

InHand Networks

Edge Computing Gateway IG902

User Manual

Issue: V2.0-2019.04

InHand Networks Global Leader in Industrial IoT www.inhandnetworks.com





Declaration

Thank you for choosing our product. Before using the product, read this manual carefully.

The contents of this manual cannot be copied or reproduced in any form without the written permission of InHand.

Due to continuous updating, InHand cannot promise that the contents are consistent with the actual product information, and does not assume any disputes caused by the inconsistency of technical parameters. The information in this document is subject to change without notice. InHand reserves the right of final change and interpretation.

© 2019 InHand Networks. All rights reserved.

Conventions

Symbol	Indication
<>	Content in angle brackets "<>" indicates a button name. For example, the <ok> button.</ok>
	"" indicates a window name or menu name. For example, the pop-up window "New User."
>	A multi-level menu is separated by the double brackets ">". For example, the multi-level menu File > New > Folder indicates the menu item [Folder] under the sub-menu [New], which is under the menu [File].
Cautions	Means reader be careful. Improper action may result in loss of data or device damage.
Note	Notes contain detailed descriptions and helpful suggestions.

Contact Us

Add: 3900 Jermantown Rd., Suite 150, Fairfax, VA 22030 USA E-mail: support@inhandneworks.com T: +1 (703) 348-2988 URL: www.inhandnetworks.com



Contents

1 Introduction	1
2 Network Connection, Web Login, and Communication Parameter Setting	2
2.1 Network Connection	2
2.1.1 Cellular Network Connection	2
2.1.2 Ethernet Connection	5
2.1.3 Wi-Fi Connection	7
2.2 Creating an IPsec Tunnel	9
3 Communication Parameter Setting (Supplementary)	10
3.1 Static Route	10
3.2 Automatic IP Address Allocation (DHCP)	11
3.3 DNS	12
3.4 DDNS	13
3.5 Port Mapping (NAT)	14
3.6 VPN Application	15
3.6.1 Point-to-Point IPsec VPN Configuration	15
3.6.2 OpenVPN	18
3.6.3 Certificate Management	20
3.7 Link Backup	21
3.7.1 Interface Backup	21
3.7.2 VRRP Hot backup	24
3.8 Access Control List (ACL)	28
4 Basic System Settings	31
4.1 User Management	31
4.2 System Time	31
4.3 System Upgrade	32
4.4 System Restart	33
4.5 Changing the Language and Gateway Name	34
4.6 Management Services	34
4.7 Checking System Logs	35
4.8 Alarm	36
4.9 Configuration Import and Backup	37
4.10 Restoring Default Settings	38
4.10.1 Webpage Mode	38
4.10.2 Hardware Mode	38
5 Connecting the Gateway to a Cloud Platform	
6 Industrial Interface (DTU)	41
7 App Development	43
7.1 InModbus App	43
7.1.1 Installing an InModbus App	43
7.1.2 Enabling the Remote Device Monitoring Platform	44
7.1.3 Enabling the Variable Editing Service	45
7.1.4 Modifying Configuration	46
8 Appendix CLI Commands	



1 Introduction

IG902 Edge Computing Gateway is a new-generation 4G edge computing gateway that is launched by InHand specifically for the Industrial Internet of Things (IIoT). It provides omnipresent and continuous Internet access through global 3G/4G wireless networks and multiple broadband services. It features a robust edge computing capability, comprehensive security, and wireless services, capable of connecting tens of thousands of devices to networks and providing high-speed data channels for device informatization.

With a robust edge computing capability, IG902 implements data optimization, real-time response, agile connection, and intelligent analysis on IoT edge nodes. This greatly reduces the data traffic between sites and centers, and prevents bottlenecks of cloud-based computing. IG902 can optimize network architectures, deliver more secure and faster responses, and implement onsite services in a more intelligent manner.

Gateway models:





IG902-H



2 Network Connection, Web Login, and Communication Parameter Setting

This chapter describes how to establish a network connection for the gateway, log in to the gateway's web-based management page, and set communication parameters based on the selected network connection mode. If the communication parameters described in this chapter do not meet your application requirements, see chapter 3 "Communication Parameter Setting (Supplementary)."

2.1 Network Connection

2.1.1 Cellular Network Connection

1) Wireless dial-up (with a SIM card)

1. Insert the SIM card in slot 1, connect the 4G LTE antenna to the ANT port, and connect the gateway to a power supply. Connect the gateway to the programmable logic controller (PLC) through the serial port or LAN port.







Before inserting or removing the SIM card, power off the gateway; otherwise, data may be lost or the gateway may be damaged.

2. Set the IP addresses of the PC and gateway to be in the same network segment.

(Recommended) Mode 1: Automatic IP address allocation.

Mode 2: Fixed IP address. Set the IP addresses of the PC and the gateway's GF ports to be in the same network segment. The initial IP address of the gateway is 192.168.2.1, and its subnet mask is 255.255.0. Select **Use the following IP address**, enter an IP address (any from 192.168.2.2 to 192.168.2.254), subnet mask (255.255.255.0), and default gateway IP address (192.168.2.1), and click **OK**.

Internet Protocol Version 4 (TCP/IPv4) Properties	X Internet Protocol Version 4 (TCP/IPv4) Properties X
General	General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically	Obtain an IP address automatically
O Use the following IP address:	Use the following IP address:
IP address:	IP address: 192 . 168 . 2 . 2
Subnet mask:	Subnet mask: 255 . 255 . 255 . 0
Default gateway:	Default gateway: 192 . 168 . 2 . 1
Obtain DNS server address automatically	Obtain DNS server address automatically
O Use the following DNS server addresses	Use the following DNS server addresses
Preferred DNS server:	Preferred DNS server: 8 . 8 . 8
Alternate DNS server:	Alternate DNS server:
Validate settings upon exit Advanced	Validate settings upon exit Advanced
OK Can	OK Cancel

Obtain an IP address automatically

Use the following IP address

3. Open the web browser and enter 192.168.2.1 (default IP address of the gateway) to access the gateway's web-based management page.



4. Log in to the gateway.



Default username:adm
Router Login
Username adm
Password
Login

5. Choose **Network** > **Cellular**, and select **Enable**. The SIM card is successfully connected to the network if the network connection status is Connected and an IP address is allocated.

inhand		Network >> Cellular		instand	Administration >> System	
Administration Network Services Link Backup Routing Firewall VPN APP		Enable Profile Roaming PIN Code Network Type Static IP Connection Mode Bedial Interval	SIM1 SIM2 auto auto auto auto auto auto auto auto auto	Network * Services * Link Backup * Routing * Firowall * VPN * APP * Industrial * Tools *	System Status Name Mane Made Made Machae Machae	Edge6ax0xxiy 109028 0170021901304588 0018.0510.0051 1.6.0110582(bene)-2019-04-02-18-50-24 2017.011.0315 2019-04-04 10.47.07 2019-04-04 10.49.17 2019-04-04 10.49.17 2019-04-04 10.49.17 2019-04-04 10.49.17 0.66 / 0.05 / 0.04 495.11M8 / 325.71M8 (05.79%)
ndustrial Fools	*	ICMP Detection Server	<u>s</u>		Cellular 1 (Settings) Status Signal Level	Connected
Wizards		ICMP Detection Interval ICMP Detection Timeout ICMP Detection Max Retries ICMP Detection Strict Show Advanced Options	30 s 5 s 5	Save Configuration Copyright ©2001- 2019 Instand Networks Co. 10d. All rights reserved.	Register Statua IP Address Netmask Gateway DNS MTU Connection time Gigabitethernet 0/1 (Settin Crater	registered 172:10:234:39 255:255:255:255 11:1:3.0.0 11:0:0.0:0:0.00 11:0:0 0:dey, 00:0:0 0:dey, 00:0:0 50 0:0 Doese

6. The dual SIM card feature is supported. Enable this feature if another SIM card is inserted in slot 2.

innand	Network >> Cellular				English 中文 Username: adm Nakegout
Administration Network Services Link Backup Routing	ICMP Detection Interval ICMP Detection Timeout ICMP Detection Max Retries ICMP Detection Strict Show Advanced Options	80 s 5 s 5			Alarm Total Alarms: 0 Alarm Summary
VPN APP Industrial Viands Wilands Save Configuration	RSSI Poll Interval Dial Timeout MTU Infinitely Dial retry Dual SIM Enable Main SIM Max Number of Dial Min Connected Time CSQ Threshold CSQ Detect Interval CSQ Detect Retries Backup SIM Timeout Debug	120 s(0: disable) 120 s 1500 8 1500 8 1500 8 1500 10 10 10 10 10 10 10 10 10	(0: disable) (0: disable)		
Copyright ©2001-2019 InHand Networks Co., Lto All rights reserved.	Profile Index Network API 1 GSM * 3gnet	Access Number	Auth Username Method Auto • gprs	Password	.



2) Wired dial-up (PPPoE server)

1. Connect cables based on the following figure if a PPPoE server is used for dial-up.



- 2. Set the IP addresses of the PC and gateway to be in the same network segment. Log in to the gateway's web-based management page. For details, see "Wireless dial-up."
- 3. Choose Wizards > New WAN. Select gigabitethernet 0/1 for Interface and ADSL Dialup (PPPoE) for Type. Enter the name and password of the PPPoE server. Enable NAT. Click Apply & Save.

inhand	Wizards >> New WAN		English 中文 Username: adm
Administration Network Services Link Backup Routing Firewall	Interface gigab Type ADSL Username PPPo Password NAT Z	itethermet 0/1 • Dialup (PPPoE) • Ename	Alarm Total Alarms: 0 Alarm Summary (* 3 s *
APP Industrial Tools Wizzrds	Pppy a core ourse		
Save Configuration Copyright ©2001-20 InHand Networks Co. All rights reserved.	9 . Adi,		

2.1.2 Ethernet Connection

1. Connect the power supply and network cable to the gateway. Connect the LAN port (GE1/1) to the PC and connect the WAN port to the Internet. Connect the gateway to the PLC through the serial port or LAN port.





- 2. Set the IP addresses of the PC and gateway to be in the same network segment. Log in to the gateway's web-based management page. For details, see section 2.1.1 "<u>Cellular</u> <u>Network Connection</u>."
- 3. Choose **Wizards** > **New WAN**. Set an IP address for the WAN port so that the gateway can connect to the Internet.

Wizards	New LAN
	New WAN
	New Cellular
	New IPsec Tunnel
	New Port Mapping

4. DHCP is recommended. If you choose to set a static IP address, set the network parameters and save them based on the actual network connection.

inphand		Wizards >> New WAN	4		inphand		Wizards >> New WA!	4			
Administration	-	Interface		gigabitethernet 0/1 •	Administration Network	:	Interface		gigabitethemet 0/1	•	
Services		Туре		Dynamic Address (DHCP) *	Services		Туре		Static IP	•	
Link Backup		NAT		*	Link Barkun		Primary IP		10.5.16.98		Use your own
Bautine		1120000 1000 1			Beatles		Netmask		255.256.255.0	-	network data
nouting		Apply & Save	Cancel		Kouting		Gateway		10.5.16.1		
Finewall					Firewall		Primary DNS		10.5 17 1		
VPN					VPN	1.	NAT		2		
APP					APP		12040				
Industrial					Industrial	•	Apply & Save	Cancel			
Tools					Tools						
Wizards	×.				Wizards						

Dynamic IP address allocation

Static IP address setting



5. Choose **Tools** > **Ping** to check whether the gateway is connected to the Internet. Enter the URL of a common website in **Host** for testing. If the following message appears, the gateway is connected to the Internet.

inhand		Tools >> Ping			English	中立 Username: adm Micegout
Administration	٠					Alarm
Network		Host	www.baidu.com	Ping		
Services	,	Ping Count	4			Alarm Summary
Link Backup		Packet Size	32 Bytes			Plant Sentitively
Routing	,	Expert Options				£ 35 Y
Firewall						Stop
VPN	•	print and ballar and Olipo	of ap 100), ap 1-1- 1-1			
APP	•	40 bytes from 180.97.33.	108: seq=0 tt1=55 tine=33.986 ns	8		
Industrial	•	40 bytes from 180, 97, 33, 40 bytes from 180, 97, 33,	108: seq=1 tt1=55 time=33.638 ns 108: seq=2 tt1=55 time=33.121 ns	8.8		
Tools	•	40 hytes from 180.97.33.	108: seq=3 ttl=55 time=33.110 ns	s		
Wizards	•	 www.baida.com ping s pockets transmitted, 4 round-trip min/org/max = 	riatistics — 4 packets received, 0% packet los 5 03 110/33,463/53,806 ms	<u>89</u>		
Save Configuration	019 Ltd.					

2.1.3 Wi-Fi Connection

1. Connect the power supply and network cable to the gateway, and connect the Wi-Fi antenna to WLAN 1 or 2. Connect the gateway to the PLC through the serial port or LAN port.



2. Set the IP addresses of the PC and gateway to be in the same network segment. Log in to the gateway's web-based management page. For details, see section 2.1.1 "<u>Cellular</u> <u>Network Connection</u>."



3. Choose **Network** > **WLAN**. Enable the WLAN port and set parameters, as shown in the following figure.

	[Stati		Wi-Fi	IP Set		SSID 5	con	
Administration Network Services Link Backup	*	Ena Sta De Clie	able ition faul ent f	i Role t Roui SSID	te			Ø Client ▼ Ø iPhone	XS123
Routing	1	Auth Method				WPA2-R	PSK •		
VPN		WPA/WPA2 PSK Key							
APP									
Industrial	•		A	oply 8	Save		Cancel		
Tools	- 16								
Winneda									

4. Click the Status tab. The network connection status is Connected.

inhand	Network >> Wi-Fi Status Wert III Score	SSID Stan		Engli	sh (中文 Us Tui	ername: adm
Administration '		Y	our password has security risk, please click here to char	ingel =		
Network *	Wi-Fi Status				Alarm	100 E
Services Link Backup Routing Firewall VPN	Station Role Wi-Fi Status Client SSID Wireless Connection MAC Address Auth Method Encrypt Mode	Client Enabled Inhand Connected D0:15:83:40:13:50 WPA2:PSK AES			Total Alarms Alarm Sumr	3 s v Refesh
APP	Network Status IP Address Natmask Gateway DNS Connection time	Connected 192.168.100.69 255.235.255.0 192.168.100.1 61.156.2.69.202.58.95.68 D day, 00.0145				
Save Configuration Copyright ©2001- 2019 InHard Notworks Co Ltd All rights reserved.				C [3 s *] Sin	P	

5. Choose **Wizard** > **New WLAN** and set the parameters.



6. Choose **Firewall** > **NAT**. The Wi-Fi connection is successful if the dot11radio 1 connection is displayed.



iministration	Networ	k Address Tran	slation(NAT) Ru	les		Alarm
rvices	Acti	on Source	Match	Translated	Description	Total Alarms: 0
k Backup	SNA	T Inside	ACL:100	cellular 1		Alarm Summary
uting	SNA	T Inside	ACL:179	gigabitethernet 0/1		/** 3s *
ewall				Add	Modify Delete	Stop
'N I					hanna hanna h	
ip i	Inside N	letwork Interfa	ces			
dustrial	12	ID		Interface		
ols		1		bridge 1	* * X	
laards I	2			,		
				Add		
	Outside	Network Inter	faces			
	10	ID		Interface		
		1		cellular 1		
Save Configuration		2	giga	bitethernet 0/1		
	3			1		
				Add		

2.2 Creating an IPsec Tunnel

You can create a dedicated virtual tunnel between the gateway and another device in the network or a cloud platform after a network connection is established. This section shows how to create an IPsec tunnel. Choose **Wizards** > **New IPsec Tunnel**, select the interface for which you want to create an IPsec tunnel, and enter the peer IP address and the subnet addresses and masks at both ends of the tunnel. During the first phase, enter the identifiers and connection keys at both ends of the tunnel, and click **Apply & Save**.

inhand		Wizards >> New IPsec Tunne		English 中	C Username: adm
Administration		New IPsec Tunnel			MLogout
Matural		Basic Parameters		8	
Network		Tunnel ID	1 •	Te	atal Alarms: 0
Services		Map Interface	gigabitethemet 0/1 •	A	arm Summary
Link Backup		Destination Address	192.168.2.1		
Routing	,	Negotiation Mode	Main Mode •		35 *
Firewall		Local Subnet	192.168.2.1		Stop
VPN		Local Netmask	255 255 255 0		
APP		Remote Subnet	10.5.16.5		
Industrial		Remote Netmask	255.255.255.0		
Tools	•	Phase 1 Parameters			
Wizards		IKE Policy	3DES-MD5-DH2 ·		
		IKE Lifetime	96400 s		
		Local ID Type	User FQDN •		
		Local ID	@19		
		Remote ID Type	FQDN .		
		Remote ID	@191		
Save Configurat	tion	Authentication Type	Shared Key •		
		Key			
		Phase 2 Parameters	0.54		
		IPSec Policy	3DES-MD5-96 •		
		IPSec Lifetime	3600 s		
Copyright ©2001	-2019	0104557556530003555			
All rights reserv	ed.	Apply & Save Cano	a		



3 Communication Parameter Setting (Supplementary)

This chapter supplements chapter 2. If the communication parameter setting described in chapter 2 does not meet your requirements, set the parameters based on this chapter.

3.1 Static Route

PC 1 and PC 2 located in two separate subnets cannot communicate with each other when no static route is configured. To enable communication between PC 1 and PC 2, you need to configure a static gateway between the two LANs, as shown in the following topology.



Configure the gateway as follows:

Step 1: Choose **Routing** > **Static Routing** to configure edge computing gateway A. Set **Destination** to the gateway address of PC 2 in the format xxx.xxx.0. The default value of **Netmask** is 255.255.255.0, whereas 0.0.0.0 indicates all subnet masks. Set either **Interface** (interface connected to gateway B) or **Gateway** (which must be configured on gateway B in advance).

inhand	Routing >> Static	Routing				English 中文 Username: adr
Administration Network Services Link Backup Routing Firewall	Destination 0.0.0 0.0.0 19216830	Netmask Inte D.0.0.0 coli D.0.0.2 gigabitet 15522552550 gigabitet	rface Gateway Jar 1 hernet 0/1 10.5.16.1 hernet 0/1 192.168.1.2 •	Distance 255	Track Id	Alarm Total Alarms: 0 Alarm Summary
VPN APP Industrial Tools Wizzeds	Apply & Save	: Cancel				
Save Configuration	9					



Step 2: Configure edge computing gateway B. Set the parameters based on the following figure.

1	C	ioute Table St	atic Routing					leLog	jout
Administration		Destination	Matematic	Toterface	Gateway	Distance	Tensk Id	Alarm	1
Network		0.0.0.0	0.0.0.0	cellular 1	outenay	255	TIPER IN	T (1.1.1)	
Services		0.0.0.0	0.0.0.0	gigabitethernet 0/1	10.5.16.1			Total Alarms	:0
Link Backup		192,168,2.0	255.255.255.0	gigabitethemet 0/1	192.168.1.1			Alarm summa	iny
Routing				•		1		0.24	-
Firewall							Add		Stop
VPN			102					1.1.1	
APP		Apply & S	ave Cance						
Industrial									
Tools									
Save Configuratio	<u>in</u>								
Copyright © 2001-20 InHand Networks Co.	02.9 , Ltd.								

Step 3: Check whether PC 1 and PC 2 can communicate with each other. If yes, the static gateway is added successfully.

3.2 Automatic IP Address Allocation (DHCP)

DHCP adopts the client/server communication mode. The client sends a configuration request to the server, which then returns corresponding configuration, such as the IP address allocated to the client. This implements dynamic configuration of the IP address and other information.

• The gateway can work as the DHCP server to allocate a different IP address to each login workstation. The DHCP server greatly simplifies network management tasks that are otherwise completed manually.

laturck	DHCP Se	rver				100	Alarm	
iervices	, Enable	Interface	Starting Address	Ending Address	Lease(Minutes)		Total Alarms: 0	
ink Rackup		bridge 1	192.168.2.2	192.168.2.100	1440		Alarm Summary	
THE BACKUP	No	gigabitethemet 0/1	192.198.2.3	192.168.2.101	1440	-		
louting	in a start	•	192.168.2.3	1192 168 2 101	1440	-	33	3
irevall	*				Add		Sto	p
PN								
PP	. NOTEDH	ICP lease time 0 indicates	infinite.					
ndustrial	, DNS Ser	iver		Edit				
lander -	Window	s Name Server						
ools	(WINS)							
Vicards	Static IP	Settings						
	1	MAC Address	IP Address					
	0000.00	00.000						
			Add					
Save Configuratio		chill South Canad					-	
		pry a save uance						



• The gateway can also work as the DHCP client to receive the IP address allocated by the DHCP server after login. This requires that the gateway's Ethernet interface be set to automatic mode.

innand	Services >> DHCP English Status DHCP Server OHCP Rebay DHCP Client	中文 Username: adm
Administration	, Bridge 1	Alarm
Network	Gigabitethemet 0/1	Total Alarmer 0
Services	,	Alarm Summary
Link Backup	Apply & Save Cancel	
Routing	•	(* 3s *
Firewall	•	Stop
VPN	•	
APP	•	
Industrial	•	
Tools	>	
Wizards	•	
Save Configuration		
Copyright ©2001-20 InHand Networks Co. All rights reserved.	9 hd.	

3.3 DNS

A domain name server (DNS) converts domain names to corresponding IP addresses that can be identified by PCs. Users only need to remember domain names. DNS is typically set only when the WAN port uses a static IP address:

DNS Server: On this tab page, you can configure the gateway to resolve dynamic domain names through the DNS.

innand	Services >> DNS DNS Server		English	中文 Username: adm <mark>MaL</mark> egout
Administration Network Services	Primary DNS Becondary DNS	8.8.8		Alarm E
Link Backup Routing Firewall	Apply & Save Cancel			C 3s r
VPN APP				
Industrial Tools Wizzeds				
Save Configuration	***			
Consider #2001-2	150			
InHand Networks Co All rights reserved	ttd.			

DNS Relay: On this tab page, you can configure the gateway as a DNS proxy to forward DNS request and response packets between the DNS client and server and resolve domain names on behalf of the DNS client.



If the DHCP service is enabled on the gateway, the DNS forwarding function is enabled by default and cannot be disabled.

You can set **Static [Domain Name <=> IP addresses] Pairing** to map IP addresses to domain names so that IP addresses can be accessed by using domain names.

inhand	Services >> DNS	English 中文 Username: adm 「Legout
Administration Network	Enable DNS Relay	Alarm
Services	Static [Domain Name < => IP addresses] Pairing	Total Alarms: 0
Link Backup	Host IP Address 1 IP Address 2	Rath Jennery
Routing	www.sohu.com 10.5.16.98	(1) 3s *
Firewall	Add	Stop
VPN		
APP	Apply & Save Cancel	
Industrial	•	
Tools		
Wizards		
Save Configuration	22	
Copyright ©2001-201 InHand Networks Co., I All rights reserved.	019 L tid. d.	

3.4 DDNS

The edge computing gateway obtains public IP addresses through dial-up. You can configure Dynamic Domain Name Server (DDNS) to map users' dynamic IP addresses to a fixed DNS.

Configure the gateway as follows:

Step 1: Set the DDNS parameters of the gateway. If a custom domain name is used, find the DDNS expression on the server's official website, and enter a URL in the format http://user name:password@ddns.oray.com/ph/update?hostname=host name, as shown in the figure "DNS parameter setting 1." If a common domain name is used, enter the registered account, password, and host name, as shown in figure "DNS parameter setting 2." DDNS is not used if **Disable** is selected.



nhand	Services >> DDNS								English	Username: ad
ninistration *	DDNS Method Lis	ŧ								Alarm
ices •	Method Name Ser	vice Type	Url		Username	Password	Hostname	Period		Total Alarms: 0
Backup	1 Cus	stom	http://gousourwang	jie123@dynupdate.no-				60	* * *	Alerin Summary
9 *	Dis	sable •	ipconymcropusters	ame swaiker1204.000sh					1	€) 3 s
•								Add		Stop
									-	
•	Specify A Method	To Interfa	ice.							
al *	Interface		Method							
•	bridge 1	•	1	•						
	Apply & Save	Cance	ei	Add						
leafiguration										
sht ©2001-2019 Networks Co., Ltd ghts reserved,										

DNS parameter setting 1

Administration		DDNS Method	List							Alarm	
Network	•					1000000000		1	100 Marca 100 Marca 100	Total Alarmer 0	
ervices	•	Method Name	DynAccess	UN		Username	Password	Hostname test dynaccess	Period minutes	Alarm Summan	
ink Backup			Disable				1	the strang market star		Plant setting y	
louting									Add	2 3 s	٧
Irewall	*										top
PN	•	Specify A Meth	od To Interfa	ice							
(PP		Interface		Method							
ndustrial	•	bridge 1		2							
ools	•				Add						
Nizards											
Save Coofiguratio	n	Apply & Se	we Cano	d							
opyright ©2001-20 Hand Networks Co. All rights reserved	19 Ltd.										

DNS parameter setting 2

Step 2: Wait for several minutes after you configure DDNS and save and apply the settings. Then, ping the host name (domain name) to check that DDNS is configured successfully.

3.5 Port Mapping (NAT)

Port mapping can be configured on the Wizards and Firewall pages.

Choose **Wizards** > **New Port Mapping** to configure the gateway to access the Internet.

bridge1: bridge interface; Cellular 1: SIM dial-up interface; Gigabitethernet0/1: WAN port.



As shown in the following figure, port 1000 of Cellular 1 is mapped to port 2000 with the IP address 10.5.16.21. The public server with the IP address 10.5.16.21 can be accessed through the gateway's Cellular 1 port.

inhand	Wizards >> New Port Mapping New Port Mapping	English 中文 Username: adm 【Legout
Administration * Network * Services * Link Backup * Routing * Firewall * VPN *	Protocol 1 TCP • Outside Interface cellular 1 • Service Port 2 1000 Internal Address 10.5.16.21 Internal Port 2000 Description	Total Alarms: 0 Alarm Summary
APP Findustrial F Tools F Wisards F	Apply & Save Cancel	
Save Configuration		
Copyright ©2001-2019 InHand Networks Co. Ltd. All rights reserved.		

Choose **Firewall** > **NAT**. Configure Internet access through dial-up. Port GE 0/2 is connected to the server with the IP address 192.168.2.23. Configure the gateway to access the server through the public network.

innand		Firewall >> NAT						English	1 中文	Usernam	ie: adin it
Administration Network Services Link Backup Routing Firewall VPN APP Industrial		Action Source Network Translation Type Match Conditions Interface Translated Address IP Address Description Log		DNAT Outside INTERFACE to IP cellular 1 192 168 2 23 2000	0				Alam Total Alam	Alarms: 0 Summary	Stop
Tools Wizards	• •	Apply & Save	Cancel	Back							
Save Coofigurat	isn										
Copyright ©2001- nHand Networks C All rights reserv	2019 5. Ltd. 1d,										

3.6 VPN Application

3.6.1 Point-to-Point IPsec VPN Configuration

Establish a security tunnel between gateways A and B to protect the data flows between the subnet (192.168.1.0/24) for customer branch A and the subnet (172.16.1.0/24) for customer branch B. Configure the use of the Encapsulation Security Protocol (ESP), 3DES encryption algorithm, and SHA authentication algorithm.



The following figure shows the IPsec VPN topology.



Networking configuration procedure:

(1) Configure gateway A

Step 1: Choose **VPN** > **IPsec** from the navigation tree to go to the **IPsec Setting** page. Set the parameters.

inhand	VPN >> II	Psec Psec Setting							English	中文 Username: adm MaLegout
Administration Network	Enable		2							Alarm
Services *	IKEVI Po	blicy								Alarm Summary
Link Backup		ID Enc	votion	Hash	Diffie-Hellman Gro	up	Lifetime			
Routing	1	1 3	DES	SHA1	Group2		86400			C 35 7
Firewall	-	3DE:	s •	SHA1 *	Group2	* 86400				Stop
VPN *								Add		
APP										
Industrial	IKEv2 Po	olicy								
Tools P	• <u>11</u> =	ID Enc	yption	integrity	Diffie-Hellman Gro	up	Lifetime			
Wizards		AES	28 •	SHA1 •	Group2	• 86400				
	IPsec Po	licy						Add		
	N	lame Fr	canculatio	n Encruet	on Authentica	tion	IPter Mo	de		
		2	ESP	3DES	MDS		Tunnel Mo	ode		
Save Coofiguration	1	ESP		 AE5128 	 SHA1 	• Tu	nnel Mode	•		
	-							Add		
	IPsec Tu	nnels								
Copyright ©2001-2019	N	lame St	atus	Local Subnet	Remote S	ubnets	Interface	IKE Version		
InHand Networks Co., Lt. All rights reserved.	1				Add	Ma	dify	Delete		

Step 2: Choose **VPN** > **IPsec** from the navigation tree to go to the **IPsec Setting** page. Click **Add** next to **IPsec Tunnel Setting**. Set the parameters on the displayed page, as shown in the following figure.

inhand					InHand Networks Edge Cor	nputing Gateway IG902 User	Manual 🧲
inhand		VPN >> IPsec				English(中文	Username: adm
Administration		Barris Barrantene				Alar	m
Network		Destination Addre	ee.	192 100 100 19	Ť		
Services	,	Man Interface	22	cellular 1	1	Tota	I Alarms: 0
Link Backup		IKE Version		IKEv1 •		Alar	n summary
Routing	,	KEVI Policy		1.			34 *
Firewall	- 31	IPsec Policy					Stop
VPN		Authentication Typ	pe	Shared Key +			
APP		Negotiation Mode		Main Mode •			
Industrial		Local Subnet		192.168.1.0	255.255.255.0		
Tools					255 255 255 0		
Wizzeds		Remote Subnet		172 16 1.0	255 255 255 0		
					255 255 255 0		
		IKE Advance(Phase	1)	Ð			
		IPsec Advance(Pha	se2)	6			
		Tunnel Advance	1011104	10			
Save Configurat	ian	Apply & Save	Cancel	Back			
Copyright ©2001 InHand Networks C All rights reserv	2019 o. Ltd. ed.						



The local and peer identifier addresses do not need to be set, unless otherwise specified.

IPsec Profile is set only when DMVPN is configured. It does not need to be set when IPsec VPN is created.

(2) Configure gateway B

Step 1: Choose **VPN** > **IPsec** from the navigation tree to go to the **IPsec Setting** page. Set the parameters.

inhand	1	/PN >> IPsec	ng					English	中文 Username: adm 「Legout
Administration Network	;	Enable		8				*	Alarm
Services	,	IKEv1 Policy							Alarm Summant
Link Backup		ID	Encryption	Hash	Diffie-Hellman Group	Lifetime			Riatin Sentimoty
Routing	,	1	3DES	SHA1	Group2	86400			(* 35 T
Firewall		1	3DES ·	SHA1 *	Group2 *	86400			Stop
VPN							Add		
APP									
Industrial		IKEv2 Policy							
Tools		ID	Encryption	integrity	Diffie-Hellman Group	Lifetime			
Wizards	5		AES128 •	SHA1 •	Group2 •	86400			
		IPsec Policy					Add		
		Name	Formerulati	an Encount	dan Authoritication	IBras Ma	de		
		2	ESP	3DES	MD5	Tunnel Mo	ode		
Save Configuratio			ESP	 AE5128 	* SHA1	Tunnel Mode			
Contraction of the second							Add		
		IPsec Tunnels							
Copyright ©2001-20	19	Name	Status	Local Subnet	s Remote Subn	ets Interface	IKE Version		
All rights reserved.	Ltd				Add	Modify	Delete	4	

Step 2: Choose **VPN** > **IPsec** from the navigation tree to go to the **IPsec Setting** page. Click **Add** next to **IPsec Tunnel Setting**. Set the parameters on the displayed page.

inhand					InHand Networks Edge (Computing Gateway I	G902 User Manual 🧲
ignand		VPN >> IPsec					English 中文 Username: adm 「McLegout
Administration		Paris Presentant					Alarm
Network		Destination Addre	c.e.	192 50 50 2			
Services	,	Man Interface		rellular 1			Total Alarms: 0
Link Backup		IKE Version		IKEv1 •			Alarm Summary
Routing	,	IKEVI Policy		1.			12 3 c v
Firewall	- 5	IPsec Policy		-			Stop
VPN		Authentication Typ	be	Shared Key +			
APP		Negotiation Mode		Main Mode •			
Industrial		Local Subnet		172.16.1.0	255.255.255.0		
Tools					255 255 255 0		
Winneds		Remote Subnet		192.168.1.0	255 255 255 0		
					255 255 255 0		
		IKE Advance(Phase	1)	0			
		IPsec Advance(Pha	se2)	10			
		Tunnel Advance		11			
Save Configurat	ian	Apply & Save	Cancel	Back			386
		rippi a care	Guice	Duca			
Copyright ©2001- InHand Networks Co All rights reserve	2019 o. Ltd. ed.						

(3) Check the VPN status

0

Go to the **Status** page and check that the VPN status is Connected.

Vame	Destination Address	IkeStatus	
IPSEC_1	Router 203.86.43.189	Connected	
			16. / / 方 . /

3.6.2 OpenVPN

OpenVPN is based on TCP/UDP and applicable to any ports. The following figure shows an example of OpenVPN topology.





In the preceding figure, an OpenVPN tunnel is established between device A and the OpenVPN server. The virtual IP addresses at both ends of the tunnel are 192.168.5.2 and 192.168.5.1.

- A. If OpenVPN of device A is configured as the gateway mode, the packets destined for the 192.168.8.0/24 subnet are forwarded to the OpenVPN tunnel through the gateway and reach the OpenVPN server. Correspondingly, a static gateway must be added on the OpenVPN server so that the packets destined for the 192.168.9.0/24 subnet are forwarded to the OpenVPN tunnel through the gateway. In this way, PC A and PC B are connected through the OpenVPN tunnel and can communicate with each other.
- B. If OpenVPN of device A is configured as the NAT mode, the static gateway 192.168.9.0/24 does not need to be added on the OpenVPN server. With this configuration, PC A can access PC B, but PC B cannot access PC A directly. This configuration is applicable to active uploading.

Configure the gateway as follows:

innand	VPN >> OpenVPN Status OpenVPN Client OpenVI	N Server	English 中文 Username: adm
Administration * Network * Services *	Enable Index	8	Alarm Control Alarms: 0
Link Backup Routing Firewall VPN App Industrial Tools Wizards	OpenVPN Server Pont 211.189.3.69 119 119 Authentication Type Username Password Description Show Advanced Options Import Configuration	Protocol Type udp udp Add User/Password test ······	i 3s * Stop
Save Configuration	No file selected.	Browse Import Export	

Step 1: Set the OpenVPN parameters of the device.

Step 2: Complete certificate configuration based on the specific authentication type after a tunnel is established. The mapping between authentication types and certificates is as follows:

None: No certificates are required.

Pre-shared Key: No certificates are required.

User/Password: Only the CA certificate is required, such as ca.crt.

X.509 Cert (multi-client), X.509 Cert: The CA certificate and the device's public and private key certificates are required, such as **ca.crt**, **my.crt**, and **my.key**.



A Note:

1. The file names of the CA certificate and public key certificate are suffixed with **.crt**, and the file name of the private key certificate is suffixed with **.key**.

2. The system time of the device must be accurate when the certificate feature is used.

Step 3: Configure the OpenVPN server. Add a static gateway with a route destined for 192.168.2.0/24 by running **route add -net 192.168.2.0 netmask 255.255.255.0 dev tun0**. Assume that the network port of the OpenVPN server is tun0.

3.6.3 Certificate Management

On the **Certificate Management** page, you can import VPN certificates. If no local certificates are available, select **Enable SCEP** (**Simple Certificate Enrollment Protocol**) to apply for a certificate online.

inhand	/PN >> Certificate Management		English 中文 Username: adm [stogout
Administration •	Certificate Mononement		Alarm
Network '	Centrate management		
Services *	Enable SCEP (Simple		Total Alarms: 0
Link Backup	Protocol)		Atarm Summary
Routing !	Protect Key		2/13
Firewall *	Protect Key Confirm		Stop
VPN +	Revocation		
APP /	En la constante das Enternantes das		
Industrial *	No file selected. Browse.	Import Public Key Certificate Export Public Key Certificate	
Tools ,	No file selected	mont Diviste Key Certificate Event Divisite Key Certificate	
Wizards	Home	index successive and respect successive set opportunities	
	No file selected. Browse	Import CA Certificate Export CA Certificate	
	No file selected. Browse	Import CRL Expert CRL	
	No file selected. Browse	Import PKCS12 Certificate Export PKCS12 Certificate	
Save Configuration	Apply & Save Cancel		
Copyright ©2001-2019 InHand Networks Co., Ltd. All rights reserved.			



Manual I	CA Name	Issuer Name	Alarm
Services 1			Total Alarmis: 0
Link Backup	ort Root CA Cerdificate		Alarm Summary
Routing , N	file selected	Browse Import Root CA Certificate	
Firewall *			2 3 s *
VPN +			COP
APP 1			
Industrial *			
Tools '			
Wizards +			
Save Configuration			

3.7 Link Backup

3.7.1 Interface Backup

You can configure interface backup to enable the gateway to access the Internet through dial-up even when the wired network is faulty. The following figure shows the topology of interface backup.



Configure the gateway as follows:

Step 1: Choose Wizards > New WAN to set the parameters of Internet access in wired mode.



inhand	Wizards >> New WAN			English	中文 Username: adm Natogout
Administration	Interface	gigabitefhemet 0/1 🔻			Alarm
Network	Type	State IP	-		Total Alarmy: 0
Services	Primary IP	10.5.3.134			Alarm Summary
Link Backup	Netmask	255 255 255 0	E I		, and a second s
Routing	Gateway	10.5.3.254			233 *
Firewall	Riman DNS	10.5 17 1			Stop
VPN	NIOT	10.5 17 1			
APP	(Inter				
Industrial	Annir & Sana	Canval			
Took	apply a pare	Galice			
14 Barriela					
vvizardis.					
Save Configuration					
Copyright @2001-2019					
All rights reserved.	4 .				

Step 2: Choose **Services** > **DNS** > **DNS Server** to set corresponding parameters. Check that the PC can access the Internet after configuration.

inhand	Services >> DNS DNS Server Data Baby		English 中文 Username: adm [subogout
Administration Network Services	Primary DNS Secondary DNS	202.106.0.20 8.8.8.8	Alarm C
Link Backup Routing	Apply & Save Cancel		Alarm Summary
VPN			- 54op
Industrial Tools			
Wizarda			
Save Configuration			
Copyright ©2001-2019 InHand Networks Co., Lt All rights reserved.			

Step 3: Choose **Link Backup** > **SLA** to set corresponding parameters. Set the IP address to a public or private IP address that supports ICMP detection. For example, 203.86.63.233 is the IP address of the enterprise gateway for the PC.



ighand	Link Back	cup >> SLA									English	中文 Usernar <mark>Tutog</mark> o	ne: adm ut
Administration	SLA Ent	TY										Narm	
Network	1		-									Total Alarmer 0	
Services	* Index	Туре	Address	Data size	Interval(s)	Timeout(ms)) Consecutive	Life	Start-ti	ime		Alarm Summary	
Link Backup	1 1	icmp-echo	203.86.63.233	56	30	5000	5	forever	now	v			
Routing	, 2	ismp-echo •		56	30	5000	5	forever *	now	-		13 3 4	*
Firewall									Add	d			Stop
VPN													
APP	1 A	oply & Save	Canpel										
Industrial													
Tools													
Wizards	3 B												
Save Configuration													
Copyright \$2001-20 InHand Networks Co. All rights reserved	19 Ltrd												

Step 4: Choose Link Backup > Track to set corresponding parameters.

	Hock Object	mitter
,	Index Type SLA ID/VRRP ID Interface Negative Delay(s) Positive Delay(s)	Total Alarmis: 0
p •		Alarm Summary
۰,		
	, ABU	5, 123
	Track Action	
,	Index Control Service Action	
	positive-statt/negative-stop	
	bbA	
	Apply & Save Cancel	
finutation		
afiguration		
afiguration		
afiguration		
nfiguration		

Step 5: Choose Link Backup > Interface Backup to set corresponding parameters.



inhand	Euron Interface Backs	ID .						Detegout
Administration			Chartum					Alarm
Network	Main Interface	Backup Interface	Delay	Up Delay	Down Delay	Track id	The second se	
Services	gigabitethemet 0/1	cellular 1	60	0	a	1]	Total Alarms: 0
Link Backup	gigabitethemet 0/1	cellular 1	• 60	10	10	11		Asarm summary
Routing	1					Add	4	12/31 *
Firewall	Internet and a second second with	288021						Stop
VPN	Apply & Save	Cancel						
APP '								
Industrial								
Tools								
Wizards								
Save Configuration								
Copyright ©2001-2019 InHand Networks Co., Lto All rights reserved.	4							

Step 6: Choose **Routing** > **Static Routing** to set corresponding parameters. Add three routes. 10.5.3.234 is the IP address of the LAN route for the PC. The distance parameter indicates the priority. The smaller the parameter value, the higher the priority.

Ind	Routing >> Static	c Routing					English	中文 Usernar TaLogo
tration •	Destination	blatmask	And a state of the	Calminar	Distance	Youth 14		Narm
6 Z	0.0.0.0	0.0.0.0	celular 1	sateway	255	THE IN		-
с <u>х</u>	0.0.0.0	0.0.0.0	gigabitethemet 0/1	10.5.3.254				Total Alarms: 0
tup 👌	203.86.63.233	255.255.255.0	gigabitethemet 0/1	10.5.3.254	10			Aserm Summary
Č 💦 🔥			•					14/3-
						Add		10.100
	Apply & Sa	ve Cancel						
al P								
,								
Configuration								
pht @2001-2019								
verwands Co., Ltd.								

Step 7: Disconnect the network cable to simulate a wired network fault. In this case, the gateway accesses the Internet through dial-up on the cellular port. Then, reconnect the network cable so that the gateway accesses the Internet through the wired network.

3.7.2 VRRP Hot backup

Several gateways are connected to the same network. Host A backs up gateway A. When gateway A is faulty, gateway B takes over the services on the faulty gateway to work as the host temporarily.

1. Networking requirements



Gateways A and B form a VRRP backup group, which is the default gateway used by host A to access host B on the Internet.

Structure of the VRRP backup group:

- The group number is 1.
- The IP address of the virtual gateway in the backup group is 192.168.2.254/24.
- Switch A is the master switch.
- Switch B is the backup switch and supports preemption.

2. Networking diagram



3. Configuration procedure

(1) Configure gateway A

Step 1: Configure G0/1.

Choose **Link Backup** > **VRRP** from the navigation tree and click the **VRRP** tab to configure VRRP.



inhand	Link Backup	>> VRRP							English 中文	Username: adm TuLogout
Administration	-		1		100050000	Adventionent		and all should be		
vetwork '	Enable Vi	rtual Route ID	Interface	Virtual IP	Priority	Interval(s)	Mode	Track ID		
ervices *	*	1	gigabitethemet 0/1	192.168.2.254	110	1	4			
nk Backup '	1 N		gigabitethemet 0 •	192 168 2 284		11				
outing '								Add		
rewall *	ETTORIST									
en P	Apply	& Save	Cancel							
PP '	5									
dustrial *										
ools ,										
/izards +	1									
Save Configuration										
pyright ©2001-2019 and Networks Co., Ltd All rights reserved.										

Choose **Link Backup** > **VRRP** from the navigation tree and click the **Status** tab to check the VRRP status.

hand	Lin	nk Back	vrrp							English 中文	Username: ad
nistration		Fuchts	Mint of Davids ID		idea al m	-	Advertisement	Preemption			
ork	· .	enable	virtual koute su	o interrace	Virtual IP	Priority	Interval(s)	Mode	TPack aD		
tes	* 1	8	1	gigabitethemet 0/1	192.168.2.254	110	1	-			
ackup	•			1 Billionen en ier e	102.1002.204						
g	*								Maa		
1	*	15725		2000200							
	*	A	oply & Save	Cancel							
	×.										
al	2										
Configuration											
ht \$2001-201	9										
Jetwanis Co., L	and .										

Step 2: Configure G0/2.

Choose Network > Ethernet from the navigation tree and click the Ethernet 0/2 tab to configure the Ethernet port 0/2.



inhand	Network >> Ethernet	3		English 무것 Userna [ktog	ime: adm jout
Administration Network Services Link Backup Routing Firewall VPN	Primary IP Netmask MTU Speed/Duplex Track L2 State Description	16.100.10.2 255.255.0 1500 Auto Negotistion		Alarm Total Alarms: Alarm Summar K. 3 s	0 y Stop
APP Industrial Tools Wizards	Multi-IP Settings Secondary IP Apply & Save Ca	Netmask	Add		
Save Configuration					
Copyright (52001-2019 InHand Networks Co., It All rights reserved.	-				1

(2) Configure gateway B

Step 1: Configure G0/1.

Choose **Link Backup** > **VRRP** from the navigation tree and click the **VRRP** tab to configure VRRP.

Addiminization Network • 1 gigabitethemet 0/1 192.108.234 100 1 • • • • • • • • • • • • • • • • •							9															-																																																																		٩.	1	101	A	1.1																																	
Services + 1 olgobietherret 0/1 192.108.2254 100 1 * • • • • • • • • • • • • • • • • • •				_		1	1		_	_	_	_	_	_		_	_	_	_	_	_	_	_	_	_		_	_							_					-																_	_	_	-	_	_	_	_	_	_	_	_	_	_	-	-	-	-	-	-		-	-	-	-			-	_	-	-	-	-	-	-	100														ŝ	k ID	ack	Tn	1.3	tion	npt	Mo	Pree	nt P	non (s)	ral(enn	ite	In	AC	1	ity	orit	rio	Pr
Link Sachup Routing Firewall App Ladustrial Tools Waraté	Jarms: 0	rms: 0	rms: 0	arms: C	darms:	Alarms	Alarm	larms	rms:	ns: O	0	-																																																																	1	1	0	0	0	1	5	15	m	ILL	ia	AJ.	1	to	To											*	*	Ŧ							4	4					1					2	00	10	
Routing · Firewall · VPN · A Apply & Save Cancel · · · · · · · · · · · · · · · · · · ·	ummary.	mmary	nmary	mmary	Jummai	Summ	Summ	umm	mai	nary	NY.																																																																			1	¥	Y	ty.	10	ar	60	110	m	ur	5	10	an	Al	1																			2	8								1					
Pirevail Apply & Save Cancel App Industrial Industrial Toole Vitrards	12-	7	7	3	17-1	4 2-	4 2	17.																																																																													1		į,	1	1			ŀ														bb	Ad																		
VPN Apply & Save Apply & Save Cancel Inductiol Tools VWtards Tools		2.5.	28.	28.	128.	11/23	0.23	128	23.	1	T		s	St	510	10	10	510	SHC .	SHC .		SHC .	St	Si	S	Si	SI	SI	51	51	51	ek e	10	10	10	10	ö	0	iii	i.	51	s	s	s	s	s	Si	51	51	s	s	Si	Sr	s	14	14	14	14	1	1	1	1	1	1	1	1	1	3	3	10	10	1	T	T	Ť	1	T	Ì	Ì	Ť	Ì	7	-	20	18	3	612	1				L																																	
App A Industrial A Toole A Witards A				- 12						1.8	1		-		-		-							-	-	1					-	-	2	2	2	2	2	2	8	8	10		-	1	1		-	10	10	-	-	-	1		-					1												1	1	1	ī	ī	1	1	1	1	1											L																																	
Industrial Tools Warands Warands																																																																																												L																																	
Tools * Witands *																																																																																												L																																	
voltaards :: • • • • • • • • • • • • • • • • • •																																																																																												L																																	
Save Configuration																																																																																												L																																	

Choose **Link Backup** > **VRRP** from the navigation tree and click the **Status** tab to check the VRRP status.



inhand	Link Backup >> VRRP	English 中文	C Username: adm
Administration	b Description of the second se	0	Varm
Network	, 1 gigabitethemet 0/1 Backup 100 -	-	
Services		10	otal Alarms: 0
Link Backup	· · · · · · · · · · · · · · · · · · ·	* Stop	and a second
Routing			(* 3 s *
Firewall			Stop
VPN			
APP			
Industrial			
Tools			
Save Configuration			
Copyright @2001-20 InHand Networks Co., I All rights reserved	19 1474		

Step 2: Configure G0/2.

Choose **Network** > **Ethernet** from the navigation tree and click the **Ethernet 0/2** tab to configure the Ethernet port 0/2.

dministration	Eturus Ethernet 0/1 Erid		Alarm
letwork	, Primary IP	10.100.10.3	
ervices	, Netmask	255 255 255 0	Total Alarms: 0
nk Backup	, MTU	1500	Alarm Summary
uting	Speed/Duplex	Auto Negotiation *	-w (2
ewall	Track L2 State		E. 23 Stop
'N	+ Description		
PP .	Multi-IP Settings		
dustrial	* Secondary IP	Netmask	
ols	•		
lizards		bbA	
	Annly & Saue C	lennel	
	a state of the		
Enus Configuratio			
save comparate			

Set the IP address of the default gateway for host A to 192.168.2.254, In normal cases, gateway A is in the running state. When it is powered off or faulty, gateway B takes over the services on gateway A. The preemption mode allows gateway A to assume the master role when it is restored.

3.8 Access Control List (ACL)

You can control the gateway to allow or prohibit access to network ports.

Configure the gateway as follows:



Step 1: Open the ACL page and click Add to add an access control list (ACL) and set parameters.

inhand	Firewall >> ACL		English 中交 Username: adm [].ikogout
Administration •	1.000.07004		Narm
Network '	lype	extended *	
Services *	1D	101	Total Alarms: 0
Link Backup	Sequence Number		Alarm Summary
Routing *	Action Match Conditions	deny 🖲	H 2
Firewall +	Protocol		Stop
VPN F	Source IP	107 168 2 1	
APP /	Source Wildcard	0.0.0266	
Industrial 1	Dectination IR	0.00200	
Tools ,	Dectination Wildcard		
Wiranda P	Eraoments		
	Log		
	Description		
Save Configuration	Apply & Save Cancel	Back	
Copyright ©2001-2019 InHand Networks Co., Ltd. All rights reserved.			

Step 2: Click **Apply & Save**. The information about the new ACL with the ID 101 is displayed on the page.

nhand	ACL									(CONTRACTOR)	Tetogou	
ninistration											Alarm	
work	Default Fil	ter Policy	Acc	ept •								
ices											Total Alarms: 0	
Backup	Access Cor	ntrol List									Alarm Summary	
ing '	ID	Sequence	Action	Proto	tol	Source	Destination	More	Description		Q 3 s	
all '	100	10	pennit	φ		any	any					\$10
	101	10	dony	έp		192.168.2.0/0.0.0.255	any					
,	179	10	pennit	P		any	ату					
trial ¹	192	10	permit&log	tcp		any	any: port=443					
	192	20	deny	tcp		any	anyt					
r '	192	30	deny	top		any	any: port=23					
	192	40	deny	tcp		any	any: port=22					
	192	50	deny	top		any	any; port=53					
	192	60	deny	udp	2	any	anyt port=53					
						Add	Mo	dify	Delirco			
Configuration	Interface L	ist				Based and the second						
		Interface	In ACL	Out ACL	Admin ACL							
	and the second second	cellular 1	none	none	192							
	bridge 1		 none 	none *	none 🔹							
ight ©2001-2019	6				Add							
lights reserved.	Apply	& Save	Cancel		(सत्त्रकाळ)							

Step 3: In Interface List, select cellular1 for Interface and 101 for Out ACL. Click Add and save the settings.



inhand		Firewall >> /	ACL							Engl	ish 中文 Username: Natiogout	adm
Administration											Alarm	189
Network		Default Fil	ter Policy	Acc	ept •						Residences	
Services	\mathbf{x}			10000							Total Alarms: 0	
Link Backup		Access Con	rtrol List								Atarm Summary	
Routing	,	ID	Sequence	Action	Protocol	Source	Destination	More	Description		1 ⁽⁴⁾ 3 s	. 4
Firewall	*	100	10	pemit	φ	any	any					Stop
VPN	.*	101	10	deny	Ψ	192.168.2.0/0.0.0.255	any					
APP		179	10	permit	iP.	any	any					
Industrial		192	10	permit®log	tcp	any	any: port=443					
Tools	•	192	20	deny	top	any	anyt					
Wizards		192	30	deny	top	any	any: port=23					
		192	40	deny	tcp	any	any: port=22					
		192	50	deny	top	any	any; port=53					
		192	60	deny	udp	any	anyt port=53					
						Ad	d Mo	dify	Oelero			
Save Configuration	20	Interface L	ist			Frank Street						
		I	nterface	In ACL	Out ACL Admin ACL							
			ellular 1	none	101 none							
		bndge 1		* anone *	none * none *							
Copyright @2001-2 InHand Networks Co	019 Ltd.				bbA							
All rights reserver		Apply	& Save	Cancel								12



4 Basic System Settings

4.1 User Management

Choose **Administration** > **User Administration** and click the **User Administration** tab. You can create and delete users and change your password.

Two user types are provided: superuser and common user.

- Only one superuser is provided and automatically created by the system. It has all the access permissions on the gateway. The superuser name is **adm**, and its default password is **123456**.
- Common users are created by the superuser and have the permission to view the gateway configuration, but cannot modify it.

User permissions are classified into three levels:

- Users of permission levels 1 to 11 can only view parameters but cannot set parameters.
- Users of permission levels 12 to 14 can configure the Ethernet interface LAN address, system time, static routes, basic firewall settings, virtual IP address mapping, system logs, and access control, apply for certificates, and upgrade the system.
- Users of permission level 15 can view and set all parameters.



The user name of the superuser (**adm**) cannot be modified, and the superuser cannot be deleted. However, its password can be changed.

4.2 System Time

You need to set the system time of the gateway accurately so that the gateway can coordinate with other devices.

Manual time synchronization: Choose **Administration** > **System Time** and click the **System Time** tab. Set time synchronization between the gateway and the connected host. Alternatively, set the system time of the gateway and select the time zone where the gateway is located. You only need to click **Sync Time** for manual time synchronization.



inhand	Administration >> System	Time	English 中文 Username: adm []stogout
Administration	2		Narm
Network	, Device Time	2019-04-04 15:49:44	
Services	PC lime	2019-04-04 15:49:44	Total Alarms: 0
Link Backup	10	Sync Lime	Atarm Summary
Routing			A 1
Firewall	 Year/Month/Date 	2019 * / 04 * / 04 *	Stop
VPN	 Hour:Min:Sec 	15 • : 49 • : 40 •	
APP		Apply	
Industrial			
Tools	* Timezone	UTC+08-00 China, Hona Kona, Western Australia, Singapore, Taiwan, Russia *	
Wizards		Apply & Save	
Save Configuratio	n		
Copyright ©2001-20 InHand Networks Co., All rights reserved	219 . kuil.		

Automatic time synchronization: Choose Administration > System Time, select SNTP or NTP, and select Enable to configure clock synchronization for all the devices in the network so that the gateway can provide multiple applications based on unified time.

SNTP is the simplified version of NTP. After SNTP is enabled, the gateway synchronizes the local time with the downstream device. SNTP is typically enabled for automatic time synchronization for InHand devices.

After NTP is enabled, the gateway assumes the client or server function to synchronize the time of all the other devices in the network.

inhand	Administration >> Syn	stem Time			English 🖛	交 Usernam	e: adm t
Administration Network Services Link Backup Routing	Enable Update Interval Source Interface Source IP	3600	s(60-2592000) T			Alarm Total Alarms: 0 Alarm Summary	
Firewall	* SNTP Servers List						Stop
VPN APP	Server Address O.pool.ntp.org	Port 123					
Industrial Tools	Lpcol.ntp.org Z.pcol.ntp.org Spcol.ntp.org	123 123 123					
Wizards -	Apply & Save	Cancel					
Save Configuration							
Copyright ©2001-201 InHand Networks Co., U All rights reserved.	9 Id						

4.3 System Upgrade

Choose Administration > Upgrade, click Browse, select an upgrade file, and click Upgrade.



inhand	Administration >> Upgrade		English 中文 Username: adm 「Logout
Administration	Select the file to use:		Alarm
Network	No file selected.	Browse Upgrade	Total Alarms: 0
Services	•		Alarm Summary
Link Backup	, Firmware Version : 1.0.0.r10575(beta)-2019-04-01-16-17-13	
Routing	· Carllelle miletiniegi estimiti		
Firewall	*:		3 s *
VPN	*		Stop
APP	E		
Industrial	*		
Tools	*		
Wizards	*		
Save Configura	tion		
Copyright ©2001 InHand Networks (All rights reserv	-2019 Joy, Ltd. red.		



Do not perform any operations on the web interface during software upgrade; otherwise, the upgrade may be interrupted.

4.4 System Restart

Choose **Administration** > **Reboot** and click **OK**. You can restart the system when the gateway module is not found on the web interface.

innand	Administration >> I	Reboot	English 中文 Username: adm
Administration	System	le .	Alarm
Network	System Time	Browse Upgrade	Test Manual O
Services	Management Services	1.0.0 r10575/hata)-2010-04-01-16-17-13	Alarm Summary
Link Backup	User Management	10.010375(Beta)-2015-04-01-10-17-15	
Routing	* AAA		č.
Firewall	Config Management		3 s *
VPN	, Device Networks		Stop
ADD	SNMP	•	
AFF	Alarm		
Industrial	Log		
Tools	Cron job		
Wizards	• Upgrade		
Save Configuration	Reboot		
Copyright ©2001-2015 InHand Networks Co. Lt All tiobs received	e.		



4.5 Changing the Language and Gateway Name

Choose Administration > System > Basic Settings to change the system language and gateway name.

inhand	管理 >> 系统	English 中文 뛰으오: adm
#10		(8.84
网络	, 界面语言 中文 *	
服务	· 设备名称 EdgeGateway	告輸受数:0
链路备彻		告册收录
路由	10.7071 (G RAN	e* 3.60 *
動火盪	. x	10 LU 10 10 10 LU
VPN		
APP		
工业体口		
IR		
快速向导		
8422		
Copyright © 2001- 오코바울레이라는 귀했 일찍 1612년 후	ecc0 남쪽에	

4.6 Management Services

When the gateway requires the HTTP, HTTPS, Telnet, and SSH functions, you need to enable the functions on the **Administration** > **Management Services** page of the web interface.

inhand	Administration >> Management Services Management Services	English 中文 Username: adm Fukegout
Administration •	HTTP	Aarm
Network '	Fashin P	Total Alarms: 0
Services *	Listen ID address	Alarm Summary
Link Backup	Port In	
Routing '	ACI Earble R	3 3 ×
Firewall *	ACCENSUIC	Stop
VPN *	Source Range IP Wildcard	
APP '		
Industrial *	Add	
Tools +		
Wizards +	HTTPS	
	Enable III	
	Listen IP address any	
	Port 441	
	ACL Emplo	
	ACC DIRDIC 100	
	Source Range IP Wildcard	
Save Configuration	Add	
	TELNET	
	Enable M	
	Listen ID arkinge	
Copyright ©2001-2019	Dest 23	
InHand Networks Co., Ltd.	ACI Facilia Ef	
	APPE Culotie and	



4.7 Checking System Logs

Choose **Administration** > **Log** to check system logs.

On this page, you can also clear and download logs, including historical logs. Historical logs are those logs with a long storage period specified on the **System Log** page.

The system diagnosis record file is encrypted and can be viewed only after being decrypted using the decryption tool provided by InHand. The gateway configuration is downloaded along with the system diagnosis record.

inhand	Lo	g System Log					TuLogout	
Administration	•						Narm	(item
Network	· ``	View recent Lines						1.000
Services	1	avel Time Content				Total Alarms: 0		
Link Backup			Too many logs, old logs are not displaye	oomanu loos, old loos are not displayed. Please download log file to check more logs!				
Deuties	. 1	info Apr 4 16:14:31	DeviceManager[1480]: cmd topic dm/tar	k/notice paylor	ad len 70 mid 9801		7011250	
Routing	1	info Apr 4 16:14:31	DeviceManager[1480]: task id 5ca5bcdd	e058fbe860de	bca type 4		14 3 5	۰.
Firewall	1	nfo Apr 4 16:14:31	DeviceManager(1480): get gateway conf	ig.				Stop
VPN	* 1	info Apr 4 16:14:31	DeviceManager[1480]: get gateway conf	successfully				
APP	, 1	info Apr 4 16:14:45	APPWatcher[1733]: Service ["app": "InMi	dous", "version	n": "1.0.0", "vendor": "Inhand", "app_id	(*: "5848cbe4390ec68b59ef902c1cc2e983") is alive		
	. 1	info Apr 4 16:15:22	DeviceManager[1480]: redial info imsi: is	cid: celid: lac: r	ncc: mnc: siglevel:0			
Industrial	1	info Apr 4 16:15:22	DeviceManager[1480]: upload lbs info (*	timestamp': "21	019-04-04108:15:22+0000*)			
Tools	1	info Apr 4 16:15:35	APPWatcher[1733]: Service ("app": "InModbus", "version": '10.0". "vendor": "Inhand", "app_id": "5848cbe4390ec68b59ef902clcc2e933") is alive					
Wizards	6 3	info Apr 4 16:16:21	DeviceManager[1480]: redial info imsi: iccid: celid: lac: mcc: mnc: siglevel(0					
	1	info Apr 4 16:16:21	DeviceManager[1480]: deviceInfo ("hw/ "iccid": "', "imsi": "', "deviceConfig": "BE	ersion"1 "", "boo ISOEEF4CF2D3I	xtVersion" "2017.01.r10319", "PN": "FE E2AE7290F703E991C7"}	278-W", "swVersion": "1.0.0:r10575(beta)-2019-04-01-16-17-13",		
	1	info Apr 4 16:16:22	DeviceManager[1480]: redial info imsk is	cid: cellid: lac: r	ncc: mnc: siglevelt0			
	1	info Apr 4 16:16:22	DeviceManager[1480]: upload lbs info (*	timestamp": "21	019-04-04108:16:22+0000")			
	1	info Apr 4 16:16:24	APPWatcher[1733]: Service ("app": "InMi	dous", "version": "10.0", "vendor": "Inhand", "app_id": "5848cbe4390ec68b59ef902c1cc2e933") is alive				
	1	Info Apr 4 16:16:31 DeviceManager[1480]: omd topic dm/task/notice payload len 70 mid 9802						
	1	nfo Apr 4 16:16:31	DeviceManager(1480); task id 5ca5bd55	e058fbe860e4	682 type 4			
	1	info Apr 4 16:16:31	DeviceManager[1490]: get gateway conf	ig .				
Enur Configuration	1	info Apr 4 16:16:31	DeviceManager[1480]: get gateway conf	successfully				
save comigeration	1	info Apr 4 16:17:12	APPWatcher[1733]: Service [*app*: 'InMi	odbus", "versior	n': "10.0", "vendor": "Inhand", "app_id	11: '5848cbe4390ec68b59ef90Zc1ccZe933') is alive		
		Info Apr 4 16:17:22	DeviceManager[1480]: redial info imsi: ic	cid: cellid: lac: r	ncc: mnc: sigleveb0			
		into Apr 4 16:17:22	DeviceManager[1480]: upload los into (*	timestamp': "2i	019-04-04708:17:22+0000")	-		
			Clear Log Download I	.og File	Download Diagnose Data			
			Clear History Log Download Hi	atory Log				
Conversion © 2001-201			8					
nHand Networks Co., L	1					Manual Refresh * Refresh		

The gateway provides a limited storage capacity, which is 512 KB by default. You need to use a remote log service, such as Kiwi Syslog Daemon, to save all log information. To obtain the software, you can contact InHand Sales Support or download it from the Internet. After you set the address and port of the log server on the web interface, the gateway uploads all system logs to the remote log server.

Administration Network Services Up3 Becker 10.516/21 514	Alarm
Services Syslogd server address Port Number Link Backup 10.5.16.21 514	
Routing + 514	Total Alarms: 0 Alarm Summary
Firewall Log to Console APP History log size Industrial History log severity Notice and above	Stop
Wizerds * Apply & Save Cancel	
Save Configuration Copyright (2001-2019 InHand Networks Co., 10.	



4.8 Alarm

The alarm function notifies you of any gateway errors promptly. The gateway reports an alarm when an error occurs. You can select predefined error types and a proper notification method to obtain error information. All alarms are recorded in alarm logs, allowing you to locate and fix errors as soon as possible.

(1) Choose **Administration** > **Alarm** > **Status** to view all alarms generated in the system since power-on.

Alarms have the following states:

- Raise: indicates that the alarm is generated but not confirmed.
- Confirm: indicates that the alarm cannot be cleared currently.
- All: indicates all generated alarms.

Alarms are classified into the following levels:

- EMERG: The gateway encounters a serious error that may cause a system reboot.
- CRIT: The gateway encounters an unrecoverable error.
- WARN: The gateway encounters an error that affects system functions.
- NOTICE: The gateway encounters an error that affects system performance.
- INFO: A normal event occurs.

inhand		Administration >> Alarm	Output Alarm Map		English	中文 Username: adm Logout
Administration		Alarm State	Roice .			Alarm
Network		ID Status Level date	All System Time Conten	1		
Services	•		Raise			Total Alarms: 0
Link Backup	•	Clear All Alarms	Confirm All Alarms	Reload		Marin Summary
Routing	,					0 35 *
Firewall						Stop
VPN						
APP						
Industrial	•					
Tools						
Wizards						
Save Configura	tion					
Copyright ©2001 InHand Networks 0 All rights reserv	-2019 io., Ltd. ed.					

(2) **Alarm Input**: Select the desired alarm type. An alarm is generated when an error of the selected type occurs.



(3) Alarm Output: When an alarm is generated, the system automatically sends the alarm content to the target email address. This function is unavailable for common users.

Enter information about the sender's email address in **Email Alarm**, and enter information about the receiver's email address in **Email Addresses**.

Mail Server IP/Name can be determined by searching the Internet. For example, if Tencent Exmail is used, enter **smtp.exmail.qq.com**.

inhand	Administration >> Alarm	English 中文 Username: adm	
ahiana	Status Alerm Input Alerm Output Alerm Map	Meggout	
Administration	, Email Alarm	Alarm	
Network Services Link Backup Routing	Enable Email Alarm; Id Mail Server IP/Name: Mail Server Port: 25 Acrower Name	Total Alarms: 0 Alarm Summary	
Firewall	Account Password:	Stop	
VPN	Crypte: NO *		
Industrial	Email Addresses(At least one address is needed.)		
Tools	* Add		
WILLIES	Apply & Save Cancel Send Test Email		
Save Coofiguration			
Copyright ©2001-2019 InHand Networks Co., Lt All rights reserved.	9 bd.		

(4) **Alarm Mapping**: You can select CLI (console port) or email for receiving alarms. To enable email mapping, you need to enable it on the **Alarm Output** tab page and set an email address.

4.9 Configuration Import and Backup

Choose Administration > Config Management, click Browse, select a configuration file, and click Import to import the configuration file to the gateway.

Click **Back Up running-config** to back up the current runtime configuration to the PC. This is a common operation.

Click **Back Up startup-config** to back up the boot file to the PC.



Administration	: 0	onfiguration					Alarm	
Network Services		No file selected.	Browse	Import	Backup running-config	Backup startup-config	Total Alarms: 0	
Link Backup		Auto Save after modify the configuration	n				Alarm Summary	
Firewall		Encrypt plain-text password					n,₽ <u>3 s</u>	* Stop
VPN	•	Backup running-config with private key	1					
APP	; [Restore default configuration						
Tools								
Wizards								
Save Configuratio	m							
Copyright ©2001-20 InHand Networks Co. All rights reserved	19 Ltd.							

4.10 Restoring Default Settings

4.10.1 Webpage Mode

Choose **Administration** > **Config Management** and click **Restore Default**. The default settings are restored after the system restarts.

4.10.2 Hardware Mode

Restore the default settings in hardware mode as follows:

Step 1: Find the **RESET** button on the gateway panel.

Step 2: Press and hold the **RESET** button for 10 seconds after the gateway is powered on.

Step 3: Release the **RESET** button when the ERR indicator is in red.

Step 4: Press and hold the **RESET** button for 1 second when the ERR indicator is off.

Step 5: Check whether the ERR indicator blinks three times and then turns off. If yes, the default settings are restored successfully.



5 Connecting the Gateway to a Cloud Platform

Two connection protocols are supported: Message Queue Telemetry Transport (MQTT, applicable to the **remote device monitoring platform**) and Open Virtual Device Protocol (OVDP, applicable to the **gateway platform**). The remote device monitoring platform is recommended because it allows the gateway to be automatically added on the cloud platform. Either of the two platforms can be selected for connection.

1) Using the remote device monitoring platform

Procedure:

Step 1: Choose Administration > Device Networks, click the Device Networks tab, and select Device Networks Enable. Enter the cloud platform address and the account that registers the cloud platform. Click Apply & Save.

Step 2: Log in to the cloud platform to add the gateway.

inhand		Administration >> Device Netv	vorks	English 中文	Username: adm
opiaio		Statia Device Networks Device	Management Legacy		Logout
Administration	٠			Alarm	n 📂
Network		Device Networks Enable	*		
Services	,	Server Address	www.shebeiyun.net	Total	Alarms: 0
Link Backup		HTTPS	8	Alarm	Summary
Routing	,	Registered Account	panjp@inhand.com.cn	3.1	35. *
Firewall		Show Advanced Options			Stop
VPN	•				
APP		Apply & Save Cancel			
Industrial	•				
Tools	•				
Wizards					
ورد المواديو المراجع					
Save Configurate	20				
Copyright ©2001-2 InHand Networks Co All rights reserve	019 Ltd. 1,				

2) Using the gateway platform

Procedure:

Step 1: Choose Administration > Device Networks, click the Device Management Legacy tab, and select Enable. Enter the cloud platform address and click Apply & Save.

Step 2: Log in to the cloud platform to add the gateway.



inhand		Administration >> Devi	e Networks	English 中文 Username: adm
ahimin		Status Device Networks	Device Management Legacy	Megout
Administration	٠			Alarm
Network		Enable	*	
Services	,	Mode	SMS & IP ·	Total Alarms: 0
Link Backup		Vendor	Default •	Alarm Summary
Routing		Device ID	902434211	2.2.
Firewall		Server	c. inhand.com.cn	Stop
VPN		Port	20003	
A99		Login Retries	3	
Industrial		Heartbeat Interval	120 s	
Tools	,	Serial Type	RS232 •	
Winneds		Protocol	UDP •	
we have us				
		Apply & Save	Cancel	
save contigutat	1911			
Convertent # 2001.	2119			
InHand Networks C	o. Ltd.			
All rights reserv	PØ,			



6 Industrial Interface (DTU)

Set the gateway's DTU function to enable the gateway to communicate with the server. The following figure shows the related topology.



Configure the gateway as follows:

Step 1: Set the DTU serial port parameters. Ensure that the parameter settings are consistent with those of the peer device's serial port.

inhand		Industrial >> DTU Serial Port OTU 1 OTU 2		English 中文 Username: adm
Administration	٠	Serial Port 1		Alarm
Network	1	Autora de la companya		Table Alternation O
Services	,	Serial Type	R5232 *	Alara Summant
Link Backup		Baudrate	9600 •	Startin Sentimery
Routing	,	Data Bits	8 bits 🔻	#12+
Firewall		Parity	None *	Stop
VPN		Stop Bit		
400		Software Flow Control		
Industrial		Description		
Industrial		Serial Port 2		
lools		Million Const		
Wizards		Serial Type	RS495 *	
		Baudrate	9600 •	
		Data Bits	8 bits •	
		Parity	None.*	
		Stop Bit	1 bit 🔹	
		Software Flow Control		
Save Configurat	ian	Description		
		Apply & Save Cancel		
Copyright ©2001- InHand Networks Co All rights reserve	2019 o. Ltd. ed.			

Step 2: Set the DTU function parameters.

inthand			InHand Networks Edge Computir	ng Gateway IG902 User Manual 🧲
inhand		Industrial >> DTU Secul Pool DTU 1 (DTU 1		English 中文 Username: adm Categout
Administration	٠	Enable		Alarm
Network		DTU Protocol	Transparent	Total Alexand
Services	,	Protocol	TCP Protocol •	Alarm Summan
Link Backup		Connection Type	Long-lived •	Roth Johnsty
Routing	•	Keepalive Interval	60 5	(%) 35 Y
Firewall	- 5	Keepalive Retry	5	Stop
VPN		Serial Buffer Frame	4 -	
APP		Packet Size	1024 Bytes	
Industrial		Force Transmit Timer	100 ms	
Tools		Min Reconnect Interval	15 5	
Winneds		Max Reconnect Interval	15 s	
(And a second s		Multi-server policy	parallel •	
		Source Interface	IP •	
		Local IP Address		
		DTU ID		
		Enable Debug	0	
Save Configurat	sn.	Enable Report ID	10	
		Destination IP Address		
		Server Address	Server Port	
Copyright ©2001- InHand Networks Co All rights reserve	2019 5. Ltd. d,		Add	

Step 3: Check that the gateway-connected PC and the server exchange data through DTU.

8	т	CP Client Server		X
	TCP Clic Firewalls & Intru	ent Serv		auditor.com
Nsauditor Netwo	rk Security Auditor - Scan	and monitor network for	vulnerabilities.	Download Now!
TCP Client Ser	ver 1.129.6 ▼ IP: 172.31.	129.6 Port 30005	Server	Listen
Peers 119.4.2	53.24-3823 V Close Conne	ction Send	C Clien	Shutdown
Send				
Receive				
Time:10:12:49	- New Connection Detected:	119. 4. 253. 24–38234		×
<				× >



7 App Development

This chapter describes how to quickly develop apps in Python. Development of an InModbus app is used as an example.

7.1 InModbus App

7.1.1 Installing an InModbus App

(1) On the gateway's web interface, choose **APP** > **APP** and click the **APP Management** tab. Select **Enable APP Manager** and **Enable IDE Debug**. Click **Browse** and select the InModbus app file package. Click **Upload** to upload the app to the gateway.

					11-					1
ration	Enable	APP Ma	nager							Alarm
	Enable	IDE Det	bug							Total Alarm
	Enable	Extende	ed Flash	8						Alarm Summ
cup *	-									
•	Import	APP Pa	ckage							
,	C.'ifakep	ath\inModba	us 2-V0 0.5 tar gz		E	rowse Upload				3 s
*	Concerne and		2611463		10					
•	APP Co	onfigurat	tion							1
•	Enable	ID	APP Name	APP Version	SDK Version	Start Parameters	Logfile Size(KB)		Operation Me	
	۲	1	InModbus	0.0.6	1.0.8		70	Import Config	Export Config Ex	1
,										Í
	APP M	anagem	ent							1
	STAR	TALL	STOP ALL							1
onfiguration	RESTA	ART ALL								
	ID	API	P Name	Оре	eration Me	thod				1
	1	InN	Aodbus	Start	Stop	Restart				1

(2) Import the custom app configuration file. If the configuration file does not need to be modified, the gateway uses the default configuration file in the app package by default.

rk F	Enable APP Manager	۲				Alarm
ns +	Enable IDE Debug					Total Alarms: 0
ackup *	Enable Extended Hash					Alarm Summary
, ,	Import APP Package					(* 3 s
	No file selected.	B	owse Upload			
	APP Configuration					
	Arr comparation	488 50V		Leafle		
	Enable ID APP Name	Version Version	Start Parameters	Size(KB)	Operation Method	
	1 InModbus	0.0.6 1.0.8		70 Import Config	Export Config Export App Uninstall	
	APP Management					
	BTART ALL STOP ALL					
	RESTART ALL					
	ID APP Name	Operation Me	hod			
	1 InModbus	Start Stop	Restart			
Configuration						
Sectored	Apply & Save Cancel	1				



(3) Configure and launch the InModbus app.

Administration	Shirhur APP I	Management V	Table Ver	Status							Alarm	ogout 📃
Network *	Enable IDE I	Debug									Total Alarm	- 0
Services *	Enable Exte	nded Rash	55								Alarm Summ	ary
Link Backup		2010										
Routing	Import APP	Package									(* 3s	
Firewall	No file select	ed.		Bro	owse Upload							Stop
VPN	APP Continu	wation										
APP												
Industrial	Enable ID	APP Nan	e ve	rsion Version	Start Parameters	Size(KB)		Operation	n Method			
TODIS	1	InModbe	s (0.6 1.0.8		70	Import Config	Export Config	Export App	Uninstall		
Wigerus	Step:1	1002.02										
	APP Manage	ement										
	BTART ALL	STOP ALL	l)									
	RESTART AL	L										
	10	APP Name		Operation Met	hod							
	1	InModbus	Start	Stop	Restart							
Save Configuration	-											
	Apply 8	Save Cano	el									
	Ste	p:2										
Copyright 8:2001-2019												

(4) Check the InModbus app status.

On the gateway's web interface, choose APP > APP > Status to view details about the Python app, for example, the app name, version, running status, runtime, and action. To view the run log of the app, click **Show Log**. The log is displayed on a new tab page. If InModbus cannot start, check whether the system firmware version matches the Python SDK version.

Administration	Status	Mer Managament, Var	Table	er Sterue					leLogo	ut (m)
Network *	Extend	ed Memory Card	Unre	cognized					Austra	
Services +	APPMa	mager Status	Runn	ning	· · · · · · · · · · · · · · · · · · ·				Total Alarms: 0	
Link Backup	SDK Ve	ersion	1.0.9	-beta U	pg/ade				Alarm Summary	
Routing +	Debug	Server Status	Stop	ped						
Elemental P	APP Fil	esystem Use%	1% c	of 6709 MI	3				W 39	Plan
VDN F	Data/U	og Filesystem Use%	1% 0	16709 M	5					Sub
APP 1	Extend	ed Filesystem Use%	0%							
ner t										
Trada t		-								
TODIS	APP Run	ining Status								
Wigards	1D	APP Name	APP Version	SDK Version	State	Uptime	Action			
	1	InModbus	0.0.6	1.0.8	running	pid 6626, uptime 0:11:27	Clear Log Show Log			
								Manual Refresh * Refresh		
Save Configuration										
Copyright © 2001-2019 InHand Networks Co., Ltd All rights received.										

7.1.2 Enabling the Remote Device Monitoring Platform

The remote device monitoring platform is the software that provides the monitoring service for onsite devices and implements the maintenance management, energy monitoring, asset management, and variable monitoring and management functions. The data collected by the InModbus app is uploaded to the platform through a built-in application of the remote device monitoring platform.



To use the remote device monitoring platform, register an account at <u>http://www.shebeiyun.net</u> and log in to the platform by using the registered email address. After login, bind the gateway to your account.



Skip this section if you need to upload data to other platforms than www.shebeiyun.net. Ensure that the platform that you use is supported by InModbus 2 and that the connection parameters are set in the configuration file.

On the gateway's web interface, choose **Administration** > **Device Networks** and click the **Device Networks** tab to enable the remote device monitoring platform. Enter the server address **www.shebeiyun.net** and register an account with your email address, such as xxx@inhand.com.cn. Retain the default settings for other options if you do not have special requirements. Click **Apply**. To check the connection status, click the **Status** tab. **Connected** indicates that the connection is normal.

-Press	Device Networks	Watagement Logocy	Legout
Administration	Step:3		Alarm
Network Step:1	Device Networks Enable	Step:4	
Services	Server Address	www.shebeiyum.net Step:5	Total Alarms: 0
Link Backup	HTTPS	8	exam summary
Routing	Registered Account	XXX@inhand.com.en	12 3.0 *
Firewall	Show Advanced Options	0	Stop
VPN			
APP	Apply & Save Cancel		
Industrial	Step:6		
Tools	Constant of the		
Wizards	•		
Save Configuration			
Copyright &2001-2019 Hand Networks Co., Lt All rights reserved.	e.		

inhand		Administration >> Device	e Networks Gentre Management Legac	English	中文 Usernar TeLogo	ne: adm ut
Administration	;	Device Networks			Narm	e
Services	x	Device Networks	Connected		Total Alarms: 0	
Link Backup		Description	Connection Accepted			
Firewall	•			Manual Refresh • Refresh	174 3 8	* \$100
VPN	×					
APP	. 2					

7.1.3 Enabling the Variable Editing Service

Choose **APP** > **Var Table**, select **Enable**, and click **Apply & Save** to enable the variable editing service. After the service is enabled, the hidden options on this page are displayed.



inhand		APP >> APP Status APP M	Step: Innegement Var Tabl	• Ver St	etas					Er	nglish 中文 Userna 「「Log	ime: adm
Administration	•	Enable		Step:3	i.						Alarm	
Services		Controller Li	icts								Total Alarm	s: 0
	1.0	controller 1									Alarm Summ	ary
Link Backup		Sequence	Controller Name	Protoco	Туре	Addr	ess	Byte Order			Constantia a	nile migh
Routing		1	IG902-1	Modbu	s TCP	10.5.10	5.21	abcd				and the
Firewall		2	IG902-2	Modbu	s TCP	10.5.16	5.21	abcd			3 s	*
VPN					Add		Modify	Delete				Stop
APP	t	Erona										
Industrial Step:	1.16	Groups										
Tools	٠	Sequence	Group Name		Polling Interval(s)	Uploading Interval(s)	Add V	ar			
Wizards	108	1	titt		5		5	add				
								Ad	bt			
		Step	:4									
Save Configurat	ion	Apply 8	Save Cancel									
		Please restar	t APP(InModbus2) af	ter editin	<mark>g in order</mark> to	reload	configure fi	ile				
Copyright ©2001- InHand Networks Co All rights reserve	2019 o., Ltd. ed.											



After the configuration is complete, restart the app manually to make the new configuration effective.

7.1.4 Modifying Configuration

7.1.4.1. Adding and Modifying Devices

This operation corresponds to the <u>Controller</u> part of configuration file editing. To add a device, click **Add** on the **Var Table** tab page and click **Apply & Save**.



Device information, such as the device name, cannot be modified after being saved.

Such device information includes:

1. Device name (special characters and numeric strings are not allowed)

2. Variable address order (which can be empty after being created and are system-defined by default)

3. Register address (which cannot be modified or deleted when being used by the collection group)



inhand		APP >> APP	Var Table	Ver Plat					English	₽Ż Userna [ielog	ime: adm out
Administration		1	and the second	Ye	our passwo	ord has security	/ risk, please (lick here to change! *			
Network	•	Enable		0						Alann	1
Link Backup		Controller Lists	U.							Total Alarms: Alarm Summar	0
Routing Firewall VPN APP Induttrial		Sequence C	Controller Name 19902-1 19902-2	Protocol T Modbus T Modbus T	Y ype TCP TCP Add	Address 10.5.16.21 10.5.16.21 Modily	Byte Order abcd abcd Deletz			<u>(</u> 1]35	7 Stop
Tools Wizards		Groups Sequence	Group Name titi PPPP		Polling Interval(s) 5	Uploading Interval(s) 5	Add Var add add	* * *			
Sare Configuration	21	Apply & Sa Please restart Al	ave Cantel PP(InModbus2) af	, ter editing	In order to r	reload configure	Add]			
Copyright ©2001-2 InHand Networks Co All rights reserve	019 , Ltd. d.										

7.1.4.2. Adding and Modifying Collection Groups

This operation corresponds to the <u>Collection Policy Group</u> configuration, in which the collected I/O values are calculated based on policies. To meet different requirements, the configuration file uses micro expressions. In the format of micro expressions, <value> indicates the value collected by the current register address, and values['id'] indicates the value calculated by the register address with the specified ID.

			Your p	assword I	has security	risk, please c	ick here to change! *	
Network	Enable							Alam
Services Link Backup	. Cantan Tan	late						Total Alarms: 0
Routing	+	LISTS						Alarm Summary
Firewall	> Sequence	Controller Name	Protocol Type	Add	iress	Byte Order		
VDN	+ 1	19902-1	Medbus TCP	10.5	15.21	abed		Ck 3.5 *
APP		10502-2	MODOUS FOF	dd b	Modily	Delata		Stop
Industrial							2	
Tools	. Groups							
Wizards	* Sequence	Group Name	Pe	iling sval(c)	Uploading Interval(s)	Add Var		
	1	tata		5	3	add		
	z	PPPP		5	5	add	a a m	
						Add		
	Apoly	& Save Cancel						
Save Configuration	Please resta	rt APP(InModbus2) a	fter editing in ord	er to reloa	d configure fil	le		

A Note:

Collection group information, such as the group name, cannot be modified after being saved.



iministration	Enable	tanagament Var Tak	e Mail Startus					6	larm (
CVICES .	Controller							To	otal Alarms: 0
k Backup	Controller L	1843						A	arm Summary
ding 1	Sequence	Controller Name	Protocol Type	Address	Byte Order				Stranger and Stranger
anny	1	19902-1	Modbus TCP Modbus TCP	10.5.16.21	abod				1. 39
FA-38		10001-1	Modulus ICF	ht.dl.	Debete				Stop
4			Muu	mouny	- Desete				
1 (Groups								
ustrial						_			
Ns .	Sequence	Group Nam	Poliir Interva	ig Uploading	Add Var				
tards 1	1	titt	5	5	add 🔫	e +	- Step:1		
	2	pppp	5	5	bbe				
					Add				
	Apply i	k Save Cancel							
	Please restar	t APP(InModbus2) a	fter editing in order	to reload configure	file				
ave Configuration									

ation *	tttt													Alarm		
1		Controller		Register	Calculate		Upleading							Total A	Jarms: 0	
2	tD.	Name	Address	Level	Mode	Unit	Data Type	Expression	Trigger	Expression(wr	nte) Des	cription		Alarm	Summary	
4p	1	16902-1	40001	1	Instant		int	«value»			4	1000				
	2	10902-1	40003	1	instant		int	<value></value>			4	0003			3 3 5	
1		15902-1 *	+0001 +	<u>10</u>	ristant •		ini 🔻	<value></value>		-value>	0.025	1	Step:2			Stop
										Delete	OK	Cancel				
												Adıt				
	S	tep:3										Adıt				
:	S	tep:3	Cancel	Bac	k							hbA				
•	S Aa 'Expressic	tep:3 Ny & Save	Cancel <value> ref</value>	Bas fer to the c	k Jurrent registe	r address	i data, valusi	es[<mark>1</mark> d] refer 1	o the spec	cific register ac	ddress d	Adat	ne id you point.			
	Si Apr 'Expressic	tep:3 Ny & Save n' Remind: -	Cancel <value> ref</value>	Bac	k Jurrent registe	r address	s data, valus	es["ld"] refer t	o the spec	cific register ac	ddress d	Add	ne id you point.			
, , ,	Si Asy 'Expressic	tep:3 /v/&Save n'Remind:	Cancel (value > ref	Bac	k urrent registe	r address	s data, valus	es[1d] refer t	o the spec	cific register ac	ddress d	Add	te id you point.			



8 Appendix CLI Commands

1 Help Command

You can enter **help** or **?** on the console to obtain command assistance. When entering a command, you can enter **?** to obtain help information about the current command or command parameters. When the entered command or command parameters are unique, they can be complemented automatically.

1.1 help

Command: help [<cmd>] Function: obtains command assistance. View: all views Parameter: <cmd> indicates a command name. Example: \$ Enter help.

- The command output lists all available commands.
- \diamond Enter **help show**.

The command output lists all the parameters of the **show** command and related ons.

instructions.

2 View Switching Commands

2.1 enable

Command: enable [15 [<password>]] Function: enters privileged EXEC mode. View: common user view Parameter: 15 indicates a user permission level. Currently, only permission level 15 (superuser) is supported. <pre

2.2 disable

Command: disable Function: exits privileged EXEC mode. View: superuser view and configuration view Parameter: none Example: Enter disable in the superuser view. The system returns to the common user view.

2.3 end and !

Command: end or ! Function: exits the current view and returns to the previous view. View: configuration view Parameter: none Example: Enter end in the configuration view. The system returns to the superuser view.

2.4 exit



Command: exit

Function: exits the current view and returns to the previous view. If the current view is the common user view, entering this command will log you out of the console.

View: all views

Parameter: none

Example:

- $\diamond \quad \text{Enter exit in the configuration view.}$
 - The system returns to the superuser view.
- ♦ Enter exit in the common user view. The system exits the console.

3 Commands for Checking the System Status

3.1 show version

Command: show version

Function: shows the model, software version, and other information about the gateway. **View:** all views

Parameter: none

Example: Enter show version.

The following information is displayed: Model: model of the gateway SN: SN of the gateway Description: www.inhand.com.cn Current version: current version of the gateway Current bootloader version: current bootloader version of the gateway

3.2 show system

Command: show system Function: shows information about the gateway system. View: all views Parameter: none Example: Enter show system. The following information is displayed: For example, 00:00:38 up 0 min, load average: 0.00, 0.00, 0.00

3.3 show clock

Command: show clock Function: shows the system time of the gateway. View: all views Parameter: none Example: Enter show clock. The following information is displayed: For example, Sat Jan 1 00:01:28 UTC 2000

3.4 show modem

Command: show modem Function: shows the modem status of the gateway. View: all views Parameter: none Example: Enter show modem. The following information is displayed: Modem type Status Vendor



Product name Information level Registration status IMSI Network type

3.5 show log

Command: show log [lines <n>]

Function: displays the system logs of the gateway. By default, the latest 100 logs are displayed.

View: all views

Parameter: **lines** $\langle n \rangle$ indicates the number of logs that can be displayed. When *n* is set to a positive integer, the *n* latest logs are displayed. When *n* is set to a negative integer, the *n* earliest logs are displayed. When *n* is set to 0, all logs are displayed.

Example: Enter **show log**.

The 100 latest logs are displayed.

3.6 show users

Command: show users Function: shows the user list of the gateway. View: all views Parameter: none Example: Enter show users. The following system user list is displayed: User:

* adm -----The user marked with an asterisk (*) is the superuser.

3.7 show startup-config

Command: show startup-config Function: shows the startup configuration of the gateway. View: superuser view and configuration view Parameter: none Example: Enter show startup-config. The startup configuration of the system is displayed.

3.8 show running-config

Command: show running-config Function: shows the runtime configuration of the gateway. View: superuser view and configuration view Parameter: none Example: Enter show running-config. The runtime configuration of the system is displayed.

4 Commands for Checking the Network Status

4.1 show interface

Command: show interface Function: shows the interface status information about the gateway. View: all views Parameter: none Example: Enter show interface.



The status of each interface is displayed.

4.2 show route

Command: Show ip route Function: shows the routing table of the gateway. View: all views Parameter: none Example: Enter Show ip route. The routing table of the system is displayed.

4.3 show arp

Command: show arp Function: shows the ARP table of the gateway. View: all views Parameter: none Example: Enter show arp. The ARP table of the system is displayed.

5 Network Test Commands

The gateway provides network test tools, such as ping, Telnet, and traceroute.

5.1 ping

Parameter: *<hostname>* indicates the IP address or domain name of the host for Telnet login.

<port> indicates the Telnet port.

source $\langle ip \rangle$ indicates the IP address used during Telnet login.

Example: Enter telnet 192.168.2.2.

Login is initiated to 192.168.2.2 through Telnet.

5.3 traceroute

Command: traceroute *<hostname>* [maxhops *<n>*] [timeout *<n>*]

Function: performs gateway detection on the specified host.

View: all views

Parameter: *<hostname>* indicates the IP address or domain name of the host to be detected. maxhops *<n>* indicates the maximum number of hops during gateway detection.

timeout *<n>* indicates the timeout period of each hop, in seconds.

Example: Enter traceroute www.g.cn.

The system performs gateway detection on www.g.cn and displays the detection results.



6 Configuration Commands

You can run the **configure** command in the superuser view to switch to the configuration view for gateway management. Some configuration commands support the **no** and default forms. The no form cancels the setting of a parameter, and the default form restores the default setting of a parameter.

6.1 configure

Command: configure terminal

Function: switches to the configuration view and enters configuration from a terminal.

View: superuser view

Parameter: none

Example: Enter **configure terminal** in the superuser view.

The system switches to the configuration view.

6.2 hostname

Command: hostname [*<hostname>*]

default hostname

Function: shows or sets the host name of the gateway.

View: configuration view

Parameter: *<hostname>* indicates a new host name.

Example:

- \diamond Enter **hostname** in the configuration view. The host name of the gateway is displayed.
- ♦ Enter hostname MyRouter in the configuration view. The host name of the gateway is set to MyRouter.
- Enter **default hostname** in the configuration view. The host name of the gateway is restored to the default one.

6.3 clock timezone

Command: clock timezone *<timezone> <n>*

default clock timezone

Function: sets the time zone information about the gateway.

View: configuration view

Parameter: <*timezone*> indicates the name of a time zone, consisting of three uppercase letters.

<*n*> indicates the time zone offset, in the range from -12 to +12.

Example:

- Enter clock timezone CST -8 in the configuration view. \diamond
 - The gateway is set to the UTC+8 time zone named CST (short for China Standard

Time).

Enter **default clock timezone** in the configuration view. ∻ The gateway is restored to the default time zone.

6.4 clock set

Command: clock set *<YEAR/MONTH/DAY>* [*<HH:MM:SS>*] Function: sets the date and time of the gateway. View: configuration view **Parameter:** <*YEAR/MONTH/DAY* > indicates a date, in the format *year-month-day*. *<HH:MM:SS >* indicates the time, in the format *hours-minutes-seconds*. Example: Enter clock set 2009-10-5 10:01:02 in the configuration view.

The time of the gateway is set to 10:01:02, October 5, 2009.

6.5 ntp server



Command: ntp server <hostname> no ntp server default ntp server Function: sets a client for the NTP server. View: configuration view Parameter: <hostname> indicates the IP address or domain name of the NTP server host. Example: Enter sntp-client server pool.ntp.org in the configuration view. The address of the NTP server is set to pool.ntp.org.

7 System Management Commands

7.1 reboot

Command: reboot Function: restarts the system View: superuser view and configuration view Parameter: none Example: Enter reboot in the superuser view. The system is restarted.

7.2 enable password

Command: enable password [<password>] Function: changes the password of the superuser. View: configuration view Parameter: <password> indicates a new password of the superuser. Example: Enter enable password in the configuration view. Enter a password as prompted.

7.3 username

Command: username <*name*> [password [<*password*>]] no username <*name*> default username Function: sets the user name and password. View: configuration view Parameter: none Example: ♦ Enter username abc password 123 in the config

- Enter username abc password 123 in the configuration view.
 A common user is added, with the user name abc and password 123.
- ♦ Enter no username abc in the configuration view. The common user abc is deleted.
- ♦ Enter default username in the configuration view. All common users are deleted.