

Grandstream Networks, Inc.

GXW42XX V1/GXW42XX V2 Series - User Manual



GXW42XX V1/GXW42XX V2 Series - User Manual

Thank you for purchasing the Grandstream GXW42XX Analog FXS IP Gateway. The GXW42XX offers an easy-to-manage, easy-to-configure IP communications solution for any business with virtual and/or branch locations. The GXW42XX supports popular voice codecs and is designed for full SIP compatibility and interoperability with third-party SIP providers, thus enabling you to fully leverage the benefits of VoIP technology, integrate a traditional phone system into a VoIP network, and efficiently manage communication costs.

This manual will help you learn how to operate and manage your GXW FXS Analog IP Gateway and make the best use of its many upgraded features, including simple and quick installation, multi-party conferencing, and direct IP-IP Calling. This IP Analog Gateway is very easy to manage and scalable, specifically designed to be an easy-to-use and affordable VoIP solution for the small - medium business or enterprise.

GATEWAY GXW42XX OVERVIEW

The new GXW42XX series has a compact and quiet design and offers superb audio quality, rich feature functionality, strong security protection, and good manageability. It is auto-configurable, remotely manageable, and scalable.

The GXW42XX series features 16, 24, 32, or 48-port FXS interface for analog telephones, dual 10/100/1000Mbps network ports, and an RJ21 analog port. In addition, it supports the option of 4 SIP Server profiles, caller ID for various countries/regions, T.38 fax, flexible dialing plans, security protection (SIPS/TLS), comprehensive voice codec including G.711 (a/u-law), G.723.1, G.726(16/24/32/40 bit rates), iLBC and G.729.

The GXW42XX is compliant with various safety standards, including FCC/CE. Its power adapter is compliant with the UL standard.

Use only the power adapter included in the GXW42XX package. Use of an alternative power adapter may permanently damage the unit.

Grandstream has a reseller agreement with our reseller customers. End users should contact the company from whom the product was purchased for replacement, repair, or refund.

If you purchased the product directly from Grandstream, please contact Grandstream Support for an RMA (Return Material Authorization) number. Grandstream reserves the right to change the warranty policy without prior notification.

Changes or modifications to this product not expressly approved by Grandstream, or operation of this product in any way other than as detailed by this User Manual, could void your manufacturer warranty.

Once the GXW42xx V2 device is upgraded to 1.0.7.2, it cannot be downgraded to 1.0.5.4 or an earlier version due to the addition of 2nd generation individual certificates.

GXW42xx V2 device uses a different firmware file from the GXW42xx V1 device. Please use the correct firmware file for V1 and V2 devices. To distinguish the GXW42xx V2 device from the V1 device, please check the label on the back of the device.

(1) GXW42xx V2 has "V2" printed for model name. For example, "Model: GXW4216 V2". If the model's name doesn't have V1 or V2 printed, the device is GXW42xx V1.

(2) GXW42xx V2 has the device password printed on the label. GXW42xx V1 does not have it.

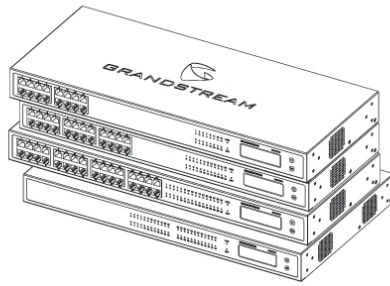
CONNECT YOUR GXW42XX GATEWAY

Connecting the GXW42XX gateway is easy. Before you begin, please verify the contents of the GXW42XX package.

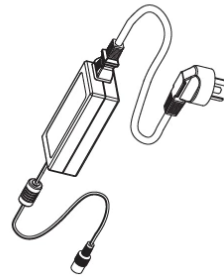
Equipment Packaging

Unpack and check all accessories. Equipment includes:

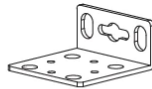
- **1 x GXW42xx V1/GXW42xx V2 Device Unit**
- **1 x RJ45 Ethernet Cable**
- **1 x Power Adapter**
 - 12V 5A universal adapter (for all models except GXW4248 V1/V2)
 - 24V 6.25A adapter (for GXW4248 V1 and V2 only)
- **2 x Rack Mount Brackets**
- **2 x Telco Cables** (included with GXW4248 V1 and V2 only)
- **1 x Quick Installation Guide**
- **1 x Regulatory Paper**



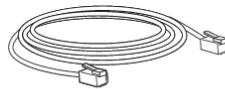
1x GXW42xx Unit



1x Power Adapter



2x Rack Mount



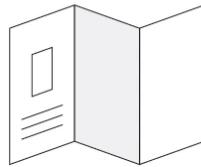
1x Ethernet Cable



2x Telco Cable
(GXW4248 Only)

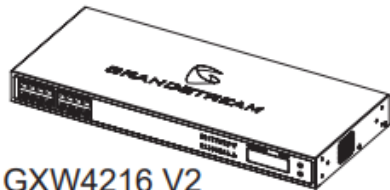


1x Regulatory Paper



1x Quick Installation
Guide

GXW42xx V1 Package Content



GXW4216 V2



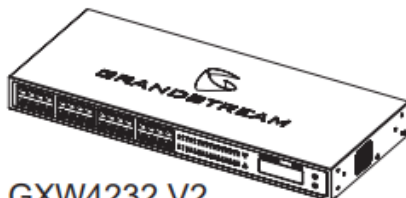
1x Power Adapter



GXW4224 V2



2x Telco Cable
(GXW4248 V2 only)



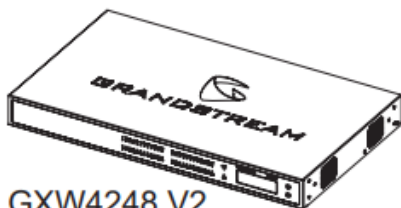
GXW4232 V2



1x Ethernet Cable



2x Rack Mount



GXW4248 V2



1x Quick Installation Guide

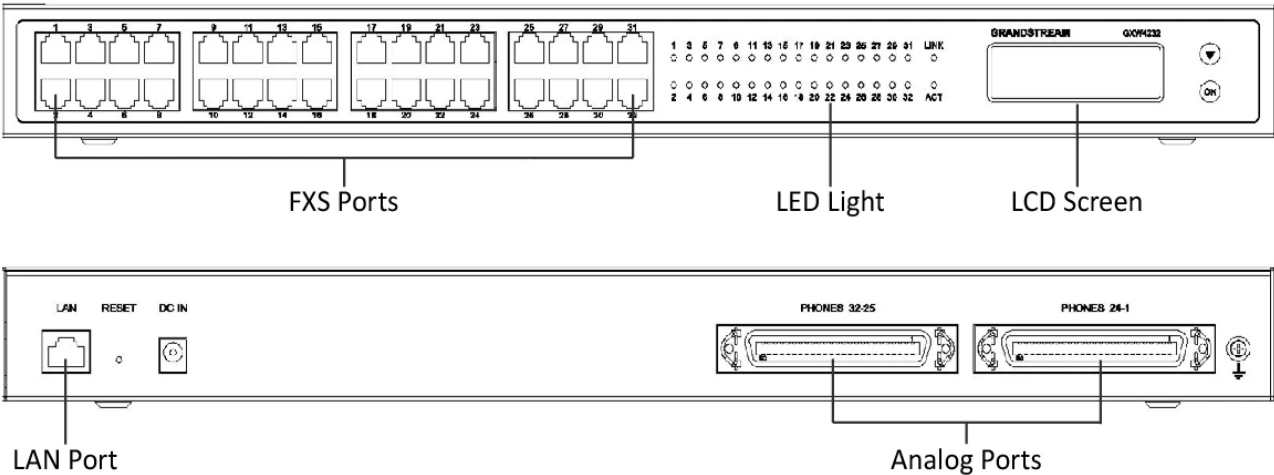
GXW42xx V2 Package Content

Connect the GXW42XX

Follow these four (4) steps to connect your GXW42XX gateway to the Internet and access the unit's configuration pages.

- 1. Connect standard touch-tone analog phones to the GXW42XX's RJ21 port with an RJ11 to RJ21 cable.
- 2. Insert an RJ45 Ethernet cable into the WAN port of GXW42XX and connect the other end to an uplink port (a router or a modem, etc.)
- 3. Plug the power adapter into the GXW42XX gateway in a power outlet.

Follow the instructions from the topic "[Configuring GXW 42XX with Web Browser](#)" for initial configuration. The GUI pages will guide you through the remaining steps to set up your gateway.

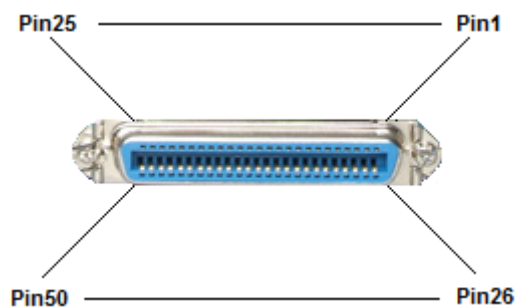


Ethernet Port	Connect to the internal LAN network or router
RESET	Factory Reset button. Press and hold for a while to reset factory default settings.
DC IN	Power adapter connection
Analog Port	Connect to analog phones / fax machines with an RJ21 to RJ11 cable
FXS Ports	FXS port to be connected to analog phones / fax machines.

Definitions of the GXW Connectors

Once the GXW42XX is turned on and configured, the front display panel indicates the status of the unit.

Act LED	Remains ON if plug the network cable.
LINK LED	Indicates Ethernet port activity.
FXS LED	Indicate status of the respective FXS Ports on the back panel Busy - ON (Solid Green) Available - OFF Slow blinking FXS LEDs indicates Voice Mail for that port. All FXS LEDs slow blinking indicates provisioning.



Pin	Signal	Pin	Signal
1	RING1	26	TIP1
2	RING2	27	TIP2
3	RING3	28	TIP3
4	RING4	29	TIP4
5	RING5	30	TIP5
6	RING6	31	TIP6
7	RING7	32	TIP7
8	RING8	33	TIP8
9	RING9	34	TIP9
10	RING10	35	TIP10
11	RING11	36	TIP11
12	RING12	37	TIP12
13	RING13	38	TIP13
14	RING14	39	TIP14
15	RING15	40	TIP15
16	RING16	41	TIP16
17	RING17	42	TIP17
18	RING18	43	TIP18
19	RING19	44	TIP19
20	RING20	45	TIP20
21	RING21	46	TIP21
22	RING22	47	TIP22
23	RING23	48	TIP23
24	RING24	49	TIP24

50 Pin Telco Connector

- For GXW4216, only the first 16 pairs are connected.
- For GXW4232, the first 24 pairs on the 1st RJ21 connector and the first 8 pairs on the 2nd RJ21 connector are connected.
- For GXW4224 and GXW4248, the last pair of pins 25 and 50 on each RJ21 is not connected.

- All LED lights display green when ON.
- LINK LED and ACT LED blinking in the following status indicate different network speeds.
 - 10M: LINK and ACT all blink, ACT blinks faster than LINK
 - 100M: LINK and ACT all blink, ACT blinks the same fast as LINK
 - 1000M: LINK does not blink, only ACT blink
- Slow blinking of the FXS LED together indicates a firmware upgrade or provisioning state.

GXW42XX FEATURES

The GXW42XX is a next-generation IP voice gateway that is interoperable and compatible with leading IP-PBXs, Soft switches, and SIP platforms. The GXW42XX FXS gateway is auto-configurable, remotely manageable, and scalable. The GXW42XX gateways come in four models - the GXW4216, GXW4224, GXW4232 and GXW4248, each offering superb voice quality, traditional telephony functionality, easy deployment, and 16, 24, 32, and 48 FXS ports, respectively. Each model features flexible dialing plans, integrated call routing to support a pure IP network call, and an external power supply.

Software Features Overview

- 16, 24, 32, or 48 FXS ports (no front panel FXS ports on GXW4248)
- RJ-45 Ethernet ports
- 4 configurable SIP profiles
- Supports Voice Codecs:

G711 (a/u, Annex I & II), G723.1A, G726 (ADPCM with 16/24/32/40 bit rates), G729 A/B, iLBC, T.38 Fax

- Comprehensive Dial Plan support for Outgoing calls.
- G.168 Echo Cancellation,
- Voice Activation Detection (VAD), Comfort Noise Generation (CNG), and Packet Loss Concealment (PLC)
- Supports PSTN/PBX analog telephone sets or analog trunks

	GXW4216	GXW4224	GXW4232	GXW4248
Telephone Interfaces	16 FXS ports	24 FXS ports	32 FXS ports	48 FXS ports
SIP Provisioning	16 SIP accounts, 4 profiles	24 SIP accounts, 4 profiles	32 SIP accounts, 4 profiles	48 SIP accounts, 4 profiles
Network Interface	10/100/1000 Mbps, RJ-45			

Number of Concurrent Calls (except when using SRTP)	16 Concurrent Calls	24 Concurrent Calls	32 Concurrent Calls	48 Concurrent Calls
Voice over Packet Capabilities	Voice Activity Detection (VAD) with CNG (comfort noise generation) and PLC (packet loss concealment), LEC with NLP Packetized Voice Protocol Unit (supports RTP and AAL2 protocol), G.168 compliant Echo Cancellation, Dynamic Jitter Buffer, Modem detection & auto-switch to G.711			
Voice Compression	G.711 + Annex I (PLC), Annex II (VAD/CNG format) encoder and decoder, G.722, G.723.1A, G.726(ADPCM with 16/24/32/40-bit rates), G.729, iLBC, G.726 provides proprietary VAD, CNG, and signal power estimation, Voice Play Out unit (reordering, fixed and adaptive jitter buffer, clock synchronization), AGC (automatic gain control), Status output, Decoder controlling via voice packet header			
DHCP Server/Client	DHCP Client only			
Fax over IP	T.38 compliant Group 3 Fax Relay up to 14.4kbps and auto-switch to G.711 for Fax Pass-through, Fax Datapump V.17, V.21, V.27ter, V.29 for T.38 fax relay			
QoS	DiffServ, TOS, 802.1P/Q VLAN tagging			
Transport Protocol	RTP			
DTMF Method	In-audio, RFC2833, and/or SIP Info			
IP Signaling	SIP (RFC 3261)			
Provisioning	TFTP, HTTP, HTTPS (additionally FTP and FTPS for V2)			
Security	SRTP, TLS/SIPS, HTTPS, 802.1x			
Management	Syslog support, HTTP/HTTPS and SSH access			
Dial Plan	Yes			
3-way Conference	3-Way conference with local mixing			
Caller ID	Bellcore Type 1 & 2, ETSI, BT, NTT, FSK and DTMF-based CID Note: The GXW42xx V2 supports customizing the Caller ID order for Vonage services to ensure Caller ID information is displayed according to the configured priority (Date & Time -> Calling Number -> Calling Name)			
Polarity Reversal / Wink	Yes			
Network Connectivity	IPv4, TCP/UDP, RTP, HTTP/HTTPS, ARP/RARP, ICMP, DNS, DHCP, NTP, TFTP, SSH, PPPoE, STUN, DDNS, OpenVPN(R) (additionally FTP and FTPS for V2)			

GXW42xx Software Specifications

Hardware Specification

The hardware specifications of the GXW FXS series are detailed in Table 4.

	GXW4216	GXW4224	GXW4232	GXW4248
Telephone Interfaces	16 RJ11 Ports/1 RJ21 Port	24 RJ11 Ports/1 RJ21 Port	32 RJ11 Ports/2 RJ21 Ports	2 RJ21 Ports only
FXS LEDs	16	24	32	48
Network Interface	LAN, Single 10/100/1000 BASE-TX, RJ45			
Power Input	Input: 100-240VAC, 50/60Hz Output: 12V DC, 5.0A (4216/24/32) 24V DC, 6.25A (4248 only)			
LCD Screen	128x32 pixel			
Telco Connector	1 RJ21 (50 pins)	1 RJ21 (50 pins)	2 RJ21 (50 pins)	2 RJ21 (50 pins)
RJ-11 Connectors	Yes	Yes	Yes	No
Function Buttons	1 button for Reset/Factory Reset			
Environmental	Operation: 0 °C to 40 °C (V1), 0 °C to 45 °C (V2) Storage: -10 °C to 60 °C Humidity: 10% to 90% Non-condensing			
Mounting	Desktop and Rack mount			
On-hook Voltage	Fixed, 48V			

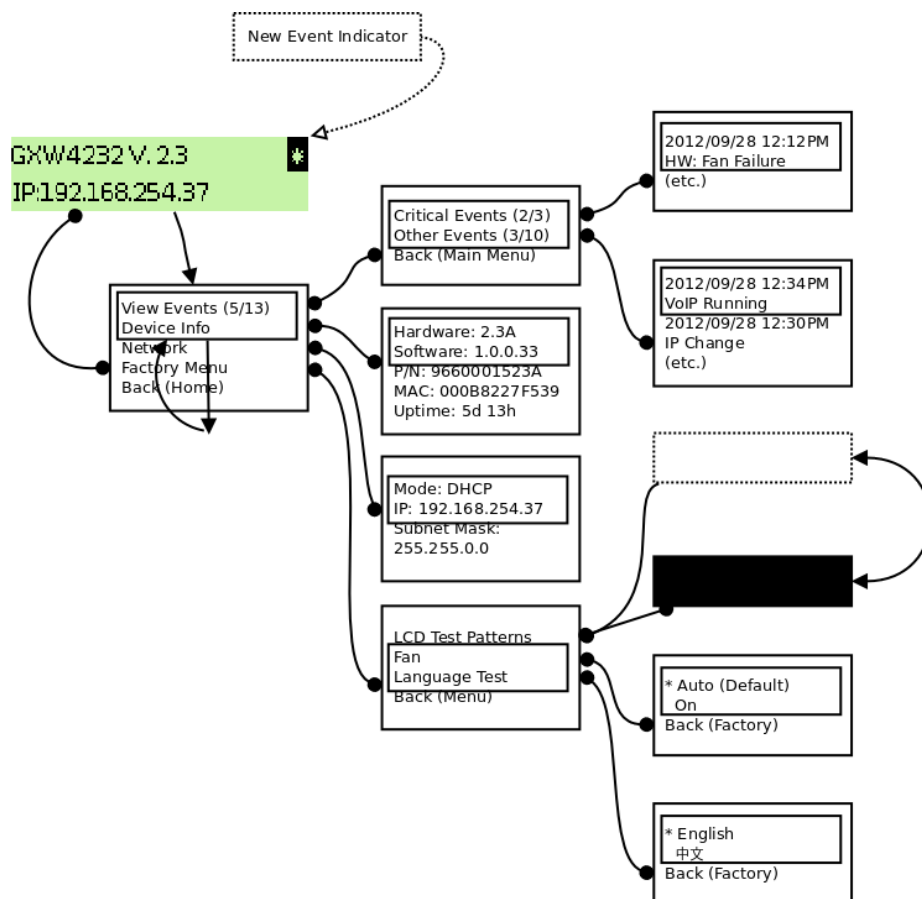
Ring Voltage	50Vrms (balanced ringing)			
Ring Frequency	20-50 Hz			
Short Haul Loop	2REN: Up to 2km on 24 AWG wire	2REN: Up to 2km on 24 AWG wire	2REN: Up to 2km on 24 AWG wire	2REN: Up to 2km on 24 AWG wire
Outdoor Protection	Over-voltage Protection and surge immunity			
Signaling	FXS Loop-start			
EMC	EN55022/EN55024 and FCC part15 Class B			
Safety	UL			
Compliance	FCC, CE, C-Tick			

GXW42xx Hardware Specifications

GXW42XX LCD Menu

The GXW42XX gateway series includes a small LCD screen for the display of basic information. The LCD has a display area of 128x32 pixels, which will allow for 2 lines of text with a 16px height limitation per line.

The LCD menu is shown in the figure: LCD Menu. The menu is navigated by the Down arrow and the OK button.



LCD Menu

BASIC OPERATIONS

Understanding GXW Voice Prompts

GXW42XX has a built-in voice prompt menu for simple device configuration. To enter the voice prompt menu, press *** on the standard analog phone that is connected to the device's FXS port.

Menu	Voice Prompt	User's Options
Main Menu	"Enter a Menu Option"	Enter "*" for the next menu option Enter "#" to return to the main menu Enter "001 - 005, 007, 010, 013 - 017, 047, 086 or 099" Menu option Enter "9" for confirming an option
001	"DHCP Mode", "PPPoE Mode" or "Static IP Mode"	Enter '9' to toggle the selection If user selects "Static IP Mode", user need configure all the IP address information through menu 002 to 005. If user selects "Dynamic IP Mode", the device will retrieve all IP address information from DHCP server automatically when user reboots the device.
002	"IP Address " + IP address	The current WAN IP address is announced Enter 12-digit new IP address if in Static IP Mode. Example: to set the IP address 192.168.5.7, enter the following 12 digits 192168005007
003	"Subnet " + IP address	Same as Menu option 002
004	"Gateway " + IP address	Same as Menu option 002
005	"DNS Server " + IP address	Same as Menu option 002
007	Preferred Vocoder	Enter "9" to go to the next selection in the list: PCMU PCMA iLBC G-726G-723G-722G-729
010	"MAC Address"	Announces the Mac address of the unit.
012	WAN Port Web Access	Press "9" to switch between enable/disable. Default is Enabled.
013	Firmware Server IP Address	Announces current Firmware Server IP address. Enter 12-digit new IP address. Example: to set the IP address 192.168.2.43, enter the following 12 digits 192168002043
014	Configuration Server IP Address	Announces current Config Server Path IP address. Enter 12-digit new IP address. Example: to set the IP address 192.168.40.155, enter the following 12 digits 192168040155
015	Upgrade Protocol	Upgrade protocol for firmware and configuration update. Enter "9" to toggle between TFTP HTTP and HTTPS
016	Firmware Version	Firmware version information.
017	Firmware Upgrade	Firmware upgrade mode. Enter "9" to rotate among the following three options: 1. always check 2. check when pre/suffix changes 3. never upgrade
020	"Certification Information"	Announces the Certification Information of the unit.
047	"Direct IP Calling"	Enter the target IP address to make a direct IP call, after dial tone. (See "Make a Direct IP Call".)
086	Voice Mail	Number of voice mails

099	"RESET"	Enter "9" to reboot the device; or Enter MAC address to restore factory default setting (See Restore Factory Default Setting section)
700-748	Phone calls between different ports of the same GW42xx	GXW42XX support inter-port calling from voice menu for easy test/verification in factory "700" Ring all ports and connect to first port pick up the call "701-732" Call individual port
	"Invalid Entry"	Automatically returns to Main Menu

Five Success Tips when using the Voice Prompt

1. "*" shifts down to the next menu option
2. "#" returns to the main menu
3. "9" functions as the ENTER key in many cases to confirm an option
4. All entered digit sequences have known lengths - 2 digits for the menu option and 12 digits for the IP address. For IP address, add **0** before the digits if the digits are less than 3 (i.e., - 192.168.0.26 should be key in like 192168**0000**26. No decimal is needed).
5. Key entry cannot be deleted, but the phone may prompt an error once it is detected

Placing a Phone Call

Phone or Extension Numbers

1. Dial the number directly and wait for 4 seconds (To change the default value, modify the following setting - "No Key Entry Timeout")
2. Or, you may dial the number directly and press # (Use # as dial key" must be configured in web configuration).

Examples: Dial a number (e.g. (626) 666-7890), first enter the prefix number (usually 1+ or international code) followed by the phone number. Press # or wait for 4 seconds. Check with your VoIP service provider for further details on prefix numbers.

Direct IP Calls

Direct IP calling allows two parties, that is, a FXS Port with an analog phone and another VoIP Device, to talk to each other in an ad hoc fashion without a SIP proxy.

Elements necessary to complete a Direct IP Call:

1. Both GXW42XX and other VoIP devices have public IP addresses, or
2. Both GXW42XX and other VoIP devices are on the same LAN using private IP addresses, or
3. Both GXW42XX and other VoIP devices can be connected through a router using public or private IP addresses (with necessary port forwarding or DMZ).

GXW42XX supports two ways to make Direct IP Calling:

Using IVR

1. Pick up the analog phone, then access the voice menu prompt by dialing "****"
2. Dial "047" to access the direct IP call menu
3. Enter the IP address using the format, ex. **192*168*0*160** after the dial tone.

Using Star Code

1. Pick up the analog phone, then dial "*47"
2. Enter the target IP address using the same format as above.

Note: **NO** dial tone will be played between steps 1 and 2.

Destination ports can be specified by using "*" (encoding for ":") followed by the port number.

Examples:

1. If the target IP address is 192.168.0.160, the dialing convention is

***47 or Voice Prompt with option 047, then 192*168*0*160** followed by pressing the "#" key if it is configured as a send key, or wait 4 seconds. In this case, the default destination port 5060 is used if no port is specified.

2. If the target IP address/port is 192.168.1.20:5062, then the dialing convention would be:

***47 or Voice Prompt with option 047, then 192*168*0*160*5062** followed by pressing the "#" key if it is configured as a send key or wait for 4 seconds.

When completing a direct IP call, the "Use Random Port" should be set to "NO".

Call Hold

Place a call on hold by pressing the "flash" button on the analog phone (if the phone has that button). Press the "flash" button again to release the previously held Caller and resume the conversation. If no "flash" button is available, use "hook flash" (toggle on-off hook quickly). You may drop a call using hook flash.

Call Waiting

Call waiting tone (Repeated short beeps as long as the caller is still calling) indicates an incoming call if the call waiting feature is enabled. Toggle between incoming call and current call by pressing the "flash" button. The first call is placed on hold. Press the "flash" button to toggle between two active calls.

Call Transfer

Blind Transfer

Assume that Caller A and B are in conversation. "A" wants to Blind Transfer "B" to "C":

1. Caller A presses **FLASH** on the analog phone to hear the dial tone.
2. Caller A dials ***87**, then dials caller C's number, and then # (or waits for 4 seconds).
3. Caller A will hear the confirmation tone. Then, A can hang up.

"Enable Call Feature" must be set to "Yes" in the web configuration page.

Caller A can place a call on hold and wait for one of three situations:

1. A quick confirmation tone (similar to call waiting tone) followed by a dial tone. This indicates the transfer is successful (the transferee has received a 200 OK from the transfer target). At this point, Caller A can either hang up or make another call.
2. A quick busy tone followed by a restored call (on supported platforms only). This means the transferee has received a 4xx response for the INVITE, and we will try to recover the call. The busy tone is just to indicate to the transferor that the transfer has failed.
3. Continuous busy tone. The phone has timed out. **Note: A** continuous busy tone does not indicate the transfer has been successful, nor does it indicate the transfer has failed. It often means there was a failure to receive the second NOTIFY - check firmware for the most recent release.

Attended Transfer

Assume that Caller A and B are in conversation. Caller A wants to Attend Transfer B to C:

1. Caller A presses **FLASH** on the analog phone for dial tone.
2. Caller A then dials Caller C's number followed by # (or wait for 4 seconds).
3. If Caller C answers the call, Caller A and Caller C are in conversation. Then A can hang up to complete transfer.
4. If Caller C does not answer the call, Caller A can press "flash" to resume call with Caller B.

When Attended Transfer fails and A hangs up, the GXW42XX will ring back user A to remind A that B is still on the call. A can pick up the phone to resume conversation with B.

3-Way Conferencing

The GXW42XX supports Bellcore style 3-way Conference.

Instructions for 3-way conference:

Assuming that call party A and B are in conversation. A (GXW42XX) wants to bring C in a conference:

1. A presses FLASH (on the analog phone, or Hook Flash for old model phones) to get a dial tone.
2. A dials C's number then # (or wait for 4 seconds).
3. If C answers the call, then A presses FLASH to bring B, C into the conference.
4. If C does not answer the call, A can press FLASH back to talk to B.
5. If A presses FLASH during the conference, C will be dropped out.
6. If A hangs up, the conference will be terminated, or transfer B to C if "Transfer on Conference Hangup" is set to yes

Hunting Group

This feature allows the user to set up a single SIP account on the gateway and have the ability to use all FXS ports to make/receive calls. Using this feature, all ports active in the same Hunting Group will have the same phone number, and incoming calls will be distributed in a Linear or Circular manner among the ports active in that Hunting Group. The number of hunting groups is limited by the number of ports each GXW model has - i.e., each port can be its own Hunting Group. The most practical and efficient way to use Hunting Groups is to assign 2 or 3 ports to separate Hunting Groups.

One additional and popular way to use the Hunting Group feature is called "multiplexed analog lines". In this configuration, a legacy PBX system with 8 FXO trunks can be connected to 8 GXW42xx ports configured as a Hunting Group. The GXW can be registered to a SIP server provider using only one phone number. If the SIP service provider allows multiple calls to the same number, the GXW will allow 8 concurrent calls to the same SIP number. All office members can be reached remotely using the same phone number in a round-robin fashion.

Example Configuration of a typical Hunting Group:

1. Configure the SIP account from your VoIP Service Provider on **FXS port 1** under the **FXS Ports** webpage.
2. Select **Active** under the **Hunting Group** drop-down for FXS port 1.
3. For the remaining ports (say 2, 3, and 4), select 1 for Hunting Group. Ports 2, 3, and 4 are now active members of the hunting group associated with port 1.

This configuration will route all calls directed to FXS port 1 to ports 2, 3, and/or 4 in round robin fashion, respectively, if port 1 is busy or times out. You can configure the ring timeout on the **Profile** page.

Example configuration of a multiple Hunting Group:

FXS Port #1: SIP UserID and Authenticate ID entered, Hunting Group set to "**Active**"

FXS Port #2: SIP UserID and Authenticate ID left blank, Hunting Group set to "**1**"

FXS Port #3: SIP UserID and Authenticate ID left blank, Hunting Group set to "**1**"

FXS Port #4: SIP UserID and Authenticate ID entered, Hunting Group set to "**Active**"

FXS Port #5: SIP UserID and Authenticate ID left blank, Hunting Group set to "**4**"

FXS Port #6: SIP UserID and Authenticate ID left blank, Hunting Group set to "**4**"

FXS Port #7: SIP UserID and Authenticate ID entered, Hunting Group set to "**Active**"

FXS Port #8: SIP UserID and Authenticate ID left blank, Hunting Group set to "**7**"

...

Hunting Group 1 contains ports 1, 2, and 3. Hunting Group 4 contains ports 4, 5, and 6.

Hunting Group 7 contains ports 7, 8.

Please be aware, the choice of 1 for ports 2 and 3, the choice of 4 for ports 5 and 6, and the choice of 7 for port 8 is required to indicate that the SIP account tied to the port marked as "Active" will be used for all members of the same Hunting group. Needless to say, those members of the same Hunting group may not be sequential ports. In the following example, ports 3, 5, and 7 are tied to the SIP Account configured in Port #1 marked as "Active", and ports 4,6,8 tied to the SIP Account configured in Port #2 marked as "**Active**" as well.

Example of a non-sequential configuration of a multiple Hunting Group:

FXS Port #1: SIP UserID and Authenticate ID entered, Hunting Group set to "**Active**"

FXS Port #2: SIP UserID and Authenticate ID entered, Hunting Group set to "**Active**"

FXS Port #3: SIP UserID and Authenticate ID left blank, Hunting Group set to "**1**"

FXS Port #4: SIP UserID and Authenticate ID left blank, Hunting Group set to "2"

FXS Port #5: SIP UserID and Authenticate ID left blank, Hunting Group set to "1"

FXS Port #6: SIP UserID and Authenticate ID left blank, Hunting Group set to "2"

FXS Port #7: SIP UserID and Authenticate ID left blank, Hunting Group set to "1"

FXS Port #8: SIP UserID and Authenticate ID left blank, Hunting Group set to "2"

...

FXS Port #24: SIP UserID and Authenticate ID left blank, Hunting Group set to "2"

- A single call directed to the SIP account will NOT result in all ports ringing at the same time. They will ring in the hunting group only. This feature is applicable to incoming calls only.
- FXS Name: GXW will use the CID name from the FXS port initiating the outgoing call if the "Name" field is entered for that specific port.

There are two types of hunting groups, Linear and Circular. Linear style will sort the call to the lowest-numbered available line; this is also called "serial hunting". Circular style will distribute the calls "round-robin". If a call is assigned to line 1, the next call goes to 2, and the next to 3. The succession throughout each of the lines continues even if one of the previous lines becomes available. When the end of the hunt group is reached, the hunting starts over at the first line. Lines are skipped if they are still busy on a previous call. These two hunting styles can be configured from the Profile X page.

Inter-Port Calling

In some cases, a user may want to make phone calls between the phones connected to multiple ports of the same gateway when it is used as a standalone unit, without the use of a SIP server. This feature will also be applicable when the gateway is used with Hunting Groups and is registered to a SIP server only with one master number. In such cases, users will still be able to make inter-port calls by using the IVR feature.

For example, on the GXW42XX inter-port, calling is achieved by dialing *** and 7 plus two extra digits corresponding to the port number. For example, the user connected to port 1 can be reached by dialing *** and 701; the user connected to port 24 can be reached by dialing *** 724.

Sending and Receiving Fax

GXW42XX supports fax in two modes: 1) T.38 (Fax over IP) and 2) Fax Pass through. T.38 is the preferred method because it is more reliable and works well in most network conditions. If the service provider supports T.38, please use this method by selecting T.38 as fax mode (default). If the service provider does not support T.38, pass-through mode may be used. If you have problems with sending or receiving faxes, toggle the Fax Tone Detection Mode setting.

CALL FEATURES

GXW42XX supports the traditional telephony features available in a PBX as well as additional advanced telephony features.

Key	Call Features
*02	Forcing a Codec (per call): *027110 (PCMU), *027111 (PCMA), *02723 (G723), *02729 (G729), *0272616 (G726-r16), *0272624 (G724-r24), *0272632 (G726-r32), *0272640 (G726-r40), *027201 (iLBC)
*03	Disable LEC (pe call) Dial "*03" + " number". No dial tone is played in the middle.
*16	Enable SRTP
*17	Disable SRTP
*30	Block CallerID (for all-config change)
*31	Send CallerID (for all-config change)
*67	Block CallerID (per call)
*82	Send CallerID (per call)
*47	Direct IP Calling. Dial "**47" + "IP address". No dial tone will be played in the middle. Detail see Direct IP Calling section on page 12.
*50	Disable Call Waiting (for all-config change)
*51	Enable Call Waiting (for all-config change)
*69	Call Return Service: Dial *69 and the phone will dial the last incoming phone number received.
*70	Disable Call Waiting (Per Call)
*71	Enable Call Waiting (Per Call)
*72	Unconditional Call Forward: Dial "*72" and then the forwarding number followed by "#". Wait for dial tone and hang up. (dial tone indicates successful forward)
*73	Cancel Unconditional Call Forward: Dial "*73" and wait for dial tone, then hang up.
*74	Enable Paging Call: Dial "*74" and then the destination phone number you want to activate in Paging mode.
*78	Enable Do Not Disturb (DND): When enabled all incoming calls will be rejected.
*79	Disable Do Not Disturb (DND): When disabled, incoming calls will be accepted.
*87	Blind Transfer
*90	Busy Call Forward: Dial "**90" and then the forwarding number followed by "#". Wait for dial tone then hang up.

*91	Cancel Busy Call Forward: dial "*91". Wait for dial tone. Hang up.
*92	Delayed Call Forward: Dial "*92" and then the forwarding number followed by "#". Wait for dial tone then hang up.
*93	Cancel Delayed Call Forward: Dial "*93" for a dial tone, then hang up.
*98	Play registration ID: Dial "*98", the registration ID will be announced.
*99	Provision start: Dial "*99", the provisioning process will be triggered.
Flash/Hook	If user hears call waiting beep, flash/hook will switch to the new incoming call. Also used to switch to a new channel for a new call.
#	Pressing pound sign will serve as Re-Dial key.

CONFIGURATION GUIDE

Configuring GXW42XX via Voice Prompt

DHCP Mode

Select voice menu option 001 to enable GXW42XX to use DHCP.

STATICIP Mode

Select voice menu option 001 to enable GXW42XX to use STATICIP mode, then use option 002, 003, 004, 005 to set up IP address, Subnet Mask, Gateway, and DNS server respectively.

PPPoE Mode

Select voice menu option 001 to enable GXW42XX to use PPPoE mode.

Firmware Server IP Address

Select voice menu option 013 to configure the IP address of the firmware server.

Configuration Server IP Address

Select voice menu option 014 to configure the IP address of the configuration server.

Upgrade Protocol

Select voice menu option 015 to choose the firmware and configuration upgrade protocol. The user can choose between TFTP, HTTP, HTTPS, FTP and FTPS.

Firmware Upgrade Mode

Select voice menu option 017 to choose firmware upgrade mode among the following three options:

- 1) Always check,
- 2) check when pre/suffix changes,
- 3) Never upgrade

Configuring GXW42XX with a Web Browser

The GXW42XX series gateway has an embedded Web server that allows users to configure the GXW42XX through a web browser. It has language support for English, Chinese, French, Russian, and Spanish.

Access the Web Configuration Menu

The GXW42XX HTML configuration menu can be accessed via the Ethernet port:

To access the HTML configuration menu from the Ethernet port:

1.
Follow table 4 to find the Ethernet port IP address.
2.
Open a web browser, type in the IP address - for example: `http://GXW42XX -IP-Address` (the GXW42XX IP-Address is the Ethernet IP address for the GXW42XX).

The IVR announces 12 digits of the IP address; you need to strip out the leading "0" in the IP address. For ex. IP address: 192.168.001.014, you need to type in `http://192.168.1.14` in the web browser.

Once the HTTP request is entered and sent from a web browser, the user will see a login screen. There are two default passwords for the login page:

User Level	Username	Password	Web Pages Allowed
End User Level	user	123	Only Status and Basic Settings
Administrator Level	admin	admin (for V1) Random password available on the sticker (for V2)	Browse all pages
Viewer Level	viewer	viewer	View all pages. Not allowed to modify the content.

- The password is case sensitive with a maximum length of 25 characters. Only an administrator can access the "ADVANCED SETTINGS", "Profile 1~4", and "FXS Ports" configuration pages.
- The user and viewer level access is disabled by default. To enable it, go under **Maintenance => Web and SSH Access**.
- The user must change their Admin/User/Viewer Account password after the first time login
- When the GXW42xx V2 device is added to the Grandstream cloud, users can access its Web UI directly from the Grandstream Cloud platform via a redirection link that opens the device's Web UI interface.

Important Settings

The end-user must configure the following settings according to the local environment.

Most settings on the web configuration pages are set to the default values.

NAT Settings

If you plan to keep the gateway within a private network behind a firewall, we recommend using STUN Server. The following three (3) settings are useful in the STUN Server scenario:

1. STUN Server (under Advanced Settings webpage)

Enter a STUN Server IP (or FQDN) that you may have, or look up a free public STUN Server on the internet and enter it in this field. If using Public IP, keep this field blank.

2. NAT Traversal (under the Profile web pages)

Set this to Yes when the gateway is behind a firewall on a private network.

DTMF Methods

DTMF Settings are in Profile pages.

- DTMF in-audio
- DTMF via RTP (RFC2833)

- DTMF via SIP INFO

You can enable set priority of DTMF methods according to your preference, from Priority 1 to 3. This setting should be based on your server's DTMF setting.

Preferred Vocoder (Codec)

The GXW42XX supports a broad range of voice codecs. Under Profile web pages, choose your preferred order of different codecs:

- PCMU/A (or G711u/a)
- G729
- G723
- G726 (16/24/32/40)
- G722
- iLBC
- AAL2 (all G726)

To enable or disable **Wideband PCM Resolution**, download the device configuration file, modify the **P28936** parameter, and upload the updated configuration file. Set the P-value to **0** for **Narrowband (8 kHz sample rate)** or **1** for **Wideband (16 kHz sample rate)**. The default setting is **1**.

PAGE DEFINITIONS

This section will describe the options in the Web configuration user interface. As mentioned, a user can log in as an administrator or end-user.

Functions available for the end-user are:

- **STATUS:** Displays the network status, account status, software version, and MAC address of the phone
- **MAINTENANCE:** Basic settings such as basic network, date and time settings, and web/SSH access settings can be set here.
- **PROFILE - AUDIO SETTINGS:** DTMF, Vocoder, and Analog Line settings can be configured here for each port.

Additional functions available to administrators are:

- **MAINTENANCE:** Full settings for network, upgrade/provisioning, TR-069, Security, and Syslog.
- **ADVANCED SETTINGS:** To set advanced Ring Tongs, FXO Failover, and System Features.
- **PROFILE X:** To configure each of the SIP accounts.
- **FXS PORTS:** To configure each of the FXS ports and Hunting Group,s etc.

Status

System Info	
Product Model	Displays the product model and hardware version.
Part Number	Displays the part number.
Serial Number	Displays the serial number.
Certificate Type	Displays the security certificate type.
Software Version	Boot: Bootloader version. Core: Core version. Base: Base version. Prog: Firmware version. This is the primary firmware release number used to identify the software version running on the GXW42xx. CPE: CPE version.
System Up Time	Displays the duration since the device was last rebooted.
System Time	Displays the current system time synchronized with the configured NTP server.
System Information	Downloads the system information file for diagnostic purposes.Note: The device supports periodically saving the system time to a local timefile for diagnostic purposes and system continuity.
Service Status	Displays ATA and GUI service information.
Network Status	
MAC Address	Displays the device MAC address in hexadecimal format. The MAC address is used for provisioning and troubleshooting and is printed on the product label and packaging.
IP Address Mode	Displays the current IP address mode: DHCP PPPoE Static IP
IP Address	Displays the current IP address assigned to the GXW42xx.
Subnet Mask	Displays the subnet mask.
Gateway	Displays the default gateway.
VPN Link	Displays the VPN connection status.
PPPoE Link Up	Displays the PPPoE connection status.
DNS Server 1/2	Display the primary and secondary DNS server addresses.
NAT Traversal	Displays the detected NAT type for each SIP profile based on the STUN protocol.

Port Status	
Port	Displays the port number.
Hook	Displays the hook status: Onhook Offhook
SIP Registration	Displays the SIP registration status: Registered Not Registered
Call Features Status	
Port	Displays the port number.
DND	Displays whether Do Not Disturb is enabled or disabled.
Forward	Displays the unconditional call forwarding destination.
Busy Forward	Displays the call forwarding destination when the line is busy.
Delayed Forward	Displays the call forwarding destination when the call is not answered.
CID	Displays whether Caller ID per Call is enabled or disabled.
Call-Waiting	Displays whether Call Waiting is enabled or disabled.
SRTP	Displays whether Secure Real-time Transport Protocol is enabled or disabled.

Maintenance

Network Settings

Network Settings for Service Interface	
IP Address Mode for Service Interface	Specifies the IP address mode. The available options are: DHCP PPPoE Static IP The default setting is "DHCP".
Preferred DNS Server	Configures the preferred DNS server used when the IP address mode is DHCP or PPPoE.
DHCP Settings	
Host name (Option 12)	Specifies the client host name used in DHCP Option 12. This field is optional but may be required by some Internet Service Providers.
DHCP Domain	Specifies the DHCP domain name. This field is optional but may be required by the Internet Service Providers.
Vendor Class ID (Option 60)	Specifies the vendor class identifier transmitted in DHCP requests.The default setting for the GXW42xx V1 is "GXW42XX".The default setting for the GXW42xx V2 is "GXW42XXV2".
Client Circuit ID (Option 82)	Specifies the Agent Circuit ID sub-option of DHCP Option 82, which identifies the circuit through which the DHCP request was received. The Circuit ID is an agent-local identifier.
Remote Agent ID (Option 82)	Specifies the Remote ID sub-option of DHCP Option 82, which carries information about the remote host end of the circuit. The relay agent may include this field in addition to or instead of the Agent Circuit ID field.
PPPoE Settings	
PPPoE Account ID	Configures the PPPoE account ID.
PPPoE Password	Configures the PPPoE password.
PPPoE Service Name	Specifies the PPPoE service name.
Static IP Settings	
IP Address	Configures the static IP address.
Subnet Mask	Configures the subnet mask.
Gateway	Configures the default gateway.

DNS Server 1	Configures the primary DNS server.
DNS Server 2	Configures the secondary DNS server.
Network settings for Management Interface	
Enable management interface	Enables or disables the management interface for HTTP, HTTPS, and SSH access. If a management VLAN is configured and differs from the service VLAN, the management interface uses the management VLAN. Otherwise, a sub-interface is created on the service interface.The default setting is "Disabled".
Management access	Specifies which interface accepts HTTP, HTTPS, and SSH connections. The available options are: Both on Service and Management Interfaces Management Interface Only The default setting is "Management Interface Only".
Enable SNMP Through Management Interface	Enables or disables routing SNMP traffic through the management interface.The default setting is "Disabled".
Enable TR069 Through Management Interface	Enables or disables routing TR-069 traffic through the management interface.The default setting is "Disabled".Supported on GXW42xx V2 only.
Enable Syslog Through Management Interface	Enables or disables routing Syslog traffic through the management interface.The default setting is "Disabled".Supported on GXW42xx V2 only.
Enable Radius Through Management Interface	Enable or disable routing the web access radius packets through management interfaceThe default setting is "Disabled".Supported on GXW42xx V2 only.
IP Address Mode for Management Interface	Specifies the IP address mode for the management interface. The available options are: DHCP Static IP The default setting is "DHCP".
Static IP Settings (Management Interface)	
IP Address	Specifies the static IP address for the management interface.The default setting is "192.168.100.100".
Subnet Mask	Specifies the subnet mask for the management interface.The default setting is "255.255.255.0".
Gateway	Specifies the default gateway for the management interface.The default setting is "192.168.100.1".
DNS Server 1	Specifies the primary DNS server for the management interface.The default setting is "0.0.0.0".
DNS Server 2	Specifies the secondary DNS server for the management interface.The default setting is "0.0.0.0".
LLDP	
Enable LLDP	Enables or disables Link Layer Discovery Protocol (LLDP).The default setting is "Enabled".
Layer 2 QoS Settings	
Enable Manual VLAN Configuration	Enables or disables allowing the gateway to keep the VLAN configuration without applying them.The default setting is "Enabled".
Layer 2 QoS 802.1Q/VLAN Tag for Service Interface	Specifies the layer 2 QoS 802.1Q/VLAN Tag for the service interface.The default setting is "0". The valid range is 0-4095.
Layer 2 QoS 802.1p Priority Value for Service Interface	Specifies the priority value of the Layer 2 QoS packets for Service Interface. The default setting is "0". The valid range is 0-7.
Layer 2 QoS 802.1p Priority Value for SIP signaling	Specifies the Layer 2 QoS 802.1p priority for SIP signaling packets.The default setting is "0". The valid range is 0-7.
Layer 2 QoS 802.1p Priority Value for RTP media	Specifies the Layer 2 QoS 802.1p priority for RTP media packets.The default setting is "0". The valid range is 0-7.
Layer 2 QoS 802.1Q/VLAN Tag for Management Interface	Specifies the layer 2 QoS 802.1Q/VLAN Tag for the management interface.The default setting is "0". The valid range is 0-4095.
Layer 2 QoS 802.1p Priority Value for Management Interface	Specifies the Layer 2 QoS 802.1p priority for management interface traffic.The default setting is "0". The valid range is 0-7.

Device Configuration(Text format)	Click to download the device configuration file in .txt format.
Device Configuration(XML format)	Click to download the device configuration file in .xml format.
Export Backup Configuration(Encrypted XML)	Click to export all device configurations in encrypted .xml format
Provision	
Allow DHCP Option 43 and Option 66 to Override Server	If set to "Yes", configuration and upgrade server's information can be obtained using DHCP option 66 from DHCP server. This option specifies the URL of the TFTP server. Notes: If DHCP Option 66 is enabled, the gateway will attempt downloading a configuration file from the server URL provided by DHCP, even though Config Server Path is left blank. When both DHCP Option 160 and Option 66 are provided, the device prioritizes DHCP Option 160 for configuration/provisioning information.
Additional Override DHCP Option	Allow users to configure additional DHCP Options to be used for the firmware server instead of the configured firmware server or the server from DHCP Options 43 and 66. It can be set to None or Option 150, it is set to None by default.
3CX Auto Provision	Default is No. If set to Yes, phone will multicast SUBSCRIBE for provision if this feature is enabled.
Enable using tags in URL	Allows users to configure variables on the configuration server path to differentiate the directories on the server. Example: When provisioning, a user can define the mac address and IP address when sending the HTTP Send request link in the following form "192.168.5.96:8060/?mac=[MAC]&lan_ip=[IP]", the link will look like this example: http://192.168.5.99/mac=000b89a9064&lan_ip=192.168.5.99/cfg.xml Default Value is "No".
Firmware Upgrade and Provisioning	Specifies how firmware upgrading and provisioning request to be sent. There are three options to choose from: "Always Check for New Firmware", "Check New Firmware only when F/W pre/suffix changes", and "Always Skip the Firmware Check".
Download and Process All Available Config Files	By default, the device first provisions cfgMAC, then attempts to provision the first available configuration file in the following order: DHCP Option 67 boot file (cfgdhcpt67.xml) -> cfgMAC.xml -> cfgProductModel.xml -> cfg.xml (corresponding to the Option 67-specific, device-specific, model-specific, and global configuration files). When this option is enabled, the device downloads and processes all available configuration files in the following order: cfg.xml -> cfgProductModel.xml -> cfgMAC.xml -> cfgMAC -> cfgMAC_override.xml -> DHCP Option 67 boot file (cfgdhcpt67.xml). Each configuration file is applied sequentially, and settings in later configuration files overwrite those applied by previously processed configuration files. Disabled by default
Provision Config Order	Configures the custom order in which the device provisions configuration files when Download and Process All Available Config Files is disabled. Select configuration files from the Available list and use the right arrow button to move them to the Selected list. To remove a configuration file from the Selected list, use the left arrow button to move it back to the Available list. Use the up and down arrow buttons to arrange the configuration files in the Selected list in the desired provisioning order. The available configuration files are: cfg.xml, cfgProductModel.xml, cfgMAC.xml, cfgMAC, cfgMAC_override.xml, cfgdhcpt67.xml. By default, the Selected list contains the following configuration files in this order: cfgMAC.xml -> cfgMAC -> cfgProductModel.xml -> cfg.xml.
Automatic Upgrade	Choose "Yes" to enable automatic upgrade and provisioning. When set to No, GXW42XX will only do upgrade once at boot up. When "Check every day" or "Check every week" is checked, user can specify "Hour of the day (0-23)" or "Day of the week (0-6)". Default time is Monday 1AM.
Randomized Automatic Upgrade	With this feature enabled, device will specify a random time to upgrade the device within the range of hours of the day or postpone the upgrade every X minute(s) by random 1 to X minute(s)
Hour of the Day (0-23)	Define the hour of the day to check TFTP/HTTP/HTTPS/FTP/FTPS server for firmware upgrades or configuration files changes

Day of the Week (0-6)	Define the days of the week to check TFTP/HTTP/HTTPS/FTP/FTPS server for firmware upgrades or configuration files changes
Advanced Settings	
Validate Hostname in Certificate	This option controls whether the device should verify the server hostname against the Common Name (CN) or Subject Alternative Name (SAN) fields in the SSL certificate during HTTPS or FTPS provisioning and upgrade. No (0) (Default): The device does not validate the hostname in the certificate. This means the upgrade or provisioning process will proceed even if the server's SSL certificate does not match the actual hostname being used. While this increases flexibility, it may expose the device to man-in-the-middle (MITM) attacks if the server is not trusted. Yes (1): The device will validate the server hostname in the SSL certificate. The connection will only be accepted if the hostname in the URL matches the certificate's CN or SAN values. This enhances security by ensuring the device is communicating with the intended and authenticated server.
Always send HTTP Basic Authentication Information	Default is No. If set to Yes, device will send configured user name and password within HTTP request before server sends authentication challenge.
Configuration File Types Allowed	Allow users to choose Allowed Configuration File Types, All or XML Only, and Set by default to All.

Web/SSH Access

HTTP Web Port	Configures the HTTP port. This field is for customizing the web port.The default setting is "80".
HTTPS Web Port	Configures the HTTPS port. This field is for customizing the web port.The default setting is "443".
Web Access Mode	Specifies Web Access Protocol. The available options are: HTTPS HTTP Disabled The default setting is "HTTPS".
Disable SSH	Disables SSH access. The default setting is "No".
SSH Port	Configures the SSH access port number.The default setting is "22".
Security Controls for SSH Access	Selects the security privileges for the SSH Access users. The available options are: Only Allow SSH private IP users to set system Pvalue Allow all SSH users to set system Pvalue Allow all SSH users to set any Pvalue Prohibit setting Pvalue The default setting is: "Allow all SSH users to set any Pvalue"
Enable Web/SSH Access	Selects how web/SSH service can be accessed. The available options are: No: All web/SSH related requests will be rejected. Yes: All web/SSH related requests will be allowed. Auto: All web/SSH related requests from private IP address will be allowed while web/SSH related requests from public IP address will be rejected. The default setting is "Yes".
Web Session Timeout	Specifies the idle time in minutes before the web session is logged out.The default setting is "10" minutes. The valid range is 1-60 minutes.
Web Access Attempt Limit	Specifies the maximum number of failed login attempts before the web access is locked out.The default setting is "5". The valid range is 1-10.
Lockout Time Interval	Specifies the lockout duration after the number of failed login attempts configured in Web Access Attempt Limit is reached.The default setting is "15" minutes. The valid range is 1-15 minutes.
Disable User Level Web Access	Disables User-level access to the web UI.The default setting is "Yes".
Disable Viewer Level Web Access	Disables Viewer-level access to the web UI.The default setting is "Yes".
Viewer Password	
New Password	Sets new password for Web GUI access as Viewer. This field is case sensitive with a maximum length of 30 characters.
Confirm Password	Confirms the new password entered in the New Password field.
User Password	

New Password	Sets new password for Web GUI access as User. This field is case sensitive with a maximum length of 30 characters.
Confirm Password	Confirms the new password entered in the New Password field.
Admin Password	
New Password	Sets new password for Web GUI access as Admin. For GXW42xx V1: The Password must contain 1-30 characters. For GXW42xx V2: The password must contain 8-30 characters, at least one number, one uppercase, and one lowercase letter.
Confirm Password	Confirms the new password entered in the New Password field.
Strict Password Rules	
Enable strict password rules	Enables or disables strict password rules, including the required password length, number of character classes, and allowed character classes.The default setting is "Yes".
Minimum password length	Specifies the minimum password length.The default setting is "8".
Required character classes	Specifies the number of character classes required in the password.The default setting is "3".
Allowed Character classes	Specifies the character classes allowed in the password. The default setting is "Lower case, upper case, numbers".
Access Control Lists	
White list for WAN side	Specifies the IP addresses allowed to access the Web GUI and SSH from the WAN side. Multiple IP addresses are supported and must be separated by spaces. Example: 192.168.5.222 192.168.5.223 192.168.7.0/24
Block list for WAN side	Specifies the IP addresses blocked from accessing the Web GUI and SSH from the WAN side. Multiple IP addresses are supported and must be separated by spaces. Example: 192.168.5.222 192.168.5.223 192.168.7.0/24

TR-069

Enable TR-069	Enables or disables TR-069 service.The default setting is "Yes".Notes: For the GXW42xx V2, firmware 1.0.13.2 comes with the possibility to configure special features with the GIBTELECOM service provider via TR-069. TR-069 now supports Extensible Messaging and Presence Protocol (XMPP) connections.
ACS URL	Configures the TR-069 Auto Configuration Server. (e.g., http://acs.mycompany.com, or IP address).
ACS Username	Specifies the ACS Username for TR-069.
ACS Password	Specifies the ACS Password for TR-069.
Periodic Inform Enable	Enables or disables periodically sending Inform messages to the TR-069 Auto Configuration Server.The default setting is "No".
Periodic Inform Interval	Specifies the interval for sending Inform messages to the TR-069 Auto Configuration Server.The default setting is "300".
Connection Request Username	Specifies the username used by the TR-069 Auto Configuration Server to connect to the device.
Connection Request Password	Specifies the password used by the TR-069 Auto Configuration Server to connect to the device.
Connection Request Port	Specifies the port used by the TR-069 Auto Configuration Server to connect to the device.The default setting is "7547".
CPE SSL Certificate	Specifies the CA certificate used to authenticate the TR-069 Auto Configuration Server's TLS certificate.
CPE SSL Private Key	Specifies the private key for the CPE SSL certificate. The maximum length is 2048 characters.

SNMP

Enable SNMP	Enables or Disables the SNMP feature. The default setting is "No".
SNMP Version	Selects the version of SNMP Agent. The available options are: Version 1 Version 2c Version 3 The default setting is "Version 3".
SNMP Port	Configures the listening port of SNMP Daemon.The default setting is "161".
SNMP Trap IP Address	Specifies the IP address of the SNMP trap receiver. Up to 3 different servers can be configured to receive SNMP traps. Separate the trap server addresses with commas.
SNMP Trap Port	Configures the port of the SNMP trap receiver The default setting is "162".
SNMP Trap Version	Selects the version of SNMP Trap. The available options are: Version 1 Version 2c Version 3 The default setting is "Version 2c".
SNMP Trap Interval	Specifies the interval between each trap sent to the trap receiver. The default setting is "5".
SNMPv1/v2c Community	Specifies the SNMPv1/v2c community name.
SNMPv1/v2c Trap Community	Specifies the SNMPv1/v2c trap community name. It must match the community string configured on the trap receiver.
SNMPv3 User Name	Specifies the username for the SNMPv3 user.
SNMPv3 Security Level	Selects the security level for the SNMPv3 user. The available options are: noAuthUser: Users with security level noAuthnoPriv and context name noAuth. authUser: Users with security level authNoPriv and context name auth. privUser: Users with security level authPriv and context name priv. The default setting is "noAuthUser".
SNMPv3 Authentication Protocol	Selects the authentication protocol for the SNMPv3 user. The available options are: None MD5 SHA The default setting is "None".
SNMPv3 Privacy Protocol	Selects the privacy protocol for the SNMPv3 user. The available options are: None DES AES AES128 The default setting is "None".
SNMPv3 Authentication Key	Configures the authentication key for the SNMPv3 user.
SNMPv3 Privacy Key	Configures the privacy key for the SNMPv3 user.
SNMPv3 Trap User Name	Specifies the username for the SNMPv3 trap user.
SNMPv3 Trap Security Level	Selects the security level for the SNMPv3 trap user. The available options are: noAuthUser: Users with security level noAuthnoPriv and context name as noAuth. authUser: Users with security level authNoPriv and context name as auth. privUser: Users with security level authPriv and context name as priv. The default setting is "noAuthUser".
SNMPv3 Trap Authentication Protocol	Selects the authentication protocol for the SNMPv3 trap user. The available options are: None MD5 SHA The default setting is "None".
SNMPv3 Trap Privacy Protocol	Selects the privacy protocol for the SNMPv3 trap user. The available options are: None DES AES AES128 The default setting is "None".
SNMPv3 Trap Authentication Key	Configures the authentication key for the SNMPv3 trap user.
SNMPv3 Trap Privacy Key	Configures the privacy key for the SNMPv3 trap user.
Download MIB	Downloads the MIB file.

RADIUS

RADIUS for Web Access Authentication	
Enable RADIUS Web Access Control	Enables or disables RADIUS for web access.The default setting is "No".
Action upon RADIUS Auth Server Error	Specifies the action taken when the RADIUS authentication server encounters an error. The available options are: Reject Access Authenticate Locally The default setting is "Authenticate Locally".

RADIUS Auth Protocol	Specifies the RADIUS authentication protocol. The available options are: PAP (Password Authentication Protocol): PAP sends the username and password in plaintext, making it less secure than other methods. CHAP (Challenge Handshake Authentication Protocol): CHAP uses a challenge-response mechanism for authentication, enhancing security. MsCHAPv1 (Microsoft Challenge Handshake Authentication Protocol version 1): An older Microsoft-specific CHAP variant. MsCHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2): A more secure and improved Microsoft-specific CHAP variant with mutual authentication support. The default setting is "PAP".
RADIUS Auth Server Address	Configures the address of the RADIUS authentication server.
RADIUS Auth Server Port	Specifies the port of the RADIUS authentication server. The default setting is "1812".
RADIUS Shared Secret	Specifies the shared secret used for communication with the RADIUS server.
RADIUS VSA Vendor ID	Specifies the RADIUS Vendor-Specific Attribute (VSA) Vendor ID to match the RADIUS server configuration. The default setting is "42397".
RADIUS VSA Access Level Attribute	Specifies the RADIUS VSA attribute ID for the access level to match the RADIUS server configuration. The default setting is "35". Note: An incorrect setting causes RADIUS authentication to fail.
RADIUS for Call	
Primary RADIUS Server	Configures the address of the primary RADIUS server used for calls.
Primary RADIUS Authentication Port	Specifies the port used for RADIUS authentication. The default setting is "1812".
Primary RADIUS Account Port	Specifies the account port of the primary RADIUS server. The default setting is "1813".
Primary RADIUS Server Secret	Specifies the shared secret for the primary RADIUS server.
Secondary RADIUS Server	Specifies the address of the secondary RADIUS server used for calls.
Secondary RADIUS Authentication Port	Specifies the port used for authentication with the secondary RADIUS server. The default setting is "1812".
Secondary RADIUS Account Port	Specifies the account port of the secondary RADIUS server. The default setting is "1813".
Secondary RADIUS Sever Secret	Specifies the shared secret for the secondary RADIUS server.
RADIUS Timeout	Specifies the time, in seconds, the device waits for a response from the RADIUS server before timing out. The default setting is "2". The valid range is 1-65535.
RADIUS Retry	Specifies the number of times the device retries a RADIUS request after a timeout. The default setting is "3". The valid range is 1-65535.

DDNS

Enable DDNS	Enable or disables the DDNS feature. The default setting is "No".
DDNS Server	Selects the DDNS server. The available options are: dyndns.org freedns.afraid.org zoneedit.com no-ip.com oray.net cloudflare.com The default setting is "dyndns.org".
DDNS Username	Configure the username of DDNS server.
DDNS Password	Configure the password of DDNS server.
DDNS Hostname	Configure the hostname of DDNS server.
DDNS Hash	Configure the hash of DDNS server.

802.1x

802.1X Mode	Enables or disables 802.1X authentication. The available options are: Disable EAP_MD5 EAP_TLS EAP-PEAPv0/MSCHAPv2 The default setting is "Disable".
802.1X Identity	Configures the Identity used for the 802.1X mode.
MD5 Password	Configures the password used for EAP-MD5 authentication.
802.1X CA Certificate	Upload: Uploads the .pem certificate file for EAP-PEAPv0/MSCHAPv2 or EAP-TLS authentication. Delete: Deletes the uploaded file.
802.1X Client Certificate	Upload: Uploads the .pem file containing both the client certificate and private key for EAP-TLS authentication. Delete: Deletes the uploaded file.

VPN

OpenVPN(R) Settings	
OpenVPN Enable	Enables or disables the OpenVPN(R) feature.The default setting is "No".
OpenVPN(R) Server Address	Specifies the IP address or FQDN of the OpenVPN(R) server.
OpenVPN(R) Port	Specifies the port used by the OpenVPN(R) server.The default setting is "1194".
OpenVPN(R) Server Secondary Address	Specifies the IP address or FQDN of the secondary OpenVPN(R) server.
OpenVPN(R) Secondary Port	Specifies the port used by the secondary OpenVPN(R) server.The default setting is "1194".
Randomly Select Server	Enables or disables random server selection. The available options are: Yes: The device attempts to establish VPN connection randomly to one of the configured OpenVPN(R) servers. No: The device attempts to connect to the configured servers in the order they are listed. The default setting is "No".
Interface type	Specifies whether the interface type is Bridge (TAP) or Router (TUN).The default setting is "TUN".
OpenVPN(R) Transport	Specifies whether the OpenVPN(R) transport type is UDP or TCP. The default setting is "UDP".
Enable LZO Compression	Enables or disables LZO compression for the VPN connection.The default setting is "Yes".Note: Enable this option only if LZO compression is also enabled on the OpenVPN(R) server.
OpenVPN(R) Encryption	Specifies the encryption algorithm used for OpenVPN(R). The available options are: BF-CBC 128 bit default key (variable) Default DES-CBC 64 bit default key (fixed) RC2-CBC 128 bit default key (variable) DES-EDE-CBC 128 bit default key (fixed) DES-EDE3-CBC 192 bit default key (fixed) DESX-CBC 192 bit default key (fixed) RC2-40-CBC 40 bit default key (variable) CAST5-CBC 128 bit default key (variable) RC2-64-CBC 64 bit default key (variable) AES-128-CBC 128 bit default key (fixed) AES-192-CBC 192 bit default key (fixed) AES-256-CBC 256 bit default key (fixed) AES-128-GCM 128 bit default key (fixed) AES-256-GCM 256 bit default key (fixed) CHACHA20-POLY1305 256 bit default key (fixed) The default setting is "BF-CBC 128 bit default key (variable) Default".
OpenVPN(R) Digest	Specifies the digest algorithm used for OpenVPN(R).The default setting is "SHA1".
OpenVPN(R) Username	Specifies the username used for OpenVPN(R) authentication. This field is optional and the maximum length is 32 characters.
OpenVPN(R) Password	Specifies the password used for OpenVPN(R) authentication. This field is optional and the maximum length is 32 characters.
OpenVPN(R) CA	Upload: Uploads the OpenVPN(R) Certification Authority (CA) certificate. Delete: Deletes the existing OpenVPN(R) Certification Authority (CA) certificate. Note: Expects a ca.crt file.

OpenVPN(R) Certificate	Upload: Uploads the OpenVPN(R) client certificate. Delete: Deletes the existing OpenVPN(R) client certificate. Note: Expects a client.crt file.
OpenVPN(R) Client Key	Upload: Uploads the OpenVPN(R) client private key. Delete: Deletes the existing OpenVPN(R) client private key. Note: Expects a client.key file.
OpenVPN(R) Client Key Password	Specifies the password used to decrypt the OpenVPN(R) Client Key.
OpenVPN(R) TLS Key	Expects a .key file. Maximum length is 8192 characters. Upload: Uploads a static TLS key used to secure OpenVPN(R) connections. Delete: Deletes the existing OpenVPN(R) TLS key. Note: The TLS key is used for HMAC authentication or encryption of the control channel, depending on the selected OpenVPN(R) TLS Key Type.
OpenVPN(R) TLS Key Type	Selects the encryption type of the OpenVPN(R) TLS key. The available options are: None. TLS-Auth: Provides authentication only for the control channel. TLS-Crypt: Encrypts and authenticates the control channel. TLS-Crypt V2: Encrypts and authenticates the control channel using TLS-Crypt V2. The default setting is "None".
OpenVPN(R) Additional Options	Specifies additional OpenVPN(R) options to append to the OpenVPN(R) configuration file. Additional options must be separated by semicolons. Example: connect-retry 5;tls-client;keepalive 10 60 Caution: Ensure that the specified options are supported by OpenVPN(R) and do not override other configurations.

Security Settings

Security

SIP TLS Certificate	Specifies the user-provided SSL certificate used for SIP over TLS. The certificate is in X.509 format. The GXW42XX series has a built-in private key and SSL certificate.
SIP TLS Private Key	Specifies the user-provided private key in X.509 format for SIP over TLS.
SIP TLS Private Key Password	Specifies the password for the SSL private key used for SIP over TLS/TCP.
Custom Certificate	Specifies a custom CA-signed certificate and private key to the device for client authentication.
Validate Server Certificates	Enables or disables server certificate validation against Grandstream's trusted list for TLS connections. The device must reboot for the setting to take effect. The default setting is "No".
Keep Security Setting After Reset	Enables or disables retaining security-related and trusted CA settings after a factory reset. This feature depends on the Reset Lock setting. The default setting is "No".
Disable Weak TLS Cipher Suites	Configures which weak TLS cipher suites and related algorithms or protocol versions are disabled. The available options are: Enable Weak TLS Ciphers Suites Disable Symmetric Encryption RC4/DDES/3DES Disable Symmetric Encryption SEED Disable Symmetric Encryption IDEA/eNULL Disable All Of The Above Weak Symmetric Encryption Disable Symmetric Authentication MD5 Disable All Of The Above Weak Symmetric Authentication Disable Protocol Version SSLv2/SSLv3 Disable All Of The Above Weak Protocol Version Disable Server Authentication aNULL/aECDH Disable All Of The Above Weak Server Authenticaion Disable Key Exchange Algorithm kRSA Disable All Of The Above Weak Key Exchange Algorithm Disable All Of The Above Weak TLS Ciphers Suites The default setting is "Disable All Of The Above Weak TLS Ciphers Suites".
Minimums TLS Version	Selects the minimum TLS version supported by the device. The available options are: Unlimited TLS 1.0 TLS 1.1 TLS 1.2 TLS 1.3 The default setting is "TLS 1.2".
Maximum TLS Version	Selects the maximum TLS version supported by the device. The default setting is "Unlimited".

Trusted CA

Trusted CA Certificate (A, B, C, D)	Configures the Trusted CA Certificate(s). The certificate entered here is used as a trusted CA to authenticate the server's TLS certificate.
Load CA Certificates	Selects which CA Certificates the gateway trusts. The available options are: Built-in trusted certificates: The gateway will verify the server certificate based on the built-in trusted certificates list. Custom trusted certificates: The gateway will verify the server certificate based on the custom trusted certificates list previously uploaded by the user. All trusted certificates: The gateway will verify the server certificate based on the built-in and custom trusted certificates. The default setting is "Built-in Trusted Certificates".

Date and Time

NTP Server	Specifies the URI or IP address of the NTP (Network Time Protocol) server used to synchronize the device's date and time. An extensive list of public NTP servers can be found at http://www.ntp.org . The default setting is "pool.ntp.org".
Secondary NTP server	Specifies the URI or IP address of the secondary NTP server used to obtain the device's date and time.
NTP Update Interval	Specifies the interval, in minutes, at which the device synchronizes its date and time with the NTP server. The default setting is "60".
Allow DHCP Option 42 to NTP Server	Enables or disables the ability to change the NTP server through DHCP Option 42. When enabled, the NTP server address can be changed through DHCP. The default setting is "Yes".
Time Zone	Specifies the time zone used to configure the device's local date and time. The device adjusts for daylight saving time (DST) according to the selected time zone, where applicable, ensuring accurate timekeeping across regions that observe seasonal time changes. Recent updates have expanded the list of supported zones to improve alignment with regional DST rules, including locations in the Middle East.
Self-Defined Time Zone	Specifies a custom time zone.
Allow DHCP Option 2 to override time zone	Enables or disables the use of DHCP Option 2 to override the device's time zone setting. The default setting is "Yes".
Local Time	Synchronizes the device's date and time with the host PC's time through the web browser. Click Sync PC to synchronize the time. A pop-up window confirms successful synchronization.

Syslog

Syslog Protocol	Selects the protocol used to send syslog messages. The available options are: UDP SSL/TLS The default setting is "UDP".
Syslog Server	Specifies the IP address or URL of the syslog server that collects system log information from the device. Note: To retain syslog settings and internal logs after a factory reset, enable P-value P82307 in the device configuration file. The available values are 0 (No) and 1 (Yes). The default setting is 0 (No).
Syslog Level	Selects the syslog level reported by the gateway. The available options are: NONE DEBUG INFO WARNING ERROR EXTRA DEBUG The default setting is "None". Syslog messages are sent based on the following events: Product model/version on boot up (INFO level) NAT related info (INFO level) Sent or received SIP message (DEBUG level) SIP message summary (INFO level) Inbound and outbound calls (INFO level) Registration status change (INFO level) Negotiated codec (INFO level) Ethernet link up (INFO level) SLIC chip exception (WARNING and ERROR levels) Memory exception (ERROR level) The Syslog uses USER facility. In addition to standard Syslog payload, it contains the following components: GS_LOG: [device MAC address][error code] error message Example: May 19 02:40:38 192.168.1.14 GS_LOG: [00:0b:82:00:a1:be][000] Ethernet link is up

Syslog Header Format	Selects the Syslog Header Format, When set to "RFC3164-compliant", the syslog header will contain the PRI and timestamp information to be compatible with RFC3164. The default setting is "Default".
Print SIP in Syslog	Enable or disable printing of full SIP messages in Syslog. The default setting is "No".
SIP Log Option	Selects how SIP log files are handled when the allocated storage is full. By default, the device divides the allocated SIP log storage into two files of equal size. When the first file is full, the device creates the second file. The available options are: Keep: Retains existing SIP log files when both files are full. No new records are stored. Overwrite: Clears the first SIP log file and resumes storing records. The default setting is "Overwrite".
Save Syslog	Saves syslog messages to the device. The device stores syslog messages in three rotating files, each with a maximum size of 3 MB. Note: Scroll down to Syslog List and The List for SIP Log Files to download the saved logs.
The List for SIP log Files	
Download	Downloads the SIP log file as a .log file.
Delete	Deletes the SIP log file.
Preview	Redirects to the Preview SIP log page, which displays SIP messages exchanged by the device.

Call Record

CDR record option	Selects how the device handles CDR records when the allocated storage is full. By default, the device divides the allocated CDR storage into two files of equal size. The device creates the first file and, when it is full, creates the second file. The available options are: Keep: Retains existing call records when both files are full. No new records are stored. Overwrite: Clears the first CDR file and resumes storing records. The default setting is "Overwrite".
Download	Downloads the CDR records as a .csv file.
Delete	Deletes the CDR records.
Preview	Redirects to Preview Call Record, which displays the following call record information: UserId ToNumber FromNumber StartTime StartTalkTime EndTime Duration State Direction

Port Record

Port	Specifies the port ID for port recording. The valid range is 1 to the maximum port ID.
Status	Displays the port recording status, indicating whether recording is stopped or in progress. For example: No port is recording or Port 1 is recording now.
The List for Port Record pcm Files	
Download	Downloads the captured .tgz file.
Start	Starts recording on the configured port.
Stop	Stops recording on the configured port.

This feature can only be used for debugging purpose, please delete all files after finishing debugging.

Ethernet Capture

With Secret Key information	Enables or disables the inclusion of secret key information in the packet capture file.The default setting is "Yes".
Status	Displays the Ethernet packet capture status: Stopped or Running.
The List for Ethernet pcap Files	
Download	Downloads the captured .tgz file.
Delete	Deletes the captured file.
Start	Starts the Ethernet packet capture.
Stop	Stops the Ethernet packet capture.

This feature can only be used for debugging purposes, please delete all files after finishing debugging.

Remote Diagnostics

Status	Displays the Remote Diagnostics status.
Start	Enables Remote Diagnostics.
Stop	Disables Remote Diagnostics.

When running, the device will allow remote access and remote collection of logs. It will automatically end when it expires.

Advanced Settings

Ring Tones	
System Ring Cadence	Configures the ring cadence for incoming calls on all FXS ports.(Syntax: c=on1/off1-on2/off2-on3/off3; [...]) The default setting is "c=2000/4000;" (US standards)

Call Progress Tones	<p>Configures the tone frequencies according to user preference. By default, the tones are set to North American frequencies. Frequencies should be configured with known values to avoid uncomfortable high pitch sounds. ON is the period of ringing (ON time in ms) while OFF is the period of silence. In order to set a continuous ring, OFF should be zero. Otherwise, it will ring ON ms and a pause of OFF ms and then repeat the pattern. The below tones can be configured with the following syntax : f1=val, f2=val[, c=on1/ off1[- on2/ off2[- on3/ off3]]]; (Frequencies are in Hz and cadence on and off are in 1 ms units) Dial Tone: This tone signals that the system is ready for dialing. Ringback Tone: This tone indicates to the originator of the call that the receiving party's device is alerting. Busy Tone: This tone is used to indicate that the dialed number is busy. Reorder Tone: This tone signals to the calling party that the call cannot be processed through the network. Confirmation Tone: This tone is used as an acknowledgement for a processed request. Call-Waiting Tone: This tone is used during an ongoing call to indicate that a new call is waiting. Prompt Dial Tone: This tone prompts the user to trigger an action such as dialing a destination number or a code. Conference Party Hangup Tone: If a user in the conference hangs up, the rest of the users will hear this tone. Conference Notification Tone: This is used to notify the user of a connection to a conference call. (GXW42xx V2 only) Special Proceed Indication Tone: This feature allows users to configure the special process indicator tone for the voice mail, the device will play the MWI tone when the user picks up. The default is the Stuttgart dial tone. (GXW42xx V2 only) Special Condition Tone: This feature allows users to configure the special condition tone. When a user is activated using the GIBTELECOM in Special Feature, the SIP server sends a NOTIFY with "special-condition-tone", "Special Condition Tone" will be played instead of the "Dial Tone". (GXW42xx V2 only) Remote On Hold Tone: This feature allows users to configure the remote on hold tone that will be played when the FXS port puts the other party on hold. (GXW42xx V2 only) Dial Tone when Call Forward Active: This feature allows users to configure dial tone for call forwarding features on the FXS Port. (GXW42xx V2 only) Please refer to the document below to determine your local call progress tones: http://www.itu.int/ITU-T/inr/forms/files/tones-0203.pdf</p>
FXO Failover	
Failover to FXO Gateway	Enable or disable the Failover FXO Gateway. The default setting is "Disabled".
FXO Gateway IP	Configures the IP Address or URI of the FXO gateway.
System Features	
Disable Direct IP Call	Disables or enables the Direct IP Call function. When set to "Yes", direct IP-to-IP calling is not supported. The default setting is "No".
Inter-port Calling	Enables or disables inter-port calling. When enabled, an unregistered FXS port can use its extension for inter-port dialing instead of ***7xx. Calls between unregistered ports do not route the INVITE to the SIP server. The default setting is "Disabled".
Enable SIP NOTIFY Authentication	Enables or disables authentication challenges for SIP NOTIFY reboot and resync messages. The default setting is "Yes".
Disable Voice Prompt	Disables or enables the voice prompt configuration. When set to "Yes", the integrated voice menu is inaccessible. The default setting is "No".
IVR Language	Selects the IVR Language. The supported languages are: English Chinese Russian Spanish The default setting is "English".
Upload/Delete Language Pack	Upload: Uploads a language package to the device. Delete: Deletes an existing language package from the device.
LCD Display Language	Selects the LCD display language. The supported languages are: English Chinese French Spanish The default setting is "English".
Prompt Dial Tone Code	Configures the prompt dial tone code to simulate an analog PBX where a code is required to dial an outside line.

Port Lock Code	Specifies the port lock code used with the star code to lock or unlock a specific port for outbound calls. The default setting is "21".The default is *21. The user is required to press *21 and the four-digit locking code twice to set the lock code. To set the lock code, press *21 followed by the four-digit locking code twice. To make a call from a locked port, press *21, enter the locking code, and then dial the destination number. If no locking code is configured, dial the destination number directly.
Play Busy Tone When Account is unregistered	Enables or disables playing the busy tone when a user goes offhook from an unregistered account.The default setting is "No".
Hunting Group Registration Mode	Select the hunting group registration mode. The available options are: Active Port Only: Only the active port will be registered within the group. All Ports: All ports within the group will be registered. The default setting is "Active Port Only".
Country Specific Deployment	Selects the tones to match the country's specifications. The available options are: None(default) USA China China ITSP Germany
Automatic Reboot	Selects the automatic reboot schedule. When a reboot schedule is selected, specify the corresponding schedule time options. The available options are: No Yes, reboot every day Yes, reboot every week Yes, reboot every month The default setting is "No".
Hour of the Day (0-23)	Defines the hour of the day to reboot the gateway.
Day of the Week (0-6)	Defines the day of the week to reboot the gateway.
Day of the Month (1-31)	Defines the day of the month to reboot the gateway.
Reset Type	Selects the type of reset to perform via the Preform Selected Reset button. The available options are: ISP Data Reset VoIP Data Reset Full Reset The default setting is "Full Reset".
Perform Selected Reset	Performs the selected reset type in Reset Type.
LED Pattern	Selects the LED pattern. The available options are: Pattern A: Onhook: OFF; Offhook: On; Voicemail: Blink Pattern B: Onhook: On; Offhook: Off; Voicemail: Blink if the phone is on the hook. Pattern C: Onhook and Registered: On; Offhook: Blink; Voicemail: Blink 1sec ON/1sec OFF The default setting is "Pattern A".
Static DNS	
A Record Settings	
Name	Configures the domain name to which the record refers. The maximum supported length is 256 characters.
TTL	Configures the Time to Live, which is the time interval that the record may be cached before the source of the information should be consulted again.The default setting is "300". The valid range is from 300 to 65535.
Address	Configures theIP address associated with the domain. The maximum supported length is 64 characters.
SRV Settings	
Name	Configures the domain name to which the record refers.The maximum supported length is 256 characters. Notes: When a SIP server returns a 5XX response, the device can automatically switch to an available backup IP address obtained through DNS SRV When a SIP server returns a 5XX response, the device can automatically switch to an available backup IP address obtained through DNS SRV During an active session established through a secondary SBC after DNS SRV failover, the device prevents REGISTER and UPDATE requests from being sent to the primary SBC.
TTL	Configures the Time to Live, which is the time interval that the record may be cached before the source of the information should be consulted again. The default setting is "300". The valid range is from 300 to 65535.

Priority	Specifies the priority of target hosts that provide the service. Lower values indicate higher priority. Target hosts with the same priority are selected according to the Weight setting. The default setting is "0". The valid range is from 0 to 65535.
Weight	Specifies the weight for entries with the same priority. Larger weight will get higher priority. The default setting is "0". The valid range is from 0 to 65535.
Port	Specifies the port on the target host of the specified service. The default setting is "0". The valid range is from 0 to 65535.
Target	Configures the domain name of the target host. The maximum supported length is 64 characters.
NAPTR Settings	
Name	Configures the domain name to which this resource record refers. The maximum supported length is 256 characters.
TTL	Configures the Time to Live, which is the time interval that the record may be cached before the source of the information should be consulted again. The default setting is "300". The valid range is from 300 to 65535.
Order	Specifies the order in which NAPTR records are processed. Lower values are processed before higher values. The default setting is "0". The valid range is from 0 to 65535.
Preference	Specifies the preference for processing NAPTR records with the same Order value. Lower values are processed before higher values. The default setting is "0". The valid range is from 0 to 65535.
Flags	Specifies the action to perform after the NAPTR lookup. The available flags are: S: The next lookup is an SRV record lookup. A: The next lookup is an A, AAAA, or A6 record lookup. U: Indicates that the next step is not a DNS lookup, but that the output of the Regexp field is a URI that adheres to the "absoluteURI" syntax. P: The remaining lookup steps are defined by the application using the NAPTR record.
Service	Specifies the services available in this domain. The Replacement field is used to locate the specified service. The maximum length is 64 characters. It can also specify the protocol used to communicate with the server that offers the service. In SIP, the following services are defined along with their resolution services (the resolution services are defined after the + sign): SIPS+D2T: Secure SIP, TLS over TCP. SIP+D2T: SIP over TCP. SIPS+D2S: Secure SIP, TLS over SCTP. SIP+D2S: SIP over SCTP. SIP+D2U: SIP over UDP. The default setting is "SIP+D2U".
Regexp	Configures a substitution expression that is applied to the original string held by the client to construct the next domain name to look up.
Replacement	Specifies the next FQDN to query for NAPTR, SRV, or address records, depending on the Flags value.

Profiles

General Settings	
Profile Active	Enables or disables the SIP profile. The default setting is "No".
SIP Server	Specifies the IP address or domain name of the SIP server provided by the VoIP service provider.
Failover SIP Server	Specifies the IP address or domain name of the failover SIP server provided by the VoIP service provider. The failover server is used when the primary SIP server becomes unavailable.
Prefer Primary SIP Server	Specifies how the gateway prioritizes the primary SIP server when a failover SIP server is configured. The available options are: No: No SIP server is preferred. Will register to primary server if failover server registration expires: Prioritizes the primary server when the failover server registration fails. Will register to primary server if primary server responds: Prioritizes primary server when it is responsive. The default setting is "No".

Primary Outbound Proxy	Specifies the IP address or domain name of the primary Outbound Proxy, Media Gateway, or Session Border Controller. The Outbound Proxy can be used to facilitate firewall or NAT traversal.
Backup Outbound Proxy	Specifies the backup Outbound Proxy used when the primary Outbound Proxy is unreachable.
Prefer Primary Outbound Proxy	Enables or disables prioritizing the primary Outbound Proxy. When enabled, the gateway re-registers through the primary Outbound Proxy when the registration expires. The default setting is "No".
Network Settings	
Layer 3 QoS Settings	
SIP Diff-Serv	Defines the Layer 3 QoS parameter for SIP signaling. This value is used for IP Precedence, Diff-Serv or MPLS. The default setting is "26". The valid range is 0 to 63.
RTP Diff-Serv	Defines the Layer 3 QoS parameter for RTP media. This value is used for IP Precedence, Diff-Serv or MPLS. The default setting is "46". The valid range is 0 to 63.
DNS Settings	
DNS Mode	Selects the DNS lookup method used to resolve the SIP server. The available options are: A Record: Resolves the IP address of the target using its domain name. SRV: Uses DNS SRV records to locate the service for various protocols. NAPTR/SRV: Uses NAPTR records according to RFC 2915 to determine the appropriate SRV records. Use Configured IP: Uses the configured IP addresses. Primary IP, Backup IP 1, and Backup IP 2 must be configured. The default setting is "A Record".
DNS SRV Use Registered IP	Enables or disables using the registered IP address as the INVITE destination instead of the highest-priority IP address from the resolved IP list. The default setting is "No". GXW42xx V1 only.
DNS SRV Failover Mode	Configures the preferred DNS SRV failover method. The available options are: Default: Attempts the primary SIP server or Outbound Proxy first for all REGISTER and INVITE requests. Use Current Server Until DNS TTL: Sends all SIP messages to the current failover SIP server or Outbound Proxy until the DNS TTL expires. Use Current Server Until No Response: Sends all SIP messages to the current failover SIP server or Outbound Proxy until it stops responding. Use Current Server Until Failback Timer Expires: Sends all SIP messages to the current failover SIP server or Outbound Proxy until the failback timer expires. The default setting is "Default". GXW42xx V2 only.
Failback Timer	Specifies the duration, in minutes, that the device remains on the failover Outbound Proxy before attempting to fail back to the primary Outbound Proxy. The default setting is "60". The valid range is 1 to 64800 minutes. GXW42xx V2 only.
Register Before DNS SRV Failover	Enables or disables sending a new registration request before directing non-registration SIP requests to the newly selected server. The default setting is "No". GXW42xx V2 only.
Maximum Number of SIP Request Retries	Specifies the maximum number of SIP request retries before failover. The default setting is "2". The valid range is 1 to 10. GXW42xx V2 only.
Primary IP	Configures the primary IP address where the phone sends DNS query to when "Use Configured IP" is selected for DNS mode.
Backup IP 1	Configures the backup IP 1 address where the phone sends DNS query to when "Use Configured IP" is selected for DNS mode.
Backup IP 2	Configures the backup IP 2 address where the phone sends DNS query to when "Use Configured IP" is selected for DNS mode.
NAT Settings	

NAT Traversal	Configures the NAT traversal. The available options are: No: Disables NAT traversal, potentially causing connection issues for the ATA if it's behind a NAT router. Keep-alive: Periodically sends signals to maintain the NAT mapping for the ATA, preventing disconnection. STUN: Utilizes the STUN protocol to discover and adapt to NAT settings for seamless VoIP communication. UPnP: Allows the ATA to dynamically configure NAT port mappings, streamlining VoIP traffic. VPN: Requires the ATA to establish a secure VPN connection for VoIP, bypassing NAT restrictions. Auto: Automatically selects the most suitable NAT traversal method based on network conditions, ensuring reliable ATA connectivity. Default setting is "No".
Use NAT IP	The NAT IP address used in SIP/SDP messages. It should ONLY be used if required by your ITSP.
Proxy-Require	A SIP Extension to notify the SIP server that the phone is behind a NAT/Firewall.
SIP Settings -> Basic Settings	
SIP Transport	Selects the transport protocol used for SIP signaling. The available options are: UDP TCP TLS/TCP The default setting is "UDP".
SIP URI Scheme When Using TLS	Specifies whether the "sip:" or "sips:" URI scheme is used when TLS/TCP is selected as the SIP transport.The default setting is "sips". GXW42xx V2 only.
SIP Registration	Enables or disables SIP registration with the proxy server.The default setting is "Yes".
Unregister on Reboot	Enables or disables unregistering when the device reboots.The default setting is "No".
Add Auth Header on Initial REGISTER	Enables or disables adding an Authorization header with a blank nonce to the initial REGISTER request.The default setting is "No".
Outgoing Calls Without Registration	Enables or disables placing outgoing calls when the SIP account is not registered. Incoming calls cannot be received when the account is not registered. Any port, member of a Hunting Group that is not registered with a SIP account, will be able to place outbound calls using the SIP credentials of the primary Hunting Group port.The default setting is "No". For example: Port 1, 3 and 5 are members of the same Hunting Group. Port 1 is registered with a SIP account. Ports 3 and 5 are not registered. Ports 3 and 5 will be able to place outbound calls using the SIP account of port 1, even if Outgoing Call without Registration is set to No.
Register Expiration	Specifies the registration expiration interval, in minutes, before the device refreshes its registration with the registrar.The default setting is "60". The valid range is 1 to 65535 minutes (about 45 days).
Subscribe Expiration	Specifies the subscription expiration interval, in minutes, subscription refreshes its subscription with the specified registrar.The default setting is "60". The valid range is 1 to 65535 minutes (about 45 days).
SIP Registration Failure Retry Wait Time	Specifies the retry interval, in seconds, before the device attempts to register again after a registration failure.The default setting is "20". The valid range is 1 to 3600 seconds.
SIP Subscription Failure Retry Wait Time	Specifies the retry interval, in seconds, before the device attempts to resubscribe when the subscription fails.The default setting is "0". The valid range is 0 to 3600 seconds.
SIP Registration Failure Retry Wait Time upon 403 Forbidden	Specifies the retry interval, in seconds, before the device attempts to register again after receiving a 403 Forbidden response. A value of 0 disables registration retries.The default setting is "1200". The valid range is 0 to 3600.
Reregister Before Expiration	Specifies the interval, in seconds, before registration expiration at which the device attempts to re-register.The default setting is "0".
Enable SIP OPTIONS/NOTIFY Keep Alive	Enables or disables SIP OPTIONS/NOTIFY keep-alive messages. The available options are: No OPTIONS NOTIFY The default setting is "No".
SIP OPTIONS/NOTIFY Keep Alive Interval	Specifies the interval, in seconds, between SIP OPTIONS/NOTIFY keep-alive messages.The default setting is "30".

SIP OPTIONS/NOTIFY Keep Alive Max Lost	Specifies the maximum number of consecutive lost SIP OPTIONS/NOTIFY keep-alive messages allowed before the device re-registers. The default setting is "3". The range is 3 to 10.
Switch SIP Server When Keep-Alive Max Lost Is Reached	Enables or disables switching to the next SIP server when the maximum number of lost SIP OPTIONS/NOTIFY keep-alive messages is reached. The default setting is "No". GXW42xx V2 only.
Local SIP Port	Specifies the local SIP port used by the device to send and receive SIP messages. The default setting is 5060 for Profile 1, 6060 for Profile 2, 7060 for Profile 3, and 8060 for Profile 4.
Use Random SIP Port	Enables or disables the use of random SIP ports instead of the configured local SIP port. This is usually necessary when multiple GXW42XX /HT50X are behind the same NAT. The default setting is "No".
Local RTP port	Specifies the local RTP port used by the device to send and receive RTP packets. The default setting is 50000 for Profile 1, 51000 for Profile 2, 52000 for Profile 3, and 53000 for Profile 4. Note: GXW42xx V2 supports calculating and adding checksum values to outbound UDP and RTP packets to improve packet integrity during transmission.
Use Random RTP Port	Enables or disables the use of a randomly generated RTP port instead of the configured local RTP port. The default setting is "Yes".
SIP T1 Timeout	Specifies the SIP T1 retransmission timer, which represents the estimated round-trip time between the device and the SIP server. The default setting is "0.5 sec". Note: If the network latency is high, select a larger value for more reliable usage.
SIP T2 Timeout	Specifies the maximum retransmission interval for non-INVITE requests and INVITE responses. The default setting is "4 sec".
SIP TIMER D	Specifies the SIP Timer D value defined in RFC 3261 in seconds. The default setting is "0". The valid range is 0 to 64.
SIP TIMER B	Specifies the SIP Timer B value defined in RFC 3261. The default setting is "0". The valid range is 0 to 128. GXW42xx V2 only.
SIP TIMER F	Specifies the SIP Timer F value defined in RFC 3261. The default setting is "0". The valid range is 0 to 128. GXW42xx V2 only.
Remove OBP from Route Header	Enables or disables removing the Outbound Proxy URI from the Route header. When enabled, the SIP extension notifies the SIP server that the extension is behind a NAT/Firewall. The default setting is "No".
Support SIP Instance ID	Enables or disables including the SIP Instance ID in the Contact header of REGISTER requests, as defined by the SIP Outbound specification. The default setting is "Yes".
Hold Target Before Refer	Enables or disables sending a re-INVITE to place the transfer target on hold before sending a REFER request. The default setting is "Yes".
Refer-To Use Target Contact	Enables or disables using the transfer target's Contact header information in the Refer-To header during an attended transfer. The default setting is "No".
SUBSCRIBE for MWI	Enables or disables sending periodic SUBSCRIBE requests for Message Waiting Indication (MWI). The default setting is "No".
Subscribe Retry Wait Time upon 403 Forbidden	Specifies the wait time, in minutes, before retrying a subscription request after receiving a 403 Forbidden response. This helps avoid unnecessary network congestion. If the value is not 0, device will retry 10 times first, then wait for the specified time before trying again. If the value is 0, device will follow "Retry-After" header if present. Otherwise, device will wait 20 minutes before sending subscribe again. The default setting is "0". The valid range is 0 to 10080. GXW42xx V2 only.
Enable 100rel	Enables or disables support for the SIP 100rel extension and the PRACK (Provisional Response Acknowledgement) method. When enabled, the 100rel tag is appended to the value of the required header in the initial signaling messages. The default setting is "No".

TEL URI	Selects the URI scheme used in SIP requests. The available options are: Disabled. User=Phone: Adds the User=Phone parameter to the Request-Line and To header to indicate the E.164 number. Recommended when the phone has an assigned PSTN telephone number. Enabled: Uses the tel: URI scheme instead of sip: in SIP requests. The default setting is "Disabled".
Use Routing ID in SIP Headers / Use Request Routing ID in SIP Headers	Enables or disables using the configured Routing ID in SIP headers. When enabled, the Routing ID is used instead of the SIP User ID in the From and Contact headers for outgoing calls. This option is typically used for SIP trunk account configurations. The setting is ignored if the Routing ID for the caller port is blank in Advanced Port Settings. The default setting is "No". GXW42xx V2 only.
Do Not Escape '#' as %23 in SIP URI	Enables or disables sending # as # instead of encoding it as %23 in the SIP URI. The default setting is "No".
Disable Multiple m Line in SDP	Enables or disables sending only one m line in the SDP, regardless of the number of m lines in the incoming SDP. The default setting is "No".
Use Privacy Header	Specifies whether the Privacy header is included in SIP messages. The available options are: Default: Adds the Privacy header only when the configured special feature is not Telkom SA or CBCOM. No: Does not add the Privacy header. Yes: Adds the Privacy header. The default setting is "Default".
Use P-Preferred-Identity Header	Specifies whether the P-Preferred-Identity (PPI) header is included in SIP INVITE messages. The available options are: Default: Adds the P-Preferred-Identity only when the configured special feature is not Telkom SA or CBCOM. No: Does not add the P-Preferred-Identity. Yes: Adds the P-Preferred-Identity. The default setting is "Default".
Use P-Access-Network-Info Header	Enables or disables including the P-Access-Network-Info header in SIP INVITE messages. The default setting is "Yes". GXW42xx V2 only.
Use P-Emergency-Info Header	Enables or disables including the P-Emergency-Info header in SIP INVITE messages. The default setting is "Yes". GXW42xx V2 only.
Use P-Asserted-Identity Header	Enables or disables including the P-Asserted-Identity header in SIP INVITE messages. The default setting is "No". GXW42xx V2 only.
Use P-Early-Media Header	Enables or disables including the P-Early-Media header in SIP INVITE messages. The default setting is "No". GXW42xx V2 only.
SIP REGISTER Contact Header Uses	Specifies whether the LAN or WAN address is used in the Contact header of SIP REGISTER requests. The default setting is "LAN Address".
Caller ID Display	Specifies how the caller ID is obtained from incoming SIP INVITE messages. The available options are: Auto: Checks the P-Asserted-Identity, Remote-Party-ID, and From headers, in that order, to obtain the caller ID. Disabled: Displays Unavailable for all incoming calls. From Header: Uses the From header to obtain the caller ID. The default setting is "Auto".
Use Actual Ephemeral Port in Contact with TCP/TLS	Enables or disables the use of the actual ephemeral port in the Via and Contact headers when TCP/TLS is selected as the SIP transport. When disabled, the device uses the permanent listening port. When enabled, the device uses the ephemeral port assigned to the connection. The default setting is "No".
Allow SIP Factory Reset	Enables or disables factory resetting the device through a SIP NOTIFY message. The default setting is "No". GXW42xx V2 only.
Ignore Alert-Info Header	Enables or disables ignoring the Alert-Info header and playing the default ringtone. The default setting is "No". GXW42xx V2 only.
SIP User-Agent	Configures the SIP User-Agent value. The User-Agent header is constructed using the configured SIP User-Agent and SIP User-Agent Postfix values. If not configured, the default User-Agent header will be used.
SIP User-Agent Postfix	Configures the postfix added to the SIP User-Agent value.

Add MAC in User-Agent	Specifies whether the gateway's MAC address is included in the User-Agent header of outgoing SIP messages. The available options are: No: The MAC address is not included in the User-Agent header of any outgoing SIP messages. Yes except REGISTER: Includes the MAC address in the User-Agent header of all outgoing SIP messages except REGISTER and UNREGISTER. Yes to All SIP: Includes the MAC address in the User-Agent header of all outgoing SIP messages. The default setting is "No".
Use MAC Header	Specifies whether the gateway's MAC address is included in the MAC header of outgoing SIP messages. The available options are: No: The MAC header is not included in any outgoing SIP messages. Register Only: Includes the MAC header in REGISTER and UNREGISTER messages only. Yes to All SIP Requests: Includes the MAC header in all outgoing SIP request messages. The default setting is "No".
CSeq Tracking Mode	Specifies whether CSeq tracking is performed on a per-call or per-dialog basis. The default setting is "Per-Call". GXW42xx V2 only.
SIP Settings -> Session Timer	
Enable Session Timer	Enable or disable Session Timer support. The default setting is "Yes". GXW42 V2 only.
Session Expiration	Specifies the session expiration interval, in seconds. A SIP session must be refreshed using an UPDATE or re-INVITE request before this interval expires; otherwise, the session is terminated. The default setting is "180".
Min-SE	Specifies the minimum session expiration interval, in seconds. The default setting is "90".
Caller Request Timer	Enables or disables the use of the session timer for outgoing calls when the remote party supports session timers. The default setting is "No".
Callee Request Timer	Enables or disables the use of the session timer for incoming calls when they include a session timer request. The default setting is "No".
Force Timer	Enables or disables the use of the session timer when the remote party does not support it. When disabled, the session timer is used only when supported by the remote party. The default setting is "No". Note: To disable the Session Timer completely, disable Caller Request Timer, Callee Request Timer, and Force Timer.
UAC Specify Refresher	Specifies which party refreshes the session when the device acts as the caller (UAC). The available options are: UAC: Uses the device as the session refresher. UAS: Uses the callee or proxy server as the session refresher. Omit (Recommended). The default setting is "Omit".
UAS Specify Refresher	Specifies which party refreshes the session when the device acts as the callee (UAS). The available options are: UAC: Uses the caller or proxy server as the session refresher. UAS: Uses the device as the session refresher. The default setting is "UAC".
Force INVITE	Enables or disables using the INVITE method to refresh the session timer. When disabled, the UPDATE method is used for session refreshes. The default setting is "No".
SIP Settings -> Security Settings	
Validate Incoming Messages	Enables or disables validation of incoming SIP messages. The default setting is "No".
Check SIP User ID for Incoming INVITE	Enables or disables checking the SIP User ID in the Request URI of incoming INVITE messages. When enabled, the call is rejected if the SIP User ID in the Request URI does not match the phone's SIP User ID. Direct IP calling is also disabled. The default setting is "No".
Accept Incoming SIP from Proxy Only	Enables or disables accepting incoming SIP messages only when the Request URI matches the SIP server address configured for the account. When enabled, incoming messages with a different Request URI are rejected. The default setting is "No".
Authenticate Incoming INVITE	Enables or disables authentication of incoming INVITE messages. When enabled, the phone challenges incoming INVITE requests with a 401 Unauthorized response. The default setting is "No".

Authenticate server certificate domain	Enables or disables verification of the server TLS certificate domain. When enabled, the device verifies that the certificate's Common Name matches the configured SIP server.The default setting is "No".
Trusted Domain Name List	Configures a list of trusted domain names used for TLS certificate domain verification. If a domain in the certificate's SAN list matches any domain in the trusted domain name list, the certificate is trusted. By default, the remote proxy domain name and SIP server domain name are trusted. The field supports letters, numbers, -, ., and *, and allows wildcard domain names such as *.mycompany.com to trust any domain ending in .mycompany.com. GXW42xx V2 only.
Authenticate server certificate chain	Enables or disables verification of the server TLS certificate chain. When enabled, the device verifies that the certificate is authorized by a trusted Certificate Authority.The default setting is "No".
Fax Settings	
Fax Mode	Specifies the fax transmission mode. The available options are: T.38 (Auto Detect): Uses T.38 FoIP for fax transmission with automatic detection. Pass-Through: Uses fax pass-through with the PCMU/PCMA codec. The default setting is "T.38 (Auto Detect)".
Fax Tone Detection Mode	Specifies whether the caller or callee initiates the Re-INVITE when a fax tone is detected. The available options are: Caller Callee Caller or Callee The default setting is "Callee".
Send Re-INVITE After Fax Completion	Enables or disables sending an INVITE after fax transmission is completed with audio vocoders to continue the session using audio only.The default setting is "No".
Send Re-INVITE After Fax Tone	Enables or disables sending a Re-INVITE after detecting a fax tone. Disabling this option only takes effect when using the BroadSoft feature.The default setting is "Yes".
Re-INVITE Upon CNG Count	Specifies the number of CNG (Calling Tone) detections required before the gateway sends a Re-INVITE to switch to T.38 or G.711 mode. A value of 0 disables this feature. When the value is 1 or greater, the gateway sends a Re-INVITE when the configured CNG count is reached. The default setting is "0". The valid range is 0 to 6. GXW42xx V2 only.
Enable Silence Detection for Fax Disconnect	Enables or disables detecting silence to determine when fax transmission has completed, for fax machines that do not send a disconnect signal. The silence detection period is fixed at 7 seconds.The default setting is "Yes".
T.38 Max Bit Rate	Specifies the maximum T.38 bit rate. Lowering the bit rate may improve fax transmission success. This setting is effective only when the fax machine is receiving a fax. The default setting is "9600bps". GXW42xx V2 only.
Enable T38 TEP	Enables or disables Talker Echo Protection (TEP) for T.38 fax calls. TEP can reduce echo interference but may affect transmission reliability on some connections.The default setting is "No".GXW42xx V2 only.
Audio Settings	
DTMF Settings	
Preferred DTMF method (1-3)	Specifies the priority order for DTMF transmission methods. The priority list supports up to 3 methods. The available options are: In-audio RTP (RFC2833) SIP INFO
DTMF-RELAY Tag Respect SIP INFO	Enables or disables considering the selected DTMF method when adding the DTMF-relay tag to the Accept header in outgoing INVITE messages. When disabled, the DTMF-relay tag is always included. When enabled, it is included only when SIP INFO is selected as a preferred DTMF method.The default setting is "No".
Force DTMF to be sent via SIP INFO simultaneously	Enables or disables transmitting DTMF digits forcibly using SIP INFO in parallel with other methods.The default setting is "No".
Disable DTMF Negotiation	Enables or disables DTMF negotiation. When enabled, the gateway uses the configured DTMF method priority without negotiation.The default setting is "No".

Enable Fast RFC2833	Enables or disables fast RFC2833 DTMF timing. When disabled, DTMF uses 240 ms timing; when enabled, DTMF uses 100 ms timing. The default setting is "No". GXV42xx V1 only.
DTMF Payload Type	Configures the RTP payload type used for DTMF when RFC2833 is selected as a preferred DTMF method. The default setting is "101".
Custom DTMF InBand Duration	Configures the duration and inter-duration of Inband DTMF tones in milliseconds. When Duration is set to 0, the gateway passes through the Inband DTMF from the analog side without modifying its duration. When Duration is set to a value other than 0, the configured Duration and Inter-Duration values are used. The Duration default setting is "0". The valid values are 0 or 40 to 2000. The Inter-Duration default setting is "50". The valid range is 40 to 2000. GXV42xx V2 only.
Inband DTMF Tx Gain	Specifies the transmission gain for Inband DTMF in dB. The default value is "6". The valid range is -12 to 12. GXV42xx V2 only.
DSP DTMF Detector Min Level	Specifies the minimum signal level required for a DTMF tone to be considered valid in dBm. The default setting is "-25". The valid range is -45 to 0. GXV42xx V2 only.
DSP DTMF Detector SNR	Specifies the signal-to-noise ratio (SNR) threshold used to determine whether a DTMF tone is valid. The default setting is "1". The valid range is 0 to 2. GXV42xx V2 only.
DSP DTMF Detector Deviation	Specifies the allowable deviation from the central frequency for DTMF detection. The default setting is "25". The valid range is 0 to 100%. GXV42xx V2 only.
DSP DTMF Detector Twist	Specifies the maximum difference between the energy levels of the two DTMF frequencies in dB. The default setting is "5". The valid range is 0 to 12. GXV42xx V2 only.
RFC2833 Events	Specifies the RFC2833 event behavior when DTMF is detected. When Events is set to 0, the gateway generates continuous RFC2833 events while DTMF is detected. When Events is set between 2 and 8, the gateway generates RFC2833 packets using the configured Events and End Events values. The Events default setting is 8. The valid values are 0 or 2 to 8. The End Events default setting is 3. The valid range is 2 to 8. GXV42xx V2 only.
Vocoder Settings	
Preferred Vocoder (1-8)	Specifies the priority order of the supported vocoders. The priority list supports up to 8 vocoders and is included in the SDP message.
Voice Frames per TX	Configures the number of voice frames transmitted per packet. It's up to 10/20/32/64 for G711/G726/G723/other codecs respectively. The default setting is "2". The valid range is 1 to 6.
G723 Rate	Specifies the encoding rate for the G.723 codec. The available options are 6.3kbps encoding rate and 5.3kbps encoding rate. The default setting is "6.3kbps rate".
G726-32 Packing Mode	Selects the packing mode for G.726-32. The available options are ITU and IETF. The default setting is "ITU". GXW42 V1 only.
iLBC Frame Size	Specifies the iLBC frame size. The available options are 20ms and 30ms. The default setting is "20ms".
iLBC Payload type	Specifies the payload type for iLBC. The default setting is "97". The valid range is 96 to 127. GXW42 V1 only.
AAL2-G726-16 Payload type	Specifies the payload type for AAL2-G726-16. The default setting is "100". The valid range is 96 to 127. GXW42 V1 only.
AAL2-G726-24 Payload type	Specifies the payload type for AAL2-G726-24. The default setting is "99". The valid range is 96 to 127. GXW42 V1 only.
AAL2-G726-32 Payload type	Specifies the payload type for AAL2-G726-32. The default setting is "104". The valid range is 96 to 127. GXW42 V1 only.
AAL2-G726-40 Payload type	Specifies the payload type for AAL2-G726-40. The default setting is "103". The valid range is 96 to 127. GXW42 V1 only.

Opus Payload Type	Specifies Opus payload type. The value cannot be the same as the iLBC or DTMF payload type.The default setting is "123". The valid range is 96 to 127. GXW42 V2 only.
Disable Opus Stereo	Disables or enables Opus Stereo.The default setting is "No".GXW42 V2 only.
Use First Matching Vocoder in 200OK SDP	When Enabled, the device will use the first matching vocoder in the received 200OK SDP as the codec.The default setting is "No".
SRTP Mode	Selects the SRTP mode. The available options are: Disabled Enabled but not Forced Enabled and Forced Optional (GXW42xx V2 only) The default setting is "Disabled".
SRTP Key Length	Selects the cipher method/key length used when SRTP is enabled. The available options are: AES 128&256 bit AES 128 bit AES 256 bit The default setting is "AES 128&256 bit". GXW42xx V2 only.
Crypto Life Time	Enables or disables the use of Crypto Life Time with SRTP. When disabled, the device does not include the Crypto Life Time in the SRTP header.The default setting is "Yes".
Silence Suppression (VAD)	Enables or disables Voice Activity Detection (VAD) to reduce bandwidth usage by transmitting VAD packets instead by audio "silent packets". This feature applies to G.723 and G.729 codecs.The default setting is "No".
Jitter Buffer Type	Select either Fixed or Adaptive based on network conditions.The default setting is "Adaptive".
Jitter Buffer Length	Specifies the jitter buffer length according to network conditions. The available options are: Low: Initial 50 ms, minimum 10 ms, maximum 100 ms. Medium: Initial 100 ms, minimum 20 ms, maximum 200 ms. High: Initial 200 ms, minimum 40 ms, maximum 600 ms. Not all vocoders can meet the high requirement. The default setting is "Medium".
RTCP	Enables or disables sending RTCP Sender Reports during an active call.The default setting is "Enabled".
Analog Line Settings	
SLIC Setting	Selects the regional SLIC settings.The default setting is "USA 1 (BELLCORE 600 ohms)".
Ringing Frequency	Configures the ringing frequency. Available options are: 20Hz 25Hz Default (GXW42xx V1 only) The default setting for the GWX42xx V1 is "Default". The default setting for the GWX42xx V2 is "20Hz".
Ringing Power	Specifies the ringing power. Available options are: 45 Vrms 50 Vrms 55 Vrms 60 Vrms The default setting is "45Vrms".
Maximum DC Feed Current	Specifies the maximum DC feed current supplied to the connected device. Available options are 20mA and 30mA. The default setting is "20mA Default". GXW42 V2 only.
Caller ID Scheme	Selects the Caller ID scheme according to the local Telco standard. The default setting is "Bellcore/Telcordia".
Polarity Reversal	Enables or disables polarity reversal upon call establishment and termination.The default setting is "No".
Loop Current Disconnect	Enables or disables loop current disconnect upon call termination. Enable this option when the connected traditional PBX uses Loop Current Disconnect.The default setting is "No".
Play busy/reorder tone before Loop Current Disconnect	Enables or disables playing a busy/reorder tone before Loop Current Disconnect when a call fails.The default setting is "No".
Loop Current Disconnect duration	Specifies the duration of the Loop Current Disconnect signal in milliseconds. The default value is "200". The valid range is 100 to 10000 ms.
Enable Pulse Dialing	Enables or disables pulse dialing. When disabled, the system ignores incoming pulse dialing digits.The default setting is "Yes".GXW42 V2 only.

Pulse Dialing Standard	Specifies the pulse dialing standard. The available options are: General Swedish New Zealand The default setting is "General". GXW42 V2 only.
Enable Hook Flash	Enables or disables Hook Flash detection. When disabled, a flash is treated as an on-hook event.The default setting is "Yes".
Hook Flash Timing (Minimum)	Specifies the minimum on-hook duration for detecting a Hook Flash in milliseconds.The default setting is "300". The valid range is 40 to 2000.
Hook Flash Timing (Maximum)	Specifies the maximum on-hook duration for detecting a Hook Flash in milliseconds.The default setting is "1100". The valid range is 40 to 2000.
On Hook Timing	Specifies the duration required to detect an on-hook event in milliseconds.The default value is "400". The valid range is 40 to 2000.
TX Gain / RX Gain	Configures the transmit and receive audio gain for the connected analog phone's handset in dB. TX Gain: Sets the gain applied to audio received from the network to the FXS port. RX Gain: Sets the gain applied to audio transmitted from the FXS port to the network. The default setting for the GXW42xx V1 is "0" for both. The valid range is -12 to +12, with RX Gain also supporting Force +x dB options, which may introduce echo. The default setting for the GXW42xx V2 is "-4" for TX Gain and "-6" for RX Gain. The valid range is -12 to +6.
Disable Line Echo Canceller (LEC)	Enables or disables the Line Echo Canceller. When enabled, the device does not use LEC to remove echo from voice communications. The default setting is "No".
Enable Voltage Off Upon Port Disabled	Enables or disables turning off the port voltage when the port is disabled.The default setting is "No".GXW42xx V2 only.
Call Settings	
Early Dial	Enables or disables sending an INVITE whenever a key is pressed while dialing a number. When disabled, the INVITE is sent when the (Re)Dial key is pressed or automatically after 4 seconds. This option should only be enabled when the SIP proxy supports the 484 Incomplete Address response; otherwise, the call may be rejected with a 404 Not Found response. This feature is not intended for direct IP-to-IP calling.The default setting is "No".
Dial Plan Prefix	Specifies the prefix added to each dialed number.
Dial Plan	Configures the dial plan rule. "1,2,3,4,5,6,7,8,9,0 ,*,#,A,a,B,b,C,c,D,d" = Accept the specific digit/character. "x" = any digit from 0-9. "xx+" = at least 2 digits number. "xx" = exactly 2 digits number. "^" = exclude. "." = wildcard, matches one or more characters. " " = the OR operand. "[3-5]" = any digit of 3, 4, or 5. "[147]" = any digit 1, 4, or 7. "<2=011>" = replace digit 2 with 011 when dialing. "<=1>" = add a leading 1 to all numbers dialed, vice versa will remove a 1 from the number dialed. "T" = when adding a "T" at the end of the dial plan, the phone will wait for 3 seconds before dialing out. e.g. with dial plan 1XXT, phone will wait for 3 seconds to let user dial more than just 3 digits if needed. Originally the phone will dial out immediately after dialing the third digit. Some Dial Plan examples: {[369]11 1617xxxxxxx} = Allow 311, 611, 911, or any 10-digit numbers of leading digits 1617 {^1900x+ <=1617>xxxxxxx} = Block any number with leading digits 1900 or add prefix 1617 for any dialed 7-digit numbers [3469]11 - allow dialing special and emergency numbers 311, 411, 611 and 911 Note: In some cases, user wishes to dial strings such as *123 to activate voice mail or other application provided by service provider. In this case * should be predefined inside dial plan feature. An example dial plan will be: { *x+ } which allows the user to dial * followed by any length of numbers. The default setting is "{ x+ +x+ *x+ *x*x+ }".
Use # as Dial Key	Enables or disables using the # key as the Send/Dial key. When enabled, pressing # sends the dialed number. When disabled, # can be included as part of the dialed number.The default setting is "Yes".
Disable # as Redial key	Disables or enables using the # key as the Redial key when Use # as Dial Key is enabled.The default setting is "No".
No Key Entry Timeout	Specifies the time, in seconds, to wait for additional digit entry before completing the call. The default setting is "4". The valid range is 1 to 15.

Off-Hook Auto-Dial Delay	Specifies the delay, in seconds, before auto-dialing the extension configured under Advanced Port Settings after the phone goes off-hook. The default setting is "0". The valid range is 0 to 60.
Special AutoDial number for an incomplete dial by user	Specifies the number to be automatically dialed when the user enters an incomplete number according to the configured dial plan Example: If the "Special Auto Dial Number for an Incomplete Dial by User" is set to 100, and a user dials an incomplete number (e.g., 12), the system will automatically dial 100 instead. GXW42xx V2 only.
Allow Auto-Dial Config Per Port	Enables or disables configuring the Auto-Dial feature individually for each port when a Hunting Group is enabled. when disabled, all hunting group ports use same auto-dial number as configured for the ACTIVE port of the group.The default setting is "Disabled".
RFC2543 Hold	Enables or disables RFC2543 hold behavior. When enabled, 0.0.0.0 is used in the INVITE SDP to place the call on hold.The default setting is "Yes".
RTP/RTCP Keep Alive On Hold	Enables or disables sending RTP/RTCP keep-alive packets while a call is on hold.The default setting is "No".GXW42xx V2 only.
Disable Call Waiting	Enables or disables Call Waiting feature on the connected analog phone.The default setting is "No".
Disable Call Waiting Caller ID	Enables or disables Call Waiting Caller ID on the connected analog phone.The default setting is "No".
Disable Call Waiting Tone	Enables or disables the stutter Call Waiting tone when a Call Waiting call arrives. The Disable Call Waiting Caller ID will still be displayed.The default setting is "No".
Disable Connected Line ID	Enables or disables displaying the Connected Line ID.The default setting is "No".
Disable Receiver Off Hook Tone	Enables or disables the Receiver Offhook (ROH) tone after the phone remains off-hook for 60 seconds.The default setting is "No".
Disable Reminder Ring for On-Hold Call	Enables or disables the reminder ring played when a call is on hold and the analog phone goes on-hook.The default setting is "No".
Disable Reminder Ring for DND	Enables or disables the reminder ring when the FXS port is in DND mode.The default setting is "Yes".
Disable Voicemail Reminder Tone	Enables or disables the reminder tone played when voicemail messages are available.The default setting is "No".
Disable Visual MWI	Enables or disables Visual Message Waiting Indication (VMWI). The GXW42xx series supports this feature. However, some phones may incorrectly interpret the VMWI signal as an incoming call. Disabling Visual MWI can prevent this behavior.The default setting is "No".
Visual MWI Type	Specifies the method used to indicate voicemail notifications on the analog phone. The available options are: FSK: Uses FSK-based VMWI and should be used with an FSK Caller ID scheme. Neon:Uses voltage-based VMWI. PR:Uses polarity-reversal-based VMWI and should be used with a non-LR Caller ID scheme and polarity reversal enabled. (GXW42xx V2 only) PR_BLINK: Uses polarity-reversal-based VMWI with a 0.5-second on and 0.5-second off cadence. (GXW42xx V2 only) The default setting is "FSK".
MWI Tone	Specifies the tone played when the user picks up the phone while voicemail is available. The available options are: Default Special Proceed Indication Tone The default setting is "Default". GXW42xx V2 only.
Transfer on Conference Hangup	Enables or disables transferring the call to the other party when the conference initiator hangs up.The default setting is "No".
Ringing Transfer	Enables or disables transferring the call to the other party when the transferer hangs up while listening to the ringback tone.The default setting is "No".GXW42xx V2 only.
Send Hook Flash Event	Enables or disables sending a Hook Flash as a DTMF event.The default setting is "No".

Send Hook Flash Event Method	Specifies the method used to send the Hook Flash event. The available options are: Default: The Hook Flash event is sent as a DTMF event. SIP INFO: The Hook Flash event is sent using SIP INFO. The default setting is "Default".
Flash Digit Control	Enables or disables using flash digit combinations to control call waiting calls. When enabled and Send Hook Flash Event is disabled. Flash+1 should release the current call and answer the waiting call. Flash+2 should put the active call on hold and answer the waiting call. Flash+3 should keep the active call and reject the waiting call. Note: Gibtelecom ITSP is now supported for Flash digit control actions mentioned above. The default setting is "No".
Callee Flash to 3WC	Enables or disables establishing a three-way conference when the device is the callee of the second call. When enabled, pressing Hook Flash bridges the two calls into a three-way conference instead of toggling between them. The default setting is "No".
Ring Timeout	Specifies the time, in seconds, after which an unanswered incoming call stops ringing. The default setting is "60".
Ringback Tone at No Early Media	Enables or disables playing a ringback tone when no early media RTP packets are received. The default setting is "No". GXW42xx V2 only.
Delayed Call Forward Wait Timeout	Specifies the delay, in seconds, before a call is forwarded when the Delayed Call Forwarding Feature is activated using the *92 code. The default setting is "20".
Send Anonymous	Enables or disables anonymous calling. When enabled, the From, Privacy, and P-Asserted-Identity headers in outgoing INVITE messages are set to anonymous, preventing the Caller ID from being disclosed. The default setting is "No".
Anonymous Call Rejection	Enables or disables rejecting incoming calls with an anonymous Caller ID. When enabled, such calls are rejected with a 486 Busy response. The default setting is "No".
Replace Beginning '+' in Caller ID with	Specifies the string used to replace the leading + in the Caller ID before it is sent to the analog phone.
Number of Beginning Digits to Strip from Caller ID	Specifies the number of leading digits to remove from the incoming Caller ID. The default setting is "0". The valid range is 0 to 10.
Hunting Group Type	Specifies how incoming calls are distributed among the available lines in a Hunting Group. The available options are: Linear (Serial Hunting): Calls are always routed to the lowest-numbered available line. If that line is busy, the system checks the next available one in ascending order. Once a line becomes free again, it will be considered first in the next incoming call cycle. Circular (Round-Robin): Calls are distributed in a rotating manner across all lines. For example, if the last call was answered by line 1, the next call will be routed to line 2, and so on. This rotation continues even if a previously used line becomes available again, ensuring fair call distribution. Busy lines are skipped during the process. Parallel: Incoming calls are broadcasted to all available lines in the group simultaneously. The first line to answer handles the call, and the others stop ringing. This method ensures the fastest possible response time. Note: Accounts inherit the Hunting Group Type configured in their assigned Profile. The default setting is "Circular".
Hunting Group Ring Timeout	Specifies the time, in seconds, an incoming call rings a Hunting Group member before being forwarded to the next member. The default setting is "20".
Special Feature	Selects the server type for special requirements. The default setting is "Standard".
Feature Key Synchronization	Enables or disables synchronization of DND and Call Forward features with the SIP server. The default setting is "No".
Call Features Settings	
Enable Call Features	Enables or disables the local Call Features. No: Uses the ITSP feature codes. Yes: Uses the local call features configured on the phone. Enable All: Overrides the individual feature settings and enables all call features. Note: When enabled, the gateway plays a stutter tone when the handset is picked up to indicate that a call feature is active, followed by the dial tone. The default setting is "Yes".

Reset Call Features	Enables or disables resetting call features through the Web UI. Disabled by default.
SRTP Feature	Enables or disables the SRTP Feature. Enable SRTP: 16 Disable SRTP: 17 The default setting is "Yes".
SRTP per call Feature	Enables or disables the SRTP per call Feature. Enable SRTP per Call: 18 Disable SRTP per Call: 19 The default setting is "Yes".
CID Feature	Enables or disables the Caller ID Feature. Enable CID: 31 Disable CID: 30 The default setting is "Yes".
CID per call Feature	Enables or disables the Caller ID per call Feature. Enable CID per Call: 82 Disable CID per Call: 67 The default setting is "Yes".
Direct IP calling Feature	Enables or disables the Direct IP calling Feature. Direct IP Calling: 47 The default setting is "Yes".
CW Feature	Enables or disables the Call Waiting Feature. Enable CW: 51 Disable CW: 50 The default setting is "Yes".
CW per call Feature	Enables or disables the Call Waiting per call Feature. Enable CW per Call: 71 Disable CW per Call: 70 The default setting is "Yes".
Call Return Feature	Enables or disables the Call Returns Feature. Enable Call Return: 69 The default setting is "Yes".
Unconditional Forward Feature	Enables or disables Unconditional Call Forwarding Feature. Enable Unconditional Forward: 72 Disable Unconditional Forward: 73 The default setting is "Yes".
Busy Forward Feature	Enables or disables Call Forwarding on Busy Feature. Enable Busy Forward: 90 Disable Busy Forward: 91 The default setting is "Yes".
Delayed Forward Feature	Enables or disables Delayed Call Forwarding Feature. Enable Delayed Forward: 92 Disable Delayed Forward: 93 The default setting is "Yes".
Paging Feature	Enables or disables the Paging Feature. Paging: 74 The default setting is "Yes".
DND Feature	Enables or disables the Do Not Disturb Feature. Enable DND: 78 Disable DND: 79 The default setting is "Yes".
Blind Transfer Feature	Enable or disable the Blind Transfer Feature. Enable Blind Transfer: 87 The default setting is "Yes".
Disable LEC per call Feature	Disables or enables the Line Echo Canceller (LEC) per call Feature. Disable LEC per Call: 03 The default setting is "Yes".
Disable Bellcore-style 3-Way Conference	Enables or disables Bellcore-style 3-Way Conferencing Feature. The default setting is "No". Star Code 3WC Feature: Enable Star Code 3-Way Conference feature, only functions if Disable Bellcore-style 3-Way Conference is set to "Yes". The default setting is "Yes". Star Code 3WC: 23
Provision Start Feature	Enables or disables the Provision Start Feature. Enable Provision Start: 99 The default setting is "Yes".
Play Registration ID Feature	Enables or disables the Play Registration ID Feature. Enable Playing Registration ID: 98 The default setting is "Yes".
Play Port Number Feature	Enable or disables the Play Port Number Feature. Enable Playing Port Number: 97 The default setting is "Yes". GXW42xx V1 only.
Forced Codec Feature	Enables or disables the forced codec feature during calls. The default setting is "Yes". Forced Codec: 02 Each codec can be enabled or disabled individually. The default setting for all codecs is "Yes". The feature codes for the available codecs are: PCMU codec: 7110 PCMA codec: 7111 G723 codec: 723 G729 codec: 729 AAL2-G728-R16 codec: 72616 AAL2-G728-R16 codec: 72624 AAL2-G728-R16 codec: 72632 AAL2-G728-R16 codec: 72640 iLBC codec: 7201 G722 codec: 722
Ring Tones	
Distinctive Ring Tones	

Distinctive Ring Tone (1-3)	Selects distinctive ring tones based on the incoming caller ID. Select the Ring Tone and enter the corresponding caller ID. Up to 3 distinctive ring tones can be configured. When a caller ID is configured, the selected ring tone is used only for matching incoming calls; other calls use the system ring tone. If no caller ID is configured, the selected ring tone is used for all incoming calls on the FXS port. Prefix matching is supported using the x+ symbol. The default setting is "Ring Tone 1". Example: If configured as 617x+, Ring Tone 1 is used for incoming calls from the 617 area code. Other incoming calls use the cadence defined by the System Ring Cadence setting under the Advanced Settings -> Ring Tones page. Notes: If the server supports the Alert-Info header and specifies a standard Bellcore ring tone or a distinctive ring tone (1-10), the ring tone specified in the Alert-Info header will be used. Bellcore ring tones and tones are independent of custom ring tones. Custom ring tones can also be specified using the Alert-Info header, for example: Alert-Info: ;info=ring5.
Ring Tone Cadences	
Ring Tone (1-10)	Configures ring tone cadences according to preference. Up to 10 ring tones can be configured. The default setting is "c=2000/4000;"
Call Waiting Tones	
Distinctive Call Waiting Tones	
Distinctive Call Waiting Tone (1-3)	Selects the distinctive call waiting tone based on the incoming caller ID. Select the Call Waiting Tone and enter the corresponding caller ID. Up to 3 distinctive call waiting tones can be configured. The default setting is "Call Waiting Tone 1".
Call Waiting Tone Cadences	
Call Waiting Tone (1-10)	Configures the cadence for each call waiting tone. Up to 10 call waiting tone cadences can be configured. The default setting is "f1=440@-13,c=300/10000;"

FXS Ports

Port Settings	
SIP User ID	Specifies the SIP user ID provided by the VoIP service provider (ITSP), usually a numeric string similar to or matching a phone number.
Authenticate ID	Specifies the authentication ID for the SIP service subscriber. It can be the same as or different from the SIP User ID.
Password	Specifies the SIP account password used by the gateway to register with the ITSP's SIP servers.
Name	Specifies the name used to identify the port. Note: GXW42XX V2 supports UTF-8 characters.
Profile	Selects the Profile assigned to the port.
Enable FXS (TR-069)	Enables or disables the FXS port. When enabled, the device reports to the ACS through TR-069 whether an analog device is connected to or disconnected from the FXS port. The CPE version must be 1.0.4.144 or later for this feature to work. The default setting is "No".
Advanced Port Settings	
Offhook Auto-dial	Specifies the number automatically dialed when the handset goes off-hook.
Hunting Group	Assigns the port to a hunting group.
Routing ID	Configures a string used to route incoming SIP calls to specific FXS ports on the GXW42xx V2 device. Each FXS port can be assigned a unique Routing ID, which acts as an internal tag or identifier. When an incoming SIP INVITE is received, the system checks for a match between the configured Routing ID and an identifier in the SIP header (based on the selected matching type). If a match is found, the call is routed to the corresponding FXS port.

Routing ID Matching Type	Determines which part of the SIP INVITE message is used to compare against the configured Routing ID. The available options are: Request URI: The device matches the Routing ID against the user portion of the Request URI (e.g., sip:1001@domain.com). This is the most common method and aligns with standard SIP routing behavior, where the user part of the Request URI is typically used for extension or port mapping. To Header: The device compares the Routing ID against the user portion of the To header field in the SIP INVITE. This is useful in scenarios where SIP proxies or softswitches rewrite the Request URI but leave the original called number in the To header. The default setting is "Request URI".
Lock/Unlock Extension Code	Specifies the extension code used to lock or unlock the FXS port. The locking password must be a four-digit numeric string.
FXO Mapping	
Map to FXO Port #	Specifies the FXO port on a Grandstream GXW410X gateway to which the FXS port is mapped. This setting applies only when peering with a GXW410X. The default setting is "1". The valid range is 1-8, corresponding to lines 1-8 on the GXW410X.
Map to FXO Gateway IP	Specifies the IP address and SIP port of the FXO gateway to which calls are sent. This setting applies when peering with an FXO gateway of any brand.
Port	Specifies the SIP port appended to the FXO gateway IP address.

Advanced Configurations

Disable WEB Configuration Access

Users can enable or disable access to the GXW42xx V2 devices directly from the LCD menu. This can enhance security and allow quick restriction of unauthorized access.

On the device's LCD screen:

1. Navigate to **Settings -> Advanced Settings -> Security**
2. Select **Enable/Disable Access**
3. Toggle between **Enable** (allow access) or **Disable** (restrict access)

Saving the Configuration Changes

After the user makes a change to the configuration, press the "Update" button in the Configuration Menu. The web browser will then display a message window to confirm saved changes.

Grandstream recommends rebooting or powering cycling the gateway after saving changes.

Rebooting from Remote

Press the "Reboot" button at the bottom of the configuration menu to reboot the phone remotely. The web browser will then display a message window to confirm that the reboot is underway. Wait 30 seconds to log in again.

Configuration through a Central Server

Grandstream GXW42XX can be automatically configured from a central provisioning system.

When GXW42XX boots up, it will send TFTP, HTTP/HTTPS, FTP, or FTPS requests to download configuration files, "cfg000b82xxxxxx" and "cfg00082xxxxxx.xml", where "000b82xxxxxx" is the LAN MAC

address of the GXW42XX. If the download of "cfgxxxxxxxxxxxx.xml" is not successful, the provision program will issue a request for a generic configuration file "cfg.xml". The configuration file name should be in lowercase letters.

The configuration data can be downloaded via TFTP, HTTP/HTTPS, FTP, or FTPS from the central server. A service provider or an enterprise with a large deployment of GXW42XX can easily manage the configuration and service provisioning of individual devices remotely from a central server.

Grandstream provides a central provisioning system, GAPS (Grandstream Automated Provisioning System), to support the automated configuration of Grandstream devices. GAPS uses enhanced (NAT-friendly) TFTP or HTTP (thus no NAT issues) and other communication protocols to communicate with each individual Grandstream device for firmware upgrade, remote reboot, etc.

Grandstream provides GAPS service to VoIP service providers. Use GAPS for either simple redirection or with certain special provisioning settings. At boot-up, Grandstream devices by default point to the Grandstream provisioning server, GAPS, based on the unique MAC address of each device. GAPS provisions the devices with redirection settings so that they will be redirected to the customer's TFTP or HTTP/HTTPS server for further provisioning. the customer's TFTP, HTTP/HTTPS, FTP, or FTPS server for further provisioning.

Configuration and Firmware Upgrade through Resync SIP NOTIFY

GXW42xx V1 and V2 series supports triggering firmware and configuration upgrade using Resync SIP NOTIFY. The **event:resync** NOTIFY allows the device to re-synchronize its configuration by checking the provisioning server to download any updates.

Below is an example of a resync SIP NOTIFY:

```
NOTIFY sip:device@domain.com SIP/2.0
Via: SIP/2.0/UDP 10.0.0.5:5060;branch=z9hG4bK-d4f2-9a75
Max-Forwards: 70
From: "Provisioning Server" <sip:provisioning@domain.com>;tag=prov-server
To: <sip:device@domain.com>;tag=device-987654
Call-ID: 987654xyz321
CSeq: 12345 NOTIFY
Event: resync
Content-Type: application/simple-message-summary
Content-Length: 45
```

Outbound Caller ID Configuration

The GXW42XX allows the Caller ID presented on outbound calls to be controlled through a combination of **FXS Port** and **SIP Profile** settings. Each FXS port can use its own SIP account and be assigned to one of the four available SIP Profiles.

Caller ID Number

By default, the SIP identity associated with the FXS port is used when generating the outbound SIP call. Under **FXS Ports -> Port Settings**, the **SIP User ID** identifies the SIP account used by the port, while the **Profile** parameter determines which SIP Profile provides the SIP server and related signaling settings.

For **GXW42xx V2**, a different outbound identity can be configured using **Routing ID**. When a Routing ID is configured for the FXS port and **Use Routing ID in SIP Headers** is enabled under the associated SIP Profile, the gateway uses the Routing ID instead of the SIP User ID in the **From** and **Contact** headers of outgoing calls. This is particularly useful for SIP trunk deployments where the authentication account and the number presented as the outbound identity are different.

The Routing ID and Use Routing ID in SIP Headers options are available only on GXW42xx V2 devices.

Caller ID Name

The Caller ID name can be configured through the **Name** field under **FXS Ports -> Port Settings**. GXW42xx V2 supports UTF-8 characters in this field.

SIP Identity Headers

The SIP Profile also provides identity-related options that may affect how the outbound Caller ID is presented to the SIP server:

- **Use P-Preferred-Identity Header** - controls whether the gateway includes the P-Preferred-Identity header in outbound SIP INVITE messages.
- **Use P-Asserted-Identity Header** - controls whether the gateway includes the P-Asserted-Identity header in outbound SIP INVITE messages. This option is available on **GXW42xx V2**.
- **Use Privacy Header** - controls whether the Privacy header is included in SIP messages.

These settings should be configured according to the requirements of the SIP server or service provider. They do not independently define the Caller ID number; rather, they control which SIP identity information is included in the outbound signaling.

Configuration

The GXW42XX can use a different number from the **SIP User ID** in the SIP headers of outgoing calls. The configuration differs slightly between V1 and V2:

GXW42XX V1

- Go to **FXS Ports -> Advanced Port Settings**.
- Configure **Request URI Routing ID** with the number to be used for outgoing calls.
- Go to **Profiles -> Profile 1-4 -> SIP Settings -> Basic Settings** for the profile assigned to the FXS port.
- Enable **Use Request Routing ID in SIP Headers**.
- The configured Request URI Routing ID will then be used instead of the SIP User ID in the relevant outgoing SIP headers.

GXW42XX V2

- Go to **FXS Ports -> Advanced Port Settings**.
- Configure **Routing ID** with the number to be used for outgoing calls.
- Go to **Profiles -> Profile 1-4 -> SIP Settings -> Basic Settings** for the profile assigned to the FXS port.
- Enable **Use Routing ID in SIP Headers**.
- The configured Routing ID will then be used instead of the SIP User ID in the **From** and **Contact** headers of outgoing calls.

Example

For example, an FXS port can be configured with:

FXS Port

- SIP User ID: 1001
- Name: Sales Department
- Profile: Profile 1

For a GXW42xx V2 connected to a SIP trunk, the same port could additionally use:

Advanced Port Settings

- Routing ID: 2125551001

Profile 1

- Use Routing ID in SIP Headers: **Yes**

In this configuration, the port continues to use the configured SIP account for registration and authentication, while the Routing ID is used in the **From** and **Contact** headers for outbound calls. The configured FXS **Name** provides the Caller ID name.

The SIP server or service provider may apply its own Caller ID policies and may replace or reject the identity presented by the gateway. The GXW42XX configuration controls the identity sent in the outbound SIP signaling; it does not guarantee that the same Caller ID will ultimately be displayed to the called party.

V1/V2 Considerations

The general Caller ID configuration through **SIP User ID**, **Name**, and **Profile** applies to the GXW42xx V1 and V2 series. **Routing ID-based Caller ID modification is specific to GXW42xx V2**, which provides the additional ability to use a value different from the SIP User ID in the From and Contact headers.

SOFTWARE UPGRADE

Software upgrade can be done via either TFTP, HTTP/HTTPS, FTP, or FTPS. The corresponding configuration settings are in the ADVANCED SETTINGS configuration page.

The GXW42xx V2 series supports adding variables to provisioning-related settings. The variables are replaced by their corresponding values. The following variables are supported:

- **PN**: The device model, such as GXW4224V2.
- **MAC**: The device's MAC address, such as c0:74:ad:a8:bc:ed.
- **VendorName**: The vendor name.
- **ModelName**: The device model.
- **HwVersion**: The hardware version.
- **FirmwareVersion**: The firmware version.
- **Suffix**: The configured server path suffix.

The variables support the following formats: **{PN}**, **\$PN**, and **\${PN}**.

Variable support is available in the following settings:

- **Firmware Server Path**: Under **Maintenance -> Upgrade and Provisioning -> Firmware**, or through P-value **P192**.
- **Config Server Path**: Under **Maintenance -> Upgrade and Provisioning -> Config File**, or through P-value **P237**.
- **HTTP/HTTPS User-Agent**: Under **Maintenance -> Network Settings -> Advanced Network Settings**, or through P-value **P1541**.
- **SIP User-Agent**: Under **Profiles -> Profile x -> SIP Settings -> Basic Settings**, or through P-values **P29071**, **P29171**, **P29271** and **P29371**.

To configure the P-value, download the configuration file, edit the P-value, and upload the updated configuration file under **Maintenance -> Upgrade and Provisioning -> Config File -> Download Device**

Configuration.

Example:

Configuring the Config Server Path as `tftp://192.168.5.2/$PN_$MAC.cfg` results in the device requesting the configuration file `tftp://192.168.5.2/GXW4224V2_c0:74:ad:a8:bc:ed.cfg`

Firmware Upgrade through TFTP/HTTP/HTTPS/FTP/FTPS

To upgrade via TFTP, HTTP, HTTPS, FTP, or FTPS, set **Upgrade via** under **Upgrade and Provisioning** -> **Firmware** and **Upgrade** to the corresponding protocol. Firmware Server Path needs to be set to a valid URL of the corresponding server; the server name can be in either FQDN or IP address format.

e.g. `firmware.mycompany.com:6688/Grandstream/1.0.4.4`

e.g. `firmware.grandstream.com`

Notes:

- Firmware upgrade server in IP address format can be configured via IVR. Please refer to the CONFIGURATION GUIDE section for instructions. If the server is in FQDN format, it must be set via the web configuration interface.
- Grandstream recommends that end-users use the Grandstream HTTP server. Its address can be found at <http://www.grandstream.com/support/firmware>. Currently, the HTTP firmware server URL is `firmware.grandstream.com`. For large companies, we recommend maintaining their own TFTP/HTTP/HTTPS/FTP/FTPS servers for upgrade and provisioning procedures.
- Once a "Firmware Server Path" is set, the user needs to update the settings and reboot the device. If the configured firmware server is found and a new code image is available, the GXW will attempt to retrieve the new image files by downloading them into the GXW420x's SRAM. During this stage, the GXW's LEDs will blink until the checking/downloading process is completed. Upon verification of the checksum, the new code image will then be saved into the Flash. If TFTP/HTTP/HTTPS/FTP/FTPS fails for any reason (e.g., TFTP/HTTP/HTTPS/FTP/FTPS server is not responding, there are no code image files available for upgrade, or checksum test fails, etc.), the GXW will stop the TFTP/HTTP/HTTPS/FTP/FTPS process and simply boot using the existing code image in the flash.
- Firmware upgrade may take as long as 15 to 30 minutes over the Internet, or just 5 minutes if it is performed on a LAN. It is recommended to conduct a firmware upgrade in a controlled LAN environment if possible. For users who do not have a local firmware upgrade server, Grandstream provides a NAT-friendly TFTP server on the public Internet for firmware upgrade.
- Grandstream's latest firmware is available at <https://www.grandstream.com/support/firmware>.

Overseas users are strongly recommended to download the binary files and upgrade firmware locally in a controlled LAN environment.

- Alternatively, the user can download a free TFTP/HTTP/HTTPS/FTP/FTPS server and conduct a local firmware upgrade. A free Windows version of the TFTP server is available for download from http://www.solarwinds.com/products/freetools/free_tftp_server.aspx. Our latest official release can be downloaded from Firmware- Grandstream Networks

Instructions for Local Firmware Upgrade

1. Unzip the file and put all of them under the root directory of the TFTP server.
2. Put the PC running the TFTP server and the GXW42XX device in the same LAN segment.
3. TFTP server's security settings should be changed from "Receive Only" to "Transmit Only" for the firmware upgrade.
4. Configure the Firmware Server Path with the IP address of the PC.
5. Update the change and reboot the unit.

Configuration File Download

Grandstream SIP Device can be configured via the Web Interface or a Configuration File through TFTP, HTTP, HTTPS, FTP, or FTPS. Set **Upgrade via** under **Upgrade and Provisioning -> Config File**, and enter the **Config Server Path**. The path must be a valid URL, either in FQDN or IP address format.

A configuration parameter is associated with each particular field in the web configuration page. A parameter consists of a Capital letter P and 1 to 3 (Could be extended to 4 in the future) digits numeric numbers. i.e., P2 is associated with "Admin Password" in the ADVANCED SETTINGS page. For a detailed parameter list, please refer to the corresponding firmware release configuration template.

When a Grandstream device boots up or reboots, it will issue a request for a configuration file "cfgxxxxxxxxxx", where "xxxxxxxxxx" is the MAC address of the device, i.e., "cfg000b820102ab". In addition, the device will also request an XML configuration file "cfgxxxxxxxxxx.xml". If the download of "cfgxxxxxxxxxx.xml" is not successful, the provision program will issue a request for a generic configuration file "cfg.xml". The configuration file name should be in lowercase letters.

- The Only acceptable Config file formats to be used when provisioning are XML or binary.
- Make sure the MAC header on the Config file is the provisioned device's MAC address, or you can remove the header completely.

Firmware and Configuration File Prefix and Postfix

Firmware Prefix and Postfix allow the device to download the firmware name with the matching Prefix and Postfix. This makes it possible to store ALL of the firmwares with different versions in one single directory. Similarly, Config File Prefix and Postfix allow the device to download the configuration file with the matching Prefix and Postfix. Thus, multiple configuration files for the same device can be stored in one directory.

In addition, when the field "Check New Firmware only when F/W pre/suffix changes" is selected, the device will only issue a firmware upgrade request if there are changes in the firmware Prefix or Postfix.

Managing Firmware and Configuration File Download

When "Automatic Upgrade" is set to "Yes", the Service Provider can use P193 to have the devices periodically check with either Firmware Server or Config Server, whenever they are defined. This allows the device to periodically check whether there are any new changes that need to be taken, similar to the Anti-Virus Software, to upgrade the Virus Definition files. Screenshot is below:

Automatic Upgrade:

☐ No ☒ Yes, every minutes (60-5256000).

☐ Yes, daily at hour (0-23). ☐ Yes, weekly on day (0-6).

RESTORE FACTORY DEFAULT SETTING

Factory Reset

Restoring the Factory Default Setting will DELETE all configuration information of the phone. Please BACKUP or PRINT out all the settings before you proceed to the following steps. Grandstream will not take any responsibility if you lose all the parameters of settings and cannot connect to your VoIP service provider.

There are two (2) methods for resetting your unit:

Reset Button

Reset default factory settings following these four (4) steps:

1. Unplug the Ethernet cable.
2. Locate a needle-sized hole on the back panel of the gateway unit next to the power connection.
3. Insert a pin in this hole, and press for more than 4 seconds.
4. Take out the pin. All unit settings are restored to factory settings.

IVR Command

Reset default factory settings using the IVR Prompt (Table 5):

1. Dial "****" for voice prompt.
2. Enter "099" and wait for the "reset" voice prompt.
3. Enter the encoded MAC address (Look below on how to encode the MAC address).
4. Wait 15 seconds, and the device will automatically reboot and restore factory settings.

Encode the MAC Address

1. Locate the MAC address of the device. It is the 12-digit HEX number on the bottom of the unit.
2. Key in the MAC address. Use the following mapping:

Key	Mapping
0-9	0-9
A	22 (press the "2" key twice, "A" will show on the LCD)
B	222
C	2222
D	33 (press the "3" key twice, "D" will show on the LCD)
E	333
F	3333

MAC Address Key Mapping

For example: if the MAC address is 000**b**8200**e**395, it should be keyed in as "000**222**8200**333**395".

- Factory Reset will be disabled if the "Lock keypad update" is set to "Yes".
- If still have difficulties to get access to the device, pushing the reset button during booting up will trigger the RECOVERY MODE, and device will use static IP 192.168.1.234/24. Put your PC under the same subnet, and then you will be able to open the RECOVERY MODE web page on 192.168.1.234 by your web browser.
- While attempting to trigger the RECOVERY MODE, do not lose reset button until device enters recovery mode.
- Admin password is needed to log in RECOVERY MODE and to get the response key if "Lock Keypad update" is set to "Yes".

CHANGE LOG

This section documents significant changes from previous versions of the GXW42XX user manuals. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware version 1.0.35.1

Product Name: GXW4216 V2, GXW4224 V2, GXW4232 V2, GXW4248 V2

- Added support for "Send SIP INFO with RFC2833". [[Force DTMF to be sent via SIP INFO simultaneously](#)]
- Added support for separate SUBSCRIBE timers. [[Subscribe Expiration](#)]
- Optimized the provisioning protocols for firmware. [[Firmware Upgrade Via](#)]
- Optimized the provisioning protocols for configuration. [[Config Upgrade Via](#)]
- Added support for the HTTP User-Agent header. [[HTTP/HTTPS User-Agent](#)]
- Added support for Layer 2 QoS 802.1p Priority Value. [[Layer 2 QoS 802.1p Priority Value for Service Interface](#)]
- Added wildcard support across provisioning settings. [[Software Upgrade](#)]

Firmware version 1.0.33.11

Product Name: GXW4216 V2, GXW4224 V2, GXW4232 V2, GXW4248 V2

- Added support for displaying the Serial Number on the System Info page. [[Serial Number](#)]
- Added support for the option "Optional" to SRTP Mode. [[SRTP Mode](#)]
- Added support for enabling and disabling FXS voltage when the port is disabled. [[Enable Voltage Off Upon Port Disabled](#)]
- Added support for the number of digits to strip from the beginning of the Caller ID. [[Number of Beginning Digits to Strip from Caller ID](#)]
- Added support for Feature Key Synchronization. [[Feature Key Synchronization](#)]
- Added the ability to configure SIP Timer B. [[SIP TIMER B](#)]
- Added the ability to configure SIP Timer F. [[SIP TIMER F](#)]
- Added support for T.38 Talker Echo Protection (TEP). [[Enable T38 TEP](#)]
- Added support for UTF-8 characters in Analog Port Name fields. [[Port Settings](#)]
- Added support for a customizable dial tone for call forwarding features on FXS ports. [[Dial Tone when Call Forward Active](#)]
- Added support for AES-GCM Encryption in "OpenVPN(R) Encryption". [[OpenVPN\(R\) Encryption](#)]
- Added support for HTTP/HTTPS Proxy settings. [[HTTP/HTTPS Proxy](#)]
- Added support for the custom config order feature on the Web UI. [[Provision Config Order](#)]
- Added support for enabling Wideband PCM Resolution using P-values. [[Wideband PCM Resolution](#)]
- Added support for Caller ID order customization for Vonage. [[Caller ID](#)]
- Added option for DHCP option 160 Priority over Option 66. [[Allow DHCP Option 43 and Option 66 to Override Server](#)]
- Added support for UDP/RTP checksum. [[Local RTP Port](#)]
- Added DNS SRV failover after 5xx responses. [[SRV Settings](#)]
- Added option to prevent REGISTER/UPDATE to primary SBC during secondary SBC session. [[SRV Settings](#)]

Firmware version 1.0.23.15

Product Name: GXW4216 V1/GXW4224 V1/GXW4232 V1/GXW4248 V1

- Added support for "Add MAC in User-Agent". [[Add MAC in User-Agent](#)]

- Added support for "Use MAC Header". [[Use MAC Header](#)]
- Added support for the MTU feature. [[Maximum Transmission Unit \(MTU\)](#)]
- Added support for "Download and Process All Available Config Files". [[Download and Process All Available Config Files](#)]
- Added support for Provision Config Order. [[Provision Config Order](#)]
- Added support for uploading config files in text format. [[Upload Device Configuration](#)]
- Added support for "OpenVPN Username" on the VPN Page. [[OpenVPN\(R\) Username](#)]
- Added support for "OpenVPN Password" on the VPN Page. [[OpenVPN\(R\) Password](#)]
- Added support for specifying the number of leading digits to strip from caller ID. [[Number of Beginning Digits to Strip from Caller ID](#)]
- Added support to display the Serial Number on the System Info page. [[Serial Number](#)]
- Added support for Firmware Upgrade Via Resync SIP NOTIFY. [[Resync SIP NOTIFY](#)]
- Added support for HTTP version 1.1 when requested by the provisioning server.

Firmware version 1.0.33.3

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- Changed the default value "Disable Weak TLS Cipher Suites" to "Disable All Of The Above Weak TLS Ciphers Suites". [[Disable Weak TLS Cipher Suites](#)]
- Changed the default value of "Minimum TLS Version" to "TLS 1.2". [[Minimum TLS Version](#)]
- Changed the default value of "Profile Active" to "No". [[Profile Active](#)]
- Changed the default value of "Enable FXS" to "No". [[Enable FXS \(TR-069\)](#)]
- Changed the default value of "Use Random SIP Port" to "Yes". [[Use Random SIP Port](#)]
- Changed the default value of "Use Random RTP Port" to "Yes". [[Use Random RTP Port](#)]
- Added support for a new option value "TLS 1.3" for "Minimum TLS Version". [[Minimum TLS Version](#)]
- Added support for RFC8760.
- Added support for enabling TR069 through the management interface. [[Enable TR069 Through Management Interface](#)]
- Added support for enabling RADIUS through the management interface. [[Enable RADIUS Through Management Interface](#)]
- Added support for Vonage IVR diagnostics.
- Added support for an IVR prompt when the WAN cable is disconnected.

Firmware version 1.0.23.11

Product Name: GXW4216 V1/GXW4224 V1/GXW4232 V1/GXW4248 V1

- No major changes

Firmware version 1.0.31.2

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- Added support for OpenVPN TLS Key. [[OpenVPN\(R\) TLS Key](#)] [[OpenVPN\(R\) TLS Key Type](#)]
- Added support for remote access to WebUI via GDMS. [[Grandstream Cloud](#)]
- Added support for the Israel time zone with daylight saving time (DST). [[Time Zone](#)]
- Added new option "2 - Parallel" to Hunting Group Type (P4395/4396/4397/4398). [[Hunting Group Type](#)]
- Update the name of "Request URI Routing ID" (P4669-4700, P21704-21719) to "Routing ID". [[Routing ID](#)]
- Added support for assigning multiple DIDs per FXS port. [[Routing ID Matching Type](#)]
- Added the ability to save time to the timefile periodically. [[System Information](#)]
- Added support for hostname validation in certificates. [[Validate Hostname in Certificate](#)]

- Added support for the MTU feature. [[Maximum Transmission Unit \(MTU\)](#)]

Firmware version 1.0.29.9

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- Added the ability to detect the connection status of FXS ports. [[Enable FXS \(TR-069\)](#)]

Firmware version 1.0.29.7

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- Added support for Firmware Upgrade Via ReSync SIP NOTIFY. [[Configuration and Firmware Upgrade through Resync SIP NOTIFY](#)]
- Added the "Enable/Disable Access" option to the LCD Menu. [[Disable Web Configuration Access](#)]
- Added support for Subscribe Retry Wait Time upon 403 Forbidden. [[Subscribe Retry Wait Time upon 403 Forbidden](#)]
- Added support to a "No Key Offhook Auto-dial number" field to trigger off-hook auto-dial when uncompleted numbers. [[Special Auto Dial Number for an Incomplete Dial by User](#)]
- Renamed the parameter "OnHook DC Feed Current" to "Maximum DC Feed Current" [[Maximum DC Feed Current](#)]
- Added support to initiate a Re-Invite for fax transmission when the fax machine is the sender. [[Re-INVITE Upon CNG Count](#)]
- Updated the term "Blacklist" to "Block list". [[Blocklist for WAN Side Port](#)] [[Blocklist for WAN side](#)]
- Added support OpenVPN(R) failover option. [[OpenVPN\(R\) Server Secondary](#)]

Firmware version 1.0.27.3

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- Added support to Enable/Disable WEB access through the IVR. [[WAN Port Web Access](#)]
- Added support for the "Switch SIP Server When Keep-Alive Max Lost Is Reached". [[Switch SIP Server When Keep-Alive Max Lost Is Reached](#)]
- Added support Conference Notification Tone. [[Conference Notification Tone](#)]
- Added support Remote On Hold Tone. [[Remote On Hold Tone](#)]
- Added support for Ringing Transfer. [[Ringing Transfer](#)]
- Added RTP/RTCP keep alive feature. [[RTP/RTCP Keep Alive On Hold](#)]
- Added ability to support Authentication based on Username/Password on OpenVPN(R). [[OpenVPN\(R\) Username](#)][[OpenVPN\(R\) Password](#)]
- Added support to configure static DNS SRV records. [[Static DNS](#)]
- Added support to configure the Strict Password Rules. [[Strict Password Rules](#)]
- Added support for XMPP-based connection request. [[XMPP](#)]
- Added support for the secondary NTP server. [[Secondary NTP server](#)]
- Added ability to set local date and time. [[Local Time](#)]
- Added support to configure the T.38 Max Bit Rate. [[T.38 Max Bit Rate](#)]
- Update the "Subscribe Retry Wait Time upon 403 Forbidden" max value to 10080 minutes. [[Subscribe Retry Wait Time upon 403 Forbidden](#)]
- Added support to save Syslog settings and internal logs across a factory reset. [[P82307](#)]

Firmware version 1.0.25.2

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- Added support to check the certificate information of the device through IVR. [[Certification Information](#)]
- Added support of \$PN and \$MAC variables in Config Server Path. [[Config Server Path](#)]

Firmware version 1.0.23.8

Product Name: GXW4216 V1/GXW4224 V1/GXW4232 V1/GXW4248 V1

- Set the "Disable User Level Web Access" (P28158) to "Yes" by default. [[Disable User Level Web Access](#)]
- Set the "Disable Viewer Level Web Access" (P28159) to "Yes" by default. [[Disable Viewer Level Web Access](#)]
- Force user to change the password upon first login using the default password to the Admin/User/Viewer Account. [[Access the Web Configuration Menu](#)]

Firmware version 1.0.25.1

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- Set the "Disable User Level Web Access" (P28158) to "Yes" by default. [[Disable User Level Web Access](#)]
- Set the "Disable Viewer Level Web Access" (P28159) to "Yes" by default. [[Disable Viewer Level Web Access](#)]
- Force user to change the password upon first login using the default password to the Admin/User/Viewer Account. [[Access the Web Configuration Menu](#)]

Firmware version 1.0.23.2

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- Added Support for "Keep Security Setting After Reset". [[Keep Security Setting After Reset](#)]

Firmware version 1.0.23.7

Product Name: GXW4216 V1/GXW4224 V1/GXW4232 V1/GXW4248 V1

- No Major Changes.

Firmware version 1.0.21.2

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- Added a "Provision" button which lets user provision manually via WebUI. [[Provision](#)]
- Changed the order of download config file requests to cfgMAC.xml, cfgMAC, cfgMODEL.xml, and cfg.xml. [[Download and Process All Available Config Files](#)]

Firmware version 1.0.19.1

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- Added new value "Auto" in NAT Traversal. [[NAT Traversal](#)]
- Added support for AVS DTMF Detector Parameters. [[DSP DTMF Detector Min Level](#)] [[DSP DTMF Detector SNR](#)] [[DSP DTMF Detector Deviation](#)] [[DSP DTMF Detector Twist](#)]
- Added option to use P-Early-Media Header. [[P-Early-Media Header](#)]
- Added the ability to force local ringback tone with 180 ringing SDP. [[Ringback Tone at No Early Media](#)]
- Added support Radius Auth Protocol. [[Radius Auth Protocol](#)]
- Added ability to lock/unlock extension from analog phones using local feature code. [[Port Lock Code](#)]
- Added Ability to lock FXS ports. [[Lock/Unlock Extension Code](#)]

Firmware version 1.0.17.1

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- Updated the "Replace Beginning '+' in Caller ID with" support a predefined string. [[Replace the beginning '+' in Caller ID with](#)]
- Added the new option "3 - PR" in "Visual MWI type" which sends MWI signaling using Polarity Reversal. [[Polarity Reversal](#)]
- Added support the " = " sign in config and firmware server path. [[Firmware Server Path](#)] [[Config Server Path](#)]

- Updated "Prefer Primary SIP Server" options "1 - No" to "1 - Will register to primary server if failover server registration expires, and "2 - Will register to primary server if primary server responds". [[Prefer Primary SIP Server](#)]

Firmware version 1.0.15.2

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- Add the Ability to specify DTMF timing for InBand. [[Custom DTMF InBand Duration](#)]

Firmware version 1.0.13.2

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- Added support for the MWI Tone. [[MWI Tone](#)]
- Added support for the Special Proceed Indication Tone. [[Special Proceed Indication Tone](#)]
- Added support for the Special Condition Tone. [[Special Condition Tone](#)]
- Added the ability to ignore the alert-info header. [[Ignore Alert-Info Header](#)]
- Added the ability to Allow SIP Factory Reset. [[Allow SIP Factory reset](#)]
- Added the "Add MAC in User-Agent" configuration. [[Add MAC in User-Agent](#)]
- Added support for "Use MAC Header" configuration. [[Use MAC Header](#)]
- Added support for "Extra Debug" in Syslog Level. [[Syslog Level](#)]
- Update the status page to show the HW version with the model's name. [[Product Model](#)]
- Added the ability to configure special features with GIBTELECOM via TR069. [[GIBTELECOM](#)]

Firmware version 1.0.23.6

Product Name: GXW4216 V1/GXW4224 V1/GXW4232 V1/GXW4248 V1

- Added Support to download system information via WebUI. [[System info](#)]

Firmware version 1.0.11.2

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- Added support for Download and Process All Available Config Files. [[Download and Process All Available Config Files](#)].
- Added support for Enabling Using tags in URL [[Enable using tags in URL](#)]
- Added the new voice prompt *98. [[Voice prompt](#)]
- Added the additional Flash digit events in the Special Feature Gibtelecom. [[Flash Digit Control](#)]
- Added support for new override config file option in "cfgMAC_override.xml". [[Download and Process All Available Config Files](#)].

Firmware version 1.0.9.1

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- Added Password length to support up to 30 Characters. [[Web and SSH Access](#)]

Firmware version 1.0.7.2

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- Added support to Define the Preferred Provisioning Method. [[Upgrade and Provisioning](#)]
- Added support of DHCP Option 150. [[Upgrade and Provisioning](#)]
- Added support for SRTP Key Length. [[Profiles](#)]
- Added support for SSL Key Log File. [[Ethernet Capture.](#)]
- Added support for Security Controls for SSH Access. [[Web and SSH Access.](#)]
- Updated Syslog to make user reading more friendly.

Firmware version 1.0.5.4

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- Added support to send SNMP traffic through Management Interface. [[Network Settings](#)]
- Added support to send Syslog traffic through Management Interface. [[Network Settings](#)]

Firmware version 1.0.23.5

Product Name: GXW4216/GXW4224/GXW4232/GXW4248

- Added ability to send SNMP traffic through Management Interface. [[Network Settings](#)]

Firmware version 1.0.3.9

Product Name: GXW4216 V2/GXW4224 V2/GXW4232 V2/GXW4248 V2

- No major changes.

Firmware version 1.0.3.4

- This is the initial release version of GXW42xx V2 firmware.

Firmware version 1.0.23.2

- No major changes.

Firmware version 1.0.21.1

- No Major changes.

Firmware version 1.0.19.4

- Added support for Play Port Number. [[Play Port Number Feature](#)]

Firmware version 1.0.17.4

- Added support for OpenVPN(R). [[VPN](#)]
- Added support for DDNS. [[DDNS](#)]
- Added support for 802.1x. [[802.1x](#)]

Firmware version 1.0.15.2

- No major changes.

Firmware version 1.0.14.2

- No major changes.

Firmware version 1.0.13.3

- Added support for Send Hook Flash Event Method. [[Send Hook Flash Event Method](#)]

Firmware version 1.0.11.3

- Added support for Israel DST time zone. [[Time Zone](#)]
- Added support for validating subject alternative name when "Validate Server Certificates" is enabled. [[Validate Server Certificates](#)]
- Added support for SIP User-Agent Header. [[SIP User-Agent](#)]
- Increased RX Gain by adding "Force + x dB" options. [[Gain](#)]

Firmware version 1.0.9.4

- Added support for DHCP Option 67. [[Download and Process All Available Config Files](#)]
- Added support to configure Minimum/Maximum TLS versions. [[Minimums TLS Version](#)][[Maximum TLS Version](#)]

- Added feature RFC2543 Hold. [[RFC2543 Hold](#)]
- Added feature Syslog Protocol. [[Syslog Protocol](#)]
- Added feature to configure distinctive call waiting tones. [[Call Waiting Tones](#)]
- Added feature "SIP Log Option". [[SIP Log Option](#)]
- Added support to keep CDR record. [[CDR record option](#)]
- Added Feature "Disable Weak TLS Cipher Suites". [[Disable Weak TLS Cipher Suites](#)]
- Added feature "Disable Reminder Ring for DND". [[Disable Reminder Ring for DND](#)]
- Added feature "Callee Flash to 3WC". [[Callee Flash to 3WC](#)]
- Added feature "Connection Request Port" for TR-069. [[Connection Request Port](#)]
- Added support for DHCP Option 82. [Client Circuit ID (Option 82)][[Remote Agent ID \(Option 82\)](#)]
- Added feature "Local DNS Setting". [[Local DNS Setting](#)]
- Added support to send SNMP trap to 3 different servers. [[SNMP Trap IP](#)]
- Added Russian language support on Web UI and IVR. [[IVR Language](#)][[Configuring GXW42XX with Web Browser](#)]

Firmware version 1.0.7.10

- Added feature "Use Actual Ephemeral Port in Contact with TCP/TLS". [Use Actual Ephemeral Port in Contact with TCP/TLS]
- Added feature "Reset Call Features". [Reset Call Features]
- Added feature "Replace Beginning '+' with 00 in Caller ID. [Replace Beginning '+' with 00 in Caller ID]
- Added support to display call feature status on Web UI. [Call Features Status]
- Increased TX Gain and RX Gain range from (-6dB - 6dB) to (-12dB - 12dB). [Gain]
- Added support to allow "Name" configured under "FXS Ports" for ports that are part of the active hunting group to take effect. [FXS Name]

Firmware version 1.0.7.8

- No Major changes.

Firmware version 1.0.7.5

- Change Feature "Validate Server Certificates" default value to No. [[Validate Server Certificates](#)]

Firmware version 1.0.7.3

- Added feature "Enable SIP OPTIONS/NOTIFY Keep Alive". [Enable SIP OPTIONS/NOTIFY Keep Alive]
- Added feature "Call Record" to download the call history records from Web GUI. [Call Record]

Firmware version 1.0.5.43

- Added feature Conference Party Hangup Tone. [[Conference Party hangup tone](#)]
- Added feature Inter-port Calling. [[Inter-port Calling](#)]
- Added feature LED Pattern. [[LED Pattern](#)]
- Added feature Reply to ICMP. [[Reply to ICMP](#)]
- Added feature Validate Server Certificates. [[Validate Server Certificates](#)]
- Added feature Load CA Certificates. [[Load CA Certificates](#)]
- Added feature Disable User Level Web Access. [[Disable User Level Web Access](#)]
- Added feature Disable Viewer Level Web Access. [[Disable Viewer Level Web Access](#)]
- Added feature Randomized Automatic Upgrade. [[Randomized Automatic Upgrade](#)]

- Added feature Virtual Network Interface. [[Network settings for Management Interface](#)]
- Added feature Disable Voicemail Reminder Tone. [[Disable Voicemail Reminder Tone](#)]
- Added feature Disable # as Redial Key. [[Disable # as Redial key](#)]
- Added feature Ringing Frequency. [[Ringing Frequency](#)]
- Added support for call waiting tone to be repeated while the caller is still calling. [[Call Waiting](#)]
- Added support to play stutter tone when call feature under Profiles -> Call Features Settings is enabled. [[Enable Call Features](#)]

Firmware version 1.0.5.36

- Added support for Allow Auto-Dial Config Per Port. [[Allow Auto-Dial Config Per Port](#)]
- Added RTCP support. [[RTCP](#)]
- Added Custom Certificate support. [[Custom Certificate](#)]
- Added support for HTTPS server based on TLSv1.2. [[HTTP/HTTPS User Name](#)]

Firmware version 1.0.5.30

- No major changes.

Firmware version 1.0.5.28

- Added option to specify the priority for caller ID display [[Caller ID Display](#)]
- Added option to save syslog locally. [[Save Syslog](#)]
- Added option "Prefer Primary Outbound Proxy" to enable registration through primary outbound proxy if registration expires. [[Prefer Primary Outbound Proxy](#)]
- Added feature "Whitelist for WAN side" and "Blacklist for WAN side" for remote management. [[Access Control Lists](#)]
- Added feature "Lockout time interval" to change banning time after too many failed login attempts. [[Lockout Time Interval](#)].
- Added option "Web Access Mode" to choose between "HTTPS" and "HTTP" to access device Web UI. [[Web Access Mode](#)]
- Added option "HTTPS Web Port" to set HTTPS web port instead of using default web port. [[HTTPS Web Port](#)]
- Added local firmware upgrade support. [[Upload Device Firmware](#)]
- Change "Disable Telnet" option to "Disable SSH" option for more security. [[Disable SSH](#)]

Firmware version 1.0.5.16

- Added option [[DTMF-RELAY Tag Respect SIP INFO](#)] [[Use Request Routing ID in SIP Headers](#)] for Profile 1-4 audio settings.
- Added the option of [[Crypto Life Time](#)] to support RTP settings.
- Added option [[Play busy/reorder tone before Loop Current Disconnect](#)] for Profile 1-4 audio settings.
- Added the option of [[Disable Connected Line ID](#)] to support not display the connected line ID.
- Added the option of [[Flash Digit Control](#)] [[Crypto Life Time](#)] to overrides the default settings for call control.
- Added option to configure [[Local RTP port](#)].
- Added the option to configure [[SIP Registration Failure Retry Wait Time upon 403 Forbidden](#)].
- Added the option to enable/disable [[Hold Target Before Refer](#)].
- Added the option to enable/disable [[Authenticate server certificate domain](#)].
- Added the option to enable/disable [[Authenticate server certificate chain](#)].

- Added the option to configure [\[Trusted CA\]](#)
- Added the function of [\[Automatic Reboot\]](#).
- Added the option to [\[Allow DHCP Option 42 to NTP Server\]](#) to support Time and Date settings.
- Added the option to [\[Allow DHCP Option 2 to override time zone\]](#) to support Time and Date settings.
- Added the option to enable/disable [\[3CX Auto Provision\]](#) to support multicast SUBSCRIBE for provision.

Firmware version 1.0.5.8

- Added option [\[SIP REGISTER Contact Header Uses\]](#) [\[Use Request Routing ID in SIP Headers\]](#) for Profile 1-4 to support NAT transfer feature.

Firmware version 1.0.5.5

- Added option [\[Enable Fast RFC2833\]](#) to set DTMF duration by RFC2833.
- Added SNMP support.[\[SNMP\]](#)
- Added QoS settings for SIP and RTP packets. Rearranged options [\[Layer 2 QoS Settings\]](#) and [\[Layer 3 QoS Settings\]](#).
- Added star code [\[*98\]](#) to play registration ID
- Added star code [\[*99\]](#) to trigger provisioning process.
- Added support to download device configuration file. [\[Download Device Configuration\]](#)

Firmware version 1.0.4.22

- Added support for audio codec G.722. [\[Preferred Vocoder \(Codec\)\]](#)
- Added option [\[Always send HTTP Basic Authentication Information\]](#) to enable sending HTTP authentication without server challenge
- Added the options to enable/disable [\[Use P-Preferred-Identity Header\]](#) and [\[Use Privacy Header\]](#)
- Added the options to enable/disable [\[Do Not Escape '#' as %23 in SIP URI\]](#)

Firmware version 1.0.4.17

- Added [\[Use Request Routing ID in SIP Headers\]](#) to enable/disable device to use configured Request URI Routing ID for certain FXS port in its SIP message Header when a trunk SIP account is used.
- Added option [\[Add Auth Header on Initial REGISTER\]](#) to enable/disable including authentication header in the initial REGISTER.

Firmware version 1.0.4.7

- Added option [\[Enable LLDP\]](#) to enable/disable LLDP.
- Added field [\[Request URI Routing ID\]](#) to allow device to route the calls to individual FXS ports based on the DID, when only have one sip registration.

Firmware version 1.0.4.4

- Added option [\[Display Language\]](#) to choose language for LCD display.
 - Added option [\[Prompt Dial Tone Code\]](#) to configure dial code.
-