

Industrial LoRaWAN[®] Gateway UG56

User Guide



Preface

Milesight

Thanks for choosing Milesight UG56 LoRaWAN[®] gateway. UG56 delivers tenacious connection over network with full-featured design such as automated failover/failback, extended operating temperature, hardware watchdog, VPN, Gigabit Ethernet and beyond.

This guide shows you how to configure and operate the UG56 LoRaWAN[®] gateway. You can refer to it for detailed functionality and gateway configuration.

Readers

This guide is mainly intended for the following users:

- Network Planners
- On-site technical support and maintenance personnel
- Network administrators responsible for network configuration and maintenance

©2011-2025 Xiamen Milesight IoT Co., Ltd.

All rights reserved.

All information in this user guide is protected by copyright law. Whereby, no organization or individual shall copy or reproduce the whole or part of this user guide by any means without written authorization from Xiamen Milesight lot Co., Ltd.

Related Documents

Document	Description
UG56 Datasheet	Datasheet for UG56 LoRaWAN® gateway.
UG56 Quick Start Guide	Quick Installation Guide for UG56 LoRaWAN® gateway.

Declaration of Conformity

UG56 is in conformity with the essential requirements and other relevant provisions of the CE, FCC, and RoHS.





For assistance, please contact Milesight technical support: Email: <u>iot.support@milesight.com</u> Support Portal: support.milesight-iot.com Tel: 86-592-5085280 Fax: 86-592-5023065 Address: Building C09, Software Park III, Xiamen 361024, China

Revision History

Date	Doc Version	Description
Aug. 9, 2022	V1.0	Initial version
Apr. 21, 2023	V 1.1	 Add BACnet Server feature Add Payload Codec feature Add Reset and all flows export feature on Node-RED Add data retransmission feature on Packet Forward Add Beacon time offset 8 profiles are pre-configured on Profiles page
Aug. 2, 2024	V 1.2	 Add cellular customize MTU and IMS feature; Support to import ovpn file for OpenVPN connection; Support packet filter feature; Add default WLAN connection password; Add username on SMTP client setting; Add BACnet object types, support object instance customization.
Jan. 8, 2025	V 1.3	 Add MQTT data re-transmission and retain option; Add metadata option and remove BACnet/IP option under Application page; Add object mapping function on Payload Codec page; Add BACnet object event detection feature and Notification-class object type; Add Modbus server feature; Add WireGuard feature; Add cellular subnet mask and DNS server customization; Compatible with DeviceHub 2.0; Add Node-RED SSL access option. Add network packet analyzer feature.
April 3, 2025	V 1.12	 Add FUOTA feature; Add MQTT Last Will Message feature; Update application key options when adding a device; Update metadata option; Update WAN default connection type as DHCP; Update web GUI access steps.

Contents

Chapter 1 Product Introduction	7
1.1 Overview	7
1.2 Advantages	7
Chapter 2 Access to Web GUI	9
Chapter 3 Web Configuration	
3.1 Status	
3.1.1 Overview	12
3.1.2 Cellular	
3.1.3 Network	14
3.1.4 WLAN	
3.1.5 VPN	16
3.1.6 Routing	
3.1.7 Host List	
3.2 LoRaWAN	19
3.2.1 Packet Forwarder	
3.2.1.1 General	
3.2.1.2 Radios	21
3.2.1.3 Noise Analyzer	
3.2.1.4 Advanced	
3.2.1.5 Custom	
3.2.1.6 Traffic	
3.2.2 Network Server	
3.2.2.1 General	
3.2.2.2 Application	
3.2.2.3 Payload Codec	
3.2.2.4 Profiles	
3.2.2.5 Device	
3.2.2.6 FUOTA	
3.2.2.7 Multicast Groups	
3.2.2.8 Gateway Fleet	
3.2.2.9 Packets	
3.3 Protocol Integration	
3.3.1 BACnet Server	
3.3.1.1 Server	50
3.3.1.2 BACnet Object	
3.3.2 Modbus Server	55
3.3.2.1 Server	55
3.3.2.2 Modbus Object	56
3.4 Network	58
3.4.1 Interface	
3.4.1.1 Port	

3.4.1.2 WLAN	61
3.4.1.3 Cellular	64
3.4.1.4 Loopback	67
3.4.1.5 VLAN Trunk	68
3.4.2 Firewall	68
3.4.2.1 Security	69
3.4.2.2 ACL	69
3.4.2.3 DMZ	71
3.4.2.4 Port Mapping (DNAT)	71
3.4.2.5 MAC Binding	72
3.4.3 DHCP	73
3.4.4 DDNS	74
3.4.5 Link Failover	75
3.4.5.1 SLA	75
3.4.5.2 Track	75
3.4.5.3 WAN Failover	
3.4.6 VPN	77
3.4.6.1 DMVPN	78
3.4.6.2 IPSec	79
3.4.6.3 GRE	
3.4.6.4 L2TP	83
3.4.6.5 PPTP	
3.4.6.6 OpenVPN Client	
3.4.6.7 OpenVPN Server	
3.4.6.8 Certifications	
3.4.6.9 WireGuard	
3.5 System	
3.5.1 General Settings	
3.5.1.1 General	
3.5.1.2 System Time	
3.5.1.3 SMTP	
3.5.1.4 Phone	
3.5.1.5 Email	
3.5.2 User Management	
3.5.2.1 Account	
3.5.2.2 User Management	
3.5.3 SNMP	
3.5.3.1 SNMP	
3.5.3.2 MIB View	
3.5.3.3 VACM	
3.5.3.4 Trap	
3.5.3.5 MIB	
3.5.4 Device Management	
3.5.4.1 Auto Provision	

3.5.4.2 Management Platform	104
3.5.5 Events	106
3.5.5.1 Events	106
3.5.5.2 Events Settings	106
3.6 Maintenance	108
3.6.1 Tools	108
3.6.1.1 Ping	108
3.6.1.2 Traceroute	108
3.6.1.3 Packet Analyzer	108
3.6.1.4 Qxdmlog	109
3.6.2 Schedule	109
3.6.3 Log	110
3.6.3.1 System Log	110
3.6.3.2 Log Settings	110
3.6.4 Upgrade	111
3.6.5 Backup and Restore	112
3.6.6 Reboot	113
3.7 APP	113
3.7.1 Python	113
3.7.1.1 Python	114
3.7.1.2 App Manager Configuration	114
3.7.1.3 Python App	115
3.7.2 Node-RED	116
3.7.2.1 Node-RED	116
Chapter 4 Application Examples	119
4.1 Restore Factory Defaults	119
4.2 Firmware Upgrade	120
4.3 Network Connection	120
4.3.1 Ethernet Connection	120
4.3.2 Cellular Connection (Cellular Version Only)	122
4.4 Wi-Fi Application Example	123
4.4.1 AP Mode	123
4.4.2 Client Mode	125
4.5 Packet Forwarder Configuration	127
4.6 Network Server Configuration	128
4.6.1 Connect to Milesight IoT Cloud	128
4.6.2 Add End Devices	130
4.6.3 Send Data to Device	134
4.6.4 Connect to HTTP/MQTT Server	136
4.7 Node-RED	
4.7.1 Start the Node-RED	138
4.7.2 Send Data by Email	139

Chapter 1 Product Introduction

1.1 Overview

UG56 is a robust 8-channel industrial LoRaWAN[®] gateway. Adopting SX1302 LoRa chip and high-performance quad-core CPU, UG56 supports connection with more than 2000 nodes. UG56 has line of sight up to 15 km and can cover about 2 km in urbanized environment, which is ideally suited to smart building, smart industries and many other indoor applications.

UG56 supports not only multiple back-haul backups with Ethernet, Wi-Fi and cellular, but also has integrated mainstream network servers (such as The Things Industries, ChirpStack, etc.) and built-in network server for easy deployment.





1.2 Advantages

Benefits

- Quad-core industrial CPU and big memory
- Multi-backhaul connectivity backups with Ethernet, 2.4GHz Wi-Fi and global 3G/4G LTE options make it easy to get connected
- Embedded network server and compliant with several third-party network servers
- MQTT, HTTP or HTTPS protocol for data transmission to application server
- Rugged enclosure, optimized for wall or pole mounting
- 3-year warranty included

Security & Reliability

- Automated failover/failback between Ethernet and Cellular
- Enable unit with security frameworks like IPsec/OpenVPN/GRE/L2TP/PPTP/ DMVPN/WireGuard

- Embedded hardware watchdog to automatically recover from various failures and ensure highest level of availability

Easy Maintenance

- Milesight DeviceHub and Milesight Development Platform provide easy setup, mass configuration, and centralized management of remote devices
- The user-friendly web interface design and various upgrading options help administrator to manage the device as easy as pie
- Web GUI and CLI enable the admin to achieve quick configuration and simple management among a large quantity of devices
- Users can efficiently manage the remote devices on the existing platform through the industrial standard SNMP

Capabilities

- Link remote devices in an environment where communication technologies are constantly changing
- Industrial quad-core 64-bit ARM Cortex-A35 processor, high-performance operating up to 1.3 GHz with low power consumption, and 8GB eMMC available to support more applications
- Support wide operating temperature ranging from -20°C to 60°C/-4°F to 140°F

Chapter 2 Access to Web GUI

This chapter explains how to access to Web GUI of the UG56. Username: **admin** Password: **password**

Configuration Steps:

1. Enable Wireless Network Connection on your computer and search for access point **"Gateway_********" to connect it, the default Wi-Fi password is **iotpassword**.

2. Open a Web browser on your PC (Chrome is recommended) and type in the IP address

192.168.1.1 to access the web GUI.

3. Enter the username and password, click "Login".

	Language English •
Lacawan Calency —	
Cagin Cagin	
Capyright © 2022 Milesight, All Rights Reserved.	

If you enter the username or password incorrectly more than 5 times, the login page will be locked for 10 minutes.

4. After logging the web GUI, follow the guide to complete the basic configurations. It's suggested that you change the password for the sake of security.

Change Your Default Pass For your device security, please change the defa	
Old Password	
New Password	
Confirm New Password	
Close Save	



5. You can view system information and perform configuration of the gateway.

			For your device	security, please ch	ange the default p	password		
Status	Overview	Cellular	Network	WLAN	VPN	Routing	Host List	Help
Status								Model
Packet Forwarder	System Inform	ation						Show the model name of gateway.
	Model		UG56-L00	E-915M				Region
Network Server	Region		US915					Show the Region of gateway.
			100000					Serial Number
Network	Serial Number		6041C223					Show the serial number of gateway.
	Firmware Versio	in	56.0.0.1-a2	2				Firmware Version
System 🕨	Hardware Versio	n	V1.0					Show the current firmware version of gateway.
	Local Time		2022-08-10) 13:22:14 Wednes	day			Hardware Version
Maintenance	Uptime		00:01:10					Show the current hardware version of gateway.
APP	CPU Load		10%					Local Time
	RAM (Available)	Capacity)	235MB/512	2MB (45.90%)				Show the current local time of system.
	eMMC (Availabl	e/Capacity)	6.2GB/7.00	GB (88.51%)				Uptime
								Show the information on how
							Manual Refresh 🗸 🛛 Refresh	long the gateway has been running.

Note: The connection type of Ethernet port is DHCP by default. The gateway also supports wired access if you select the connection type of Ethernet port as static IP and assign an IP address to Ethernet port.

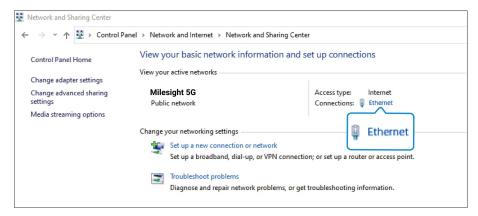
1. Go to **Network > Interface > Port** page to select connection type as **Static IP** and configure an IP address for the Ethernet WAN port.

Status	Port	WLAN	Cellular	Loopback	VLAN Trunk	
Packet Forwarder	- Port_1					
Network Server	Port			eth 0	~	
Protocol Integration	Conne IP Add	ection Type Iress		Static IP 192.168.23.150	~	
Network 👻	Netma	ask		255.255.255.0		
	Gatew	/ay		192.168.23.1		
Interface	MTU			1500		
Firewall	Prima	ry DNS Server		8.8.8.8		
DHCP	Secon	idary DNS Server		223.5.5.5		
DDNS	Enable	e NAT				

2. Connect PC to UG56 ETH port directly or through PoE injector.

3. Assign the IP address to computer manually. Take Windows 10 system as an example,

A. Go to "Control Panel" \rightarrow "Network and Internet" \rightarrow "Network and Sharing Center", then click "Ethernet" (May have different names).



B. Go to "Properties" \rightarrow "Internet Protocol Version 4(TCP/IPv4)" and select "Use the following IP address", then assign a static IP manually within the same subnet of the gateway.

							pports	
							nnorte	
					aan	ninis	trator	
Y								
192		168		23	. 2	00]	
255 . 255 . 255 . 0 192 . 168 . 23 . 150]			
					50]		
atical	ly							
esse	5:							
8		8	•	8	,	8]	
	ł		•]	
					A	d⊻ar	nced	0
	Г	_	OK			_	Cano	al
	192 255 192 atical	192 . 255 . 192 . atically esses:	192 . 168 255 . 255 192 . 168 atically esses:	192 . 168 . 255 . 255 . 192 . 168 . atically esses: 8 . 8 . 	192 . 168 . 23 255 . 255 . 255 192 . 168 . 23 atically esses:	192 . 168 . 23 . 2 255 . 255 . 255 . 192 . 168 . 23 . 1 atcally esses: 8 . 8 . 8 . A	192 . 168 . 23 . 200 255 . 255 . 255 . 0 192 . 168 . 23 . 150 atcally esses: 8 . 8 . 8 . 8 Adyan	192 . 168 . 23 . 200 255 . 255 . 255 . 0 192 . 168 . 23 . 150 atcaly esses: 8 . 8 . 8 . 8 Adyanced

C. Open a Web browser on your PC (Chrome is recommended) and type in the IP address of the Ethernet port to access the web GUI.

Chapter 3 Web Configuration

3.1 Status

3.1.1 Overview

You can view the system information of the gateway on this page.

System Information	
Model	UG56-L04EU-868M
Region	EU868
Serial Number	6041E0305345
Firmware Version	56.0.0.4
Hardware Version	V2.0
Local Time	2024-07-22 20:06:47 Monday
Uptime	3days,05:31:58
CPU Load	6%
RAM (Capacity/Available)	512MB/136MB (26.56%)
eMMC (Capacity/Available)	8.0GB/6.2GB (77.52%)



System Information					
Item	Description				
Model	Show the model name of gateway.				
Region	Show the LoRaWAN® used frequency of gateway.				
Serial Number	Show the serial number of gateway.				
Firmware Version Show the currently firmware version of gateway.					
Hardware Version Show the currently hardware version of gateway.					
Local Time	Show the currently local time of system.				
Uptime	Show the information on how long the gateway has been running.				
CPU Load	Show the current CPU utilization of the gateway.				
RAM (Capacity/Available) Show the RAM capacity and the available RAM m					
eMMC (Capacity/Available)	Show the eMMC capacity and the available eMMC memory.				
	Table 3-1-1-1 System Information				

3.1.2 Cellular

You can view the cellular network status of gateway on this page.

Modem		
Status	Ready	
Model	EC25	
Version	EC25ECGAR06A07M1G	
Signal Level	26asu (-61dBm)	
Register Status	Registered (Home network)	
IMEI	860425047368939	
IMSI	460019425301842	
ICCID	89860117838009934120	
ISP	CHN-UNICOM	
Network Type	LTE	
PLMN ID		
LAC	5922	
Cell ID	340db80	
	F ' 0.4.0.4	

Figure 3-1-2-1

Modem Information			
ltem	Description		
Status	Show corresponding detection status of module and SIM card.		
Model	Show the model name of cellular module.		
Version	Show the version of cellular module.		
Signal Level	Show the cellular signal level.		
Register Status	Show the registration status of SIM card.		
IMEI	Show the IMEI of the module.		
IMSI	Show IMSI of the SIM card.		
ICCID	Show ICCID of the SIM card.		
ISP	Show the network provider which the SIM card registers on.		
Network Type	Show the connected network type, such as LTE, 3G, etc.		
PLMN ID	Show the current PLMN ID, including MCC, MNC, LAC and Cell ID.		
LAC	Show the location area code of the SIM card.		
Cell ID	Show the Cell ID of the SIM card location.		

Table 3-1-2-1 Modem Information

Network		
Status	Connected	
IP Address	10.53.241.18	
Netmask	255.255.255.252	
Gateway	10.53.241.17	
DNS	218.104.128.106	
Connection Duration	0 days, 00:04:26	

Figure 3-1-2-2

Network Status		
Item	Description	
Status	Show the connection status of cellular network.	
IP Address	Show the IP address of cellular network.	
Netmask	Show the netmask of cellular network.	
Gateway	Show the gateway of cellular network.	
DNS	NS Show the DNS of cellular network.	
Connection Duration	Show information on how long the cellular network has been connected.	
Table 3-1-2-2 Network Status		

3.1.3 Network

On this page you can check the Ethernet port status of the gateway.

Overvie	ew (Cellular	Network	WLAN	VPN	Host List		
WAN								
Port	Status	Туре	IP Address	Netmask		Gateway	DNS	Duration
eth 0	up	Static	192.168.22.32	255.255.254.0	1	192.168.22.1	8.8.8.8	10h 52m 03s

Figure 3-1-3-1

Network	Network		
ltem	Description		
Port	Show the name of the Ethernet port.		
Status	Show the status of the Ethernet port. "Up" refers to a status that WAN is enabled and Ethernet cable is connected. "Down" means Ethernet cable is disconnected or WAN function is disabled.		
Туре	Show the dial-up type of the Ethernet port.		
IP Address	Show the IP address of the Ethernet port.		
Netmask	Show the netmask of the Ethernet port.		
Gateway	Show the gateway of the Ethernet port.		

DNS	Show the DNS of the Ethernet port.
	Show the information about how long the Ethernet cable has been
Duration	connected to the Ethernet port when the port is enabled. Once the port
	is disabled or Ethernet cable is disconnected, the duration will stop.

Table 3-1-3-1 WAN Status

3.1.4 WLAN

You can check Wi-Fi status on this page, including the information of access point and client.

Overview	Cellular	Network	WLAN	VPN
WLAN Status				
Wireless Status		Enabled		
MAC Address		24:e1:24:f1:22:58		
Interface Type		AP		
SSID		Gateway_F12258		
Channel		Auto		
Encryption Type		No Encryption		
Status		Up		
IP Address		192.168.1.1		
Netmask		255.255.255.0		
Connection Duratio	n	0 days, 10:52:23		

Figure 3-1-4-1

WLAN Status		
Item	Description	
Wireless Status	Show the wireless status.	
MAC Address	Show the MAC address.	
Interface Type	Show the interface type, such as "AP" or "Client".	
SSID	Show the SSID.	
Channel	Show the wireless channel.	
Encryption Type	Show the encryption type.	
Status	Show the connection status.	
IP Address	Show the IP address of the gateway.	
Netmask	Show the wireless MAC address of the gateway.	
Gateway	Show the gateway address in wireless network.	
Connection Duration	Show information on how long the Wi-Fi network has been connected.	

Table 3-1-4-1 WLAN Status

Associated Stations			
IP Address	MAC Address	Connection Duration	
	Figure 3-1-4-2		
Associated Stations			
Item	Description		
IP Address	Show the IP address of access point or client.		
MAC Address	Show the MAC address of the access point or client.		
Connection Duration	Show information on how long the Wi-Fi network has been connected.		

Table 3-1-4-2 WLAN Status

3.1.5 VPN

You can check VPN status on this page, including PPTP, L2TP, IPsec, OpenVPN and DMVPN.

Name	Status	Local IP	Remote IP
pptp_1	Disconnected	-	<u>.</u>
pptp_2	Disconnected	-	-
pptp_3	Disconnected	2	5
Name	Status	Local IP	Remote IP
l2tp_1	Disconnected	2	<i>a</i>
l2tp_2	Disconnected	2	2
I2tp_3	Disconnected	5	Manual Refresh 🗸 Refres
	pptp_1 pptp_2 pptp_3 Name 12tp_1 12tp_2	pptp_1 Disconnected pptp_2 Disconnected pptp_3 Disconnected Name Status l2tp_1 Disconnected l2tp_2 Disconnected	pptp_1Disconnected-pptp_2Disconnected-pptp_3Disconnected-NameStatusLocal IPI2tp_1Disconnected-I2tp_2Disconnected-

Figure 3-1-5-1

1	IPsec	Tunnel
	IF Sec	runner

Name	Status	Local IP	Remote IP
ipsec_1	Disconnected	<i></i>	122
ipsec_2	Disconnected		1.00
ipsec_3	Disconnected	-	-

OpenVPN Client

Topentri it olient			
Name	Status	Local IP	Remote IP
openvpn_1	Disconnected		<i></i>
openvpn_2	Disconnected	-	*
openvpn_3	Disconnected	<i></i>	-



GRE Tunnel				
	Name	Status	Local IP	Remote IP
	gre_1	Disconnected	87	
	gre_2	Disconnected	-	-
	gre_3	Disconnected	æ	
DMVPN Tunnel				
	Name	Status	Local IP	Remote IP
	dmvpn	Disconnected	15	



VPN Status	
Item	Description
Name	Show the name of the VPN tunnel.
Status	Show the status of the VPN tunnel.
Local IP	Show the local tunnel IP of VPN tunnel.
Remote IP	Show the remote tunnel IP of VPN tunnel.
	Table 2.1.5.1 V/DN Statue

Table 3-1-5-1 VPN Status

3.1.6 Routing

You can check routing status on this page, including the routing table and ARP cache.

Milesight

Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.40.1	eth 0	25
127.0.0.0	255.0.0.0	ē.	Loopback	51
192.168.40.0	255.255.255.0	σ.	eth 0	-
IP		MAC		Interface
1 92.168.40.1	b8:e3:b1:90:fd:0b			eth 0
192.168.40.41	50:eb:f6:9f:aa:60			eth 0
192.168.40.11	24:4b:fe:48:2a:e9			Manual Refresh V Refre
	0.0.0.0 127.0.0.0 192.168.40.0 IP 192.168.40.1 192.168.40.41	0.0.0.0 0.0.0.0 127.0.0.0 255.0.0.0 192.168.40.0 255.255.255.0 IP I 192.168.40.1 B8 192.168.40.41 50	0.0.0.0 0.0.0.0 192.168.40.1 127.0.0.0 255.255.255.0 - 192.168.40.0 255.255.255.0 - 192.168.40.1 - <td>0.0.0.0 0.0.0.0 192.168.40.1 eth 0 127.0.0.0 255.0.0.0 - Loopback 192.168.40.0 255.255.0 - eth 0 IP 192.168.40.1 b8:e3:b1:90:fd:0b 192.168.40.11 50:eb:f6:9f.aa.60 192.168.40.11</td>	0.0.0.0 0.0.0.0 192.168.40.1 eth 0 127.0.0.0 255.0.0.0 - Loopback 192.168.40.0 255.255.0 - eth 0 IP 192.168.40.1 b8:e3:b1:90:fd:0b 192.168.40.11 50:eb:f6:9f.aa.60 192.168.40.11

Figure 3-1-6-1

ltem	Description
Routing Table	
Destination	Show the IP address of destination host or destination network.
Netmask/Prefix	Show the netmask or prefix length of destination host or
Length	destination network.
Gateway	Show the IP address of the gateway.
Interface	Show the outbound interface of the route.
Metric	Show the metric of the route.
ARP Cache	
IP	Show the IP address of ARP pool.
MAC	Show the IP address's corresponding MAC address.
Interface	Show the binding interface of ARP.

Table 3-1-6-1 Routing Information

3.1.7 Host List

You can view the host information on this page.

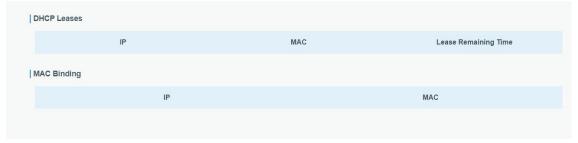


Figure 3-1-7-1

Host List	
ltem	Description
DHCP Leases	

IP Address	Show IP address of DHCP client	
MAC Address	Show MAC address of DHCP client	
Lease Time Remaining	Show the remaining lease time of DHCP client.	
MAC Binding		
IP & MAC	Show the IP address and MAC address set in the Static IP list of DHCP service.	

Table 3-1-7-1 Host List Description

3.2 LoRaWAN

3.2.1 Packet Forwarder

3.2.1.1 General

General	Radios	Advanced	Custom	Traffic			
General Setting	3						
Gateway EUI		24E124FFFEF5A6A8					
Gateway ID		24E124FFFEF5A6A8					
Frequency-Sync		Disabled	~				
Data Retransmis	sion						
Multi-Destinatio	'n						
ID		Enable	1	Гуре	Server Address	Connect Status	Operation
0		Enabled	Embe	edded NS	localhost	Connected	
1		Disabled	Remote E	mbedded NS	192.168.40.244	Disconnected	
							E

Figure 3-2-1-1

General Settings	
ltem	Description
Gateway EUI	Show the identifier of the gateway and it's non-editable. The EUI is consist of Ethernet Port's MAC address and FFFE in the middle.
Gateway ID	Fill in the corresponding ID which you've used for register gateway on the remote network server, such as TTN. It is usually the same as gateway EUI and can be changed.
Frequency-Sync	Sync frequency configurations from network server by selecting the corresponding ID.
Data Retransmission	When the gateway connects to a single Chirpstack/Semtech/Basic Station/Remote Embedded NS type package forwarder, it supports dat a storage up to 1 million pieces of data when network is disconnected and re-transmits the data after network recovery.
Multi-Destination	The gateway will forward the data to the network server address that was created and enabled in the list.
Connection Status	Show the connection status of package forwarder.

Table 3-2-1-1 General Setting Parameters

Milesight

Packet Filters			
Filters by NetID default mode	White List []		
Proprietary Message Filter			
Filters by NetID	White List	~	
		±	
Filters by JoinEUI	Black List	~	
		То	+
Filters by DevEUI	White List	~	
		То	H

Figure 3-2-1-2

Packet Filters	
Parameters	Description
Filters by NetID Default Mode	 Select the filter mode as black list or white list. White List: Only forward the packets on this list to the network server. Black List: Only forward the packets except this list to the network server.
Proprietary Message Filter	Enable to not forward the proprietary message packets (Mtype=111).
Filters by NetID	Forward/Not forward the uplink packets that match the NetID.
Filters by JoinEUI	Forward/Not forward the join request packets that match the JoinEUI range.
Filters by DevEUI	Forward/Not forward the join request packets that match the DevEUI range.
List	Set the specific filtering value or range list. Every condition supports to add 5 lists at most.

Table 3-2-1-2 Packet Filters Parameters

Note:

1. When join EUI and dev EUI are both configured, only packets that match both conditions will be forwarded.

2. This feature is not supported when the packet forwarder type is Loriot or Everynet.

3. When a third-party network server assigns filter condition to gateway, the gateway will use network server settings in priority.

20

Related Configuration Example

Packet forwarder configuration

3.2.1.2 Radios

Radio Channel Setting	
Supported Freq	US915 🗸
Name	Center Frequency/MHz
Radio 0	904.3
Radio 1	905.0

Figure 3-2-1-2

Radios-Radio Channel Setting		
ltem	Description	
Region	Choose the LoRaWAN [®] frequency plan used for the upstream and downlink frequencies and datarates. Available channel plans depend on the gateway's model.	
Center Frequency	Change the frequencies to receive packets from LoRaWAN® nodes.	

Table 3-2-1-2 Radio Channels Setting Parameters

	Multi	Channels	Setting
1			

Index	Radio	Frequency/MHz
0	Radio 0 🔻	923.2
1	Radio 0 🔻	923.4
2	Radio 0 🔻	923.6
3	Radio 1 🔹	922.2
4	Radio 1 🔻	922.4
5	Radio 1 🔻	922.6
6	Radio 1 🔹	922.8
7	Radio 1 🔹	923.0
	0 1 2 3 4 5	0 Radio 0 ▼ 1 Radio 0 ▼ 2 Radio 0 ▼ 3 Radio 1 ▼ 4 Radio 1 ▼ 5 Radio 1 ▼ 6 Radio 1 ▼



Radios-Multi Channel Setting		
ltem	Description	Default
Enable	Click to enable this channel to transmit packets.	Enabled
Index	Indicate the ordinal of the list.	/
Radio	Choose Radio 0 or Radio 1 as center frequency.	Radio 0
Frequency/MHz	Enter the frequency of this channel. Range: center frequency±0.4625.	Based on the LoRaWAN [®] regional document

Table 3-2-1-3 Multi Channel Setting Parameters

LoRa Channel Setting				
Enable	Radio	Frequency/MHz	Bandwidth/KHz	Spread Factor
	Radio 0 🔻	923.8	250KHZ •	SF7 *

Figure 3-2-1-4

Radios-LoRa Cha	Radios-LoRa Channel Setting		
ltem	Description	Default	
Enable	Click to enable this channel to transmit packets.	Enabled	
Radio	Choose Radio 0 or Radio 1 as center frequency.	Radio 0	
Frequency/MHz	Enter the frequency of this channel. Range: center frequency±0.9.	Based on the supported frequency	
Bandwidth/MHz	Enter the bandwidth of this channel.	500KHz	
Spread Factor	Choose the selectable spreading factor. The channel with large spreading factor corresponds to a low rate, while the small one corresponds to a high rate.	Based on what is specified in the LoRaWAN [®] regional parameters document	

Table 3-2-1-4 LoRa Channel Setting Parameters

I	FSK Channel Setting				
	Enable	Radio	Frequency/MHz	Bandwidth/KHz	DataRate
		Radio 0 🔻	924.0	125KHZ 🔻	50000

Figure 3-2-1-5

Radios-FSK Channel Setting			
Item	Description	Default	
Enable	Click to enable this channel to transmit packets.	Disabled	
Radio	Choose Radio 0 or Radio 1 as center frequency.	Radio 0	
Frequency/MHz	Frequency/MHz Enter the frequency of this channel. Range: center frequency±0.9.		
Bandwidth/MHz	Enter the bandwidth of this channel. Recommended value: 125KHz, 250KHz, 500KHz	Based on the supported frequency	
Data Rate	Enter the data rate. Range: 500-25000.	500	
Table 3-2-1-5 FSK Channel Setting Parameters			

3.2.1.3 Noise Analyzer

Noise analyzer is used for scanning the noise of every frequency channel and giving a diagram for users to analyze the environment interference condition and select best deployment. RSSI indicates the sensitivity for every channel. Lower the RSSI value, better the signal. It's not suggested to enable this feature when using package forwarder since it will affect the downlink transmission.

Radio Channel Setting				
Supported Freq		US915	~	Noise Analyzer 🔺
Noise Analyzer	Running			
Settings	Sweep Freq Genaral Freq 🗸			
	0-63: 902.3-914.9 MHz			
	64-71: 903-914.2 MHz			
	Sweep Time Custom 🗸			
	24 h			
	ОК			
	UK			
	-O- Current Value -O- Weighted Ave	rage Value		
RSSI/dBm				
0	· · · · ·			MHz
-20 -				
-40 -	â			
-60 - A	. A	-		
	\wedge			
-80-				
-100-				
-116-902.3 902.7 90	03.1 903 5 903.9 904.3 904.7	905.1 905.5 905.9	906.3	

Figure 3-2-1-6

Noise Analyzer			
ltem	Description	Default	
Enable	Click to enable noise analyzer feature.	Disabled	
Sweep Freq	Select the frequency sweeping range. General Freq: frequencies based on the LoRaWAN [®] regional parameters document Custom: custom the frequency range	General Feq	
Sweep Time	Enable the noise analyzer continuously or within a period of time. If Custom is selected, the noise analyzer will stop automatically after the pre-configured time. Note: It's suggested to custom the time since noise analyzer feature will affect the normal data transmission.	Custom/2 4h	

Table 3-2-1-6 Noise Analyzer Setting Parameters

3.2.1.4 Advanced

This section is about settings in details of beacon transmitting and validating.

0	~ s
869525000	Hz
SF9	~
1	•
200000	Hz
125000	✓ Hz
27	dBn
0	S
	869525000 SF9 1 200000 125000 27



Advanced-Beacon Setting				
ltem	Description	Default		
Beacon Period	Interval of gateway sending beacons for Class B device time synchronization. 0 means the gateway will not send beacons.	0		
Beacon Freq	The frequency of beacons.	Based on the supported frequency		
Beacon Datarate	The datarate of beacons.	Based on the supported frequency		
Beacon Channel Number	When selecting Custom, it allows users to custom range from 1 to 8.	1		
Beacon Freq Step	Frequency interval of beacons.	200000		
Beacon Bandwidth	The bandwidth of beacons. Unit: Hz	12500 Hz		
Beacon TX Power	The TX power of beacons.	Based on the supported frequency		
Beacon Time Offset	The gateway will plus this offset on system time and assign the time result to Class B devices.	0		

Table 3-2-1-7 Advanced-Beacon Parameters

Milesight

Intervals Setting		
Keep Alive Interval	10	s
Stat Interval	30	s
Push Timeout	100	ms
Forward CRC Setting		
Forward CRC Disabled		
Forward CRC Error		
Forward CRC Valid		

Figure 3-2-1-8

ltem	Description	Default
Keep Alive Interval	Enter the interval of keepalive packet which is sent from gateway to network server to keep the connection stable and alive. Range: 1-3600.	10
Stat Interval	Enter the interval to update the network server with gateway statistics. Range: 1-3600.	30
Push Timeout	Enter the timeout to wait for the response from server after the gateway sends data of node. Rang: 1-1999.	100
Forward CRC Disabled	Enable to send packets received with CRC disabled to the network server.	Disabled
Forward CRC Error	Enable to send packets received with CRC errors to the network server.	Disabled
Forward CRC Valid	Enable to send packets received with CRC valid to the network server.	Enabled

Table 3-2-1-8 Advanced Parameters

LBT Settings		
Enable		
RSSI Target	-80	dBm

Figure 3-2-1-9

ltem	Description	Default
Enable	Enable or disable LBT feature. Listen before talk (LBT) is used to detect whether the downlink channel is idle and avoid channel access conflicts. Note: AU915 and US915 do not support LBT feature.	Disabled
RSSI Target	Enter the criteria of an idle channel. If actual RSSI of a	-80

channel is less than the criteria/target, the channel is	
considered as idle. Range: -120~0	

Table 3-2-1-9 Advanced-LBT Parameters

3.2.1.5 Custom

When Custom Configuration mode is enabled, you can write your own packet forwarder configuration file in the edit box to configure packet forwarder. Click "Save" to save your custom configuration file content, and click "Apply" to take effect. You can click "Clear" to erase all content in the edit box. If you don't know how to write configuration file, please click "Example" to go to reference page.

Note: customized configuration will overwrite the packet forward configurations of web GUI.

General	Radios	Advanced	Custom	Traffic	
Custom Config	guration				
Enable					
				Example	
{					
"SX1302_conf					
	"/dev/spidev0.0",				
"lorawan_publi	ic": true,				
"clksrc": 0,	202002 N 2				
	ı": 0, /* antenna gair	n, in dBi */			
"antenna_cfg":					
"full_duplex": f					
"precision_time					
"enable": false					
"max_ts_metri					
"nb_symbols":	1				
},					
"radio_0": {					
"enable": true,					
"type": "SX125	50",				

Figure 3-2-1-10

3.2.1.6 Traffic

When navigating to the traffic page, any recent traffic received by the gateway will display. To watch live traffic, click **Refresh**.

Traffic Setting	i)							
Refresh	Clear							
Rfch	Direction	Time	Ticks	Frequency	Datarate	Coderate	RSSI	SNR
1	up		83002508	922.8	SF9BW125	4/5	-103	-13.2
1	up	-	71108156	922.6	SF9BW125	4/5	-102	-13.2
1	up	~	35426956	922.8	SF9BW125	4/5	-103	-9.8
1	up	-	3171639508	922.6	SF9BW125	4/5	-100	-10.5
1	up	-	3159744804	922.6	SF9BW125	4/5	-102	-13.0
1	up	-	3155781348	922.6	SF9BW125	4/5	-101	-12.2
1	up	2	3147851660	922.6	SF9BW125	4/5	-102	- <mark>13.8</mark>
1	ир	¢	3143888916	922.8	SF9BW125	4/5	-102	-13.2
1	ир	<i>e</i>	3139922740	922.8	SF9BW125	4/5	-100	-12.2
1	up	-	3124065788	922.8	SF9BW125	4/5	-100	-12.8

Figure 3-2-1-11

ltem	Description
Refresh	Click to obtain the latest data.
Clear	Click to clear all data.
Rfch	Show the channel of this packet.
Direction	Show the direction of this packet.
Time	Show the receiving time of this packet.
Ticks	Show the ticks of this packet.
Frequency	Show the frequency of the channel.
Datarate	Show the datarate of the channel.
Coderate	Show the coderate of this packet.
RSSI	Show the received signal strength.
SNR	Show the signal to noise ratio of this packet.

Table 3-2-1-10 Traffic Parameters

3.2.2 Network Server

3.2.2.1 General

Enable	Image: A start of the start		
Platform Mode			
NetID	010203		
Join Delay	5		sec
RX1 Delay	1		sec
Lease Time	8760-0-0		hh-mm-s
Log Level	info	~	
Global Channel Plar	n Setting		
Channel Plan	US915	~	
Channel	8-15		

ltem	Description	Default
General Setting		
Enable	Click to enable Network Server mode.	Enabled
Platform Mode	Enabled to connect gateway to Milesight IoT Cloud.	Disabled
NetID	Enter the network identifier.	010203
Join Delay	Enter the interval time between when the end-device sends a Join_request_message to network server and when the end-device prepares to open RX1 to receive the Join_accept_message sent from network server.	5
RX1 Delay	Enter the interval time between when the end-device sends uplink packets and when the end-device prepares to open RX1 to receive the downlink packet.	1
Lease Time	Enter the amount of time till a successful join expires. The format is hours-minutes-seconds. If the join-type is OTAA, then the end-devices need to join the network server again when it exceeds the lease time.	
Log level	Choose the log level.	Info
Channel Plan Se	etting	
Channel Plan	Choose LoRaWAN [®] channel plan used for the upstream and downlink frequencies and datarates. Available channel plans depend on the gateway's model.	Depend on the gateway's frequency
Channel	Enabled frequencies are controlled using channel mask. Leave it blank means using all the default standard usable channels specified in the LoRaWAN® regional parameters document. It allows to enter the index of the cahnnels. Examples: 1, 40: Enabling Channel 1 and Channel 40 1-40: Enabling Channel 1 to Channel 40 1-40, 60: Enabling Channel 1 to Channel 40 All: Enabling all channels Null: Indicates that all channels are disabled	Depend on the gateway's frequency

Note: For some regional variants, if allowed by your LoRaWAN[®] region, you can use Additional Plan to configure additional channels undefined by the LoRaWAN[®] Regional

Table 3-2-2-1 General Parameters

Parameters, like EU868 and KR920, as the following picture shows:

Additional Channels				
Frequer	cy(MHz)	Min Datarate	Max Datarate	Operation
				H



Additional Channels			
Item	Description	Default	
Frequency/MHz	Enter the frequency of the additional plan.	Null.	
Max Datarate	Enter the max datarate for the end-device. The range is based on what is specified in the LoRaWAN [®] regional parameters document.	DR0(SF12,125kHz)	
Min Datarate	Enter the min datarate for the end-device. The range is based on what is specified in the LoRaWAN [®] regional parameters document.	DR3(SF9,125kHz)	

Table 3-2-2-2 Additional Plan Parameters

3.2.2.2 Application

An application is a collection of devices with the same purpose/of the same type. Users can add a series of devices to the same application which needs to send to the same server.

You can edit the	e application by	clicking 🖉	or create a new app	plication by clicking	+
Applications					
Name	cloud				
Description	cloud				
Metadata					
Metadata Details	🖌 devEUI 🔽 deviceName 🗹 a	applicationID 🗌 gatewayTim	e 🗌 cellularIP		
Data Transmission					
	Туре			Operation	
				E	
Save Cancel					

Figure 3-2-2-3

ltem	Description
Name	Enter the name of the application profile.
Name	E.g Smoker-sensor-app.
Description	Enter the description of this application.
	E.g a application for smoker sensor.
Metadata	Enable to select the details to report with uplink packets
Wielauala	automatically when the device adds the payload codec.
Data	Data will be sent to your custom server using the MQTT, HTTP or

Transmission	HTTPS protocol. One application can only add one MQTT
	transmission and one HTTP (HTTPS) transmission.

Table 3-2-2-3 Application Parameters

MQTT Integration

Type	MQTT	~
Status	-	
General		
Broker Address		
Broker Port		
Client ID		
Connection Timeout/s	30	
Keep Alive Interval/s	60	
Data Retransmission		

Figure 3-2-2-4

User Credentials	
Enable	
Username	
Password	<i>₹</i>
TLS	
Enable	
Mode	CA signed server certificate 🖌
Will	
Enable	
Will Topic	
Will QoS	QoS 0 🗸
Will Retain	
Will Message	

Figure 3-2-2-5

Topic					
	Data Type	topic	Retain		
	Uplink data			QoS 0	~
	Downlink data			QoS 0	~
	Multicast downlink data			QoS 0	~
	Join notification		0	QoS 0	~
	ACK notification			QoS 0	~
	Error notification			QoS 0	~
	Request data			QoS 0	~
	Response data			QoS 0	~

Figure 3-2-2-6

MQTT Settin	igs
ltem	Description
General	
Broker Address	MQTT broker address to receive data.
Broker Port	MQTT broker port to receive data.
Client ID	Client ID is the unique identity of the client to the server. It must be unique when all clients are connected to the same server, and it is the key to handle message at QoS 1 and 2.
Connection Timeout/s	If the client does not get a response after the connection timeout, the connection will be considered as broken. The Range: 1-65535
Keep Alive Interval/s	After the client is connected with the server, the client will send heartbeat packet to the server regularly to keep alive. Range: 1-65535
Data Restransmi ssion	After enabled, it supports data storage of up to 10,000 pieces of data when the network is disconnected and re-transmits the data after network recovery.
User Creden	-
Enable	Enable user credentials. Note: if MQTT broker type is HiveMQ, please enable TLS and set the option as CA signed server certificate.
Username	The username used for connecting to MQTT broker.
Password	The password used for connecting to MQTT broker.
TLS	
Enable	Enable the TLS encryption in MQTT communication.
Mode	 Select from "Self-signed certificates", "CA signed server certificate". CA signed server certificate: verify with the certificate issued by Certificate Authority (CA) that pre-loaded on device. Self-signed certificates: upload the custom CA certificates (.crt or .pem), client Certificates (.crt) and secret key(.key) for verification.
Will	

Last will message is automatically sent when the MQTT client is abnormally disconnected. It is usually used to send device status information or inform other devices or proxy servers of the device's offline status. Customize the topic to receive last will messages. QoS0, QoS1 or QoS2 are optional. Enable to set last will message as retain message. Customize the last will message contents.
Customize the topic to receive last will messages. QoS0, QoS1 or QoS2 are optional. Enable to set last will message as retain message. Customize the last will message contents.
QoS0, QoS1 or QoS2 are optional. Enable to set last will message as retain message. Customize the last will message contents.
Enable to set last will message as retain message. Customize the last will message contents.
Customize the last will message contents.
Data type cent to MOTT broker
Data type cont to MOTT broker
Data type sent to MQTT broker. Uplink Data: receive device uplink packets Downlink Data: send downlink commands to devices. If you require to send downlink command to a single device, please add the wildcard "\$deveui" to this topic and replace this as real device EUI when subscribing this topic. Multicast Downlink Data: send downlink commands to multicast group Join Notification: receive join notifications if he gateway sends join accept packets to allow the devices to join the network ACK Notification: receive ACK packets from devices when sending downlink commands Error Notification: receive error packets from devices Request data: send requests to enquire and configure the gateway NS Response data: receive the request responses
Topic name of the data type using for publish.
Enable to set the latest message of this topic as retain message.
QoS 0 - Only Once This is the fastest method and requires only 1 message. It is also the most unreliable transfer mode. QoS 1 - At Least Once This level guarantees that the message will be delivered at least once, but may be delivered more than once. QoS 2 - Exactly Once QoS 2 is the highest level of service in MQTT. This level guarantees that each message is received only once by the intended recipients. QoS 2 is
- (

Table 3-2-2-4 MQTT Settings Parameters

HTTP/HTTPS Integration

HTTP Header				
	Header Name	Header Value	Operation	
			H	
URL				
	Data Type	URL		
	Uplink data]	
	Join notification]	
	ACK notification]	
	Error notification]	



HTTP/HTTPS Settings		
ltem	Description	
HTTP Header		
Header Name	A core set of fields in HTTP header.	
Header Value	Value of the HTTP header.	
URL		
	Data type sent to HTTP/HTTPS server.	
	Uplink Data: receive device uplink packets	
	Join Notification: receive join notifications if he gateway sends join	
Data Type	accept packets to allow the devices to join the network	
	ACK Notification: receive ACK packets from devices when sending	
	downlink commands	
	Error Notification: receive error packets from devices	
Topic	Topic name of the data type using for publish.	
URL	HTTP/HTTPS server URL to receive data.	

Table 3-2-2-5 HTTP/HTTPS Settings Parameters

Related Configuration Example

Application configuration

3.2.2.3 Payload Codec

Payload Codec provides the inbuilt payload codec library of Milesight LoRaWAN[®] devices to decode and encode the data easily. Users can also customize the payload codec of other brands of devices or adjust the uplink and downlink contents as requirements.

built Payload Codec Library				
ibrary Version 1.3.1				
Obtaining Type Or	line 🗸			
Obtain				
lote: Ensure that the Internet access is availa	ble.			
Name	Payload Decoder Function	Payload Encoder Function	Object Mapping Function	Details
AM102	~	×	~	0
AM102L	~	~	\checkmark	0
AM103	~	\checkmark	\checkmark	0
AM103L	~	~	\checkmark	0
AM104	~	~	\checkmark	0
AM107	~	\checkmark	~	0
AM307	~	~	\checkmark	0
AM307L	~	~	\checkmark	0
AM308	~	\checkmark	\checkmark	0
AM308L	~	~	~	0
howing 1 to 10 of 96 rows 10 🔺 rows pe	rpage		< 1 2 3	l 5 10

Figure 3-2-2-8

Inbuilt Payload Codec Library		
ltem	Description	
Library Version	Show the version of the Milesight device payload codec library.	
Obtaining Type	Select the type to update the Milesight devices payload codec library. Online: update automatically if gateway detects there is version update every time gateway powers on and accesses the Internet. Users can also click Obtain button to check update status manually. Local Upload: click Browse to upload the zip format payload codec package and click Import to update the library. For Milesight payload codec package, please download here.	
Name	Show the corresponding Milesight product model of the payload codec.	
Payload Decoder Function	Show if decoders exist.	
Payload Encoder Function	Show if encoders exist.	
Object Mapping Function	Show if object mapping functions exist.	
Details	Show the details of decoder and encoder. If this does not meet your requirement, please customize your payload codec.	

Table 3-2-2-6 Inbuilt Payload Codec Library Parameters

Name	
Description	
Template	None
Payload decoder	
Payload decoder function	<pre>1 // Decode decodes an array of bytes into an object. // - front contains the LORBAWA Proor number // - bytes is an array of bytes, e.g. [225, 230, 255, 0] // The function must return an object, e.g. {"temperature": 22.5} function Decode(PPort, bytes) { return {}; }</pre>
Payload encoder	
Payload encoder function	<pre>1 // Encode encodes the given object into an array of bytes. // - fort contains the LORAWAW POort number // - obj is an object, e.g. {'teenperature': 22.55 // The function must return an array of bytes, e.g. [225, 230, 255, 0] function Encode(fPort, obj) { return []} }</pre>



Payload Codec Test	
	<pre>1 // input decoded test payloed or encoded test payload // decoded bytes // 01 75 5C 03 67 34 01 04 68 65 05 6A 49 00 06 65 1C 00 79 00 14 00 07 7D E7 04 08 7D 07 00 09 73 3F 27 // encoded objs // { // "battery": 92, // "temperature": 30.8, // "humidity": 50.5 // }</pre>
	fPort 1 Decode Encode
	1 // output decoded or encoded result
Object Mapping	
Object Mapping Function	<pre>1* { 2</pre>
	15 J, 14 → { 15 "id": "hardware_version", 16 "name": "Hardware Version", 17 "value": "", 18 "unit": "".

Custom Payload Codec		
Item	Description	
Name	Enter the unique name of the custom payload codec.	
Description	Enter the description of this payload codec.	
Template	Select an existing inbuilt payload codec as a template.	
Payload Decoder Function	Customize the device payload decoder to convert hex format data to JSON format. Note that the function header should be the same as the example on the blanks.	
Payload Encoder Function	Customize the device payload encoder to convert JSON format message to hex format command. Note that the function header should be the same as the example on the blanks.	
Payload Codec Test	Disable or enable payload codec test. fPort : Application port of LoRaWAN [®] devices. It's 85 by default for Milesight LoRaWAN [®] devices. Decode : Enter the hex format raw data without blank spaces and click Decode to check the result. Encode: Enter the JSON format command and check Encode to check the result.	
Object Mapping Function	Customize the mapping to convert LoRaWAN [®] message to BACnet or Modbus objects. For more details click <u>here</u> .	
	Table 3-2-2-7 Custom Payload Codec Parameters	

Figure 3-2-2-10

Note:

1. The supported JavaScript version of payload decoder and encoder is ES5.

2. The variable names used in decoders and encoders of one Payload Codec must be the same if they point to the same items.

3.2.2.4 Profiles

A Profile defines the device capabilities and boot parameters that are needed by the Netwo rk Server for setting the LoRaWAN[®] radio access service. These information elements shall be provided by the end-device manufacturer. UG56 has pre-configured 8 device files and users can also create a new device profile.

L D	evic	D P	rofil	
10	evic	C F	1011	162

Device Profiles					
	Name	Max TXPower	Join Type	Class Type	Operation
	ClassA-ABP	0	ABP	Class A	[/] [×]
	ClassA-OTAA	0	OTAA	Class A	$[l] \times$
	ClassB-ABP	0	ABP	Class A Class B	
	ClassB-OTAA	0	OTAA	Class A Class B	$\mathbb{Z}[\times]$
	ClassC-ABP	0	ABP	Class A Class C	$[\mathcal{I}]\times$
	ClassC-OTAA	0	OTAA	Class A Class C	
	ClassCB-ABP	0	ABP	Class A Class B Class C	$[\mathcal{L}] \times$
	ClassCB-OTAA	0	OTAA	Class A Class B Class C	
	test	0	OTAA	Class A Class B Class C	$[l] \times$
	test	0	OTAA	Class A Class B Class C	
					H



Device Profiles		
Name		
Max TXPower	0	
Join Type	ΟΤΑΑ	~
Class Type	Class A 🗌 Class	s B 🔲 Class C
Advanced		



Device Profiles	s Settings	
ltem	Description	
Name	Enter the name of the device profile.	
Name	E.g. Smoker-sensor-app.	
	Enter the maximum transmit power.	
Max	The TXPower indicates power levels relative to the Max EIRP level of the	
TXPower	end-device. 0 means using the max EIRP. EIRP refers to the Equivalent	
	Isotropically Radiated Power.	
Join Type	Select from: "OTAA" and "ABP".	
	Device type is Class A by default. Users can check the box of Class B or	
Class Type	Class C to add the class type.	
	Note: Beacon period should be set to nonzero value in Packet	
	Forwarder> Advanced if you use Class B.	

Table 3-2-2-8 Device Profiles Setting Parameters

37

Milesight

Advanced			
MAC Version	1.0.2	~	
Regional Parameters Revision	В	~	
RX1 Datarate Offset	0	~	
RX2 Datarate	DR0 (SF12, 125 kHz)	~	
RX2 Channel Frequency	505300000		Hz
Frequency List			Hz
Device Channel			

Device Profile Advanced Settings				
ltem	Description	Default		
MAC Version	Choose the version of the LoRaWAN [®] supported by the end-device.	1.0.2		
Regional Parameter Revision	Revision of the Regional Parameters document supported by the end-device.	В		
RX1 Datarate Offset	The offset which used for calculating the RX1 data-rate, based on the uplink data-rate.	Based on what is specified in		
RX2 Datarate	Enter the RX2 datarate which used for the RX2 receive-window.	the LoRaWAN® regional		
RX2 Channel Frequency	RX2 channel frequency which used for the RX2 receive-window.	parameters document		
Frequency List	List of factory-preset frequencies. The range is based on what is specified in the LoRaWAN [®] regional parameters document.	Null		
Device Channel	Change this device frequency channel by typing the channel indexs. When configured, it takes precedence over the global channel. This setting only works for CN470/US915/AU915 gateway.	Null		
PingSlot Period	Period of opening the pingslot.	Every Second		
PingSlot DataRate	Datarate of the node receiving downlinks.	Based on the supported frequency		
PingSlot Freq	Frequency of the node receiving downlinks.	Based on the supported frequency		
ACK Timeout	The time for confirmed downlink transmissions. This option is only applicable to class B and class	Class B: 10 Class C: 10		

С.	
0.	

Table 3-2-2-9 Device Profiles Advanced Setting Parameters

3.2.2.5 Device

A device is the end-device connecting to, and communicating over the LoRaWAN® network.

Add Bulk	Import Delete All					Search	
Device Name	Device EUI	Device-Profile	Payload Codec	Application	Last Seen	Activated	Operatio
AM308	24E124707E043923	ClassA-OTAA	AM308	cloud	1 day ago	~	2 ×
WT101	24E124714E092925	ClassA-OTAA	WT101	cloud	23 days ago	~	2×
GS301-kevin	24E124798D054774	ClassA-OTAA	GS301	cloud	20 days ago	~	1 ×
CT103	24E124746D488108	ClassA-OTAA	CT103	cloud	33 days ago		2×

Showing 1 to 4 of 4 rows

Figure	3-2-2-14
riguie	52214

ltem	Description
Add	Add a device.
Bulk Import	Download template and import multiple devices.
Delete All	Delete all devices in the list.
Device Name	Show the name of the device.
Device EUI	Show the EUI of the device.
Device-Profile	Show the name of the device's device profile.
Davida and Oa da a	Show the used payload codec of the device. Click to check the
Payload Codec	details of this payload codec.
Application	Show the name of the device's application.
Last Seen	Show the time of last packet received.
Activated	Show the status of the device. \checkmark means that the device has
	been activated.
Operation	Edit or delete the device.

Table 3-2-2-10 Device Parameters

Device Name	lora-sensor	
Description	a short description of y	our node
Device EUI	24e16411947884358	
Device-Profile	ClassA-OTAA	•
Application	test	~
Payload Codec		•
fPort	1	
Modbus RTU Data Transmission	Disable	~
Frame-counter Validation		
Application Key	🔿 Default Value 💿 Cus	stom Value
	ſ.	
Device Address		
Network Session Key		
Network Session Key	0	

Figure 3-2-2-15

Device Configuration				
Item	Description			
Device Name	Enter the name of this device.			
Description	Enter the description of this device.			
Device EUI	Enter the EUI of this device.			
Device-Profile	Choose the device profile.			
Application	Choose the application profile.			
Payload Codec	Choose the payload codec existed on Payload Codec page.			
fPort	Enter the downlink port of device, it's 85 by default for Milesight			
	devices.			
	Choose from: "Disable", "Modbus RTU to TCP", "Modbus RTU over			
	TCP". This feature is only applicable to Milesight LoRaWAN®			
Modbus RTU	controllers.(UC501/UC300, etc.)			
Data	Modbus RTU to TCP: TCP client can send Modbus TCP commands to			
Transmission	ask for controller Modbus data.			
	Modbus RTU over TCP: TCP client can send Modbus RTU commands			
	to ask for controller Modbus data.			

Modbus RTU Fport	Enter the LoRaWAN [®] frame port for transparent transmission between Milesight LoRaWAN [®] controllers and UG56. Range: 2-84, 86-223. Note: this value must be the same as the Milesight LoRaWAN [®] controller's Fport.
TCP Port	Enter the TCP port for data transmission between the TCP Client and UG56 (as TCP Server). Range: 1-65535.
Frame-Counter Validation	If disable the frame-counter validation, it will compromise security as it enables people to perform replay-attacks.
Application Key	 Whenever an end-device joins a network via over-the-air activation, the application key is used for derive the Application Session key. Default Value: The default value of Milesight end devices is 5572404C696E6B4C6F52613230313823. Custom Value: Define the appkey according to the end devices.
Device Address	The device address identifies the end-device within the current network.
Network Session Key	The network session key specific for the end-device. It is used by the end-device to calculate the MIC or part of the MIC (message integrity code) of all uplink data messages to ensure data integrity.
Application Session Key	The AppSKey is an application session key specific for the end-device. It is used by both the application server and the end-device to encrypt and decrypt the payload field of application-specific data messages.
Uplink Frame-counter	The number of data frames which sent uplink to the network server. It will be incremented by the end-device and received by the end-device. Users can reset the a personalized end-device manually, then the frame counters on the end-device and the frame counters on the network server for that end-device will be reset to 0.
Downlink Frame-counter	The number of data frames which received by the end-device downlink from the network server. It will be incremented by the network server. Users can reset the a personalized end-device manually, then the frame counters on the end-device and the frame counters on the network server for that end-device will be reset to 0.

Table 3-2-2-11 Device Setting Parameters

Related Configuration Example

Device configuration

3.2.2.6 FUOTA

Firmware Update Over the Air (FUOTA) is a standard for distributing firmware to end devices updates using unicast or multicast. **Before using this feature, ensure the end device supports the standard LoRaWAN® FUOTA protocol.**

UOTA								
Add	Delete						Search	Q
	Task Name	Firmware	Status	Progress	Create Time	Start Time	End Time	Operation
	task1	CTXXX.0000.0100.0103.bin	Pending	0/2	2025-04-14 10:09:52+08:00	2025-04-14 11:09:00+08:00	-	🖉 🗎 🔁 🗙

Figure 3-2-2-16

FUOTA				
ltem	Description			
Add	Click to add a task.			
Delete	Check the boxes of the task list and click to delete these tasks.			
Task Name	The task name.			
Firmware	The firmware to upgrade in this task.			
	The task status. Pending: Wait for the scheduled time to process the task.			
	Waiting: Prepare to create the session for an upgrade.			
Status	Executing: At least one device replies to the upgrade result.			
	Finished: All devices reply the upgrade results including success and			
	failure.			
Progress	The device amount that is upgraded successfully/is planned to be			
Create Time	upgraded. The time to create this task.			
Start Time	The time to create this task. The time to start this task.			
End Time	The time to complete this task.			
	Edit this task when task status is Pending.			
	E Check task details, including the success and failure status of every			
Operation	device.			
operation	Retry the task to devices which are upgraded failed when task			
	status is Finished.			
	E Delete this task when task status is Pending or Finished.			
1				

Table 3-2-2-12 FUOTA Parameters

Add FUOTA Tasks

- 1. Click **Add** button to add a FUOTA task.
- 2. Configure the task settings.

Milesight

Task Settings				
Task Name]		
Start Time	2025-04-10 10:13]		
Description]		
Firmware Setting				
Firmware		Upload a new firmware file	Select an official firmware file	Delete
Fragment Size	88	Bytes		
Fragment Interval	5000] ms		
Redundancy percent	30	%		
Multicast Setting				
Datarate	DR3 (SF9, 125kHz)			
Frequency	505300000	Hz		

Figure 3-2-2-17	Figure	3-2-2-17
-----------------	--------	----------

Add Task Setti	ngs
ltem	Description
Basic Informat	ion
Task Name	Customize a task name.
Start Time	Set the time to start this task.
Description	Enter the description for this task.
Firmware Setti	ngs
	Import the firmware to upgrade. Upload a new firmware file: Import a firmware locally. Select an Official Firmware file: Select the product model first and select the firmware to download from the official website. It requires the gateway to access the Internet.
Firmware	Select an official firmware file Please select the product model first Search Firmware Name Product Model Firmware Version Support Hardware Version Support Firmware Version Description No matching records found
Fragment Size	The firmware file will be split as this size to assign to devices. Usually please keep this value as default. If the network environment is complex or bad, it is suggested to reduce this value to 64 or a lower value; if the network environment is good, this value can be added to increase to improve transmission speed.
Fragment Interval	The interval to assign firmware fragments to devices. Usually please keep this value as default. If the network environment is complex or bad, it is suggested to reduce this value to 3 or a lower value; if the network environment is

43

	good, this value can be added to increase to improve transmission speed.		
Redundancy Percent	The device will send 30% redundancy packets for firmware file packet correction. Usually please keep this value as default. If the network environment is complex or bad, it is suggested to reduce this value to 20% or a lower value; if the network environment is good, this value can be added to improve transmission success.		
Multicast Settings			
Datarate	Datarate to assign the firmware fragments to devices.		
Frequency	Downlink frequency to assign the firmware fragments to devices.		

Table 3-2-2-13 Task Parameters

3. Select the devices to execute this task. Please select the devices with the same model.

e current	list has filtered out devices that are	e currently executing OTA tasks and	automatically matched devices that	t meet the upgrade conditions		
						Search O
	Device Name	Device EUI	Product Model	Profile Name	Current Firmware Version	Current Hardware Version
	em320-th	24e124	EM32X	ClassA-OTAA	v1.3	v1.2
	009569060000ef35	009569		ClassA-OTAA	-	-
	WS302	24e124	WS302	ClassA-OTAA	÷	-
	TERRY-WT101	24e124	WT10X,wt10X	ClassA-OTAA		
	WS502	24e124	WS50X	ClassC-OTAA	-	-
	cl	24e124	EM30X	ClassA-OTAA	-	-
	300	24e124	UC300	ClassC-OTAA	Ξ.	
	terry-wt101	24e124	WT10X,wt10X	ClassA-OTAA	v1.3	v1.1



4. Click **Save** to save these task settings.

3.2.2.7 Multicast Groups

Milesight gateways support for creating Class B or Class C multicast groups to send downlink messages to a group of end devices. A multicast group is a virtual ABP device (i.e. shared session keys), does not support uplink, confirmed downlink nor MAC commands.

Add			Search	C
Multicast Address	Group Name	Number of Devices	Opera	ition

Figure	3-2-2-19
riguie	52215

ltem	Description
Add	Add a multicast group.
Group Name	Show the name of the group.

Number of Devices	Show the device number of the group.			
Operation	Edit or delete the multicast group.			
Т	able 3-2-2-14 Multicast Group Parameters			
Group Name]		
Multicast Address Multicast Network Session Key]		
Multicast Application Session Key]		
Class Type	Class C 🗸	·		
Datarate	DR8(SF12,500KHz)	·		
Frequency	923300000	Hz		
Frame-counter	0]		
Selected Devices		_		
Add Device				
		•		

Figure 3-2-2-20

Multicast Gro	up Configuration
ltem	Description
Group Name	Enter the name of this multicast group.
Multicast Address	Device address (Dev Addr) of all devices in this group.
Multicast Network Session Key	The network session key (Netwks Key) of all devices in this group.
Multicast Application Session Key	The application session key (AppSKey) of all devices in this group.
Class Type	Class B and Class C are optional.
Datarate	Datarate of the node receiving downlinks
Frequency	Downlink frequency of all devices in this group.
Frame-count	The number of data frames which received by the end-device downlink
er	from the network server. It will be incremented by the network server.
Ping Slot	Period of opening the pingslot. This is only applied to Class B end
Periodicity	devices.
Selected	Show all device names in this group.

Devices	
Add Device	Add devices in the pull-down list.

Table 3-2-2-15 Multicast Group Setting Parameters

3.2.2.8 Gateway Fleet

Milesight gateways can connect to UG56 network server. A gateway supports to add 100 gateways at most.

Gateway Fleet				
Gateway ID	Name	Status	Last Seen	Operation
24E124FFFEF12263	Local Gateway	Connected	2021-04-19 16:12:27	2 ×
				+

Figure 3-2-2-21		
Item	Description	
Gateway ID	Show the gateway ID.	
Name	Show the name of the gateway.	
Status	Show the connection status of the gateway.	
Last Seen	Show the time of last packet received.	
Operation	Edit or delete the gateway.	

Table 3-2-2-16 Gateway Fleet Parameters

Ga <mark>t</mark> eway ID		
Name		
Location		
GPS info will be displa	ayed by default or can be changed manually	
	ayed by default or can be changed manually Eg:0.026811	
GPS info will be displa Latitude Longitude		



ltem	Description
Gateway ID	Enter the unique gateway ID to recognize the gateway.
Name	Enter the name of this gateway.
Location	GPS data of the gateway can be edited here. If gateway sends GPS data it will replace your customized data.

Table 3-2-2-17 Gateway Setting Parameters

3.2.2.9 Packets

The gateway supports to display latest 1000 pieces of packets and send command to devices.

Device EUI	Туре		Payload	Port	Confirme	d
000000000000000	ASCII	•		85		S
d Data to Multicast Grou Multicast Group	р Туре		Payload	Port		
watcoust oroup	1	~	T uyioud	85		S
vork Server						
Clear				Search		

Figure 3-2-2-23

Send Data To Device/Multicast Group		
ltem	Description	
Device EUI	Enter the EUI of the device to receive the payload.	
Multicast Group	Select the multicast group to send downlinks. Multicast groups can be added under Multicast Groups tab.	
Туре	Choose the payload type to enter in the payload Input box: ASCII, Hex, base64.	
Payload	Enter the message to be sent to this device.	
Port	Enter the LoRaWAN [®] frame port for packet transmission between device and Network Server.	
Confirmed	After enabled, the end device will receive downlink packet and should answer "confirmed" to the network server. Multicast feature does not support confirmed downlink.	

Table 3-2-2-18 Send Data to Device Parameters

Network Server		
Item	Description	
Device EUI/Group	Show the EUI of the device or multicast group.	
Frequency	Show the used frequency to transmit packets.	
Datarate	Show the used datarate to transmit packets.	
SNR	Show the signal-noise ratio.	
RSSI	Show the received signal strength indicator.	
Size	Show the size of payload.	
Fcnt	Show the frame counter.	
	Show the type of the packet:	
Туре	JnAcc - Join Accept Packet	
	JnReq - Join Request Packet	

UpUnc - Uplink Unconfirmed Packet
UpCnf - Uplink Confirmed Packet - ACK response from
network requested
DnUnc - Downlink Unconfirmed Packet
DnCnf - Downlink Confirmed Packet- ACK response from
end-device requested
Show the time of packet was sent or received.

Table 3-2-2-19 Packet Parameters

Click **I** to get more details about the packet. As shown:

Packet Details		×
Dev Addr/Multicast Addr	0614B991	A .
GwEUI	24E124FFFEF0E225	
AppEUI	24E124C0002A0001	
Device EUI/Group Name	24E124126A210644	
Class Type	Class C	
Immediately		
Timestamp	2721022973	
Туре	UpUnc	
Adr	false	
AdrAcKReq	false	
Ack	false	
Fcnt	969	
Port	85	Ŧ



ltem	Description
Dev	
Addr/Multicast	Show the address of the device/multicast group.
Addr	
GwEUI	Show the EUI of the gateway.
AppEUI	Show the App EUI of the end device.
DevEUI/Group	Show the EUL of the device (multicent group name
Name	Show the EUI of the device/multicast group name.
Class Type	Show the class type of the device or multicast group.
Immediately	Whether to send this downlink packet immediately.
Timootomp	Show the time to receive this packet after packet forwarder starts
Timestamp	running. Unit: ms
	Show the type of the packet:
	JnAcc - Join Accept Packet
Туре	JnReq - Join Request Packet
	UpUnc - Uplink Unconfirmed Packet
	UpCnf - Uplink Confirmed Packet - ACK response from network

	requested
	DnUnc - Downlink Unconfirmed Packet
	DnCnf - Downlink Confirmed Packet- ACK response from end-device requested
Adr	True: The end-node has enabled ADR.
	False: The end-node has not enabled ADR.
	In order to validate that the network is receiving the uplink messages,
	nodes periodically transmit ADRACKReq message. This is 1 bit long.
AdrAcKReq	True: Network should respond in ADR_ACK_DELAY time to confirm that
	it is receiving the uplink messages.
	False: ADR is disabled or Network does not respond in ADR_ACK_DELAY.
	True: This frame is ACK.
Ack	False: This frame is not ACK.
	Show the frame-counter of this packet. The network server tracks the
Fcnt	uplink frame counter and generates the
	downlink counter for each end-device.
	The FPort to transmit this packet. If this packet is MAC command, the
FPort	port is 0; if this packet is include application data, the port is not 0
	(1-233).
Modulation	LoRa means the physical layer uses the LoRa modulation.
Bandwidth	Show the bandwidth of this channel.
SpreadFactor	Show the spreadFactor of this channel.
Bitrate	Show the bitrate of this channel.
CodeRate	Show the coderate of this channel.
SNR	Show the SNR of this channel.
RSSI	Show the RSSI of this channel.
Power	Show the transmit power of the device.
Payload (b64)	Show the application payload of this packet.
Payload (hex)	Show the application payload of this packet.
Json	Show the data after decoded.
	Show the MIC of this packet. MIC is a cryptographic message integrity
MIC	code, computed over the fields MHDR, FHDR, FPort and the encrypted
	FRMPayload.

Table 3-2-2-20 Packets Details Parameters

Related Topic

Send Data to Device

3.3 Protocol Integration

3.3.1 BACnet Server

UG56 can work as LoRaWAN[®] to BACnet gateway to integrate with BMS system easily. Before using this feature, ensure the version of inbuilt payload codec library is latest and

49

corresponding LoRaWAN $^{\ensuremath{\$}}$ devices have added correct payload codec.

3.3.1.1 Server

Server		
Enable		
UDP Port	47808	
Device ID	40185	
Device Name	UG67-6222B4620088	
BBMD		
IP Address		
IP Port	47808	
Time TO Live	60000	s

Figure 3-3-1-1

Server Settings	
Item	Description
Enable	Enable or disable BACnet server function.
UDP Port	Set communication port of BACnet/IP. Range: 1-65535.
ODF FUIL	The default port is 47808.
Device ID	The unique BACnet device identifier which needs to avoid conflict
Device ID	with other devices.
Device Name	The device name to represent the device.
BBMD	Enable BBMD(BACnet/IP Broadcast Management Device) if
עואוסס	BACnet devices of different network subnets should work together.
IP Address	Fill in the IP address of BBMD device or external device registrar.
IP Port	Fill in the UDP/IP port for external device registration.
Time TO Live	Number of seconds used on external device registration.

Table 3-3-1-1 Server Parameters

3.3.1.2 BACnet Object

ACT	let G	bject								
Ad	ld Ob	ject Add NC Ob	ject Bulk Import	Bulk Export	Delete				Search	0
÷		Object Name	Object Type	Object Instance Nr	Present Value	Unit	Updates	Update Time	cov	Operatio
ł		WT101								
		WT101.temperat	Analog-Value	0	-	°C	0	-	Disabled	2 ×
		WT101.temperat	Analog-Value	ॉ	-	°C	0	-	Disabled	2 ×

ltem	Description						
	Click to select desired objects to add to this server. The gateway supports adding 2000 objects at most. Note: Ensure the content of payload codec is correct, and the device selects the correct payload codec.						
Add Object	Add BACnet Object						
	Object Name Object Type Unit Related Object Operation						
	- AM308 AM308 battery AM308 battery Am309 heatery Am309 heatery -						
	Andog-Input Andog-Input ** - Battery Andog-Input * * - Battery Andog-Input * - Battery						
	S co2 Antiop-input v ppm -						
Bulk Import	of alarms. The gateway supports adding 200 NC objects at most. Download template to import multiple BACnet objects.						
Bulk Export	Select desire objects to export as .xlsx format file.						
Delete	Select desire objects to delete.						
Object Name	-						
Object Type	Show the name of the BACnet object. Show the type of this object.						
Object Instance Nr	Show the instance number of this object.						
Present Value	Show the latest value of object.						
Units	Show the unit of this object value.						
Updates	Show the update times of this object value.						
Update time	Show the time for this object to get and update the data.						
COV	Show if COV (Change of value) is enabled.						
Operation	Edit or delete the object.						
	· · · · · · · · · · · · · · · · · · ·						

Figure 3-3-1-2

Table 3-3-1-2 BACnet Object List Parameters

BACnet Object

Device Name	AM308	•
LoRa Object	battery	•
Object Name	AM308.battery	
Object Type	Analog-Input	~
The Object Instance	105	
Unit	%(98)	•
Description		
COV		
Event Detection		

Figure 3-3-1-3

BACnet Object Co	onfiguration
ltem	Description
Device Name	Show the name of devices.
LoRa Object	Show the corresponding name of LoRa object.
Object Name	Customize an unique name for this object.
	Select the object type as Binary Input/Output/Value, Analog
Object Type	Input/Output/Value, MultiState Input/Output/Value and
	CharacterString value.
The Object Instance	Customize the object instance.
Description	Enter the description of this object.
Event Detection	Enable to report the alarm of this value. It requires to define at least
Event Detection	one notification class object first.
Analog Input/Out	put/Value
Units	Select the unit of this object value.
	When object value changes, the BACnet server (gateway) will send
COV	notification of new value to BACnet client. This only applies to
	analog type objects.
COV Increment	Only when the object value reaches or over this increment, the
	BACnet server (gateway) will send the notification.
Relinquish	If there is no command, the analog output will be set as this
Default	relinquish default value.
Binary Input/Outp	out/Value

Polarity	Define the binary input/output status as Normal or Reverse.
	Characterize the intended effect of active state of binary type object
Active Text	value. Example: when a button is pressed and binary input is 1,
	active text can be defined as "Pressed".
	Characterize the intended effect of inactive state of binary type
Inactive Text	object value. Example: for a button, inactive text can be defined as
	"Unpressed".
Relinquish	If there is no command, the binary output will be set as this
Default	relinquish default value.
MultiState Input/	Output/Value
Number of	Set the number of states and define the name of every state.
States	Set the number of states and define the name of every state.
Relinquish	If there is no command, the multistate output will be set as this
Default	relinquish default value.
Event Detection	
Notification	Select the notification class to determine the recipients of this
Class	alarm.
Event	Select the event type to report.
Limit Event	When object type is analog type, select if reporting the event when
	reaching the high limit or low limit.
	Under To Offnormal status, when current value returns to (high
Deadband	limit-deadband) value or (low limit+deadband) lasting the delay
Deauballu	time, the device will generate To Normal event. Only Analog types
	have this option.
	Only when current value matches the threshold condition or is out
Time Delay	of threshold for this time, the device will report the corresponding
	event.
	Report the To Offnormal event if the current value is equal to alarm
Alarm Value	value for delay time; report To Normal event if the current value is
Aldini value	not equal to alarm value for delay time. Only Binary Input, Binary
	Value, Multi-State Input or Multi-State Value has this option.
Fault Value	
	Report the To Fault event if the current value is equal to fault value.
	Report the To Fault event if the current value is equal to fault value. Only Multi-State Input or Multi-State Value has this option.
	Only Multi-State Input or Multi-State Value has this option.
Feedback Value	Only Multi-State Input or Multi-State Value has this option. Report the To Offnormal event if the current value is equal to
	Only Multi-State Input or Multi-State Value has this option. Report the To Offnormal event if the current value is equal to feedback value for delay time; report To Normal event if the current
	Only Multi-State Input or Multi-State Value has this option. Report the To Offnormal event if the current value is equal to feedback value for delay time; report To Normal event if the current value is not equal to feedback value for delay time. Only Multi-State

Table 3-3-1-3 BACnet Object Configuration Parameters

Milesight

MAKE SENSING MATTER

BACnet Object					,
Object Name					
Object Type	Notification-Class	~			
The Object Instance	0				
Description					
To-Offnormal Priority					
To-Fault Priority					
To-Normal Priority					
Ack Required	To Offnormal	To Fault	🗹 To Nor	mal	
Recipient List					
Device ID Valid Days	From time To Time	Process Identifier	Issue Notifications Type	Transitions	Operation
					H



Notification Class	s BACnet Object Configuration
Item	Description
Object Name	Customize a unique name for this object.
Object Type	It is fixed as Notification-Class.
The Object Instance	Customize the object instance.
Description	Enter the description of this object.
To-Offnormal Priority	Set the priority number which is used by recipients to sort the event
To-Fault Priority	notifications. Range: 0-255 (0 being most important, 255 least
To-Normal Priority	important)
Ack Required	Specify if this event requires the recipient to send the Acknowledgement Alarm message back to gateway.
Recipient List	 When event detection is enabled and this notification class is selected, the event notification will be sent to recipients in this list. One list supports to add 10 recipients at most. Device ID: the target recipient device ID. Valid Days: valid days to send notifications. From time to time: valid time to send notifications. Process Identifier: the identifier to indicate what process the alarm is intended for. For example, maybe process identifier 1 means maintenance alarms, 2 means critical alarms and 3 means life safety alarms, etc. Issue Notifications Type: select the notification type as confirmed or unconfirmed. If the gateway does not receive the response of Confirmed notification, it will send the notification once again. Transitions: select the reported event types.

54

Table 3-3-1-4 Notification Class BACnet Object Configuration Parameters

3.3.2 Modbus Server

UG56 can work as Modbus server (slave) to receive Modbus RTU or Modbus TCP commands from PLC/BMS systems to read or write to LoRaWAN[®] devices. Before using this feature, ensure the version of inbuilt payload codec library is latest and corresponding LoRaWAN[®] devices have added correct payload codec.

3.3.2.1 Server

Add						Search	
Status	Name	IP Address	Port	Connection Type	Slave ID	Modbus Object Count	Operation
Enable	server1	192.168.45.217	7001	Modbus RTU Over TCP	1	0	2 ×

Figure 3-3-2-1

Item	Description
Add	Add a Modbus server (slave). One gateway supports to add 15
Auu	servers at most.
Status	Show the enable status of this server.
Name	Show the name of the server.
IP Address	Show the IP address of this server and click to check the details.
Port	Show the communication port of this server.
Connection Type	Show the connection type of this server.
Sever ID	Show the server ID of this server.
Modbus Object	Show the Modbus object amount of this server and click the
Count	number to check the details.
Operation	Edit or delete this server.

Table 3-3-2-1 Server Parameters

Enable		
Name		
Network Interface	eth 0	~
Port		
Connection Type	Modbus TCP	~
Slave ID		
Description		

Figure 3-3-2-2

Server Settings	
Item	Description
Enable	Enable or disable this Modbus server.
Name	Customize a unique name to identify this server.
Network Interface	Select the network interface for this server to communicate with Modbus clients (master). The device supports to use different network interfaces to communicate with different remote platforms.
Port	Set communication port of this server. Range: 1-65535.
Connection Type	Select the connection type of this server. Modbus TCP: Modbus client will send Modbus TCP format commands to this Modbus server. Modbus RTU over TCP: Modbus client will send Modbus RTU format commands to this Modbus server.
Server ID	Set the server ID of this Modbus server. This is used for Modbus client to identify every server.
Description	Add description for this server.

Table 3-3-2-2 Server Settings Parameters

3.3.2.2 Modbus Object

Nodbus Modbus (Object Object	server1(port	7001) 🗸					
Ad		Delete					Search	O,
+	Name 🕴	Register Type	Register Address 🔅	Data Format	Related Object	Present Value	Update Time	Operation
- 🗆	WT101							
	battery	Input Register	0	UINT16_ba	-	-	-	

Figure 3-3-2-3

ltem	Description			
Modbus Object	Select the Modbus server to add and edit the objects.			
Add	Click to select desired objects to add to this server. The gateway supports adding 2000 objects at most. Note: ensure the content of payload codec is correct, and the device selects the correct payload codec.			
	Image report_enable Coll Flag 1 - Image report_enable Image report_ena			
Bulk Export	Select desire objects to export as .xlsx format file.			
Delete	Select desire objects to delete.			
Name	Show the name of this object.			

Register Type	Show the register type of this object.	
Register Address	Show the register address of this object.	
Data Format	Show the data format of this object.	
Related Object	Show the related objects.	
Present value	Show the latest value of object.	
Update time	Show the time for this object to get and update the data.	
Operation	Edit or delete the object.	

Table 3-3-2-3 Modbus Object List Parameters

Modbus Object			
	Object Name	battery	
	LoRa Object	battery	
	Register Type	Input Register	~
	Register Address	0	
	Data Format	UINT16_ba	~
	Register Quantity	1	
	Description		
	Unit	%	•
	Related Object	-	
		Save	

Figure 3-3-2-4

Modbus Object Configuration			
ltem	Description		
Object Name	Customize a unique name for this object.		
LoRa Object	Show the corresponding name of LoRa object.		
Object Name	Customize a unique name for this object.		
	Select the Modbus register type.		
	Discrete Input: read-only, only including 0 and 1 status.		
Register Type	Coil: read-write, only including 0 and 1 status.		
	Holding Register: read-write, including analog values, strings, etc.		
	Input Register: read-only, including analog values, strings, etc.		
	When adding an object, this address will generate automatically.		
	And this address support to change. Range: 0-65535		
Pogistor Address	Note:		
Register Address	1) The address of the same register type must be different in one		
	Modbus server.		
	2) The address is related to register quantity. If the address of this		

	object is 0 and register quantity is 2, the address of next object must be 2(0+2) or higher values.
Data Format	Show or select the data format of this object.
Register Quantity	Show the register occupied quantity of this object.
Description	Enter the description of this object.
Unit	Select the unit of this object.
Related Register	Show the related registers. When writing this object, related registers should be written together. Otherwise, this object will be failed to change.

Table 3-3-2-4 Modbus Object Configuration Parameters

3.4 Network

3.4.1 Interface

3.4.1.1 Port

The Ethernet port can be connected with Ethernet cable to get Internet access. It supports 3 connection types.

- Static IP: configure IP address, netmask and gateway for Ethernet WAN interface.

- **DHCP Client**: configure Ethernet WAN interface as DHCP Client to obtain IP address automatically.

- PPPoE: configure Ethernet WAN interface as PPPoE Client.

Port_1	
Port	eth 0 🗸
Connection Type	Static IP 🗸
IP Address	192.168.23.150
Netmask	255.255.255.0
Gateway	192.168.23.1
MTU	1500
Primary DNS Server	8.8.8.8
Secondary DNS Server	223.5.5.5
Enable NAT	
	Figure 3-4-1-1

Port Setting		
ltem	Description	Default

Port	The port that is fixed as eth0 port and enabled.	eth 0
Connection Type	Select from "Static IP", "DHCP Client" and "PPPoE".	DHCP
MTU	Set the maximum transmission unit.	1500
Primary DNS Server	Set the primary DNS.	8.8.8.8
Secondary DNS Server	Set the secondary DNS.	223.5.5.5
Enable NAT	Enable or disable NAT function. When enabled, a private IP can be translated to a public IP.	Enable

Table 3-4-1-1 Port Parameters

Related Configuration Example

Ethernet Connection

1. Static IP Configuration

If the external network assigns a fixed IP for the Ethernet port, user can select "Static IP" mode.

- Port_1		
Port	eth 0	~
Connection Type	Static IP	~
IP Address	192.168.23.150	
Netmask	255.255.255.0	
Gateway	192.168.23.1	
MTU	1500	
Primary DNS Server	8.8.8.8	
Secondary DNS Server	223.5.5.5	
Enable NAT		
Multiple IP Address		
	IP Address	

Figure 3-4-1-2

Static IP				
ltem	Description	Default		
IP Address	Set the IP address which can access Internet.	192.168.23.150		
Netmask	Set the Netmask for Ethernet port.	255.255.255.0		
Gateway	Set the gateway's IP address for Ethernet port.	192.168.23.1		
Multiple IP Address	Set the multiple IP addresses for Ethernet port.	Null		

Table 3-4-1-2 Static IP Parameters

2. DHCP Client

Milesight

If the external network has DHCP server enabled and has assigned IP addresses to the Ethernet WAN interface, user can select "DHCP client" mode to obtain IP address automatically.

- Port_1		
Port	eth 0	~
Connection Type	DHCP Client	~
MTU	1500	
Use Peer DNS		
Primary DNS Server	8.8.8.8	
Secondary DNS Server	223.5.5.5	
Enable NAT		

Figure 3-4-1-3

DHCP Client			
Item Description			
Use Peer DNS	Obtain peer DNS automatically during PPP dialing. DNS is necessary when user visits domain name.		
Table 3-4-1-3 DHCP Client Parameters			

3. PPPoE

PPPoE refers to a point to point protocol over Ethernet. User has to install a PPPoE client on the basis of original connection way. With PPPoE, remote access devices can get control of each user.

Port_1		
Port	eth 0	~
Connection Type	PPPoE	~
Username		
Password		
Link Detection Interval(s)	60	
Max Retries	0	
MTU	1500	
Use Peer DNS		
Primary DNS Server	8.8.8.8	
Secondary DNS Server	223.5.5.5	
Enable NAT		



PPPoE				
ltem	Description			
Username	Enter the username provided by your Internet Service Provider (ISP).			
Password	Enter the password provided by your Internet Service Provider (ISP).			
Link Detection Interval (s)	Set the heartbeat interval for link detection. Range: 1-600.			
Max Retries	Set the maximum retry times after it fails to dial up. Range: 0-9.			
Use Peer DNS	Obtain peer DNS automatically during PPP dialing. DNS is necessary when user visits domain name.			

Table 3-4-1-4 PPOE Parameters

3.4.1.2 WLAN

This section explains how to set the related parameters for Wi-Fi network. UG56 supports 802.11 b/g/n, as AP or client mode.

Port	WLAN	Cellular	Loopbac	k
WLAN				
Enable				
Work Mode	3	AP		~
SSID Broa	dcast			
AP Isolatio	n			
Radio Type		802.11n	(2.4GHz)	~
Channel		Auto		~
SSID				
BSSID				
Encryption	Mode	No Encr	yption	~
Bandwidth		20MHz		~
Max Client	Number	10		
IP Setting				
Protocol		Static IP		~
IP Address				
		DHCP Set	tings	
Netmask				

Figure 3-4-1-5

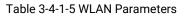
WLAN			
Enable			
Work Mode	Client	~	Scan
SSID			
BSSID			
Encryption Mode	WPA-PSK/WPA2-PSK	~	
Cipher	Auto	~	
Key			
IP Setting			
Protocol	Static IP	~	
IP Address			
Netmask	255.255.255.0		
Gateway			

Figure 3-4-1-6

WLAN	
Item	Description
Enable	Enable/disable WLAN.

Work Mode	Select work mode. The options are "Client" or "AP".		
AP Mode			
BSSID	Show the MAC address of this WLAN interface.		
Radio Type	Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)".		
Channel	Select wireless channel. The options are "Auto", "1", "2""11".		
Bandwidth	Select bandwidth. The options are "20MHz" and "40MHz".		
SSID	Fill in the SSID of the access point.		
Encryption Mode	Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK".		
Cipher	Select cipher of WPA encryption. The options are "Auto", "AES", "TKIP" and "AES/TKIP".		
Key	Fill the key to connect to this access point. The default key is iotpassword .		
Max Client Number	Set the maximum number of clients to access.		
IP Setting			
Protocol	It's fixed as Static IP.		
IP Address	Set the IP address in wireless network.		
Netmask	Set the netmask in wireless network.		
Client Mode			
Scan	Click to scan the access points around this device.		
SSID	Fill in the SSID of the access point.		
BSSID	Fill in the MAC address of the access point. Either SSID or BSSID can be filled to join the network.		
Encryption Mode	Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK", "WPA-PSK/WPA2-PSK", "WPA-Enterprise", "WPA2-Enterprise" and "WPA-Enterprise/WPA2-Enterprise".		
Cipher	Select cipher of WPA encryption. The options are "Auto", "AES", "TKIP" and "AES/TKIP".		
Key	Fill the key to connect to this access point.		
Xsupplicant Type	Select from "Peap", "Leap", "TLS" and "TTLS".		
User	Fill the username of WPA/WPA2-Enterprise.		
Anonymous Identity	Fill the anonymous identity of WPA/WPA2-Enterprise.		
Phase 2	Fill the phase of WPA/WPA2-Enterprise.		
Public Server	The public server certificate used for verifying with WPA/WPA2-Enterprise		
Certificate	access point.		
IP Setting			
Protocol	Set the protocol to get the WLAN IP address.		
IP Address	Set the IP address in wireless network when protocol is Static IP.		

Netmask	Set the netmask in wireless network when protocol is Static IP.
Gateway	Set the gateway in wireless network when protocol is Static IP.
Primary DNS Server	Set the primary IPv4 DNS server.
Secondary DNS Server	Set the secondary IPv4 DNS server.



Port	WLAN	Cellular	Lo	opback				
< GoBack								
S	SSID	Channel	Signal	Cipher	BSSID	Security	Frequency	
Vison Ser	nsor_006602	Auto	-94dBm	Auto	24:e1:24:00:66:02	No Encryption	2462MHz	Join Network
Milesi	ight_Test	Auto	-88dBm	AES	ec:26:ca:99:3a:a4	WPA-PSK/WPA2-PSK	2437MHz	Join Network

Figure 3-4-1-7

Client Mode-Scar	n		
SSID	Show SSID.		
Channel	Show wireless channel.		
Signal	Show wireless signal.		
BSSID	Show the MAC address of the access point.		
Security	Show the encryption mode.		
Frequency	Show the frequency of radio.		
Join Network	Click the button to join the wireless network.		

Table 3-4-1-6 WLAN Scan Parameters

Related Topic

Wi-Fi Application Example

3.4.1.3 Cellular

This section explains how to set the related parameters for cellular network.

I

Auto 🗸
ø
ø
None 🗸
1500



Connection Setting		
Enable NAT		
Restart When Dial-up failed		
ICMP Server	8.8.8.8	
Secondary ICMP Server	114.114.114.114	
ICMP Detection Max Retries	3	
ICMP Detection Timeout	5	s
ICMP Detection Interval	15	s
SMS Settings		
SMS Mode	PDU	~

Figure 3-4-1-9

General Settings		
ltem	Description	
Enable	Check the option to enable the corresponding SIM card.	

Milesight

	Select from "Auto", "Auto 3G/4G", "4G Only" and "3G Only".				
Network Type	Auto: connect to the network with the strongest signal automatically.				
	4G Only: connect to 4G network only. And so on.				
	Enter the Access Point Name for cellular dial-up connection provided				
APN	by local ISP.				
	Enter the username for cellular dial-up connection provided by local				
Username	ISP.				
	Enter the password for cellular dial-up connection provided by local				
Password	ISP.				
	Enter the dial-up center NO. For cellular dial-up connection provided				
Access Number	by local ISP.				
PIN Code	Enter a 4-8 characters PIN code to unlock the SIM.				
Authentication	Coloct from "Nono" "DAD" "OLIAD"				
Туре	Select from "None", "PAP", "CHAP".				
Roaming	Enable or disable roaming.				
Customized					
MTU	Enable or disable to customize the maximum transmission units.				
MTU	When disabled, the device will use operator's MTU settings.				
WITO .	Set the maximum transmission units. Range: 68-1500. Customize the cellular subnet mask. If blank, the device will use the				
Custom Subnet	subnet mask provided by the cellular base station.				
Mask	Note: this feature is only supported by parts of cellular modules.				
Custom DNS	Customize the cellular DNS server. If blank, the device will use the				
Server	DNS server provided by the cellular provider.				
Enable IMS	Enable or disable IMS function.				
0140 0	Enter the local SMS center number for storing, forwarding, converting				
SMS Center	and delivering SMS message.				
Enable NAT	Enable or disable NAT function.				
Restart When	When this function is enabled, the gateway will restart automatically if				
Dial-up failed	the dial-up fails several times.				
	Set the ICMP detection server's IP address.				
ICMP Server	Note: Please get in touch with the ISP to determine whether ping				
	detection is allowed and get the correct ICMP server addresses. If				
	ping detection is not allowed, leave this sever address blank.				
Secondary ICMP	Set the secondary ICMP detection server's IP address.				
Server					
ICMP Detection Max Retries	Set max number of retries when ICMP detection fails.				
ICMP Detection					
Timeout	Set timeout of ICMP detection.				
ICMP Detection					
Interval	Set interval of ICMP detection.				
SMS Mode	Select SMS mode from "TEXT" and "PDU".				

Table 3-4-1-7 Cellular Parameters

Connection Setting	
Connection Mode	Connect on Demand 🗸
Redial Interval(s)	5
Max Idle Time(s)	60
Triggered by Call	
Triggered by SMS	

Figure 3-4-1-10

ltem	Description		
Connection Mode			
Connection Mode	Select from "Always Online" and "Connect on Demand".		
Redial Interval(s)	Set the time interval between redials. Range: 0-3600.		
Max Idle Time(s)	Set the maximum duration of the gateway when current link is under idle status. Range: 10-3600.		
Triggered by Call	The gateway will switch from offline mode to cellular network mode automatically when it receives a call from the specific phone number.		
Call Group	Select a call group for call trigger. Go to "System > General Settings > Phone" to set up phone group.		
Triggered by SMS	The gateway will switch from offline mode to cellular network mode automatically when it receives a specific SMS from the specific mobile phone.		
SMS Group	Select a SMS group for trigger. Go to "System > General Settings > Phone" to set up SMS group.		
SMS Text	Fill in the SMS content for triggering.		

Table 3-4-1-8 Cellular Parameters

Related Topics

<u>Cellular Connection Application Example</u> <u>Phone Group</u>

3.4.1.4 Loopback

Loopback interface is used for replacing gateway's ID as long as it is activated. When the interface is DOWN, the ID of the gateway has to be selected again which leads to long convergence time of OSPF. Therefore, Loopback interface is generally recommended as the ID of the gateway.

Loopback interface is a logic and virtual interface on gateway. Under default conditions, there's no loopback interface on gateway, but it can be created as required.

Port	WLAN	Cellular	Loopback		
Loopback	Address				
IP Address		127.0.0.1			
Netmask		255.0.0.0			
Multiple IP	Addresses				
	IP	Address		Netmask	Operation
					•
Save					

Figure 3-4-1-11

Loopback				
ltem	Description	Default		
IP Address	Unalterable	127.0.0.1		
Netmask	Unalterable	255.0.0.0		
Multiple IP Addresses	Apart from the IP above, user can configure other IP addresses.	Null		

Table 3-4-1-9 Loopback Parameters

3.4.1.5 VLAN Trunk

UG56 gateway supports the Ethernet port working as VLAN Trunk client and be assigned a VLAN ID, which easy to traffic classification. When VLAN ID is set, port on "**Network**" > "Interface" > "Port" can be chosen as eth0.x with x being VLAN ID. VLAN Setting is blank

by default, you can add a new VLAN label to certain interface by clicking \square .

Interface		VID	Operation
eth 0	~		×
			H

Figure 3-4-1-12

VLAN Trunk			
ltem	Description		
Interface	Select the VLAN interface, it's fixed as eth0.		
VID	Set the label ID of the VLAN. Range: 1-4094.		

Table 3-4-1-10 VLAN Trunk Parameters

3.4.2 Firewall

This section describes how to set the firewall parameters, including website block, ACL, DMZ, Port Mapping and MAC Binding.

The firewall implements corresponding control of data flow at entry direction (from Internet to local area network) and exit direction (from local area network to Internet) according to the content features of packets, such as protocol style, source/destination IP address, etc. It ensures that the gateway operate in a safe environment and host in local area network.



Security	ACL	DMZ	Port Mapping	MAC Binding
Website Block	ing by URL Ad	dress		
URL Address		http://		×
				±
Website Block	ing by Keywor	d		
Keyword				×
				8
		Figure 3	-4-2-1	

Enter the HTTP address which you want to block.
You can block specific website by entering keyword. The maximum number of character allowed is 64.

Table 3-2-2-1 Security Parameters

3.4.2.2 ACL

Access control list, also called ACL, implements permission or prohibition of access for specified network traffic (such as the source IP address) by configuring a series of matching rules so as to filter the network interface traffic. When gateway receives packet, the field will be analyzed according to the ACL rule applied to the current interface. After the special packet is identified, the permission or prohibition of corresponding packet will be implemented according to preset strategy.

The data package matching rules defined by ACL can also be used by other functions requiring flow distinction.

Security	ACL	DMZ	Port Mapping	MAC Binding			
ACL Setting							
Default Filter Po	blicy	Accept	~				
Access Contro	l List						
			Туре	extended	~		
			ID				
			Action	permit	*		
			Protocol	ip	~		
			Source IP				
			Source Wildcard Mask	0.0.0.0			
			Destination IP				
			Destination Wildcard Mask	0.0.0.0			
			Description				
			Save	Cancel			
Interface List							
	Interface		In ACL			Out ACL	Operation
							æ

Figure 3-4-2-2

ltem	Description				
ACL Setting					
	Select from "Accept" and "Deny".				
Default Filter Policy	The packets which are not included in the access control list will				
	be processed by the default filter policy.				
Access Control List					
Туре	Select type from "Extended" and "Standard".				
ID	User-defined ACL number. Range: 1-199.				
Action	Select from "Permit" and "Deny".				
Protocol	Select protocol from "ip", "icmp", "tcp", "udp", and "1-255".				
Source IP	Source network address (leaving it blank means all).				
Source Wildcard	Wildcard mask of the source network address.				
Mask	wildcard mask of the source network address.				
Destination IP	Destination network address (0.0.0.0 means all).				
Destination Wildcard	Wildcard mask of destination address.				
Mask	wildcard mask of destination address.				
Description	Fill in a description for the groups with the same ID.				
ICMP Type	Enter the type of ICMP packet. Range: 0-255.				
ICMP Code	Enter the code of ICMP packet. Range: 0-255.				
Source Port Type	Select source port type, such as specified port, port range, etc.				
Source Port	Set source port number. Range: 1-65535.				
Start Source Port	Set start source port number. Range: 1-65535.				
End Source Port	Set end source port number. Range: 1-65535.				

Destination Port	Select destination port type, such as specified port, port range,			
Туре	etc.			
Destination Port	Set destination port number. Range: 1-65535.			
Start Destination Port	Set start destination port number. Range: 1-65535.			
End Destination Port	Set end destination port number. Range: 1-65535.			
More Details	Show information of the port.			
Interface List				
Interface	Select network interface for access control.			
In ACL	Select a rule for incoming traffic from ACL ID.			
Out ACL	Select a rule for outgoing traffic from ACL ID.			

Table 3-4-2-2 ACL Parameters

3.4.2.3 DMZ

DMZ is a host within the internal network that has all ports exposed, except those forwarded ports in port mapping.

Security	ACL	DMZ	Port Mapping
Enable			
DMZ Host			
Source Address			



DMZ				
Item	Description			
Enable	Enable or disable DMZ.			
DMZ Host	Enter the IP address of the DMZ host on the internal network.			
Source Address	Set the source IP address which can access to DMZ host. "0.0.0.0/0" means any address.			

Table 3-4-2-3 DMZ Parameters

3.4.2.4 Port Mapping (DNAT)

When external services are needed internally (for example, when a website is published ext ernally), the external address initiates an active connection. And, the router or the gateway on the firewall receives the connection. Then it will convert the connection into the an internal connection. This conversion is called DNAT, which is mainly used for external and interval services.

Click 🛨 to add a new port mapping rules.

Milesight

Security	ACL	DMZ	Port Mapping	MAC E	Binding		
Port Mapping							
Source	P IP	Source Port	Destination IP	Destination Port	Protocol	Description	Operation
0.0.0/0					TCP 🗸		×
							Ð

Figure 3-4-2-4

Port Mapping				
ltem	Description			
Source IP	Specify the host or network which can access local IP address.			
	0.0.0/0 means all.			
Source Port	Enter the TCP or UDP port from which incoming packets are			
Source Fort	forwarded. Range: 1-65535.			
Destination IP	Enter the IP address that packets are forwarded to after being			
Destination in	received on the incoming interface.			
Destination Port	Enter the TCP or UDP port that packets are forwarded to after			
Destination Fort	being received on the incoming port(s). Range: 1-65535.			
Protocol	Select from "TCP" and "UDP" as your application required.			
Description	The description of this rule.			

Table 3-4-2-4 Port Mapping Parameters

Related Configuration Example

NAT Application Example

3.4.2.5 MAC Binding

MAC Binding is used for specifying hosts by matching MAC addresses and IP addresses that are in the list of allowed outer network access.

Security	ACL	DMZ	Port Mapping	MAC Binding		
MAC Binding	List					
,	MAC Address		IP Address		Description	Operation
						E

Figure 3-4-2-5

MAC Binding Lis	st
ltem	Description

MAC Address	Set the binding MAC address.
IP Address	Set the binding IP address.
Description	Fill in a description for convenience of recording the meaning of the binding rule for each piece of MAC-IP.
	Table 2.4.2.5 MAC Binding Decomptore

Table 3-4-2-5 MAC Binding Parameters

3.4.3 DHCP

UG56 can be set as a DHCP server to distribute IP address when Wi-Fi work as AP mode.

DHCP Server_1			
Enable			
Interface	wlan0 🗸		
Start Address	192.168.66.100		
End Address	192.168.66.199		
Netmask	255.255.255.0		
Lease Time(Min)	1440		
Primary DNS Server	8.8.8.8		
Secondary DNS Server			
Windows Name Server			
Static IP			
MAC Ad	ldress	IP Address	Operat

Figure 3-4-3-1

DHCP Server	DHCP Server						
ltem	Description	Default					
Enable	Enable or disable DHCP server.	Enable					
Interface	Only wlan interface is allowed to distribute IP addresses.	wlan0					
Start Address	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.100					
End Address	Define the end of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.199					
Netmask	Define the subnet mask of IP address obtained by DHCP clients from DHCP server.	255.255.255.0					
Lease Time (Min)	Set the lease time on which the client can use the IP address obtained from DHCP server. Range: 1-10080.	1440					

Primary DNS Server	Set the primary DNS server.	8.8.8.8
Secondary DNS Server	Set the secondary DNS server.	Null
Windows Name Server	Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever. Generally you can leave it blank.	Null
Static IP		
MAC Address	Set a static and specific MAC address for the DHCP client (it should be different from other MACs so as to avoid conflict).	Null
IP Address	Set a static and specific IP address for the DHCP client (it should be outside of the DHCP range).	Null

Table 3-4-3-1 DHCP Server Parameters

3.4.4 DDNS

Dynamic DNS (DDNS) is a method that automatically updates a name server in the Domain Name System, which allows user to alias a dynamic IP address to a static domain name. DDNS serves as a client tool and needs to coordinate with DDNS server. Before starting configuration, user shall register on a website of proper domain name provider and apply for a domain name.

-	DNS										
D	ONS Metho Name	d List	Service Type	Username	User ID	Password	Server	Server Path	Hostname	Appe nd IP	Oper ation
[wlan0 🗸	DynDI 🗸								×
											Ŧ

Figure 3-4-4-1

DDNS	
ltem	Description
Name	Give the DDNS a descriptive name.
Interface	Set interface bundled with the DDNS.
Service Type	Select the DDNS service provider.
Username	Enter the username for DDNS register.
User ID	Enter User ID of the custom DDNS server.
Password	Enter the password for DDNS register.
Server	Enter the name of DDNS server.
Hostname	Enter the hostname for DDNS.
Append IP	Append your current IP to the DDNS server update path.

Table 3-4-4-1 DDNS Parameters

3.4.5 Link Failover

This section describes how to configure link failover strategies, such as VRRP strategies.

Configuration Steps

- 1. Define one or more SLA operations (ICMP probe).
- 2. Define one or more track objects to track the status of SLA operation.
- 3. Define applications associated with track objects, such as VRRP or static routing.

3.4.5.1 SLA

SLA setting is used for configuring link probe method. The default probe type is ICMP.

SLA	Track	WAN Failover							
SLA Entry									
ID	Тур	e Destinati	ion Address Secondary Destinatio Address	n Data Size	Interval(s)	Timeout(ms)	Packet Loss Count	Start Time	Operation
1	icmp-echo	♥ 8.8.8.8	223.5.5.5	56	15	5000	3	now 🗸	×
									+

Figure 3-4-5-1

SLA		
ltem	Description	Default
ID	SLA index. Up to 10 SLA settings can be added. Range: 1-10.	1
Туре	ICMP-ECHO is the default type to detect if the link is alive.	icmp-echo
Destination Address	The detected IP address.	8.8.8.8
Secondary Destination Address	The secondary detected IP address.	223.5.5.5
Data Size	User-defined data size. Range: 0-1000.	56
Interval (s)	User-defined detection interval. Range: 1-608400.	30
Timeout (ms)	User-defined timeout for response to determine ICMP detection failure. Range: 1-300000.	5000
Packet Loss Count	Define packet loss count in each SLA probe. SLA probe fails when the preset packet loss count is exceeded.	5
Start Time	Detection start time; select from "Now" and blank character. Blank character means this SLA detection doesn't start.	now

Table 3-4-5-1 SLA Parameters

3.4.5.2 Track

Track setting is designed for achieving linkage among SLA module, Track module and

Milesight

Application module. Track setting is located between application module and SLA module with main function of shielding the differences of various SLA modules and providing unified interfaces for application module.

Linkage between Track Module and SLA module

Once you complete the configuration, the linkage relationship between Track module and SLA module will be established. SLA module is used for detection of link status, network performance and notification of Track module. The detection results help track status change timely.

- For successful detection, the corresponding track item is Positive.
- For failed detection, the corresponding track item is Negative.

Linkage between Track Module and Application Module

After configuration, the linkage relationship between Track module and Application module will be established. When any change occurs in track item, a notification that requires corresponding treatment will be sent to Application module.

Currently, the application modules like VRRP and static routing can get linkage with track module.

If it sends an instant notification to Application module, the communication may be interrupted in some circumstances due to routing's failure like timely restoration or other reasons. Therefore, user can set up a period of time to delay notifying application module when the track item status changes.

SLA	Track	WAN Failover				
Track Object						
ID	Туре	SLA ID	Interface	Negative Delay(s)	Positive Delay(s)	Operation
1	sla	∨ 1 ∨	wlan0 🗸 🗸	0	1	

Figure	3-4-5-2
--------	---------

ltem	Description	Default
Index	Track index. Up to 10 track settings can be configured. Range: 1-10.	1
Туре	The options are "sla" and "interface".	SLA
SLA ID	Defined SLA ID.	1
Interface	Select the interface whose status will be detected.	cellular0
Negative Delay (s)	When interface is down or SLA probing fails, it will wait according to the time set here before actually changing its status to Down. Range: 0-180 (0 refers to immediate switching).	0
Positive Delay (s)	When failure recovery occurs, it will wait according to the time set here before actually changing its status to Up. Range: 0-180 (0 refers to immediate	1

switching).	

Table 3-4-5-2 Track Parameters

3.4.5.3 WAN Failover

WAN failover refers to failover between Ethernet WAN interface and cellular interface. When service transmission can't be carried out normally due to malfunction of a certain interface or lack of bandwidth, the rate of flow can be switched to backup interface quickly. Then the backup interface will carry out service transmission and share network flow so as to improve reliability of communication of data equipment.

When link state of main interface is switched from up to down, system will have the pre-set delay works instead of switching to link of backup interface immediately. Only if the state of main interface is still down after delay, will the system switch to link of backup interface. Otherwise, system will remain unchanged.

SLA	Trac	:k	WAN Fa	ilover				
WAN Failo Main Int		Backup Ir	nterface	Startup Delay(s)	Up Delay(s)	Down Delay(s)	Track ID	Operation
Cellular () ~	eth 0	~	30	0	0	1 ~	
								8

Figure 3-4-5-3

WAN Failover				
Parameters	Description	Default		
Main Interface	Select a link interface as the main link.			
Backup Interface	Select a link interface as the backup link.			
Startup Delay (s)	Set how long to wait for the startup tracking detection policy to take effect. Range: 0-300.	30		
Up Delay (s)	When the primary interface switches from failed detection to successful detection, switching can be delayed based on the set time. Range: 0-180 (0 refers to immediate switching)	0		
Down Delay (s)	When the primary interface switches from successful detection to failed detection, switching can be delayed based on the set time. Range: 0-180 (0 refers to immediate switching).	0		
Track ID	Track detection, select the defined track ID.			

Table 3-4-5-3 WAN Failover Parameters

3.4.6 VPN

Virtual Private Networks, also called VPNs, are used to securely connect two private

networks together so that devices can connect from one network to the other network via secure channels.

UG56 supports DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN, as well as GRE over IPsec and L2TP over IPsec.

3.4.6.1 DMVPN

A dynamic multi-point virtual private network (DMVPN), combining mGRE and IPsec, is a secure network that exchanges data between sites without passing traffic through an organization's headquarter VPN server or gateway.

DMVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client
DMVPN Setting	gs				
Enable					
Hub Address					
Local IP Addres	S				
GRE HUB IP Ad	Idress				
GRE Local IP A	ddress				
GRE Mask			255.255.255.0		
GRE Key					
Negotiation Mod	le		Main	•	
Authentication A	lgorithm		DES	Ŧ	
Encryption Algo	rithm		MD5	٣	
DH Group			MODP768-1	Ŧ	
Key					
Local ID Type			Default	Ŧ	
IKE Life Time(s)	r,		10800		
SA Algorithm			DES-MD5	•	
PFS Group			NULL	٣	
Life Time(s)			3600		
		Fi	gure 3-4-6-1		



Figure 3-4-6-2

DMVPN				
ltem	Description			
Enable	Enable or disable DMVPN.			
Hub Address	The IP address or domain name of DMVPN Hub.			
Local IP address	DMVPN local tunnel IP address.			
GRE Hub IP Address	GRE Hub tunnel IP address.			
GRE Local IP Address	GRE local tunnel IP address.			

GRE Netmask	GRE local tunnel netmask.
GRE Key	GRE tunnel key.
Negotiation Mode	Select from "Main" and "Aggressive".
Authentication	Select from "DES", "3DES", "AES128", "AES192" and
Algorithm	"AES256".
Encryption Algorithm	Select from "MD5" and "SHA1".
DI L Croun	Select from "MODP768_1", "MODP1024_2" and
DH Group	"MODP1536_5".
Key	Enter the preshared key.
Local ID Type	Select from "Default", "ID", "FQDN", and "User FQDN"
IKE Life Time (s)	Set the lifetime in IKE negotiation. Range: 60-86400.
	Select from "DES_MD5", "DES_SHA1", "3DES_MD5",
SA Algorithm	"3DES_SHA1", "AES128_MD5", "AES128_SHA1",
SA Algonunn	"AES192_MD5", "AES192_SHA1", "AES256_MD5" and
	"AES256_SHA1".
PFS Group	Select from "NULL", "MODP768_1", "MODP1024_2" and
	"MODP1536-5".
Life Time (s)	Set the lifetime of IPsec SA. Range: 60-86400.
DPD Interval Time (s)	Set DPD interval time
DPD Timeout (s)	Set DPD timeout.
Cisco Secret	Cisco Nhrp key.
NHRP Holdtime (s)	The holdtime of Nhrp protocol.

Table 3-4-6-1 DMVPN Parameters

3.4.6.2 IPSec

IPsec is especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers.

IPsec provides three choices of security service: Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE). AH essentially allows authentication of the senders' data. ESP supports both authentication of the sender and data encryption. IKE is used for cipher code exchange. All of them can protect one and more data flows between hosts, between host and gateway, and between gateways.

DMVPN	IPsec	GRE	L2TP	PPTP
IPsec Settings				
- IPsec_1				
Enable				
IPsec Gat	eway Address			
IPsec Mo	de	Т	unnel	Ŧ
IPsec Pro	tocol	E	SP	¥
Local Sub	net			
Local Sub	net Mask			
Local ID T	уре)efault	¥
Remote S	ubnet			
Remote S	ubnet Mask			
Remote II	О Туре		efault	•

Figure 3-4-6-3

IPsec			
Item	Description		
Enable	Enable IPsec tunnel. A maximum of 3 tunnels is allowed.		
IPsec Gateway Address	Enter the IP address or domain name of remote IPsec server.		
IPsec Mode	Select from "Tunnel" and "Transport".		
IPsec Protocol	Select from "ESP" and "AH".		
Local Subnet	Enter the local subnet IP address that IPsec protects.		
Local Subnet Netmask	Enter the local netmask that IPsec protects.		
Local ID Type	Select from "Default", "ID", "FQDN", and "User FQDN".		
Remote Subnet	Enter the remote subnet IP address that IPsec protects.		
Remote Subnet Mask	Enter the remote netmask that IPsec protects.		
Remote ID type	Select from "Default", "ID", "FQDN", and "User FQDN".		
	Table 2.4.6.2 IDaga Devenators		

Table 3-4-6-2 IPsec Parameters

IKE Parameter		
IKE Version	IKEv1	•
Negotiation Mode	Main	•
Encryption Algorithm	DES	•
Authentication Algorithm	MD5	•
DH Group	MODP768-1	۲
Local Authentication	PSK	*
Local Secrets		
XAUTH		
Lifetime(s)	10800	
SA Parameter		
SA Algorithm	DES-MD5	۲
PFS Group	NULL	•
Lifetime(s)	3600	
DPD Time Interval(s)	30	
DPD Timeout(s)	150	
IPsec Advanced		
Enable Compression		
VPN Over IPsec Type	NONE	•

Figure 3-4-6-4

IKE Parameter	IKE Parameter				
ltem	Description				
IKE Version	Select from "IKEv1" and "IKEv2".				
Negotiation Mode	Select from "Main" and "Aggressive".				
Encryption Algorithm	Select from "DES", "3DES", "AES128", "AES192" and "AES256".				
Authentication Algorithm	Select from "MD5" and " SHA1"				
DH Group	Select from "MODP768_1", "MODP1024_2" and "MODP1536_5".				
Local Authentication	Select from "PSK" and "CA".				
Local Secrets	Enter the preshared key.				
XAUTH	Enter XAUTH username and password after XAUTH is enabled.				
Lifetime (s)	Set the lifetime in IKE negotiation. Range: 60-86400.				
SA Parameter					
	Select from "DES_MD5", "DES_SHA1", "3DES_MD5",				
SA Algorithm	"3DES_SHA1", "AES128_MD5", "AES128_SHA1", "AES192_MD5",				
	"AES192_SHA1", "AES256_MD5" and "AES256_SHA1".				
PFS Group	Select from "NULL", "MODP768_1" , "MODP1024_2" and "MODP1536_5".				
Lifetime (s)	Set the lifetime of IPsec SA. Range: 60-86400.				

DPD Interval Time(s)	Set DPD interval time to detect if the remote side fails.		
DPD Timeout(s)	Set DPD timeout. Range: 10-3600.		
IPsec Advanced			
Enable Compression	The head of IP packet will be compressed after it's enabled.		
VPN Over IPsec Type	Select from "NONE", "GRE" and "L2TP" to enable VPN over IPsec function.		

Table 3-4-6-3 IPsec Parameters

3.4.6.3 GRE

Generic Routing Encapsulation (GRE) is a protocol that encapsulates packets in order to route other protocols over IP networks. It's a tunneling technology that provides a channel through which encapsulated data message can be transmitted and encapsulation and decapsulation can be realized at both ends.

In the following circumstances the GRE tunnel transmission can be applied:

- GRE tunnel can transmit multicast data packets as if it were a true network interface. Single use of IPSec cannot achieve the encryption of multicast.
- A certain protocol adopted cannot be routed.
- A network of different IP addresses shall be required to connect other two similar networks.

DMV	PN	IPsec	GRE	L2TP	PPTP
GRE S	Settings				
- 0	GRE_1				
	Enable			v	
ļ	Remote IP Add	ress			
	Local IP Addre	58			
1	Local Virtual IP	Address			
1	Netmask			255.255.255.0	
1	Peer Virtual IP	Address			
	Globa <mark>l T</mark> raffic F	orwarding			
i	Remote Subne	ť			
	Remote Netma	sk			
	UTN			1500	
	Key				
	Enable NAT				

Figure 3-4-6-5

GRE	
Item	Description
Enable	Check to enable GRE function.

Remote IP Address	Enter the real remote IP address of GRE tunnel.	
Local IP Address	Set the local IP address.	
Local Virtual IP Address	Set the local tunnel IP address of GRE tunnel.	
Netmask	Set the local netmask.	
Peer Virtual IP Address	Enter remote tunnel IP address of GRE tunnel.	
Global Traffic	All the data traffic will be sent out via GRE tunnel when this	
Forwarding	function is enabled.	
Remote Subnet	Enter the remote subnet IP address of GRE tunnel.	
Remote Netmask	Enter the remote netmask of GRE tunnel.	
MTU	Enter the maximum transmission unit. Range: 64-1500.	
Кеу	Set GRE tunnel key.	
Enable NAT	Enable NAT traversal function.	
	Table 2.4.6.4 CDE Deremetere	

Table 3-4-6-4 GRE Parameters

3.4.6.4 L2TP

Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet.

DMVPN IPsec		GRE	L2TP	PPTP
— L2TP_1				
Enable			i	
Remote IF	Address			
Username				
Password				
Authentica	ition		Auto	~
Global Tra	ffic Forwarding	C)	
Remote S	ubnet		10.5.22.0	
Remote S	ubnet Mask		255.255.255.0	
Key				
Use L2TP	Peer DNS		1	

Figure 3-4-6-6

L2TP	
Item	Description
Enable	Check to enable L2TP function.
Remote IP Address	Enter the public IP address or domain name of L2TP server.

Username	Enter the username that L2TP server provides.	
Password	Enter the password that L2TP server provides.	
Authentication	Select from "Auto", "PAP", "CHAP", "MS-CHAPv1" and "MS-CHAPv2".	
Global Traffic	All of the data traffic will be sent out via L2TP tunnel after	
Forwarding	this function is enabled.	
Remote Subnet	Enter the remote IP address that L2TP protects.	
Remote Subnet Mask	Enter the remote netmask that L2TP protects.	
Key	Enter the password of L2TP tunnel.	
Use L2TP Peer DNS	Enable to use the DNS address of peer L2TP server .	

Table 3-4-6-5 L2TP Parameters

Advanced Settings	
Local IP Address	
Peer IP Address	
Enable NAT	
Enable MPPE	
Address/Control Compression	
Protocol Field Compression	
Asyncmap Value	fffffff
MRU	1500
MTU	1500
Link Detection Interval(s)	60
Max Retries	0
Expert Options	

Figure 3-4-6-7

Advanced Settings	
Item	Description
Local IP Address	Set tunnel IP address of L2TP client. Client will obtain tunnel IP address automatically from the server when it's null.
Peer IP Address	Enter tunnel IP address of L2TP server.
Enable NAT	Enable NAT traversal function.
Enable MPPE	Enable MPPE encryption.
Address/Control Compression	For PPP initialization. User can keep the default option.
Protocol Field Compression	For PPP initialization. User can keep the default option.
Asyncmap Value	One of the PPP protocol initialization strings. User can keep the default value. Range: 0-ffffffff.

MRU	Set the maximum receive unit. Range: 64-1500.
MTU	Set the maximum transmission unit. Range: 128-1500
Link Detection Interval (s)	Set the link detection interval time to ensure tunnel connection. Range: 0-600.
Max Retries	Set the maximum times of retry to detect the L2TP connection failure. Range: 0-10.
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with blank space.
	Table 2.4.6.6.1.2TD Decemptore

Table 3-4-6-6 L2TP Parameters

3.4.6.5 PPTP

Milesight

Point-to-Point Tunneling Protocol (PPTP) is a protocol that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network.

DMVPN	IPsec	GRE	L2TP	PPTP
PPTP Settings				
- PPTP_1				
Enable				
Remote IP	Address			
Username				
Password				
Authentica	tion	- <u>-</u>	Auto	Ŧ
Global Trat	ffic Forwarding			
Remote Su	ibnet			
Remote Su	ibnet Mask			

Figure 3-4-6-8

РРТР	
Item	Description
Enable	Enable PPTP client. A maximum of 3 tunnels is allowed.
Remote IP Address	Enter the public IP address or domain name of PPTP server.
Username	Enter the username that PPTP server provides.
Password	Enter the password that PPTP server provides.
Authentication	Select from "Auto", "PAP", "CHAP", "MS-CHAPv1", and "MS-CHAPv2".
Global Traffic Forwarding	All of the data traffic will be sent out via PPTP tunnel once enable this function.
Remote Subnet	Set the peer subnet of PPTP.

Remote Subnet Mask	Set the netmask of peer PPTP server.	
	Table 3-4-6-7 PPTP Parameters	
Advanced Settings		
Local IP Address		
Peer IP Address		
Enable NAT	8	
Enable MPPE	×.	
Address/Control Comp	pression	
Protocol Field Compre	ession	
Asyncmap Value	filling .	
MRU	1500	
MTU	1500	
Link Detection Interval	l(s) 60	
Max Retries	0	
Expert Options		

Figure 3-4-6-9

PPTP Advanced Settings	
ltem	Description
Local IP Address	Set IP address of PPTP client.
Peer IP Address	Enter tunnel IP address of PPTP server.
Enable NAT	Enable the NAT faction of PPTP.
Enable MPPE	Enable MPPE encryption.
Address/Control Compression	For PPP initialization. User can keep the default option.
Protocol Field Compression	For PPP initialization. User can keep the default option.
Asyncmap Value	One of the PPP protocol initialization strings. User can keep the default value. Range: 0-ffffffff.
MRU	Enter the maximum receive unit. Range: 64-1500.
MTU	Enter the maximum transmission unit. Range: 128-1500.
Link Detection Interval (s)	Set the link detection interval time to ensure tunnel connection. Range: 0-600.
Max Retries	Set the maximum times of retrying to detect the PPTP connection failure. Range: 0-10.
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with blank space.

Table 3-4-6-8 PPTP Parameters

3.4.6.6 OpenVPN Client

OpenVPN is an open source virtual private network (VPN) product that offers a simplified security framework, modular network design, and cross-platform portability. UG56 supports running at most 3 OpenVPN clients at the same time. You can import the ovpn file directly or configure the parameters on this page to set clients.

OpenVPN Client Settings	
- OpenVPN Client_1	
Enable	
Configuration Method	File Configuration 🗸
Configuration File	openvpn_1-custom.conf Browse Import Export Delete
+ OpenVPN Client_2	
+ OpenVPN Client_3	

Figure 3-4-6-10

OpenVPN Client - File Configuration		
ltem	Description	
Browse	Click to browse the client configuration ovpn format file including the settings and certificate contents. Please refer to the client configuration file according to sample: <u>client.conf</u>	
Edit	Click to edit the imported file.	
Export	Export the server configuration file.	
Delete	Click to delete the configuration file.	

Table 3-4-6-9 OpenVPN Client Parameters

Configuration Method	Page Configuration 🗸
Protocol	UDP 🗸
Remote IP Address	
Port	1194
Interface	tun 🗸
Authentication	None 🗸
Local Tunnel IP	
Remote Tunnel IP	
Enable NAT	
Compression	LZO 🗸
Link Detection Interval(s)	60
Link Detection Timeout(s)	300
Cipher	None 🗸
MTU	1500
Max Frame Size	1500
Verbose Level	ERROR ¥
Expert Options	
Local Route	
Sub	onet

Figure 3-4-6-11

OpenVPN Client - Page Configuration		
Item	Description	
Protocol	Select a transport protocol used by connecting UDP and TCP.	
Remote IP Address	Enter remote OpenVPN server's IP address or domain name.	

Milesight

Port	Enter the TCP/UCP service number of remote OpenVPN server. Range: 1-65535.
Interface	Select virtual VPN network interface type from TUN and TAP. TUN devices encapsulate IPv4 or IPv6 (OSI Layer 3) while TAP devices encapsulate Ethernet 802.3 (OSI Layer 2).
Authentication Type	Select authentication type used to secure data sessions. Pre-shared: use the same secret key as server to complete the authentication. After selecting, go to Network > VPN > Certifications page to import a static.key to PSK field. Username/Password: use username/password which is preset in server side to complete the authentication. X.509 cert: use X.509 type certificate to complete the authentication. After selecting, go to Network > VPN > Certifications page to import CA certificate, client certificate and client private key to corresponding fields. X.509 cert + user: use both username/password and X.509 cert authentication type.
Local Virtual IP	Set local tunnel address when authentication type is None or Pre-shared .
Remote Virtual IP	Set remote tunnel address when authentication type is None or Pre-shared .
Global Traffic Forwarding	All the data traffic will be sent out via OpenVPN tunnel when this function is enabled.
Enable TLS Authentication	Disable or enable TLS authentication when authentication type is X.509 cert. After being enabled, go to Network > VPN > Certifications page to import a ta.key to TA field. Note: this option only supports tls-auth. For tls-crypt, please add this format string on expert option: tls-crypt /etc/openvpn/openvpn-client1-ta.key
Compression	Select to enable or disable LZO to compress data.
Link Detection Interval (s)	Set link detection interval time to ensure tunnel connection. If this is set on both server and client, the value pushed from server will override the client local values. Range: 10-1800 s.
Link Detection Timeout (s)	OpenVPN will be reestablished after timeout. If this is set on both server and client, the value pushed from server will override the client local values. Range: 60-3600 s.
Cipher	Select from NONE, BF-CBC, DES-CBC, DES-EDE3-CBC, AES-128-CBC, AES-192-CBC and AES-256-CBC.
MTU	Enter the maximum transmission unit. Range: 128-1500.
Max Frame Size	Set the maximum frame size. Range: 128-1500.
Verbose Level	Select from ERROR, WARING, NOTICE and DEBUG.
Expert Options	User can enter some initialization strings in this field and separate the strings with semicolon. Example: ncp-ciphers AES-128-GCM; key direction 1
Local Route	
Subnet	Set the local route's IP address.

88

Subnet Mask	Set the local route's netmask.

Table 3-4-6-10 OpenVPN Client Parameters

3.4.6.7 OpenVPN Server

UG56 supports OpenVPN server to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. You can import the ovpn file directly or configure the parameters on this page to set this server.

OpenVPN Server Settings	
Enable	
Configuration Method	File Configuration
Configuration File	Browse import Export Delete

Figure 3-4-6-12

OpenVPN Server - File Configuration		
ltem	Description	
Browse	Click to browse the server configuration ovpn format file including the settings and certificate contents. Please refer to the server configuration file according to sample: <u>server.conf</u>	
Edit	Click to edit the imported file.	
Export	Export the server configuration file.	
Delete	Click to delete the configuration file.	

Table 3-4-6-11 OpenVPN Server Parameters

Enable		
Configuration Method	Page Configuration	~
Protocol	UDP	~
Port	1194	
Listening IP		
Interface	tun	~
Authentication	None	~
Local Virtual IP		
Remote Virtual IP		
Ena <mark>bl</mark> e NAT		
Compression	LZO	~
Link Detection Interval	60	
Link Detection Timeout	150	
Cipher	None	~
MTU	1500	
Max Frame Size	1500	
Verbose Level	ERROR	~
Expert Options	C.	



Account				
	Username		Password	Operation
				Œ
Local Route				
	Subnet		Netmask	Operation
				E
Client Subnet				
	Name	Subnet	Netmask	Operation
				E



OpenVPN Server - Page Configuration		
Item	Description	
Protocol	Select a transport protocol used by connection from UDP and TCP.	
Listening IP	Enter the local hostname or IP address for bind. If left blank, OpenVPN	

90

	server will bind to all interfaces.
Port	Enter the TCP/UCP service number for OpenVPN client connection. Range: 1-65535.
Interface	Select virtual VPN network interface type from TUN and TAP. TUN devices encapsulate IPv4 or IPv6 (OSI Layer 3) while TAP devices encapsulate Ethernet 802.3 (OSI Layer 2).
Authentication Type	 Select authentication type used to secure data sessions. Pre-shared: use the same secret key as server to complete the authentication. After select, go to Network > VPN > Certifications page to import a static.key to PSK field. Username/Password: use username/password which is preset in server side to complete the authentication. X.509 cert: use X.509 type certificate to complete the authentication. After select, go to Network > VPN > Certifications page to import CA certificate, client certificate and client private key to corresponding fields. X.509 cert + user: use both username/password and X.509 cert authentication type.
Local Virtual IP	Set local tunnel address when authentication type is None or Pre-shared .
Remote Virtual IP	Set remote tunnel address when authentication type is None or Pre-shared .
Client Subnet	Define an IP address pool for openVPN client.
Client Netmask	Set the client subnet netmask to limit the IP address range.
Renegotiation Interval	Renegotiate data channel key after this interval. 0 means disable.
Max Clients	Limit server to a maximum of concurrent clients, range: 1-20. Note: please adjust log severity to Info if you need to connect many clients.
Enable CRL	Enable or disable CRL verify.
Enable Client to Client	When enabled, openVPN clients can communicate with each other.
Enable Dup Client	Allow multiple clients to connect with the same common name or certification.
Enable TLS Authentication	Disable or enable TLS authentication when authentication type is X.509 cert. After being enabled, go to Network > VPN > Certifications page to import a ta.key to TA field. Note: this option only supports tls-auth. For tls-crypt, please add this format string on expert option: tls-crypt /etc/openvpn/openvpn-client1-ta.key
Compression	Select to enable or disable LZO to compress data.
Link Detection Interval (s)	Set link detection interval time to ensure tunnel connection. If this is set on both server and client, the value pushed from server will override the client local values. Range: 10-1800 s.
Link Detection Timeout (s)	OpenVPN will be reestablished after timeout. If this is set on both server and client, the value pushed from server will override the client local
	values. Range: 60-3600 s.

	AES-192-CBC and AES-256-CBC.	
MTU	Enter the maximum transmission unit. Range: 64-1500.	
Max Frame Size	Set the maximum frame size. Range: 64-1500.	
Verbose Level	Select from ERROR, WARING, NOTICE and DEBUG.	
	User can enter some initialization strings in this field and separate the	
Expert Options	strings with semicolon.	
	Example: ncp-ciphers AES-128-GCM; key direction 1	
Account		
Username & Password	Set username and password for OpenVPN client when authentication type	
Usemanie & Passworu	is username/password.	
Local Route		
Subnet	Set the local route's IP address.	
Subnet Mask	Set the local route's netmask.	
Client Subnet		
Name	Set the name as OpenVPN client certificate common name.	
Subnet	Set the subnet of OpenVPN client.	
Subnet Mask	Set the subnet netmask of OpenVPN client.	
	·	

Table 3-3-6-12 OpenVPN Server Parameters

3.4.6.8 Certifications

When working as OpenVPN server, OpenVPN client or IPsec Server, user can import/export necessary certificate and key files to this page according to the authentication types.

Op	enVPN Client						
-	OpenVPN client_1						
	СА	Browse	Import	Export	Delete		
	Public Key	Browse	Import	Export	Delete		
	Private Key	Browse	Import	Export	Delete		
	ТА	Browse	Import	Export	Delete		
	Preshared Key	Browse	Import	Export	Delete		
	PKCS12	Browse	Import	Export	Delete		
-	OpenVPN client_2						
-	OpenVPN client_3						

Figure 3-4-6-15

Ope	nVPN Server				
_	OpenVPN Server				
	СА	Browse	Import	Export	Delete
	Public Key	Browse	Import	Export	Delete
	Private Key	Browse	Import	Export	Delete
	DH	Browse	Import	Export	Delete
	TA	Browse	Import	Export	Delete
	CRL	Browse	Import	Export	Delete
	Preshared Key	Browse	Import	Export	Delete

_	24616
Figure	3-4-6-16

IPsec				
- IPsec_1				
CA	Brows	e Import	Export	Delete
Client Key	Brows	e Import	Export	Delete
Server Key	Brows	e Import	Export	Delete
Private Key	Brows	e Import	Export	Delete
CRL	Brows	e Import	Export	Delete

Figure 3-4-6-17

3.4.6.9 WireGuard

WireGuard is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cry ptography. WireGuard passes traffic over UDP protocol.

Enable				
Interface	wg0			
Customized Private Key				
Private Key	ø]		
Public Key	F8xRHUqMQ0fgJTw4V4M7gvm]		
IP Address]		
Listening Port]		
DNS				
MTU]		
Peer	Public Key	Allowed IP	Endpoint Address	Operation

WireGuard					
Item	Description				
Enable	Enable WireGuard interface. A maximum of 3 WireGaurd interfaces is allowed.				
Interface	Show the WireGuard interface name.				
Customized Private Key	Enable or disable to customize the private key of this WireGuard interface. If disabled, the client will use the private key generated by this router.				
Public Key	Show the public key generated by the private key.				
IP Address	Set the local virtual IP address and netmask. Example: 10.8.0.2/24				
Listening Port	Set the port to send or receive WireGuard packets. The port numbers of different WireGuard interfaces should be different.				
DNS	Set the DNS server address of this WireGuard interface. If left blank, the router will use DNS server address of common network interfaces (WAN, cellular, etc.).				
MTU	Set the maximum transmission unit of this WireGuard interface. If left blank, the router will use MTU of common network interfaces (WAN, cellular, etc.).				
Peer Table	Click "+" to add WireGuard peers of this WireGuard interface. One WireGuard interface can add 20 peers at most.				

Figure 3-4-6-18

Table 3-4-6-13 WireGuard Parameters

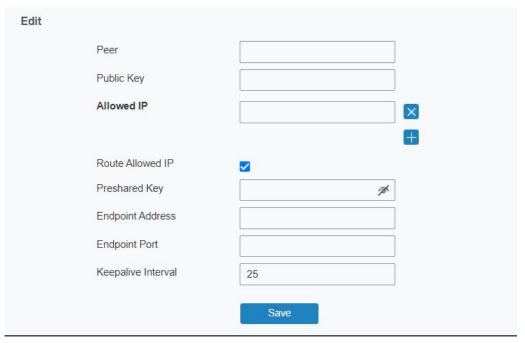


Figure 3-4-6-19

WireGuard-Peer			
Item	Description		
Peer	Set a WireGuard peer name. This name should be unique in this		

	WireGuard client.	
Public Key	Set the public key of WireGuard peer server/client.	
Allowed IP	Set the real IP address and netmask of WireGuard peer's LAN network. Example: 192.168.1.0/24	
	One WireGuard peer supports to add 8 allowed IP addresses.	
Route Allowed IP Enable or disable to add static routings of allowed IP addresses.		
Dracharad Kay	Set the presahred key and both this interface and peer interface	
Preshared Key	should set the same key value.	
Endpoint Address	Set IP address or domain name of WireGuard peer server/client.	
Endpoint Port	Set the destination port of WireGuard peer server/client.	
Kaanaliya Intanyal	After the connection is established, this WireGuard interface will	
Keepalive Interval	send heartbeat packet regularly to keep alive. 0 means disabled.	
	Table 3-4-6-13 WireGuard-Peer Parameters	

Table 3-4-6-13 WireGuard-Peer Parameters

3.5 System

This section describes how to configure general settings, such as administration account, access service, system time, common user management, SNMP, event alarms, etc.

3.5.1 General Settings

3.5.1.1 General

General settings include system info, access service and HTTPS certificates.

General	System Time	SMTP	Phone	Email	
System					
Hostname		GATEWAY			
Web Login Tim	eout(s)	1800			
Access Servi	ce				
	Enable	Serv	rice	Port	
		HT	ΓP	80	
		HTT	PS	443	
		TELM	NET	23	
		SS	н	22	
HTTPS Certifi	icates				
Certificate	https.crt	Browse	Import Export	Delete	
Key	https.key	Browse	Import Export	Delete	

Figure 3-5-1-1

General					
ltem	Description	Default			
System					
Hostname	User-defined gateway name, needs to start with a letter.	GATEWAY			
Web Login Timeout (s)	You need to log in again it it times out Range: 100-3600				
Access Servic	e				
Port	Set port number of the services. Range: 1-65535.				
HTTP	Users can log in the device locally via HTTP to access and control it through Web after the option is checked.	80			
HTTPS	Users can log in the device locally and remotely via HTTPS to access and control it through Web after option is checked.	443			
TELNET	Users can log in the device locally and remotely via TELNET to access and control it through Web after option is checked.	23			
SSH	Users can log in the device locally and remotely via SSH after the option is checked.	22			
HTTPS Certifi	cates				
Certificate	Click "Browse" button, choose certificate file on the PC, and then click "Import" button to upload the file into gateway. Click "Export" button will export the file to the PC. Click "Delete" button will delete the file.				
Кеу	Click "Browse" button, choose key file on the PC, and then click "Import" button to upload the file into gateway. Click "Export" button will export file to the PC. Click "Delete" button will delete the file.				

Table 3-5-1-1 General Setting Parameters

3.5.1.2 System Time

This section explains how to set the system time including time zone and time synchronization type.

Note: to ensure that the gateway runs with the correct time, it's recommended that you set the system time when configuring the gateway.

Milesight

General	System Time	SMTP	Phone	Email
System Time S	ettings			
Current Time		2019-06-12 20:34:32	2 Wed	
Time Zone		8 China (Beijing)	•	
Sync Type		Sync with Browser	•	
Browser Time		2019-06-12 20:34:32	2 Wed	

Figure 3-5-1-2

System Time				
ltem	Description			
Current Time	Show the current system time.			
Time Zone	Click the drop down list to select the time zone you are in.			
	Click the drop down list to select the time synchronization			
	type.			
Sync Type	Sync with Browser: Synchronize time with browser.			
	Sync with NTP Server: Synchronize time with NTP Server.			
	Set up Manually: configure the time manually.			
Sync with NTP Server				
NTP Server Address	Set NTP server address (domain name/IP).			
Enable NTP Server	NTP client on the network can achieve time synchronization			
	with gateway after "Enable NTP Server" option is checked.			

Table 3-5-1-2 System Time Parameters

3.5.1.3 SMTP

SMTP, short for Simple Mail Transfer Protocol, is a TCP/IP protocol used in sending and receiving e-mail. This section describes how to configure email settings.

25	
0	
	25

Figure 3-5-1-3

SMTP				
Description				
SMTP Client Settings				
Enable or disable SMTP client function.				
Enter the sender's email account.				
Enter the sender's email username.				
Enter the sender's email password.				
Enter SMTP server's domain name.				
Enter SMTP server port. Range: 1-65535.				
Enable or disable TLS encryption.				

Table 3-5-1-3 SMTP Setting

Related Topics

Events Setting

3.5.1.4 Phone

Phone settings involve in call/SMS trigger and SMS alarm for events. This is only applied to gateway with cellular feature.

General	System Time	SMTP	Phone	Email		
Phone Number	List					
	Name				Number	Operation
	List1				654321;123456	
						+
Save	l					

Figure 3-5-1-4

Phone	
Item	Description
Phone Number List	
Name	Set phone group name.
Number	Enter the telephone number. Digits, "+" and "-" are allowed. You can divide multiple numbers by ";".

Table 3-5-1-4 Phone Settings

Related Topic

Connect on Demand

3.5.1.5 Email

Email settings involve email alarm for events.

General	System Time	SMTP	Phone	Email		
Email List						
	Nam	е			Email Address	Operation
	list1				sam@user.com;hot@gmail.com	×
						H
Save	I					



Email	
Item	Description
Email List	
Name	Set Email group name.
Email Address	Enter the Email address. You can divide multiple Email addresses by ";".

Table 3-5-1-5 Email Settings

3.5.2 User Management

3.5.2.1 Account

Here you can change the login username and password of the administrator. Note: it is strongly recommended that you modify them for the sake of security.

Change Account I		// <u></u>	
Jsername		admin	
Old Password			
New Password			
Confirm New Passw	ord		



Account			
Item	Description		
Username	Enter a new username. You can use characters such as a-z, 0-9, "_", "-". The first character can't be a digit.		
Old Password	Enter the old password.		
New Password	Enter a new password. You can use any ASCII characters		

e	except blank.
Confirm New Password	Enter the new password again.

Table 3-5-2-1 Account Information

3.5.2.2 User Management

This section describes how to create common user accounts. The common user permission includes Read-Only and Read-Write.

Account U	ser Management			
User List				
Userna	ame	Password	Permission	Operation
steve			Read-Write	•
test	••	••••	Read-Only	•
				•

Figure 3-5-2-2

User Management				
ltem	Description			
Username	Enter a new username. You can use characters such as a-z, 0-9, "_", "-". The first character can't be a digit.			
Password	Set password. You can use any ASCII characters except blank.			
Permission	 Select user permission from "Read-Only" and "Read-Write". Read-Only: users can only view the configuration of gateway in this level. Read-Write: users can view and set the configuration of gateway in this level. 			

Table 3-5-2-2 User Management

3.5.3 SNMP

SNMP is widely used in network management for network monitoring. SNMP exposes management data with variables form in managed system. The system is organized in a management information base (MIB) which describes the system status and configuration. These variables can be remotely queried by managing applications.

Configuring SNMP in networking, NMS, and a management program of SNMP should be set up at the Manager.

Configuration steps are listed as below for achieving query from NMS:

- 1. Enable SNMP setting.
- 2. Download MIB file and load it into NMS.
- 3. Configure MIB View.
- 4. Configure VCAM.

3.5.3.1 SNMP

UG56 supports SNMPv1, SNMPv2c and SNMPv3 version. SNMPv1 and SNMPv2c employ community name authentication. SNMPv3 employs authentication encryption by username and password.

Status	Î	SNMP	MIB View	VACM	Trap	MIB
Packet Forwarder		SNMP Settin	gs			
		Enable				
Network Server		Port		<mark>1</mark> 61		
Network 🕨		System Name	l.	24E124FF	FEF24660	
	•	SNMP Version	12 70	SNMPv2		~
0	-	Location Infor	mation			
System		Contact Inform	nation	[
General Settings			-	<u>.</u>		
User Management		Save				
SNMP						

Figure 3-5-3-1

SNMP Settings		
ltem	Description	
Enable	Enable or disable SNMP function.	
Dout	Set SNMP listened port. Range: 1-65535.	
Port	The default port is 161.	
System Name	Fill in the system name to represent the gateway.	
SNMP Version	Select SNMP version; support SNMP v1/v2c/v3.	
Location Information	Fill in the location information.	
Contact Information	Fill in the contact information.	

Table 3-5-3-1 SNMP Parameters

3.5.3.2 MIB View

This section explains how to configure MIB view for the objects.

SNMP	MIB View	VACM	Trap	MIB	
View List					
V	iew Name		Filter	View OID	Operation
All		Included	•	1	×
system		Included	•	1.3.6.1.2.1.1	
					8

Figure 3-5-3-2

MIB View	
Item	Description
View Name	Set MIB view's name.
View Filter	Select from "Included" and "Excluded".
View OID	Enter the OID number.
Included	You can query all nodes within the specified MIB node.
Excluded	You can query all nodes except for the specified MIB node.
	Table 2 F 2 2 MID View Decomptore

Table 3-5-3-2 MIB View Parameters

3.5.3.3 VACM

This section describes how to configure VCAM parameters.

SNMP	MIB View	VACM	Trap	MIB		
NMP v1 & v2	User List					
Commu	nity	Permission	MIB Vie	W	Network	Operation
private	Rea	d-write 🔻	All	•	0.0.0/0	×
public	Rea	d-only 🔻	none	•	0.0.0/0	×



VACM		
Item	Description	
SNMP v1 & v2 Us	er List	
Community	Set the community name.	
Permission	Select from "Read-Only" and "Read-Write".	
MIB View	Select an MIB view to set permissions from the MIB view list.	
Network	The IP address and bits of the external network accessing the MIB view.	
Read-Write	The permission of the specified MIB node is read and write.	

Read-Only	The permission of the specified MIB node is read only.
SNMP v3 User Lis	st
Group Name	Set the name of SNMPv3 group.
Security Level	Select from "NoAuth/NoPriv", "Auth/NoPriv", and " Auth/Priv".
Deed Only Mary	Select an MIB view to set permission as "Read-only" from the MIB view
Read-Only View	list.
Read-Write View	Select an MIB view to set permission as "Read-write" from the MIB view
Redu-wille view	list.
Inform View	Select an MIB view to set permission as "Inform" from the MIB view list.
	Table 3-5-3-3 VACM Parameters

3.5.3.4 Trap

This section explains how to enable network monitoring by SNMP trap.

SNMP	MIB View	VACM	Тгар	MIB
SNMP Trap				
Enable				
SNMP Version		SNMPv2		Ŧ
Server Address				
Port				
Name				

Figure 3-5-3-4

SNMP Trap	
ltem	Description
Enable	Enable or disable SNMP Trap function.
SNMP Version	Select SNMP version; support SNMP v1/v2c/v3.
Server Address	Fill in NMS's IP address or domain name.
Port	Fill in UDP port. Port range is 1-65535. The default port is 162.
Name	Fill in the group name when using SNMP v1/v2c; fill in the username when using SNMP v3.
Auth/Priv Mode	Select from "NoAuth & No Priv", "Auth & NoPriv", and "Auth & Priv".

Table 3-5-3-4 Trap Parameters

3.5.3.5 MIB

This section describes how to download MIB files.

SNMP	MIB View	VACM	Тгар	MIB
MIB Downloa				
MIB File		AGENTX	MIB txt 🔻	Download

Figure 3-5-3-5

MIB		
Item	Description	
MIB File	Select the MIB file you need.	
Download Click "Download" button to download the MIB file to PC.		
	Table 3-5-3-5 MIB Download	

3.5.4 Device Management

3.5.4.1 Auto Provision

Users can customize and assign the configuration profile from Milesight Development Platform. When Auto Provision is enabled and the device is connected to Internet, the device will receive the profile to achieve initial configuration. This feature will work even the device does not configure to connect Milesight Development Platform.

Auto Provision	Management Platform
Auto Provision	
Enable	
Status	Connection Failed
Save & Apply	

Figure 3-5-4-1

3.5.4.2 Management Platform

You can connect the device to the DeviceHub or Milesight Development Platform on this page so as to manage the gateway centrally and remotely.

Milesight

Auto Provision	Management Platform
Management Platform	
Enable	
Platform Type	DeviceHub 1.0 🗸
Activation Server Address	
Device Management Server A	Address
Activation Method	By ID 🗸
ID	
Password	
Status	Disconnected

Figure 3-5-4-2

Management Platform	n	
ltem	Description	
Enable	Enable or disable to connect gateway to management platform.	
Platform Type	DeviceHub 1.0, DeviceHub 2.0 or Milesight Development Platform is optional.	
Status	Show the connection status between the gateway and the management platform.	
DeviceHub 1.0		
Activation Server Address	IP address or domain of the DeviceHub.	
DeviceHub Management Address	The URL address for the device to connect to the DeviceHub, e.g. http://220.82.63.79:8080/acs.	
Activation Method	Select activation method to connect the gateway to the DeviceHub server, options are "By Authentication ID" and "By ID".	
Authentication Code	Fill in the authentication code generated from the DeviceHub.	
ID	Fill in the registered DeviceHub account (amail) and paceword	
Password	Fill in the registered DeviceHub account (email) and password.	
DeviceHub 2.0		
Server Address	IP address or domain of the DeviceHub.	

Table 3-5-4-1

3.5.5 Events

Event feature is capable of sending alerts by Email when certain system events occur.

3.5.5.1 Events

You can view alarm messages on this page.

ıs
oRaWAN
letwork
ystem 🔻
ieneral Settings
User Management
AAA
Device Management
Events

Figure 3-5-5-1

Events			
ltem	Description		
Mark as Read	Mark the selected event alarm as read.		
Delete	Delete the selected event alarm.		
Mark All as Read	Mark all event alarms as read.		
Delete All Alarms	Delete all event alarms.		
Status	Show the reading status of the event alarms, such as "Read" and "Unread".		
Туре	Show the event type that should be alarmed.		
Time	Show the alarm time.		
Message	Show the alarm content.		

Table 3-5-5-1 Events Parameters

3.5.5.2 Events Settings

In this section, you can decide what events to record and whether you want to receive email and SMS notifications when any change occurs. Cellular Up

Cellular Down

WAN Up

WAN Down

VPN Up

VPN Down

Power On

Events	Events Se	ettings			
Events Settir	ngs				
Enable					
Phone for Noti	ification		~		
Email for Notif	ication		~		
	Events		Record	Email Email Setting	SMS SMS Setting

~

Figure 3-5-5-2

Event Settings			
ltem	Description		
Enable	Check to enable "Events Settings".		
Phone for Notification	Select phone group to receive SMS alarm.		
Email for Notification	Select Email group to receive Email alarm.		
Events	Event type the gateway supports to record.		
Record	The relevant content of event alarm will be recorded on "Event" page if this option is checked.		
Email	The relevant content of event alarm will be sent out via email if this option is checked.		
Email Setting	Click and you will be redirected to the page "Email" to configure the Email group.		
SMS	The relevant content of event alarm will be sent out via SMS if this option is checked.		
SMS Setting	Click and you will be redirected to the page of "Phone" to configure phone group list.		
Phone Group List	Select phone group to receive SMS alarm.		
Email Group List	Select Email group to receive Email alarm.		

Table 3-5-5-2 Events Parameters

Related Topics

Email Setting

Phone Setting

3.6 Maintenance

This section describes system maintenance tools and management.

3.6.1 Tools

Troubleshooting tools includes ping and traceroute.

3.6.1.1 Ping

Ping tool is engineered to ping outer network.

IP Ping		
Host		Ping Stop
		Figure 3-6-1-1
	PING	
	ltem	Description
	Host	Ping outer network from the gateway.
		Table 3-6-1-1 IP Ping Parameters

3.6.1.2 Traceroute

Traceroute tool is used for troubleshooting network routing failures.

Traceroute			
Host		Trace	Stop
	Figure 3-6-1-2		

Traceroute		
ltem	Description	
Host	Address of the destination host to be detected.	

Table 3-6-1-2 Traceroute Parameters

3.6.1.3 Packet Analyzer

Packet Analyzer is used for capturing the packet of different interfaces.

Ethernet Interface	Any	•
IP Address		
Port		
Advanced		



Packet Analyzer		
ltem	Description	
Ethernet Interface	Select the interface to capture packages.	
IP Address	Set the IP address that the router will capture.	
Port	Set the port that the router will capture.	
Advanced	Set the rules for sniffer. The format is tcpdump.	

Table 3-6-1-3 Packet Analyzer Parameters

3.6.1.4 Qxdmlog

This section allow collecting diagnostic logs via QXDM tool.



3.6.2 Schedule

This section explains how to configure scheduled reboot on the gateway.

chedule				
Schedule	Frequency	Hour	Minute	Operation
~	Every Month V 1 V	0 ~	0 ~	×
				H

Figure 3-6-2-1

Schedule	
ltem	Description
Schedule	Select schedule event: Reboot: Reboot the gateway regularly.

Frequency	Select the frequency to execute the schedule.
	Table 3-6-2-1 Schedule Parameters

3.6.3 Log

The system log contains a record of informational, error and warning events that indicates how the system processes. By reviewing the data contained in the log, an administrator or user troubleshooting the system can identify the cause of a problem or whether the system processes are loading successfully. Remote log server is feasible, and gateway will upload all system logs to remote log server such as Syslog Watcher.

3.6.3.1 System Log

This section describes how to download log file and view the recent log on web.

Download			
File	Log File	▼ Download	
Log			
View recent(lines)	20	¥	
Thu Jul 18 15:01:25 2019 use	r.notice redis[1859]: Background s	wing terminated with success	
Thu Jul 18 15:06:26 2019 use	r.notice redis[1859]: 10 changes in	300 seconds. Saving	
Thu Jul 18 15:06:26 2019 use	r.notice redis[1859]: Background s	iving started by pid 11683	
Thu Jul 18 15:06:26 2019 use	r.notice redis[11683]: DB saved on	disk	
	r.notice redis[1859]: Background s	iving terminated with success	
Thu Jul 18 15:06:26 2019 use			
	r.notice redis[1859]: 10 changes in	300 seconds. Saving	
Thu Jul 18 15:11:27 2019 use	r.notice redis[1859]: 10 changes in r.notice redis[1859]: Background sa		
Thu Jul 18 15:11:27 2019 use Thu Jul 18 15:11:27 2019 use		ving started by pid 15776	
Thu Jul 18 15:11:27 2019 use Thu Jul 18 15:11:27 2019 use Thu Jul 18 15:11:27 2019 use	r.notice redis[1859]: Background sa	ving started by pid 15776 disk	
Thu Jul 18 15:11:27 2019 use Thu Jul 18 15:11:27 2019 use	r.notice redis[1859]: Background sa r.notice redis[15776]: DB saved on	ving started by pid 15776 disk ving terminated with success	
Thu Jul 18 15:11:27 2019 use Thu Jul 18 15:16:28 2019 use	r.notice redis[1859]: Background s r.notice redis[15776]: DB saved on r.notice redis[1859]: Background s	ving started by pid 15776 disk ving terminated with success 300 seconds. Saving	
Thu Jul 18 15:11:27 2019 use Thu Jul 18 15:16:28 2019 use Thu Jul 18 15:16:28 2019 use	r.notice redis[1859]: Background si r.notice redis[15776]: DB saved on r.notice redis[1859]: Background si r.notice redis[1859]: 10 changes in	ving started by pid 15776 disk ving terminated with success 300 seconds. Saving ving started by pid 19899	

Figure 3-6-3-1

System Log	
Item	Description
Download	Download log file.
View recent (lines)	View the specified lines of system log.
Clear Log	Clear the current system log.

Table 3-6-3-1 System Log Parameters

3.6.3.2 Log Settings

This section explains how to enable remote log server and local log setting.

System Log	Log Settings			
Remote Log Server				
Enable				
Syslog Server Address			añ eu]
Port		514]
Local Log File				
Storage		local	•]
Size		1024		КВ
Log Severity		Info	•]

Figure 3-6-3-2

Log Settings	
ltem	Description
Remote Log Server	
Enable	With "Remote Log Server" enabled, gateway will send all system logs to the remote server.
Syslog Server Address	Fill in the remote system log server address (IP/domain name).
Port	Fill in the remote system log server port.
Local Log File	
Storage	User can store the log file in memory or TF card.
Size	Set the size of the log file to be stored.
Log Severity	The list of severities follows the syslog protocol.

Table 3-6-3-2 System Log Parameters

3.6.4 Upgrade

This section describes how to upgrade the gateway firmware via web. Generally you don't need to do the firmware upgrade.

Note: any operation on web page is not allowed during firmware upgrade, otherwise the upgrade will be interrupted, or even the device will break down.

Gateway			
Firmware Version	56.0.0.5		
Reset Configuration to Factory Default			
Upgrade Firmware		Browse	Upgrade

Figure 3-6-4-1

Upgrade	
Item	Description
Firmware Version	Show the current firmware version.
Reset Configuration to	When this option is checked, the gateway will be reset to
Factory Default	factory defaults after upgrade.
Upgrade Firmware	Click "Browse" button to select the new firmware file, and click "Upgrade" to upgrade firmware.

Table 3-6-4-1 Upgrade Parameters

Related Configuration Example

Firmware Upgrade

3.6.5 Backup and Restore

This section explains how to create a backup of the whole system configurations to a file, replicate parts of important configuration only for batch backup, restore the config file to the gateway and reset to factory defaults.

Backup and Restore	<u>19</u> 19		
Restore Config			
Config File		Browse	Import
Backup Running-cor	nfig		
Full Backup	Batch Backup		
Restore Factory Defa	aults		
Reset			

Figure 3-6-5-1

Backup and Restore			
ltem	n Description		
Config File	Click "Browse" button to select configuration file, and then click "Import"		
	button to upload the configuration file to the gateway.		
Full Backup Click "Full Backup" to export the current configuration file to the PC.			

	Click "Batch Backup" to export current configuration except gateway ID
Batch	of packet forwarder, all embedded NS settings, static IP address of
Backup	WAN, WLAN settings, user management settings, DeviceHub
	authentication code, all APP settings.
Reset	Click "Reset" button to reset factory default settings. gateway will
Resel	restart after reset process is done.

Table 3-6-5-1 Backup and Restore Parameters

Related Configuration Example

Restore Factory Defaults

3.6.6 Reboot

On this page you can reboot the gateway and return to the login page. We strongly recommend clicking "Save" button before rebooting the gateway so as to avoid losing the new configuration.

Network Server	*
Network	•
System	•
Maintenance	•
Tools	
Schedule	
Log	
Upgrade	
Backup and Res	store
Rebool	

Figure 3-6-6-1

3.7 APP

3.7.1 Python

Python is an object-oriented programming language that has gained popularity because of its clear syntax and readability.

As an interpreted language, Python has a design philosophy that emphasizes code readability, notably using whitespace indentation to delimit code blocks rather than curly

brackets or keywords, and a syntax that allows programmers to express concepts in fewer lines of code than it's used in other languages such as C++ or Java. The language provides constructs and intends to enable writing clear programs on both small and large scale.

Users can use Python to quickly generate the prototype of the program, which can be the final interface of the program, rewrite it with a more appropriate language, and then encapsulate the extended class library that Python can call.

This section describes how to view the relevant running status such as App-manager, SDK version, extended storage, etc. Also you can change the App-manager configuration, and import the Python App package from here.

3.7.1.1 Python

Python	AppManager Configuration		Python APP		
Python					
AppManager S	tatus	Uninstalled			
SDK Version					
SDK Path					
Available Stora	ige	local	~		
SDK Upload			Bro	owse Insta	11
	ige	local		owse Inst	a

Figure 3-7-1-1

Python		
Item	Description	
AppManager Status	Show AppManager's running status, like "Uninstalled", "Running" or "Stopped".	
SDK Version	Show the version of the installed SDK.	
SDK Path	Show the SDK installation path.	
Available Storage	Select available storage to install SDK.	
SDK Upload	Upload and install SDK for Python.	
Uninstall	Uninstall SDK.	
View	View application status managed by AppManager.	

Table 3-7-1-1 Python Parameters

3.7.1.2 App Manager Configuration

Milesight

Python	AppManager Configura	ation Python APP		
AppManager				
Enable				
App Manageme	ent			
11	D Aj	op Command	Logfile Size(MB)	Uninstall
App Status				
	App Name	App Version		SDK Version



AppManager Configuration		
ltem	Description	
Enable	After enabling Python AppManager, user can click "View" button on the "Python" webpage to view the application status managed by AppManager.	
App Management		
ID	Show the ID of the imported App.	
App Command	Show the name of the imported App.	
Logfile Size(MB)	User-defined Logfile size. Range: 1-50.	
Uninstall	Uninstall APP.	
App Status		
App Name	Show the name of the imported App.	
App Version	Show the version of the imported App.	
SDK Version	Show the SDK version which the imported App is based on.	

Table 3-7-1-2 APP Manager Parameters

3.7.1.3 Python App

Python	AppManager Configuration	Python APP	
Import App P	ackage		
App Package		Browse Import	
Import App C	configuration		
App Name		*	
App Configura	tion	Browse Import	
Debug Script			
Debug File		Export	
Debug Script		Browse Import	

Figure 3-7-1-3

Python APP		
Description		
Select App package and import.		
Select App to import configuration.		
Select configuration file and import.		
Export script file.		
Select Python script to be debugged and import.		

Table 3-7-1-3 APP Parameters

3.7.2 Node-RED

Node-RED is a flow-based development tool for visual programming and wiring together hardware devices, APIs and online services as part of the Internet of Things. Node-RED provides a web-browser-based flow editor, which can easily wire together flows using the wide range of nodes in the palette. For more guidance and documentation please refer to Node-RED official website.

3.7.2.1 Node-RED

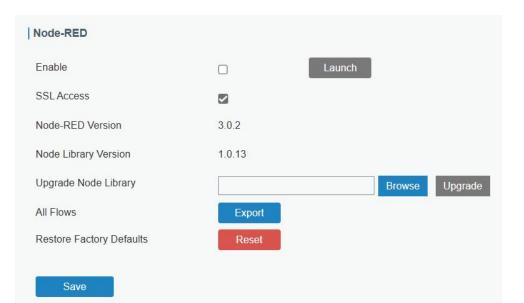


Figure 3-7-2-1

Node-RED	Node-RED			
Item	Description			
Enable	Enable the Node-RED.			
Launch	Click to launch the web GUI of Node-RED.			
SSL Access	Enable to access the Node-RED web GUI via HTTPS service only.			
Node-RED Version	Show the version of the Node-RED. Node-RED version can be upgraded only when you upgrade the gateway.			
Node Library Version	Show the version of the node library.			
Upgrade Node Library	Upgrade the node library by importing the library package.			
All Flows Export	Export all flows as a JSON format file.			
Restore Factory Default	Erase all flows data of Node-RED.			

Table 3-7-2-1 Node-RED Parameters

Milesight provides a customized node library to use the interfaces of the gateway.

Milesight



Figure 3-7-2-2

Node Library	Node Library		
Node	Description		
LoRa Input	Receive LoRaWAN [®] packets from the gateway. This only works when the network server is enabled.		
LoRa Output	Send downlink commands to LoRaWAN® nodes.		
Device Filter	Filter out the data of one or more specific LoRaWAN [®] nodes via device EUIs.		
GW Info	Monitor events of gateway, this needs to ensure the event detection is enabled in General > Events > Events Settings .		
Email Output	Send an Email. If you select STMP option as "Same as the gateway", it is necessary to go to System > General Settings > SMTP page to configure SMTP client settings.		
SMS Input	Receive SMS message. This only works when the cellular is connected.		
SMS Output	Send an SMS message. This only works when the cellular is connected.		

Table 3-7-2-2 Node Library Parameters

Related Configuration Example

Node-RED

Chapter 4 Application Examples

4.1 Restore Factory Defaults

Method 1:

Log in web interface, and go to **Maintenance > Backup and Restore**, click **Reset** button, you will be asked to confirm if you'd like to reset it to factory defaults. Then click **Reset** button.

Network Server		Backup and Restore	
Protocol Integration	•	Config File	Browse Import
Network	•	Backup Running-config	×
System	•	Full Backup Batch Backup	Reset operation will erase all configuration data on Gateway
Maintenance	-	Restore Factory Defaults	and reset the system to factory defaults. Continue?
Tools			
Schedule			
Log			
Upgrade			
Backup and Restore			

Then the gateway will reboot and restore to factory settings immediately.

Restore Config	
Config File	Browse
Backup Running-config	
Backup	Reset, please do not power off
Restore Factory Defaults	
Reset	

Please wait till SYS light statically and the login page pops up again, which means the gateway has already been reset to factory defaults successfully.

Related Topic

Restore Factory Defaults

Method 2:

Locate the reset button on the gateway, press and hold the reset button for more than 5s until the SYS LED blinks.

4.2 Firmware Upgrade

It is suggested that you contact Milesight technical support first before you upgrade gateway firmware. Gateway firmware file suffix is ".bin".

After getting firmware file, please refer to the following steps to complete the upgrade.

- 1. Go to "Maintenance > Upgrade".
- 2. Click "Browse" and select the correct firmware file from the PC.
- 3. Click "Upgrade" and the gateway will check if the firmware file is correct. If it's correct, the firmware will be imported to the gateway, and then the gateway will start to upgrade.
- 4. After upgrade, open the gateway web GUI via browser to check if upgrade success. **Before opening, it is suggested to clean the caches of browser.**

Gateway			
Firmware Version	56.0.0.5		
Reset Configuration to Factory Default			
Upgrade Firmware		Browse	Upgrade
Please k	eep the power on during upgrade.		

Related Topic

Upgrade

4.3 Network Connection

The gateway supports multiple methods to set up network connections.

4.3.1 Ethernet Connection

1. Go to "Network > Interface > Port" page to select the connection type and configure Ethernet port configuration, click "Save & Apply" for configuration to take effect.

Port	WLAN	Cellular	Loopback	VLAN Trunk
- Port_	1			
Port			eth 0	~
Conn	ection Type		Static IP	~
IP Ad	dress		192.1 <mark>68.44.186</mark>	
Netm	ask		255.255.255.0	
Gate	way		192.168.44.1	
MTU			1500	
Prima	ary DNS Server		8.8.8	
Seco	ndary DNS Server		223.5.5.5	
Enab	le NAT			

Note: If there is IP conflict when changing the IP address of Ethernet port, please change the subnet of WLAN first.

Port	WLAN	Loopback	VLAN Trunk
WLAN			
Enable			
Work Mode		AP	~
1.00			
IP Setting			
Protocol		Static IP	~
IP Address		192.168.10.	
		DHCP Setting	
Netmask		255.255.255	.0

- 2. Connect Ethernet port of gateway to devices like router or modem.
- 3. Go to "Maintenance > Tools > Ping" to check network connectivity.

Network Server	Ping Traceroute Qxdmlog
Protocol Integration	IP Ping Host www.google.com Ping St
Network	PING www.google.com (172 217.25.4): 56 data bytes 64 bytes from 172.217.25.4: seg=0 ttl=117 time=20.090 ms
System	♦ 64 bytes from 172.217.25.4: seq=1 ttl=117 time=19.786 ms 64 bytes from 172.217.25.4: seq=2 ttl=117 time=19.797 ms 64 bytes from 172.217.25.4: seq=3 ttl=117 time=19.750 ms
Maintenance	 www.google.com ping statistics 4 packets transmitted, 4 packets received, 0% packet loss
Tools	round-trip min/avg/max = 19.750/19.855/20.090 ms

Related Topic

Port Setting

4.3.2 Cellular Connection (Cellular Version Only)

1. Go to "Network > Interface > Cellular > Cellular Setting" and configure the necessary cellular info of SIM card, click "Save" and "Apply" for configuration to take effect.

Cellular Setting		
Enable		
Network Type	Auto	~
APN		
Username		
Password		
Access Number		
PIN Code		
Authentication Type	None	~
Roaming		
Customize MTU		
MTU	1500	
Enable IMS		
SMS Center		

2. Click "Status > Cellular" to view the status of the cellular connection. If it shows 'Connected', SIM has dialed up successfully.

Overview	Packet Forward	Cellular	Network	WLAN
Modem				
Status		Ready		
Model		EC25		
Version		EC25ECGAR06A07M	11G	
Signal Level		23asu (-67dBm)		
Register Status		Registered (Home net	twork)	
IMEI		860425047368939		
IMSI		460019425301842		
ICCID		898601178380099341	120	
ISP		CHN-UNICOM		
Network Type		LTE		
PLMN ID				
LAC		5922		
Cell ID		340db83		
Network				
Status		Connected		
IP Address		10.132.132.59		
Netmask		255.255.255.240		
Gateway		10.132.132.60		

Related Topic

Cellular Setting Cellular Status

4.4 Wi-Fi Application Example

4.4.1 AP Mode

Application Example

Configure UG56 as AP to allow connection from users or devices.

Configuration Steps

1. Go to "Network > Interface > WLAN" to configure wireless parameters as below.

Milesight

Port	WLAN	Cellular	Loopback	
WLAN				
Enable				
Work Mode	э	AP		~
SSID Broa	dcast			
AP Isolatio	n			
Radio Type	9	802.11n	(2.4GHz)	~
Channel		Auto		~
SSID		Gateway	_F1200F	
BSSID		24:e1:24	:f1:20:0f	
Encryption	Mode	No Encr	ryption	~
Bandwidth		20MHz		~
Max Client	Number	10		

Click "Save" and "Apply" buttons after all configurations are done.

2. Use a smart phone to connect the access point of gateway. Go to "Status > WLAN", and you can check the AP settings and information of the connected client/user.

Overview	Packet Forward	Cellular	Network	WLAN	VPN
WLAN Status					
Wireless Status		Enabled			
MAC Address		24:e1:24:f1:20:0f			
Interface Type		AP			
SSID		Gateway_F1200F			
Channel		Auto			
Encryption Type		No Encryption			
Status		Up			
IP Address		192.168.1.1			
Netmask		255.255.255.0			
Connection Duration	n	0 days, 02:40:52			

4.4.2 Client Mode

Application Example

Configure UG56 as Wi-Fi client to connect to an access point to have Internet access.

Configuration Steps

1. Go to **Network > Interface > Port** page to select connection type as **Static IP** and configure an IP address for the Ethernet WAN port.

Status	Port	WLAN	Cellular	Loopback	VLAN Trunk
Packet Forwarder	- Port_1				
Network Server	Port			eth 0	~
Protocol Integration	Connec IP Addr	ction Type ress		Static IP 192.168.23.150	~
Network 🔻	Netmas	sk		255.255.255.0	
	Gatewa	ay		192.168.23.1	
Interface	MTU			1500	
Firewall	Primary	y DNS Server		8.8.8.8	
DHCP	Second	dary DNS Server		223.5.5.5	
DDNS	Enable	NAT			

- 2. Connect PC to UG56 ETH port directly or through PoE injector.
- 3. Assign the IP address to computer manually. Take Windows 10 system as an example:

nternet Protocol Version 4 (TCP)	/IPv4) Properties
General	
	automatically if your network supports eed to ask your network administrator
O Obtain an IP address auton	natically
• Use the following IP addres	s:
IP address:	192 . 168 . 23 . 200
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 23 . 150
Obtain DNS server address	automatically
• Use the following DNS serve	er addresses:
Preferred DNS server:	8.8.8.8
Alternative DNS server:	
Ualidate settings upon exit	Advanced
	OK Cancel

4. Open a Web browser and type in the IP address of the Ethernet port to access the web GUI.

5. Go to **Network > Interface > WLAN** and click **Scan** to search for WiFi access point.

Port	WLAN		Cellular	Loc	opback			
< GoBack								
SSID		Channel	Signal	Cipher	BSSID	Security	Frequency	
AAA		Auto	-61dBm	AES	24:e1:24:f0:c4:13	WPA-PSK/WPA2-PSK	2412MHz	Join Network

6. Select one access point and click Join Network, then type the password of the access

point.

Port	WLAN	Cellular Loopba	ack	
WLAN				
Enable				
Work Mode		Client	~	Scan
SSID		AAA		
BSSID		24:e1:24:f0:c4:13		
Encryption	Mode	WPA-PSK/WPA2-PSK	< ~	
Cipher		AES	~	
Key		••••••		
IP Setting				
Protocol		DHCP Client	~	

Click **Save** and **Apply** buttons after all configurations are done.

7. Go to **Status > WLAN** to check the connection status of the client.

WLAN Status	
Wireless Status	Enabled
MAC Address	24:e1:24:f0:de:14
Interface Type	Client
SSID	ААА
Channel	Auto
Encryption Type	WPA-PSK/WPA2-PSK
Cipher	AES
Status	Connected
IP Address	192.168.1.145
Netmask	255.255.255.0
Connection Duration	0 days, 02:44:45

8. Go to **Network > Failover > WAN Failover** to switch the wlan0 as main interface, then gateway can use the Wi-Fi to access the network.

	SLA	Track	WAN Fa	ilover				
Network 👻	WAN Failo	/er						
Interface	Main Int	erface Ba	ckup Interface	Startup Delay(s)	Up Delay(s)	Down Delay(s)	Track ID	Operation
Firewall	wlan0	 ✓ et 	n 0 🗸	30	0	0	1 ~	×
DHCP								H
DDNS	Save							
Link Failover								

Related Topic

WLAN Setting

WLAN Status

4.5 Packet Forwarder Configuration

UG56 gateway has installed multiple packet forwarders including Semtech, Basic station, Chirpstack, etc. Before connecting make sure the gateway has connected to network.

1. Go to **Packet Forwarder > General**.

General	Radios	Advanced	Custom	n Traffic		
General Setting						
Gateway EUI	24E124FFFE	F12257				
Gateway ID	24E124FFF	EF12257				
Frequency-Sync	Disabled		~			
Multi-Destination						
ID	Enable		Туре	Server Address	Connect Status	Operation
0	Enabled	Emb	edded NS	localhost	Connected	
						•

2. Click to add a new network server. Fill in the network server information and enable this server.

Туре	Semtech ~
Server Address	eu1.cloud.thethings.network
Port Up	1700
Port Down	1700

3. Go to **Packet Forwarder > Radio** page to configure the center frequency and channels. The channels of the gateway and network server need to be the same.

egion		US915		~
	Name			Center Frequency/MHz
	Radio 0		904	1.3
	Radio 1		905	5.0
lulti Channels Settin	g			
Enable	Index	Radio		Frequency/MHz
	0	Radio 0	~	903.9
	1	Radio 0	~	904.1
	2	Radio 0	~	904.3
	3	Radio 0	~	904.5
	4	Radio 1	~	904.7
	5	Radio 1	~	904.9
	6	Radio 1	~	905.1
	7	Radio 1	~	905.3

4. Add the gateway on network server page. For more details about the network server connection please refer to <u>Milesight IoT Support portal</u>.

4.6 Network Server Configuration

The gateway can work as a LoRaWAN[®] network server to receive and analyze the data of LoRaWAN[®] end devices, and then achieve the flexible integration with different systems.

4.6.1 Connect to Milesight IoT Cloud

1. Go to **Packet Forwarder > General** page to enable the embedded network server.

Status		General	Radios	Advanced	Custom	Traffic		
Packet Forwarder		General Setting						
Network Server		Gateway EUI Gateway ID	24E124FFF 24E124FF					
Network	•	Frequency-Sync	Disabled		~			
System	×	Multi-Destination						
		ID	Enable	1	Гуре	Server Address	Connect Status	Operation
Maintenance		0	Enabled	Embe	edded NS	localhost	Connected	
APP	×							H

2. Go to **Packet Forwarder > Radio** page to configure the center frequency and channels. The channels of the gateway and end devices need to be the same.

Region		US915	~
	Name		Center Frequency/MHz
	Radio 0		904.3
	Radio 1		905.0
Multi Channels Settin	g		
Enable	Index	Radio	Frequency/MHz
	0	Radio 0 🗸	903.9
	1	Radio 0 🗸	904.1
	2	Radio 0 🗸	904.3
	3	Radio 0 🗸	904.5
	4	Radio 1 🗸	904.7
	5	Radio 1 🗸	904.9
	6	Radio 1 🗸	.905.1
	7	Radio 1 🗸 🗸	905.3

3. Go to **Network Server > General** page to enable the network server and "Cloud mode", then select "Milesight IoT Cloud" mode.

Status		General	Applications	Profiles	Device
Packet Forwarder		General Setting			
		Enable			
Network Server		Cloud Mode			
Network	•		Milesight	t IoT Cloud	~
		NetID	010203		
System	•	Join Delay	5		sec
Maintenance	•	RX1 Delay	1		sec
Maintenance		Lease Time	8760-0-0	d (hh-mm-ss
APP	•	Log Level	info		~

4. Log in the Milesight IoT Cloud. Then go to **My Devices** page and click "+New Devices" to add gateway to Milesight IoT Cloud via SN. Gateway will be added under "Gateways" menu.

O Dashboard	Devices Gateway	s Histo	ry +			
My Devices	Search Q	0 No	ormal 1 🙇 Alarm 1 💐 Offli	ne 1 🛞 Inactive 3		+ New Devices
Map	□ ⊗ <u>真实设备-EN</u> 6136A39023	dd Device		×	ā	@ M @
Reports	UC3X52-虚 61151109	* SN :		sociated with your	-	@ M 0
· Event Center 30 · Sharing Center	C3X5 6123A124	- Name.			15 minutes ago	© <u>v</u> ©
R Me	AM102- 6128A2175	CO2	Cancel Confir TVOC Barometric Pi	-	a few seconds ago	<u>۵ ما</u> @
	A	27℃ Temperature	51% 0 Humidity Activity Level	2lux (PIR) Illumination		
≡•						

5. The gateway is online on Milesight IoT Cloud.

② Dashboard	Devices	Gatew		+		
My Devices	Search	٩	4	⊘ Normal 1 🔊 Offline 0 ⊗ Inactiv	e 0	+ New Devices
Map		Status	Name	Associated Devices (Joined /Not Joined /Failed)	Last Updated	
Reports		all	UG Gateway 621793129987	0/1/0 Detail	2 minutes ago	<u>ک س</u>
Event Center 94						

4.6.2 Add End Devices

1. Go to **Packet Forwarder > General** page to enable the embedded NS.

Status	General	Radios	Advanced	Custom	Traffic		
Packet Forwarder	General Setting						
Network Server	Gateway EUI Gateway ID	24E124FFF 24E124FF					
Network 🕨	Frequency-Sync	Disabled		~			
System 🕨	Multi-Destination						
Maintenance >	ID	Enable	Т	уре	Server Address	Connect Status	Operation
	0	Enabled	Embe	dded NS	localhost	Connected	
APP 🕨							H

2. Go to **Packet Forwarder > Radio** page to configure the center frequency and channels. The channels of the gateway and end devices need to be the same.

Region		US915	~
	Name		Center Frequency/MHz
	Radio 0		904.3
	Radio 1		905.0
Multi Channels Settin	g		
Enable	Index	Radio	Frequency/MHz
	0	Radio 0	♥ 903.9
	1	Radio 0	♥ 904.1
	2	Radio 0	904.3
	3	Radio 0	♥ 904.5
	4	Radio 1	♥ 904.7
	5	Radio 1	♥ 904.9
	6	Radio 1	905.1
	7	Radio 1	♥ 905.3

3. Go to **Network Server > General** page to enable the network server.

Status	General	Applications	Payload Codec	Profiles
Packet Forwarder	General Settin	g		
Network Server	Enable Platform Mode			

4. Go to **Network Server > Applications** page to add an application.

Appl	ications					
		ID		Name	Description	Operation
		1		Test	Test	l ×
						H
						1
		Applications				
		Name	cloud			
		Description	cloud			
		Metadata	0			
		Data Transmission				
			Туре		Operation	
					•	
		Save Cancel				

5. Go to **Network Server > Device** page and click **Add** to add a LoRaWAN[®] node device. You can also click **Bulk Import** to use template to add bulk devices at once.

Device						
Add	Bulk Import	Delete All			Search	Q
Device Name	Device EUI	Device-Profile	Application	Last Seen	Activated	Operation
		No matc	hing records found			

6. Fill in the information of the end device and click **Save&Apply**. The information can be found on the end device's configuration page or from manufacturer's manuals. Here are the default settings of Milesight end devices:

- Device EUI: this can be found on the device.
- Device-Profile: OTAA type files
- Payload Codec: select the model
- fPort: 85
- Application Key: select Default Value. If you use random keys, please select Custom Value.

Device Name	lora-sensor
Description	a short description of your node
Device EUI	000000000000000000000000000000000000000
Device-Profile	ClassA-OTAA
Application	cloud 🗸
Payload Codec	•
fPort	1
Frame-counter Validation	
Application Key	●Default Value○Custom Value
Device Address	
Network Session Key	
Application Session Key	
Uplink Frame-counter	0
Downlink Frame-counter	0
	Save & Apply

7. Go to **Network Server > Packets** page to check if any uplinks from this device.

twork Server									
Clear								Search	C
Device EUI/Group	Gateway ID	Frequency	Datarate	RSSI/SNR	Size	Fcnt	Туре	Time	Details
24E12	24E124	868300000	SF7BW125	-44/14.5	23	678	UpUnc	2025-04-03 10:09:25+08:00	0
24E12	24E124	868500000	SF7BW125	-44/10.2	23	677	UpUnc	2025-04-03 10:08:25+08:00	0
24E12	24E124	868100000	SF7BW125	-53/14.0	10	289	UpUnc	2025-04-03 10:07:46+08:00	0
24E12	24E124	868100000	SF7BW125	-39/14.2	23	676	UpUnc	2025-04-03 10:07:25+08:00	0
24E12	24E124	868100000	SF7BW125	-40/13.8	23	675	UpUnc	2025-04-03 10:06:25+08:00	0
24E12	24E124	868100000	SF7BW125	-40/14.0	23	674	UpUnc	2025-04-03 10:05:25+08:00	0
24E12	24E124	868500000	SF7BW125	-40/11.5	23	673	UpUnc	2025-04-03 10:04:25+08:00	0
24E12	24E124	868300000	SF7BW125	-49/13.8	18	0	JnReq	2025-04-03 10:04:16+08:00	0

Click **Details** to check packet details and decoded results.

Packet Details		×
Danuwium	120	
SpreadFactor	7	
Bitrate	0	
CodeRate	4/5	
SNR	13.5	
RSSI	-54	
Power		
Payload(b64)	AXVjA2fqAARoPA==	
Payload(hex)	0175630367ea0004683c	- 1
JSON	{ "battery": 99, "humidity": 30, "temperature": 23.4 }	
MIC	7f3664cd	ļ

4.6.3 Send Data to Device

1. Go to **Network Server > Packets**, check the packet in the network server list to make sure that the device has joined the network successfully.

1122612191	868100000	SF7BW125	17	: 2)	17	0	JnAcc	2019-08-06T09:22:29+08:00	0
112261219	868100000	SF7BW125	9.5	-77	18	0	JnReq	2019-08-06T09:22:29+08:00	0

2. Fill in the device EUI or select the multicast group which you need to send downlinks. Then fill in the downlink commands, ports.

Send Data To Device				
Device EUI	Туре	Payload	Fport	Confirmed
11226121913	ASCII	15	15	۲
. Click "Send".				
	Send	send success		

4. Check the packet in the network server list to make sure that the device has received this message successful. It's suggested to enable "Confirmed". Multicast feature does not support confirmed downlinks.

Device EUI	Туре	Payload	Fport	Confirmed
11226121913	ASCII	15	15	

You can click "Refresh" to refresh the list or set automatic refreshing frequency for the list. If the device's class type is Class C, then the device will constantly receive packets.

This packet's type is DnCnf (Downlink Confirmed Packet) and if the packet's color is gray, then it means the packet cannot be transmitted now because at least one message has been in the queue. If the packet record is white, it means the packet has been delivered

successfully.

2019-08-06T09:22:55+08:00 Success ()	DnCnf	2	6	- 20	SF12BW125	869525000	1122612191311123
Pending 🕕	DnCnf	2	6			0	1122612191311123

If the device receives this downlink confirmed packet, then the device will reply "ACK" when delivering next.

Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fent	Туре	Time	Details
11226121913	868300000	SF10BW125	(-)		0	3	DnUnc	2019-08-06T09:23:44+08:00	0
1122612191	868300000	SF10BW125	10.5	-75	64	2	UpCnf	2019-08-06T09:23:44+08:00	_ 0
112261219	869525000	SF12BW125	12	1	6	2	DnCnf	2019-08-06T09:22:55+08:00	0
112261219	0				6	2	DnCnf		0
112261219	868500000	SF10BW125	(-)		0	1	DnUnc	2019-08-06T09:22:49+08:00	•

Packets Details		×
Dev Addr	07e7	^
GwEUI	24e124ff	
AppEUI	557240	
DevEUI	1122612191311123	
Immediately	323	
Timestamp	874346044	
Туре	UpCnf	
Adr	false	
AdrAcKReq	false	
Ack	true	
Fcnt	21	
Fport	55	
Modulation	LORA	

Ack is "true" means that the device has received this packet.

If the device's class type is Class A, only after the device sends out an uplink packet will the network server sends out data to the device.

Clear								Search	C
Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Туре	Time	Details
1122612191311123	868300000	SF10BW125	-	2	0	19	DnUnc	2019-08-06T09:49:38+08:00	0
1122612191311123	868300000	SF10BW125	10.8	-76	64	21	ACK	2019-08-06T09:49:38+08:00	0
1122612191311123	868300000	SF10BW125	10.8	-76	64	21	UpCnf	2019-08-06T09:49:38+08:00	0
1122612191311123	868100000	SF10BW125	-	76	6	18	DnCnf	2019-08-06T09:48:43+08:00	Success
1122612191311123	868100000	SF10BW125	9.8	-77	64	20	UpCnf	2019-08	0
1122612191311123	0				6	18	DnCnf	Pending	0
1122612191311123	868500000	SF10BW125		-	0	17	DnUnc	2019-08-06T09:47:38+08:00	0
1122612191311123	868500000	SF10BW125	8.0	-76	64	19	UpCnf	2019-08-06T09:47:38+08:00	0
1122612191311123	868100000	SF10BW125	(2)	2	0	16	DnUnc	2019-08-06T09:46:38+08:00	0
1122612191311123	868100000	SF10BW125	11.2	-74	64	18	UpCnf	2019-08-06T09:46:37+08:00	0

Clear								Search	0
Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Туре	Time	Details
1122612191311123	868300000	SF10BW125	2	2	0	19	DnUnc	2019-08-06T09:49:38+08:00	0
1122612191311123	868300000	SF10BW125	10.8	-76	64	21	ACK	2019-08-06T09:49:38+08:00	0
1122612191311123	868300000	SF10BW125	10.8	-76	64	1	UpCnf	2019-08-06T09:49:38+08:00	
1122612191311123	868100000	SF10BW125	means	the d	evice	has re		2019-08-06T09:48:43+08:00 he packet you send.	0
1122612191311123	868100000	SF10BW125	9.8	-77	64	20	UpCnf	2019-08-06T09:48:43+08:00	0
1122612191311123	0				6	18	DnCnf		0
1122612191311123	868500000	SF10BW125	-		0	17	DnUnc	2019-08-06T09:47:38+08:00	0
1122612191311123	868500000	SF10BW125	8.0	-76	64	19	UpCnf	2019-08-06T09:47:38+08:00	0
1122612191311123	868100000	SF10BW125	2	2	0	16	DnUnc	2019-08-06T09:46:38+08:00	0
1122612191311123	868100000	SF10BW125	11.2	-74	64	18	UpCnf	2019-08-06T09:46:37+08:00	0

Related Topic

Packets

Milesight

4.6.4 Connect to HTTP/MQTT Server

The gateway supports choosing the data transport protocol to send data to another server address using MQTT, HTTP or HTTPS protocol.

- 1. Go to Network Server > Application to select the application to edit.
- 2. Click

to add a data transmission type.

HTTP or HTTPS:

Step 1: select HTTP or HTTPS as transmission protocol.

Туре	HTTP	•
	2010/2010	

Step 2: Enter the destination URL. Different types of data can be sent to different URLs.

URL

Data Type	URL
Uplink data	
Join notification	
ACK notification	
Error notification	

Enter the header name and header value if there is user credentials when accessing the HTTP(s) server.

HTTP Header				
	Header Name	Header Value	Operation	
			H	

MQTT:

Step 1: select the transmission protocol as MQTT. Step 2: Fill in MQTT broker general settings.

Туре	MQTT	~
Status	-	
General		
Broker Address		
Broker Port		
Client ID		
Connection Timeout/s	30	
Keep Alive Interval/s	60	
Data Retransmission		

Step 3: Select the authentication method required by the server.

If you select user credentials for authentication, you need to enter the username and password for authentication.

User Credentials	
Enable	
Username	
Password	

If certificate is necessary for verification, please select mode and import CA certificate, client certificate and client key file for authentication.

TLS				
Enable				
Mode	Self signed certificates	×		
CA File		Browse	Import	Delete
Client Certificate File		Browse	Import	Delete
Client Key File		Browse	Import	Delete

Step 4: Enter the topic to receive data or send downlinks, and choose the QoS.

opic				
	Data Type	topic	Retain	
	Uplink data		0	QoS 0 🗸
	Downlink data			QoS 0 🗸
	Multicast downlink data			QoS 0 🗸
	Join notification			QoS 0 🗸
	ACK notification			QoS 0 🗸
	Error notification			QoS 0 🗸
	Request data			QoS 0 🗸
	Response data			QoS 0 🗸

4.7 Node-RED

4.7.1 Start the Node-RED

1. Go to "App > Node-RED" to enable the Node-RED feature.

2. After enabled, click "Launch" to go to the Node-RED web GUI and to log in with the same username and password as gateway.

Node-RED				
		Usemame:		
	Node-RED	Lo	ogin	

4.7.2 Send Data by Email

Application Example

Send AM102 device data by Email.

harry	test1	test	chenpan	test2	Flow 1	+	i≣ #	debug		i 🖉	÷.	٥
							1			T selecte		
							msç	21/4/30下午4:1 9 payload : strin 4L/ /w=="		ode: 5034	lec07.ffa3	.c4
elle Lo	oRa Input	AM100	AM 100 Decoder	AM100 Data to Email			msg	21/4/30下午4:3 g.payload:Obj object		ode: 24a6	i8c41.c9fi	754
								temperature humidity: 5				
		\subset	msg.payload					illuminance 0: 1	_sensi	or: arra	JY[3]	
								1: 6 2: 1 actuation:	8			
							Em		3:15 n	ode: AM10	00 Data te	D
								g : string[8] uccesss"				

Configuration Steps

1. Add a "LoRa Input" node. Before adding please ensure network server mode is enabled and LoRaWAN devices have joined the network.

2. If you add many devices and only need one device data, add "Device Filter" node behind the "LoRa Input" and type the device EUI.

harry	test1	test	chenpan	Edit Device Filte	er node	
				Delete		Cancel Done
				Properties		• 2 12
				Name	AM100	
				Device EUI	24E124127A270222	+
(IP LoRa Input					

3. Add a "Decoder" node to decode the Milesight sensor data.

harry	test1	test	chenpan	Edit Decoder node	2	
				Delete		Cancel Done
				Properties		¢ 2 1
LoRa	Inout	AM100	AM 100 Decoder	Name	AM 100 Decoder	
Loka	mput y	AMILO	AM TOU DECOUET	Device Type	AM100 Series 🗸	

4. Add an "Email Output" and type the SMTP client settings, destination email address and contents. Example content:

The time is {{time}} Deveui is {{deveui}} Humidity is {{payload.humidity}}

harry	test1	test	chenpan	Edit Email Outp	ut node		
				Delete		Cancel	Done
				© Properties		4	• 2 2
				Name	AM100 Data to Email		
	LoRa Input	AM100 9	AM 100 Decoder	SMTP Option	Custom 🗸		
				User ID	@milesight.com		
			msg.payload	Password			
				SMTP Server Address	smtp.exmail.qq.com		
				Port [1-65535]	25		
				Enable TLS			
	WAN UP			То	@milesight.com	+	
				Торіс	AM100 Data		
				Payload	The time is {{time}} Deveui is {{deveui}} counter is {{payload humidity}}	ß	

Note:

1) When you select SMTP Option as "Same as Gateway", go to **System > General Settings > SMTP** to configure the SMTP clients.

2) Basic format to call LoRaWAN node data is {{property name}}, you can click "Help" page for more info about the Email or SMS payload format.

3) If you need to check the output content in every node, please add debug node.

5. After completing the configuration, click "Deploy" to save all your configuration.



6. When AM102 sends data to gateway, gateway will transfer the data to email.

		2021-0
From	@milesight.com>	
То	@milesight.com>	
Time: 2021年	4月30日 (周五) 17:13 🔊	
Size: 2 KB		

Related Topic

Node-RED

[END]