTP Server settings.	
PPTP Server	🔿 Enable 💿 Disable
Server IP :	192.168.10.1
Clients IP:	192.168.10.150-180
PPP Options:	🗌 require-chap
	🗌 require-mschap
	🗹 require-mschap-v2
	🗹 require-mppe
Routing Option:	Enable Routing Protocols through PPTP VPN Connection
CHAP-Secrets:	admin * admin *

Label	Description
PPTP Server	Enables or disables PPTP VPN server
Server IP	Enter the server IP address. The default value is the IP address of the
	connected LAN port.
Client IP	Enter the IP address range in the form of 192.168.10.xx-xx. The



	connected client will be assigned with an IP address.	
PPP Options	Require-chap: check to use chap authentication on your PPTP server	
	Require-mschap: check to use mschap authentication on your PPTP	
	server	
	Require-mschap-v2: check to use mschap-v2 authentication on your	
	PPTP server	
	Require mppe: check to use MPPE (Microsoft Point-to-Point	
	Encryption) encryption on data transmitted through PPP (Point-to-Point	
	Protocol) and VPN links.	
Routing Option	Check to enable routing protocols through PPTP VPN connections	
CHAP-Secrets	Enter the username and password pairs in the form of user * pass * .	
	Multiple username and password pairs are allowed.	

PPTP Client

If a router wants to link to the device in different networks, you should enable PPTP client in the following page.





Advanced Setting> Vpn Setting -> PPTP Client	
PPTP Client settings.	
PPTP Client	O Enable 💿 Disable
Server IP/Hostname:	
Username:	
Password:	
Options:	Reconnect on failure
	default route
	🗌 require-chap
	require-mschap
	🗹 require-mschap-v2
	🗹 require-mppe
Routing Option:	Enable Routing Protocols through PPTP Client Connection
Operations:	Connect Disconnect
Link Status:	Disconnected

Label	Description	
PPTP Client	Enables or disables PPTP client	
Server	Enter the conver ID address or bestrome	
IP/Hostname		
Username/Pas	Enter the vegeneers and personnel engineer by DDD conver	
sword	Enter the username and password assigned by PPTP server	
	Choose the rules to be applied	
	Reconnect on failure: prompts automatic reconnection when the link	
	fails.	
	Require-chap: check to use chap authentication on your PPTP server	
	Require-mschap: check to use mschap authentication on your PPTP	
Options	server	
	Require-mschap-v2: check to use mschap-v2 authentication on your	
	PPTP server	
	Require MPPE: check to use MPPE (Microsoft Point-to-Point	
	Encryption) encryption on data transmitted through PPP (Point-to-Point	
	Protocol) and VPN links.	
Operations	Click Connect to link to the server or Disconnect to disconnect from the	
	server	
Link Status	Show the status of the link	

Routing Protocol Routing Setting

ORing Industrial Networking Corp.



This page shows the information of the routing table. You can configure static and dynamic routing settings in this page.

Destination	Gateway	Subnet Mask	Metric	Interface
192.168.10.0	0.0.0.0	255.255.255.0	0	br0(LAN)
127.0.0.0	0.0.0.0	255.0.0.0	0	lo(LOOPBACK)

Static Routing

When RIPv1 & v2 is **Disabled**, the router will operate in static routing mode, which means devices forward packets using either route information from route table entries that you manually configure or the route information that is calculated using dynamic routing algorithms.

Advanced Setting> Routing Protocol -> Routing Setting				
Current Routing Table:				
Destination	Gateway	Subnet Mask	Metric	Interface
192.168.10.0	0.0.0.0	255.255.255.0	0	br0(LAN)
127.0.0.0	0.0.0.0	255.0.0.0	0	lo(LOOPBACK)

Static Route Entry:

Destination	Gateway	Subnet Mask	Metric	Interface	Oper	ations
192.168.11.0	0.0.0.0	255.255.255.0	0	WAN	Commit	Deete
Destination	Gateway	Subnet Mask	Metric	Inter	face	Operation
				WAN	1 💙	Add
Mode: RIPv1 & v2:	Gateway Disable Cateway Disable Disable Port: 23 Password: Cateway Disable Di					

Dynamic Routing

Dynamic routing lets routing tables in devices change as the routes change. If the best path to a destination cannot be used, dynamic routing protocols change routing tables when necessary to keep your network traffic moving. Dynamic routing protocols include RIP, OSPF, and BGP; however, the device only supports RIP (Routing Information Protocol).

Do not choose **Disable** in the RIPv1 & v2 list if you want to enable Dynamic Routing. After clicking **Apply**, more information will be displayed in Current Routing Table.



Advanced Setting --> Routing Protocol -> Routing Setting

Current Routing Table:

Destination	Gateway	Subnet Mask	Metric	Interface	
192.168.10.0	0.0.0.0	255.255.255.0	0	br0(LAN)	
127.0.0.0	0.0.0.0	255.0.0.0	0	lo(LOOPBACK)	

Static Route Entry:

Destination	Gateway	Subnet Mask	Metric	Interface	Operations	
Destination	Gateway	Subnet Mask	Metric	Interface	:	Operation
				WAN 💌		Add

Mode: RIPv1 & v2:	Gateway 👻
Telnet Setting:	🔿 Enable 💿 Disable
	Port: 23
	Password:

Label	Description
Current	Shows all routing information, including static and dynamic routing (if
Routing Table	enabled)
Static Route	Fills in corresponding information to add new entries to the static routing
Entry	tablet
	Destination: Specifies the destination network for this static route.
	Gateway: Specifies the gateway for the destination network that is
	specified in this static route.
	Subnet Mask: The Subnet Mask determines which portion of an IP
	address is the network portion, and which portion is the host portion.
	Metric: Specifies an integer value of the relative preference of this route
	against other defined routes that have the same IP address.
	Interface: Depending on where the Destination IP Address is located,
	select LAN & WLAN or WAN from the Interface drop-down menu.
Mode	Choose Gateway Mode if you want PCs in the LAN to visit external
	network, otherwise choose Router Mode
RIPv1 &v2	Choose Disable to disable dynamic routing or other options to configure
	the interfaces for dynamic routing
Telnet Setting	This option is only available when dynamic routing is enabled. It allows
	you to make detailed configurations via simple comments.



	Telnet 192.168.10.1
	Command incomplete.
	lello, this is zebra (version 0.94).
	Copyright 1996-2002 Kunihiro Ishiguro.
	[APR654978>
	enable Turn on privileged mode command exit Exit current mode and down to previous mode
	ListPrint command listpingsend echo messagesquitExit current mode and down to previous modeshowShow running system informationtelnetOpen a telnet connectiontracerouteTrace route to destination
Port	Enter a port number for the entry
Password	Enter a password for the entry



Routing Topography

Miscellaneous

DDNS

DDNS (Dynamic Domain Name System) allows you to configure a domain name for your IP address which is dynamically assigned by your ISP. Therefore, you can use a static domain name that always points to the current dynamic IP address.



Advanced Setting> Miscellaneous> DDNS				
DDNS settings.				
DDNS Service:				
Apply Cancel	disable www.3322.org www.dhs.org www.dyndns.org www.tzo.org www.easydns.org http://gnudip.cheapnet.net www.ods.org www.justlinux.com			

Label	Description
DDNS Service	Choose a DDNS service provider from the list

5.2.4 System Tools

Date & Time

In this page, you can set the date & time of the device. A correct date and time will help the system log events. You can set up a NTP (Network Time Protocol) client to synchronize date & time with a NTP server on the Internet.

System Tools> Date & Time			
Date/Time settings.			
Local Date:	2010 Year 1 Month 1 Day		
Local Time:	0 Hour 20 Minute 58 Second		
Time Zone:	GMT+08:00 💌		
	Get Current Date & Time from Browser		
NTP:	🗹 Enable		
NTP Server 1:	pool.ntp.org		
NTP Server 2:	time.nist.gov (optional)		
Synchronise:	Every Day 🖌 🖌 at 00 🖌 : 00 🖌		



Label	Description
Local Date	Set a local date manually
Local Time	Set local time manually.
Time Zone	Select the time zone manually
Get Current Date &	Click this button; you can set the time from your browser
Time from Browser	
NTP	Enable or disable NTP function to synchronize time from the NTP
	server
NTP Server 1	The primary NTP Server
NTP Server 2	The secondary NTP Server
Synchronize	This is the scheduled time when the NTP synchronization
	performed

System Event

When the WAN Link Down option is enabled, the system will notify you when the link is down.

System Tools --> System Event

WAN Link Down Alarm

- 💿 Disable WAN Link Down Alarm
- Enable WAN Link Down Alarm

Login Setting

You can change login name and password in page. The default login name and password are both **admin**.



System Tools --> Login Setting

Login settings.	
Old Login Name:	admin
Old Password:	
New Login Name:	admin
New Password:	•••••
Confirm New Password:	•••••
Web Protocol:	⊙ HTTP ○ HTTPS
Port:	80

Label	Description		
Old Name	This field shows the old login name.		
Old Password	Type in current password		
New Name	Enter a new login name. Acceptable characters contain '0-9',		
	'a-z', 'A-Z' and the length must be 1 to 15 characters. An empty		
	name is not acceptable.		
New Password	Enter a new login password. Acceptable characters contain		
	'0-9', 'a-z', 'A-Z' and the length must be 0 to 15 characters.		
Confirm New Password	Retype the new password to confirm it.		
Web Protocol	Choose a web management page protocol from HTTP and		
	HTTPS. HTTPS (HTTP over SSL) encrypts data sent and		
	received over the Web. Choose HTTPS if you want a secure		
	connection.		
Port	Choose a web management page port number. For HTTP,		
	default port is 80. For HTTPS, default port is 443.		

M2M Gateway Restart

If you want restart the M2M Gateway through the Warm Reset, click Restart Now to restart the Wireless M2M Gateway. Also, you can set a Scheduling time to make the M2M Gateway restart



System Tools> Router	Restart
Router Restart Utility.	
Restart Now	
Scheduling:	Enable Restart Every Day I OO V : OO V

Label	Description	
Restart Now	Click to restart the M2M Gateway via warm reset	
Scheduling	Enable: check to activate the setting	
	Restart at: specify the time for resetting the M2M Gateway. You can	
	configure the action to be performed periodically.	

Firmware Upgrade

Newer firmware may provide better performance or function extensions. To upgrade the new firmware, you need a firmware file which matches the model of this M2M Gateway. It will take several minutes to upload and update the firmware.

After the upgrade is done successfully, reboot the M2M Gateway to utilized new firmware





During firmware upgrading, do not turn off the power or press the reset button.

Save/Restore Configurations

This page allows you to save configurations or return settings to previous status. You can download the configuration file from the Web. Note: users using old versions of Internet Explorer may have to click on the warning on top of the browser and choose Download File.



System Tools --> Save/Restore Configurations

Save/Restore Configurations.

Save Current Configurations

Save

Restore previous saved configurations

瀏覽... Restore

Restore factory default settings

Restore Factory Default Settings

Label	Description				
Save	Click to save existing configurations as a file for future usage.				
Select File	You can restore configurations to previous status by installing a				
	previous configuration file. To do this, choose Web Restore or				
	Tftp Restore. If you choose Web Restore, you need to choose a				
	file and click Web Restore. If you selet Tftp Restore, fill in a Tftp				
	server IP address and the file name before clicking Tftp Restore.				
Restore Factory	You may also reset the M2M Gateway to the factory settings by				
Default Setting	clicking on Restore Default Settings. The M2M Gateway will				
	reboot to validate the default settings.				

Remote Management

Set the Remote Management to access the M2M Gateway web pages from WAN side.

system loois> Remote Management					
Set the Remote Manager	Set the Remote Management to access the Router web pages from WAN side.				
Remote Management: Management Port:	○ Enable ⊙ Disable				
Permission:	 Any Host Host with IP address: Host within IP range: 				

Label	Description
Remote Management	Enables or disables remote management function



Management Port	Enter the port number that will be open to outside access. This				
	port must be used when you establish a remote connection.				
Permission	You can grant remote access to specific users. Tick Any Host or				
	enter a hostname or IP address if you only want a specific				
	computer or device to be able to access the device.				

Miscellaneous (Ping)

This page enables you to run ping test which will send out ping packets to test if a computer is on the Internet or if the WAN connection is OK. Enter a domain name or IP address in the destination box and click **Ping** to test.

System Tools> Miscellaneous						
Miscellaneous utilities.						
Ping Test: Ping Test Result:	Destination:		Ping			

5.2.5 System Status System Info

This page displays the details information for the M2M Gateway including model name, model description, firmware version, WAN, LAN settings.

System Info				
System Ino.				
Model:	IMG-111			
Model Description:	M2M 1 Port Serial Gatew	M2M 1 Port Serial Gateway		
WAN:				
	Mode	Modom/2G		
	Mode	Hodelly30		
LAN:	IP Address	192.168.10.1		
	Subnet Mask	255.255.255.0		
	MTU	1500		
	MAC Address	00:32:12:31:31:31		
	DHCP Server	Enabled		

Refresh

System Log

The M2M Gateway keeps a running log of events and activities occurring on the M2M Gateway, several filters are provided for displaying related log entries.

Click the button 'Refresh' to refresh the page.



Click the button 'Clear Logs' to clear the log entries.

System Status> S	ystem Log				
System log.					
Log Option:	DHCP Server	Boot Message UPNP Modem			
	Select All	Deselect All	Save Option		
System Log:				Refresh	Clear Logs
# Date Time	Item		Content		

Traffic Statistics

This page displays network traffic statistics for packets both received and transmitted through Ethernet ports and wireless connections.

System Status> Traffic Statistics		
Traffic statistics.		
Interface	Send	Receive
LAN	592916 Bytes (1433 Packets)	178571 Bytes (1468 Packets)
WAN	O Bytes (O Packets)	0 Bytes (0 Packets)

5.3 DS-tool

The IMG basic information and some serial port related function can be configure by using DS-tool, including the VCOM Mapping.

5.3.1 General settings

This page display some basic information of the device and also includes the setting of device name.



General Security Ethernet Upgrade Firmware Reboot Device	
Model	
IMG-111	
LAN IP Address LAN MAC Address Version	
192.168.10.1 00:32:12:31:31:31 1.0g	
Device Marro / continu	
JIMG-111313131	

Label	Description
Device Name/location	Input the name of the device.

5.3.2 Security

General	Security Ethernet Upgrade Firmware Reboot Device
Passwoi	rd
New Pa	issword
Confirm	New Password
Old Pas:	sword
	nge Password

Label	Description	
New Password	Enter a new login password.	
Confirm New	Retype the new password to confirm it.	
Password		
Current Password	Type in current password	



5.3.3 Network Setting

General Security	Ethernet Upgrade Firmware Reboot Device
LAN	
IP Address	192.168.10.1
Netmask	255.255.255.0

Label	Description		
IP Address	Assigning an IP address.		
Notwork	All devices on the network must have the same subnet mask to		
Network	communicate with each other on the network.		

5.3.4 Upgrade Firmware

General Security Ethernet	Upgrade Firmware	Reboot Device			
Firmuero Imago					
			Browsing	Upgrade	

Label	Description
Firmware	Browse to the location where the firmware image file is located and click
Image	update.

5.3.5 Reboot Device

General Security Ethernet Upgrade Firmware	Reboot Device
Reboot Device	
 Reboot Device 	



Label	Description
Reboot Device	Click to reboot the device (warm start).

5.3.6 Serial Settings

Serial Settings Service Mode		
port1		
Port Alias Port0		
Baudrate 38400 V Stop Bits 1 V Performance Throughput V		
Parity No Flow Control No Flow		
Data Bits 8 Interface RS232		
Delimiter Settings		
Serial to Ethernet Ethernet to Serial		
Delimiter 1 Delimiter 2 0 (HEX) Enabled Enabled Delimiter 3 Delimiter 4 0 (HEX) Enabled Enabled Delimiter 3 Delimiter 4 Delimiter 4 Delimiter 4 Delimiter 4 Delimiter 4		
Flush Ethernet to Serial Data Buffer After		
0 (0-65535) ms		
The received data will be queueing in the buffer until all the delimiters are matched. When the buffer is full (4K Bytes) or after "flush E2S data buffer" timeout, the data will also be sent.		
Sefresh Apply Only Apply and Save		

Label	Description		
Port Alias	Remark the port to hint the connected device		
Interface	RS232		
Doud roto	110bps/300bps/1200bps/2400bps/4800bps/9600bps/19200bps/		
Baud rate	38400bps/57600bps/115200bps		
Data Bits	5, 6, 7, 8		
Stop Bits 1, 2 (1.5)			
Parity	No, Even, Odd, Mark, Space		
Flow Control	No, XON/XOFF		
Performance	Throughput: This mode optimized for highest transmission speed.		
	Latency: This mode optimized for shortest response time.		
Serial to Ethernet	Delimiter:		
	You can define max. 4 delimiters (00~FF, Hex) for each way. The data will		
	be hold until the delimiters are received or the option "Flush Serial to		



	Ethernet data buffer" times out. 0 means disable. Factory default is 0.
	Flush Data Buffer After:
	The received data will be queuing in the buffer until all the delimiters are
	matched. When the buffer is full (4K Bytes) or after "flush S2E data buffer"
	timeout the data will also be sent. You can set the time from 0 to 65535
	seconds
	Delimiter:
	You can define max. 4 delimiters (00~FF, Hex) for each way. The data will
	be hold until the delimiters are received or the option "Flush Ethernet to
	Serial data buffer" times out. 0 means disable. Factory default is 0.
Ethernet to	
Serial	Flush Data Buffer After:
	The received data will be queuing in the buffer until all the delimiters are
	matched. When the buffer is full (4K Bytes) or after "flushE2S data buffer"
	timeout the data will also be sent. You can set the time from 0 to 65535
	seconds.
Force TX	Force TX interval time is to specify the timeout when no data has been
	transmitted. When the timeout is reached or TX buffer is full (4K Bytes),
	the queued data will be sent. 0 means disable. Factory default value is 0.

5.3.7 Service Mode Virtual COM Mode

In Virtual COM Mode, The driver establishes a transparent connection between host and serial device by mapping the Port of the serial server serial port to local COM port on the host computer. Virtual COM Mode also supports up to 5 simultaneous connections, so that multiple hosts can send or receive data by the same serial device at the same time.



Serial Settings Service Mode	
Service Mode Virtual COM Mode	
Virtual COM Mode	
Virtual COM Settings Encryption with SSL Data Port 4000 Edit IP Port Number Control Port 4001 IP Map Virtual COM	Misc. Idle Timeout 0 (0-65535) Seconds Alive Check 0 (0-65535) Seconds
Multilink	
Max Connections	
Destination Host VCDM Name	
Waiting for VCOM connect	📥 Goto VCom 🖣 Unmap VCom
	🚘 Goto VCom
	🛳 Goto VCom 🛛 🗬 Unmap VCom
	🛥 Goto VCom 🛛 🗬 Unmap VCom
	🛥 Goto VCom 🛛 🗬 Unmap VCom
Refresh	Apply Only 🏾 🍛 Apply and Save

Label	Description
Encryption with SSL	Use SSL to encrypt data.
Map Virtual COM	Select a Virtual COM name to map to.
	When serial port stops data transmission for a defined period of
	time (Idle Timeout), the connection will be closed and the port will
Idle Timeout	be freed and try to connect with other hosts. ${f 0}$ indicate disable this
	function. Factory default value is 0 . If Multilink is configured, only
	the first host connection is effective for this setting.
	The serial device will send TCP alive-check package in each
	defined time interval (Alive Check) to remote host to check the
Alive Check	TCP connection. If the TCP connection is not alive, the
	connection will be closed and the port will be freed. ${\bf 0}$ indicate
	disable this function. Factory default is 0 .



Max Connection	The number of maximum connections can be supported. The		
Max Connection	maximum value is 5 , default values is 1 .		

*Mapping Virtual COM from web is not allowed.

TCP Server Mode

In TCP Server Mode, IMG is configured with a unique Port combination on a TCP/IP network. In this case, IMG waits passively to be contacted by the device. After a connection is established, it can then proceed with data transmission. TCP Server mode also supports up to 5 simultaneous connections, so that multiple device can receive data from the same serial device at the same time.

Serial Settings Service Mode	
Service Mode TCP Server Mode	
TCP Server Mode	
TCP Server Settings Encryption with SSL Data Port 4000 🗠 Auto Scan	Misc. Idle Timeout 0 (0-65535) Seconds Alive Check 0 (0-65535) Seconds
Control Port 4001	
Multilink	
Max Connections 1 Image: Sector Sec	
	et
	st
	et
	et
	et
Refresh	Apply Only 🏾 🍛 Apply and Save

Label		Description
Encryption	with	Lice SSL to enerypt data
SSL		Use SSE to encrypt data
Data Port		Set the port number for data transmission.

ORing Industrial Networking Corp.



Auto Scan	Scan the data port automatically.
	When serial port stops data transmission for a defined period of time
	(Idle Timeout), the connection will be closed and the port will be freed
Idle Timeout	and try to connect with other hosts. 0 indicate disable this function.
	Factory default value is 0. If Multilink is configured, only the first host
	connection is effective for this setting.
	The serial device will send TCP alive-check package in each defined
	time interval (Alive Check) to remote host to check the TCP
Alive Check	connection. If the TCP connection is not alive, the connection will be
	closed and the port will be freed. 0 indicate disable this function.
	Factory default is 0 .
Max Connection	The number of maximum connections can be supported. The
	maximum value is 5 , default values is 1 .

TCP Client Mode

In TCP Client Mode, device can establish a TCP connection with server by the method you have settled (Startup or any character). After the data has been transferred, device can disconnect automatically from the server by using the TCP alive check time or Idle time settings.



Serial Settings Service Mode
Service Mode TCP Client Mode
TCP Client Mode
TCP Client Settings Encryption with SSL Misc. Idle Timeout 0 (0-65535) Seconds
Destination Host Port 4000 Auto Scan
Enable Control Port
Multilink
Destination Host Port
2 Auto Scan
Auto Scan
4 EQ. Auto Scan
Pefresh Apply Only Apply and Save

Label	Description
Encryption with SSL	Use SSL to encrypt data.
Destination Host	Set the IP address of the host.
Port	Set the port number of data port.
	When serial port stops data transmission for a defined period of time
	(Idle Timeout), the connection will be closed and the port will be
Idle Timeout	freed and try to connect with other hosts. ${\bf 0}$ indicate disable this
	function. Factory default value is ${\bf 0}.$ If Multilink is configured, only the
	first host connection is effective for this setting.
	The serial device will send TCP alive-check package in each
	defined time interval (Alive Check) to remote host to check the TCP
Alive Check	connection. If the TCP connection is not alive, the connection will be
	closed and the port will be freed. ${\bf 0}$ indicate disable this function.
	Factory default is 0 .
Connect on Startup	The TCP Client will build TCP connections once the connected

ORing Industrial Networking Corp.



			serial device is started.
Connect	on	Any	The TCP Client will build TCP connections once the connected
Character			serial device starts to send data.

UDP Mode

Compared to TCP communications, UDP is faster and more efficient. In UDP mode, you can Uni-cast or Multi-cast data from the serial device server to host computers, and the serial device can also receive data from one or multiple host

Serial Settings Service Mode
Service Mode
UDP Mode
UDP Settings
Listening Port 4000 ES Auto Scan
Multilink
Destination Host Begin Destination Host End Sending Port
to 🔤 🗠 Auto Scan
2 to Auto Scan
to Can
4 to eQ. Auto Scan
Sefresh Apply Only



Technical Specifications

ORing M2M Model	IMG-111	IMG-111-2G
Physical Ports		
10/100 Base-T(X) Ports in RJ45 Auto MDI/MDIX	1	
Sim card slot	1	
Cellular Interface		
Cellular Standard	GSM / GPRS / EGPRS / EDGE / WCDMA / HSDPA / HSUPA	GSM / GPRS
Band options	Dual band:HSUDPA 1900 / 2100 MHz Quad band:GSM / GPRS / EDGE 850 / 900 / 1800 / 1900 MHz / WCDMA / HSDPA 850 / 900 / 1900 / 2100MHz	Dual-band (Qual-band) GSM/GPRS 900/1800MHz or 900MHz/1800MHz/850MHz/1900MHz
Antenna Connector	Reverse SMA	
Antenna	GSM/DCS/UMT antenna x1	
Serial Ports		
Connector	DB9 Male x 1	
Operation Mode	RS-232	
Serial Baud Rate	110 bps to 115.2 Kbps	
Data Bits	5, 6, 7, 8	
Parity	odd, even, none, mark, space	
Stop Bits	1, 1.5, 2	
Serial signals	RS-232 : TxD, RxD, GND	
LED Indicators		
Power indicator	Green On: Power is on and functioning Normally.	
Status indicator	Green : System status indicator	
Fault indicator	Amber on : WAN connection link down	
WAN	Green on : 2G/3.5G dial up Green blinking : 2G/3.5G disconnect	
Serial TX/RX LED	Red : Receiving data Green : Transmitting data	
10/100TX RJ45 port indicator	Green for port Link/Act.	
Fault Contac		
Relay	Relay output to carry capacity of 1A at 24VDC	
Power		
Power input	12-48VDC power input on terminal block	
Power consumption	4.5 Watts	
Physical Characteristic		
Enclosure	IP-30	
Dimension (W x D x H)	41 (W) x 70 (D) x 95 (H) mm (1.61 x 2.76 x 3.74 inch)	
Weight (g)	360 g	
Environmental		
Storage Temperature	-40 to 85°C (-40 to 185°F)	
Operating Temperature	-10 to 60°C (14 to 140°F)	



Operating Humidity	5% to 95% Non-condensing
Regulatory Approvals	
EMI	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11
Shock	IEC60068-2-27
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6
Safety	EN60950-1
Warranty	3 years