

Grandstream Networks, Inc.

GXW450X series

1, 2 or 4 T1/E1/J1 Interfaces

Digital VoIP Gateway

User Manual



COPYRIGHT

©2019 Grandstream Networks, Inc. <http://www.grandstream.com>

All rights reserved. Information in this document is subject to change without notice. Reproduction or transmittal of the entire or any part, in any form or by any means, electronic or print, for any purpose without the express written permission of Grandstream Networks, Inc. is not permitted.

The latest electronic version of this guide is available for download here:

<http://www.grandstream.com/support>

Grandstream is a registered trademark and Grandstream logo is trademark of Grandstream Networks, Inc. in the United States, Europe and other countries.

Caution

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 guide, could void your manufacturer warranty.

Safety Compliance

The GXW450X adaptor complies with FCC/CE and various safety standards. The GXW450X power adaptor is compliant with UL standard. Only use the universal power adapter provided with the GXW450X package. The manufacturer's warranty does not cover damages to the device caused by unsupported power adaptors



FCC Compliance Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Important: Any Changes or modifications not expressly approved by the party responsible could void the user's authority to the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.



Administrative Council for Terminal Attachments (ACTA) Customer Information

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. Located on the equipment label that contains, among other information, the ACTA registration number and ringer equivalence number (REN). If requested, this information must be provided to the telephone company.

The REN is used to determine the quantity of devices which may be connected to the telephone line. Excessive REN's on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of the REN's should not exceed five (5.0). To be certain of the number of devices that may be connected to the line, as determined by the total REN's contact the telephone company to determine the maximum REN for the calling area.

This equipment cannot be used on the telephone company-provided coin service. Connection to Party Line Service is subject to State Tariffs.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. If advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

If trouble is experienced with this equipment, please contact Grandstream Networks, Inc.

If the trouble is causing harm to the telephone network, the telephone company may request you to remove the equipment from the network until the problem is resolved.



Table of Contents

CHANGE LOG	15
Firmware version 1.0.0.24	15
Firmware version 1.0.0.22	15
Firmware version 1.0.0.20	15
Firmware version 1.0.0.18	15
WELCOME	16
GATEWAY GXW450X OVERVIEW.....	17
Feature Highlights.....	17
GXW450X Technical Specifications.....	17
GETTING STARTED.....	20
Equipment Packaging	20
Connecting the GXW450X.....	20
Using GXW450X Keypad Menu	21
Use the LED Indicators	23
Configuring GXW450X via Web GUI	24
<i>Web GUI Access.....</i>	<i>24</i>
<i>Reset Password at First Login.....</i>	<i>25</i>
<i>Setup Wizard</i>	<i>25</i>
<i>Web GUI Configurations.....</i>	<i>26</i>
<i>Web GUI Languages</i>	<i>27</i>
<i>Save and Apply Changes</i>	<i>27</i>
SYSTEM STATUS.....	28
Dashboard	28
<i>Space Usage</i>	<i>28</i>
<i>Resource Usage</i>	<i>29</i>
<i>Disk Capacity.....</i>	<i>30</i>
<i>PBX Status</i>	<i>31</i>
<i>Interfaces Status.....</i>	<i>31</i>
<i>Trunks</i>	<i>32</i>



System Information	33
<i>General</i>	33
<i>Network</i>	35
Active Calls	36
Network status	36
SYSTEM SETTINGS.....	38
HTTP Server	38
Network Settings	39
<i>DHCP Client List</i>	42
<i>802.1X Settings</i>	44
<i>Static Routes</i>	45
<i>Port Forwarding</i>	46
OpenVPN®	47
DDNS Settings	49
Security Settings	51
<i>Static Defense</i>	51
<i>Dynamic Defense</i>	54
<i>Fail2Ban</i>	56
<i>SSH Access</i>	58
Time Settings	58
<i>Automatic Date and Time</i>	58
<i>Set Date and Time</i>	60
<i>NTP Server</i>	61
<i>Office Time</i>	62
<i>Holiday</i>	64
Email Settings	66
<i>Email Settings</i>	66
<i>Email Template</i>	68
<i>Email Send Log</i>	70
TRUNKS	72
Digital Trunks	72
<i>Digital Hardware Configuration</i>	72
<i>Digital Trunk Configuration</i>	85
<i>Digital Trunk Troubleshooting</i>	86
VoIP Trunks	87



Outbound Routes.....	93
Inbound Routes.....	96
<i>Inbound Route Configuration</i>	96
<i>Inbound Route: Import/Export Inbound Route</i>	97
PBX SETTINGS.....	99
SIP Settings.....	99
<i>General</i>	99
<i>Misc</i>	99
<i>Session Timer</i>	101
<i>TCP and TLS</i>	101
<i>NAT</i>	103
<i>ToS</i>	103
RTP Settings.....	105
<i>RTP Settings</i>	105
<i>Payload Type Settings</i>	105
Voice Prompt.....	106
<i>Download and Install Voice Prompt Package</i>	106
<i>Manual Upload of Prompt Package</i>	108
Jitter Buffer.....	108
Interface Settings.....	109
MAINTENANCE.....	110
User Management.....	110
Change Information.....	111
<i>Change Password</i>	111
<i>Change Binding Email</i>	112
<i>Login Settings</i>	113
Operation Log.....	114
Syslog.....	116
System Events.....	118
<i>Alert Log</i>	118
<i>Alert Events List</i>	119
<i>Alert Contact</i>	121
Upgrade.....	122
<i>Upgrading via Network</i>	122
<i>Upgrading via Local Upload</i>	124



<i>Upgrading via a Local Server</i>	125
<i>No Local Firmware Server</i>	125
Backup	125
<i>Backup/Restore</i>	126
<i>Data Sync</i>	128
<i>Restore Configuration from Backup File</i>	130
System Cleanup/Reset	131
<i>Reset & Reboot</i>	131
<i>Cleaner</i>	132
<i>USB/SD Card Files Cleanup</i>	133
Network Troubleshooting	134
<i>Ethernet Capture</i>	134
<i>IP Ping</i>	135
<i>Traceroute</i>	135
Signaling Troubleshooting	136
Service Check	136
CDR (CALL DETAIL RECORD).....	137
CDR Filter	137
CDR Report Operations	139
Automatic Download	140
CDR Report Data Fields	141
EXPERIENCING THE GXW450X SERIES DIGITAL GATEWAY.....	144



Table of Tables

Table 1: GXW450X Features Highlights	17
Table 2: GXW450X Technical Specifications	17
Table 3: Definitions of the GXW450X Connectors	21
Table 4: LCD Menu Options	22
Table 5: GXW450X LED Indicators	23
Table 6: System information→General	33
Table 7: GXW450X Network Settings→Basic Settings.....	39
Table 8: GXW450X Network Settings→802.1X	45
Table 9: GXW450X Network Settings→Static Routes	45
Table 10: GXW450X System Settings → Network Settings→Port Forwarding	46
Table 11: GXW450X System Settings→Network Settings→OpenVPN®	47
Table 12: GXW450X Static Defense→Current Service	51
Table 13: Firewall Rule Settings.....	53
Table 14: Firewall Rule Settings.....	54
Table 15: GXW450X Firewall Dynamic Defense.....	54
Table 16: Fail2Ban Settings	56
Table 17: Automatic Date and Time Settings	59
Table 18: Date and Time Manual Settings	61
Table 19: Office Time Settings	63
Table 20: Holiday Settings.....	65
Table 21: Email Settings.....	66
Table 22: Email Log Filter.....	71
Table 23: Digital Hardware Configuration Parameters: E1 – PRI_NET/PRI_CPE	74
Table 24: Digital Hardware Configuration Parameters: E1 - SS7	76
Table 25: Digital Hardware Configuration Parameters: E1 - MFC/R2	78
Table 26: Digital Hardware Configuration Parameters: T1/J1 - PRI_NET/PRI_CPE.....	81
Table 27: Digital Hardware Configuration Parameters: T1/J1 - SS7.....	83
Table 28: Digital Trunk Configuration Parameters	85
Table 29: Create New SIP Trunk.....	88
Table 30: VoIP Trunk Configuration Parameters – Register SIP Trunk	89
Table 31: VoIP Trunk Configuration Parameters – Peer SIP Trunk	91
Table 32: Inbound Rule Configuration Parameters.....	96
Table 33: SIP Settings - General.....	99



Table 34: SIP Settings - Misc	100
Table 35: SIP Settings/Session Timer	101
Table 36: SIP Settings/TCP and TLS	101
Table 37: NAT Settings.....	103
Table 38: ToS Settings	103
Table 39: RTP Settings.....	105
Table 40: Payload Type Configuration	105
Table 41: Jitter Buffer Settings	109
Table 42: Create New User Information.....	111
Table 43: Change Password Parameters	112
Table 44: Operation Log Column Header	115
Table 45: Network Upgrade Configuration	123
Table 46: Data Sync Configuration	129
Table 47: Cleaner Configuration	132
Table 48: Ethernet Capture Parameters	134
Table 49: CDR Filter parameters	137
Table 50: CDR Report Data Fields.....	141



Table of Figures

Figure 1: GXW450X Package Contents	20
Figure 2: Diagram of GXW4504 Back and Front Panel.....	21
Figure 3: GXW450X Web GUI Login Page.....	24
Figure 4: Reset Password.....	25
Figure 5: GXW450X Setup Wizard	26
Figure 6: GXW450X Web GUI Languages	27
Figure 7: GXW450X Dashboard	28
Figure 8: Space Usage	29
Figure 9: Resource Usage	30
Figure 10: Device Storage Capacity	30
Figure 11: PBX Status.....	31
Figure 12: Interface Status.....	32
Figure 13: Trunks Status	32
Figure 14: Digital Trunk Channels Status	33
Figure 15: System Information→General	34
Figure 16: System Information→Network	35
Figure 17: Active Calls	36
Figure 18: Active connections	36
Figure 19: Active Unix Domain Sockets.....	37
Figure 20: DHCP Client List.....	42
Figure 21: Add Bind New MAC Address Bind.....	43
Figure 22: Batch Add MAC Address Bind	43
Figure 23: GXW450X Using 802.1X as Client	44
Figure 24: GXW450X using 802.1X EAP-MD5.....	44
Figure 25: OpenVPN® Feature on the GXW450X	48
Figure 26: Register Domain Name on Noip.com	49
Figure 27: GXW450X DDNS Settings.....	50
Figure 28: Using Domaine Name to Connect to GXW450X.....	50
Figure 29: Create New Firewall Rule	52
Figure 30: Dynamic Defense Configuration	55
Figure 31: Fail2Ban Settings.....	56
Figure 32:SSH Access	58
Figure 33: Automatic Date and Time Settings.....	59
Figure 34: Date and Time Manual Configuration	61



Figure 35: GXW450X NTP Server	62
Figure 36: Add New Office Time	63
Figure 37: Time Settings→Office Time	64
Figure 38: Add a Holiday.....	64
Figure 39: Time Settings→Holiday.....	65
Figure 40: Email Settings	68
Figure 41: Email Templates.....	69
Figure 42: Alert Events Template	70
Figure 43: Email Send Log.....	71
Figure 44: Digital Hardware Configuration.....	73
Figure 45: Digital Port Configuration.....	73
Figure 46: Troubleshooting Digital Trunks	87
Figure 47: Create Outbound Route.....	94
Figure 48: Create Inbound Routes.....	96
Figure 49: Import/Export Inbound Route.....	98
Figure 50: SIP Settings - General	99
Figure 51: SIP Settings/Misc.....	100
Figure 52: Language Settings for Voice Prompt	107
Figure 53: Voice Prompt Package List.....	107
Figure 54: New Voice Prompt Language Added	108
Figure 55: Upload Voice prompt Package	108
Figure 56: User Management Page Display	110
Figure 57: Create New User	111
Figure 58: Change Password.....	112
Figure 59: Change Binding Email	113
Figure 60: Login Timeout Settings	114
Figure 61: Operation Logs	115
Figure 62: Operation Logs Filter	116
Figure 63: Syslog Settings	117
Figure 64: System Events→Alert Log.....	118
Figure 65: Alert Log Filter.....	118
Figure 66: System Events→Alert Events Lists: Disk Usage.....	119
Figure 67: System Events→Alert Events Lists: External Disk Usage.....	120
Figure 68: System Events→Alert Events Lists: Memory Usage.....	120
Figure 69: System Events→Alert Events Lists: System Crash.....	121
Figure 70: Alert Contact	122



Figure 71: Network Upgrade	123
Figure 72: Upgrading Firmware Files	124
Figure 73: Create New Backup	126
Figure 74: Backup / Restore	127
Figure 75: Schedule Backup	128
Figure 76: Data Sync	129
Figure 77: Restore GXW450X from Backup File	130
Figure 78: Reset and Reboot	131
Figure 79: Cleaner	132
Figure 80: SB/SD Card Files Cleanup	133
Figure 81: Ethernet Capture	134
Figure 82: IP Ping	135
Figure 83: Traceroute	136
Figure 84: Service Check	136
Figure 85: CDR Filter	137
Figure 86: Call Report	138
Figure 87: Automatic CDR Download	140



GNU GPL INFORMATION

GXW450X firmware contains third-party software licensed under the GNU General Public License (GPL). Grandstream uses software under the specific terms of the GPL. Please see the GNU General Public License (GPL) for the exact terms and conditions of the license.

Grandstream GNU GPL related source code can be downloaded from Grandstream web site from:
<http://www.grandstream.com/support/faq/gnu-general-public-license/gnu-gpl-information-download>



CHANGE LOG

This section documents significant changes from previous versions of GXW450X 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 1.0.0.24

- No major changes.

Firmware version 1.0.0.22

- No major changes.

Firmware version 1.0.0.20

- No major changes.

Firmware version 1.0.0.18

- This is the initial version.



WELCOME

Thank you for purchasing the Grandstream GXW450X Digital VoIP Gateway. The GXW450X offers an easy to manage, easy to configure IP communications solution for any business with virtual and/or branch locations. The GXW450X 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 an ISDN system into a VoIP network, and efficiently manage communication costs.

This manual will help you learn how to operate and manage your GXW450X Digital 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 Digital VoIP Gateway is very easy to manage and scalable, specifically designed to be an easy to use and affordable VoIP solution for large and medium sized enterprises

Safety Compliance

The GXW450X is compliant with various safety standards including FCC/CE. Its power adapter is compliant with UL standard.

Warning: *Use only the power adapter included in the GXW450X package. Use of alternative power adapter may permanently damage the unit.*

Warranty

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, contact your Grandstream Support for an RMA (Return Materials Authorization) number. Grandstream reserves the right to change the warranty policy without prior notification.

Caution: *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.*




GATEWAY GXW450X OVERVIEW

The GXW450X series are E1/T1/J1 Digital VoIP Gateways that allow digital PSTN and ISDN trunks to be integrated with VoIP networks. By connecting the GXW450X series with a VoIP network and traditional PBX or E1/T1/J1 providers, businesses can drastically increase the number of PSTN/ISDN trunks integrated with their VoIP network and the concurrent calls supported. The GXW450X series offer three models that provide 1, 2 or 4 T1/E1/J1 spans and support 30, 60 or 120 concurrent calls.

Feature Highlights

The following table contains the major features of the GXW450X:

Table 1: GXW450X Features Highlights

 <p style="text-align: center;">GXW450X</p>	<ul style="list-style-type: none"> • 1,2 or 4 Software configurable E1/T1/J1 ports • Support of PRI, SS7 and MFC R2 Signaling protocols • Dual Gigabit Auto-sensing RJ45 Network ports with integrated NAT router • Support of T.38 FAX for creating Fax-over-IP • Support of a wide range of voice codecs, including G.722, G.729, iLBC, OPUS and more • TLS and SRTP security encryption technology to protect calls and accounts • Support of multi-language voice prompt • Supports up to 120 concurrent calls
--	--

GXW450X Technical Specifications

The following table resumes all the technical specifications including the protocols/standards supported, voice codecs, languages and upgrade/provisioning settings for the GXW450X

Table 2: GXW450X Technical Specifications

Interfaces	
T1/E1/J1 Interface	1/2/4 RJ45 ports, supporting up to 30/60/120 simultaneous VoIP calls
Network Interfaces	Dual self-adaptive Gigabit ports (switched or routed)
Peripheral Ports	(2) USB 3.0, (1) SD card interface
LED Indicators	WAN, LAN, T1/E1/J1



LCD Display	128x32 dot matrix graphic LCD with DOWN and OK buttons
Reset Switch	Yes, long press for factory reset and short press for reboot
Voice Capabilities	
Voice-over-Packet Capabilities	LEC with NLP Packetized Voice Protocol Unit, 128ms-tail-length carrier grade Line Echo Cancellation, Dynamic Jitter Buffer, Modem detection & auto-switch to G.711
Voice and Fax Codecs	G.711 A-law/U-law, G.722, G.723.1 5.3K/6.3K, G.726, G.729A/B, Opus, iLBC, GSM-FR, AAL2-G.726-32
Fax over IP	T.38 compliant Group 3 Fax Relay up to 14.4kpbs and auto-switch to G.711 for Fax Passthrough, Fax data pump V.17, V.21, V.27ter, V.29 for T.38 fax relay.
Voice-quality Enhancement	Echo cancellation (G.168-2004), Jitter buffer, Silence suppression (VAD, CNG), PLC
QoS	Layer 2 QoS (802.1Q, 802.1p) and Layer 3 (ToS, DiffServ, MPLS) QoS
Signaling & Control	
DTMF Methods	In-audio, RFC2833 and/or SIP INFO
Digital Signaling	SIP (RFC 3261) over UDP/TCP/TLS, PRI, SS7, MFC R2, RBS (pending) PRI switch types: Euro ISDN, nation, Q.SIG CAS: MFC R2 (Argentina, Brazil, China, Czech Republic, Colombia, Ecuador, Indonesia, ITU, Mexico, Philippines, Venezuela) SS7: ITU, ANSI, China
Upgrade	Firmware upgrade via TFTP / HTTP / HTTPS or local HTTP upload
Device Management	Syslog, HTTPS, Web browser, voice prompt, TR-069 management, backup and restore, port capture and packet capture
Network Protocols	TCP/UDP/IP, RTP/RTCP, ICMP, ARP, DNS, DDNS, DHCP, NTP, TFTP, SSH, HTTP/HTTPS, PPPoE, STUN, SRTP, TLS, LDAP, PPP, Frame Relay (pending), IPV6, OpenVPN®
Status and statistic	Call status and history, device status monitoring and ISDN status monitoring
Security	
Media Encryption	SRTP, TLS, HTTPS, SSH, 802.1X



User-defined ports	SIP port, RTP port, HTTP/HTTPS port
Advanced Defense	Fail2ban, alert events, Whitelist, Blacklist, strong password-based access control
Physical	
Universal Power Supply	Input: 100-240VAC, 50/60Hz Output: DC+12V/2A
Physical & Dimensions	GXW4501: Unit Weight: 2350g; Package Weight: 3130g GXW4502: Unit Weight: 2360g; Package Weight: 3140g GXW4504: Unit Weight: 2380g; Package Weight: 3160g Unit Dimensions: 485mm(L) x 191mm(W) x 46.2mm (H)
Temperature and Humidity	Operating: 32 - 113°F / 0 ~ 45°C, Humidity 10 - 90% (non-condensing) Storage: 14 - 140°F / -10 ~ 60°C, Humidity 10 - 90% (non-condensing)
Mounting	Rack mount & Desktop
Additional Features	
Multi-Language Support	Web UI: English, Simplified Chinese, Traditional Chinese, Spanish, French, Portuguese, German, Russian, Italian, Polish, Czech; Customizable IVR/voice prompts: English, Chinese, British English, German, Spanish, Greek, French, Italian, Dutch, Polish, Portuguese, Russian, Swedish, Turkish, Hebrew, Arabic; Customizable language pack to support any other languages
Compliance	FCC: 47 CFR FCC Part 15 Class B 47 CFR FCC Part 68 (TIA-968-B Section 5.2.4 (T1+ISDN)) CE: EN 55032, EN 55035, EN 61000-3-2, EN 61000-3-3, EN 60950-1, TBR 4 (E1+ISDN), TBR 12 (E1), TBR 13 (E1+ISDN) RCM: AS/NZS CISPR 32, AS/NZS 61000.3.2, AS/NZS 61000.3.3, AS/NZS 60950.1, AS/ACIF S016 (E1), AS/ACIF S038 (E1+ISDN) ITU K.21 (Enhanced Levels) UL 60950-1 (Power adapter)



GETTING STARTED

This chapter provides basic installation instructions including the list of the packaging contents and also information for obtaining the best performance with the GXW450X.

Equipment Packaging

Unpack and check all accessories. Equipment includes

- One device unit (GXW4501, GXW4502 or GXW4504)
- One RJ45 Ethernet cable
- One 12V universal power adapter
- One Quick Installation
- One GPL Statement

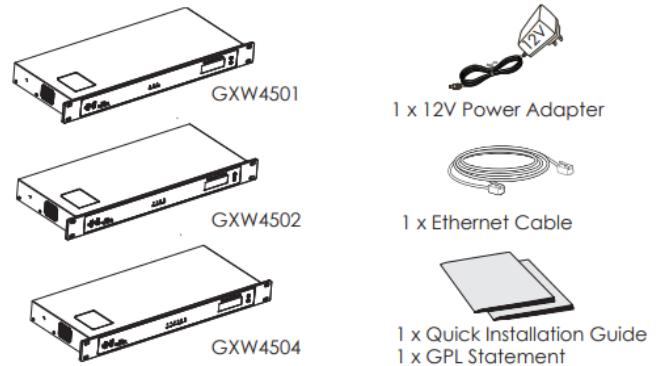


Figure 1: GXW450X Package Contents

Connecting the GXW450X

Connecting the GXW450X gateway is easy. Follow these steps to connect your GXW450X gateway to the Internet and access the unit's configuration pages.

1. Connect one end of a straight through RJ45 Ethernet cable into the WAN port of the GXW450X; connect the other end into the uplink port of an Ethernet switch/hub.
2. Connect the 12V DC power adapter into the DC 12V power jack on the back of the GXW450X. Insert the main plug of the power adapter into a surge-protected power outlet.
3. Connect one end of the T1/E1/J1 cable provided from the service provider into the T1/E1/J1 port of the GXW450X; connect the other end into the T1/E1/J1 wall jack.
4. Wait for the GXW450X to boot up. The front LCD display will show the GXW450X hardware information when the boot process is completed.
5. Once the GXW450X is successfully connected to the network via WAN port, the Network LED indicator will be lit green, and an IP address will be shown on the LCD display.

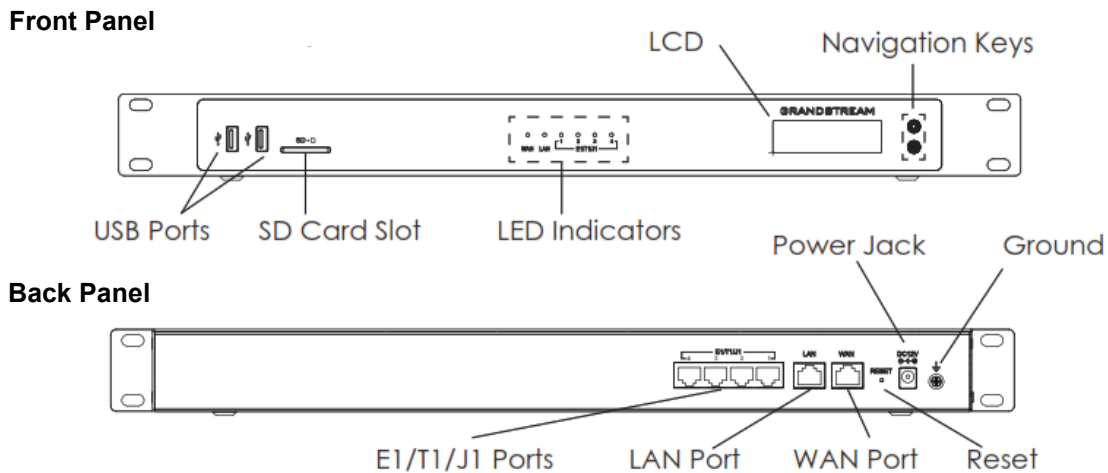


Figure 2: Diagram of GXW4504 Back and Front Panel

Table 3: Definitions of the GXW450X Connectors

WAN/LAN ports	Ethernet ports used to connect the GXW to the local and external network
RESET	Factory Reset button. Press and hold for a while to reset factory default settings.
Power Jack	Power adapter connection
E1/T1/J1 ports	Digital port to be connected to a digital line.
USB port	2 Ports used to connect external USB drives to the GXW
SD Card Slot	Reads the SD cards memory
Ground	The ground screw that needs to be connected to the ground.

Using GXW450X Keypad Menu

The keypad menu of the GXW450X consists of 2 buttons: OK and Down keys to navigate different options.

1. Press “OK” key to start browsing menu options.
2. Press “Down” to browse different menu options. Press “OK” to select an entry.
3. In the menu option, select “Back” to go back to previous menu.
4. The LCD will return to default display after being idle in menu for longer than 20 seconds.

The following table shows the LCD menu options.



Table 4: LCD Menu Options





View Events	<ul style="list-style-type: none"> • Critical Events • Other Events
Device Info	<ul style="list-style-type: none"> • Hardware: Hardware version number • Software: Software version number • P/N: Part number • MAC: Device MAC address • Uptime: System up time since the last reboot
Network Info	<ul style="list-style-type: none"> • LAN Mode: DHCP, Static IP or PPPoE • LAN IP: IP address • LAN Subnet Mask
Network Menu	<ul style="list-style-type: none"> • LAN Mode: Select LAN mode as DHCP, Static IP or PPPoE • Static Routes Reset: Click to reset the static route setting
Factory Menu	<ul style="list-style-type: none"> • Reboot • Factory Reset • LCD Test Patterns Press “OK” to start. Then press “Down” button to test different LCD patterns. When done, press “OK” button to exit. • Fan Mode Select “Auto” or “On”. • LED Test Patterns Select “All On” “All Off” or “Blinking” and check LED status for USB, SD, T1/E1/J1, Phone 1/Phone 2, Line 1/Line 2 ports. After the LED test, select “Back” in the menu and the device will show the LED actual status again. • RTC Test Patterns Select “2022-02-22 22:22” or “2011-01-11 11:11” to start the RTC (Real-Time Clock) test pattern. Check the system time from LCD idle screen by pressing “DOWN” button, or from Web GUI→System Status→General page. After

	<p>the test, reboot the device manually and the device will display the correct time.</p> <ul style="list-style-type: none"> • Hardware Testing <p>Select “Test DSP” to perform DSP test on the device.</p> <p>This is mainly for factory testing purpose which verifies the hardware connection inside the device. The diagnostic result displays on the LCD after the test is done.</p>
Default Password	Showing the default Web login password. Once the password was changed, this menu will not show again.
Web Info	<ul style="list-style-type: none"> • Protocol: Web access protocol. HTTP or HTTPS. By default, it's HTTPS • Port: Web access port number. By default, it's 8089
SSH Switch	<ul style="list-style-type: none"> • Enable SSH: Enable SSH access. • Disable SSH: Disable SSH access. <p>By default, the SSH access is disabled.</p>

Use the LED Indicators

The GXW450X has LED indicators in the front to display connection status. The following table shows the status definitions.

Table 5: GXW450X LED Indicators

LED Indicator	LED Status
Power LAN WAN	 Solid: Connected  OFF: Disconnected
T1/E1/J1	 Solid: Connected and working  Blinking: No cable is connected; or connected but the link is not working at all.



Configuring GXW450X via Web GUI

Web GUI Access

The GXW450X embedded Web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a Web browser such as Microsoft IE, Mozilla Firefox, Google Chrome.

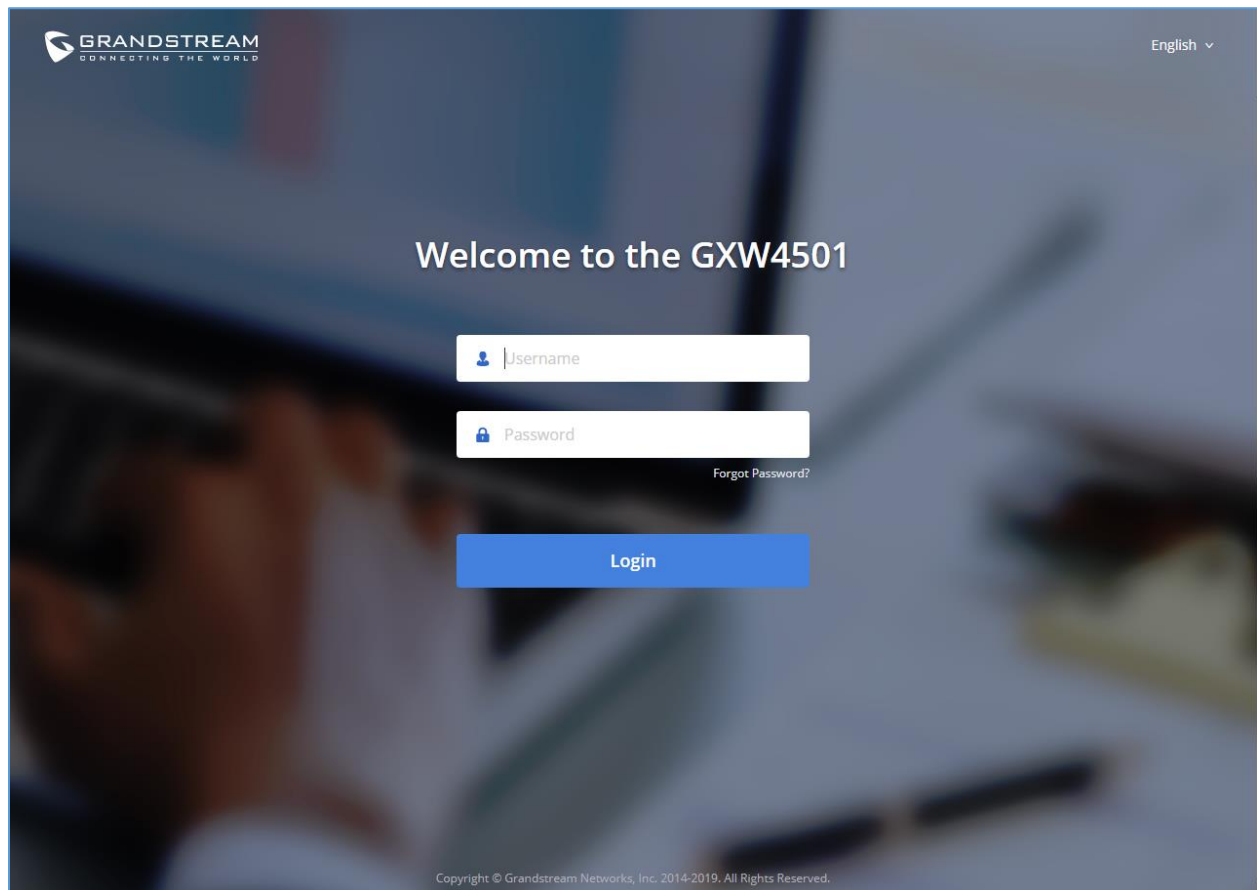


Figure 3: GXW450X Web GUI Login Page

To access the Web GUI:

1. Connect the computer to the same network as the GXW450X.
2. Ensure the GXW450X is properly powered on and displays the IP address on the LCD screen.
3. Open a web browser on the computer and enter the displayed IP address into the search bar in the following format: **https://ipaddress:portnumber**
4. Enter username and password to login. (The default administrator username is “admin” and the default random password can be found at the sticker on the GXW450X).



Reset Password at First Login

At first login, users will be forced to change default admin password. The following screen will be shown, enter requested information to proceed:

- **Enter New Password**
- **Re-enter New Password**
- **Email Addresses:** Email to be used to recover password if lost.

Press “Confirmed” to apply the settings and access web GUI.

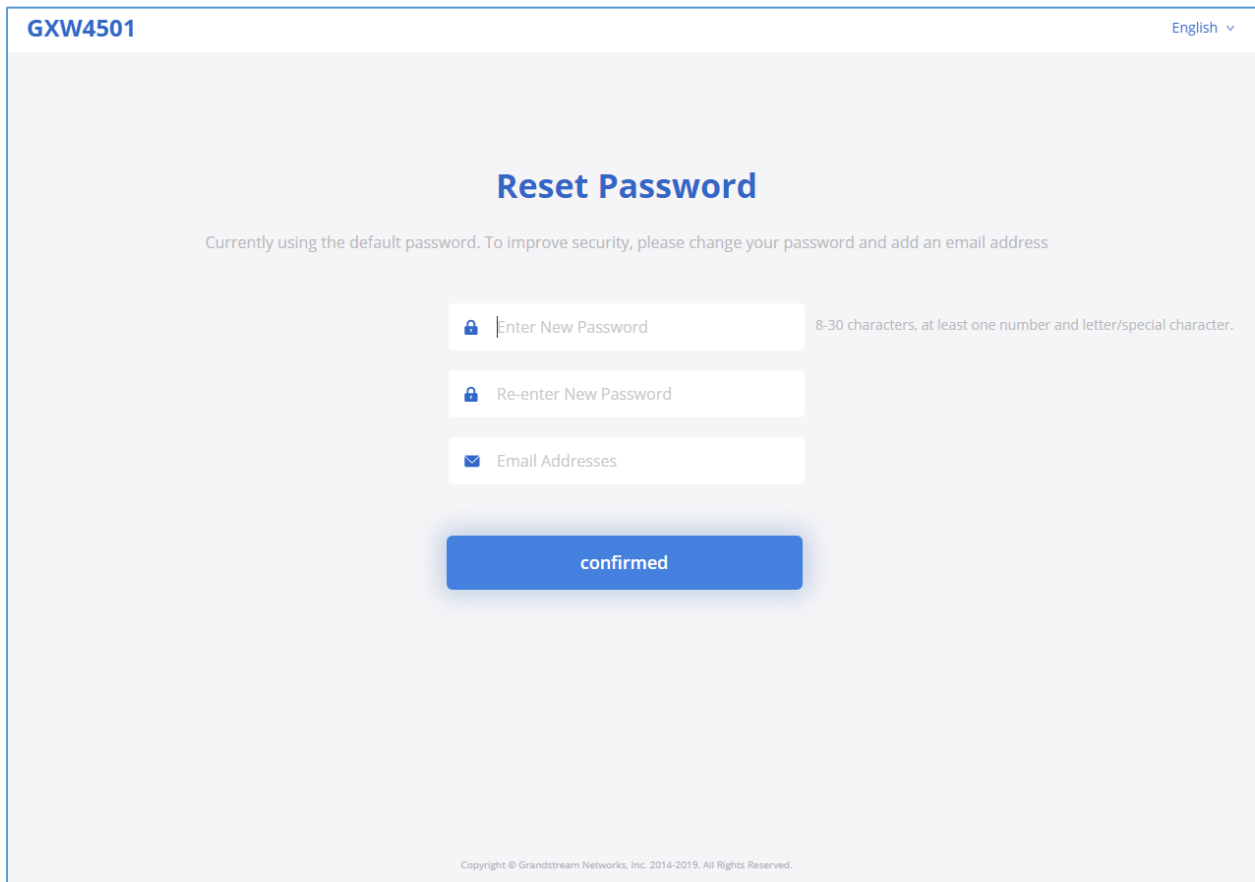
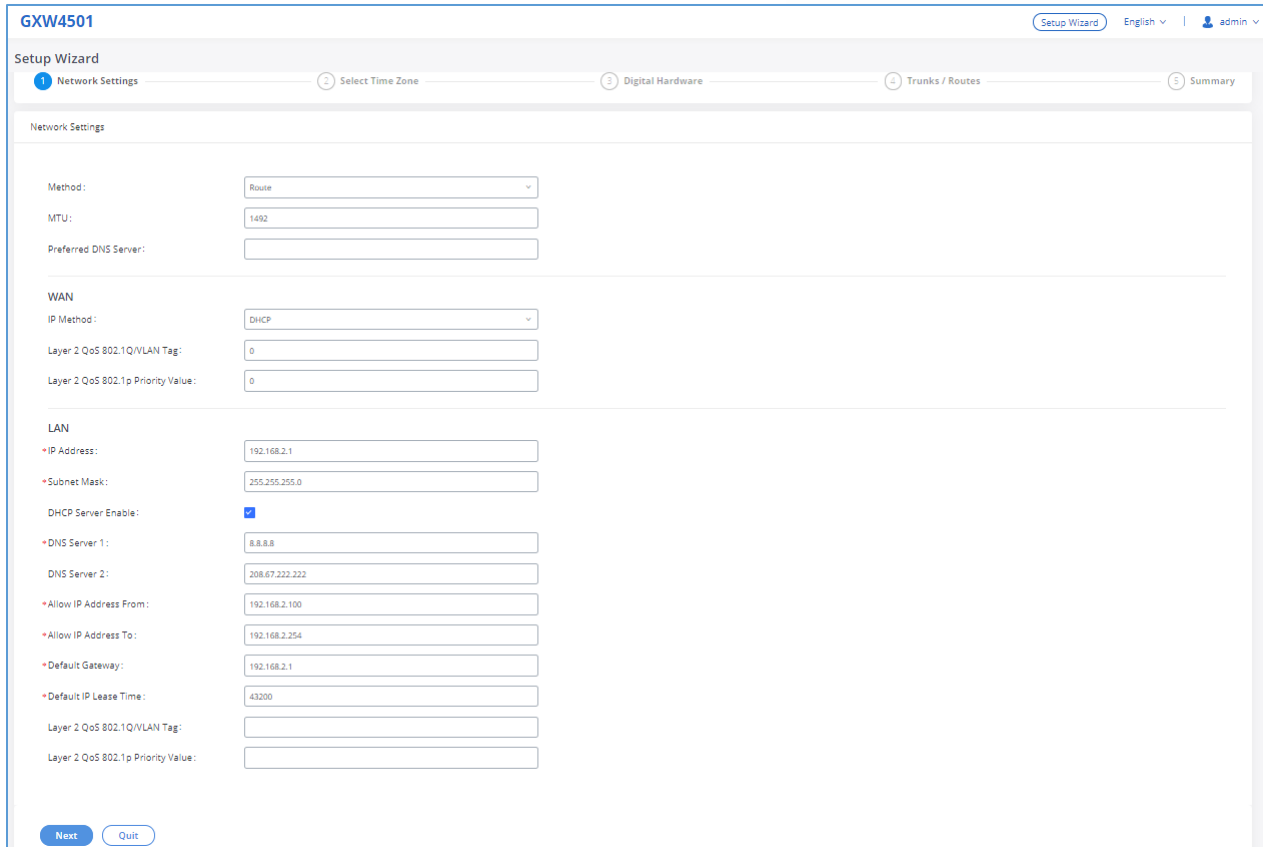


Figure 4: Reset Password

Setup Wizard

When the user logs in the GXW450X Web GUI for the first time, he will be asked to change default password and add an email address to improve security, and a setup wizard will provide guidance to set up basic configuration. Configurations in setup wizard include: Network settings, Time zone and Trunk/routes.



GXW4501 Setup Wizard | English | admin

1 Network Settings | 2 Select Time Zone | 3 Digital Hardware | 4 Trunks / Routes | 5 Summary

Network Settings

Method:

MTU:

Preferred DNS Server:

WAN

IP Method:

Layer 2 QoS 802.1Q/VLAN Tag:

Layer 2 QoS 802.1p Priority Value:

LAN

* IP Address:

* Subnet Mask:

DHCP Server Enable:

* DNS Server 1:

DNS Server 2:

* Allow IP Address From:

* Allow IP Address To:

* Default Gateway:

* Default IP Lease Time:

Layer 2 QoS 802.1Q/VLAN Tag:

Layer 2 QoS 802.1p Priority Value:

Figure 5: GXW450X Setup Wizard

Web GUI Configurations

There are six main sections in the Web GUI for users to view the Gateway status, configure and manage the GXW450X.

- **System Status:** Displays GXW450X Dashboard, System Information, Active calls and network status.
- **Trunk:** To Digital and VoIP trunks and manage inbound/outbound call routes.
- **PBX Settings:** SIP Settings, RTP Settings and interfaces settings.
- **System Settings:** To configure The HTTP server, network settings, OpenVPN®, security settings, Email Settings, Time Settings.
- **Maintenance:** To perform firmware upgrade, backup configurations, user management cleaner setup, reset/reboot, syslog setup and troubleshooting
- **CDR:** View call records and download CDR reports.

Web GUI Languages

Currently the GXW450X series Web GUI supports **English, Simplified Chinese, Traditional Chinese, Spanish, French, Portuguese, Russian, Italian, Polish, German etc.**

Users can select the displayed language in Web GUI login page or at the upper right tab of the Web GUI after logging in.

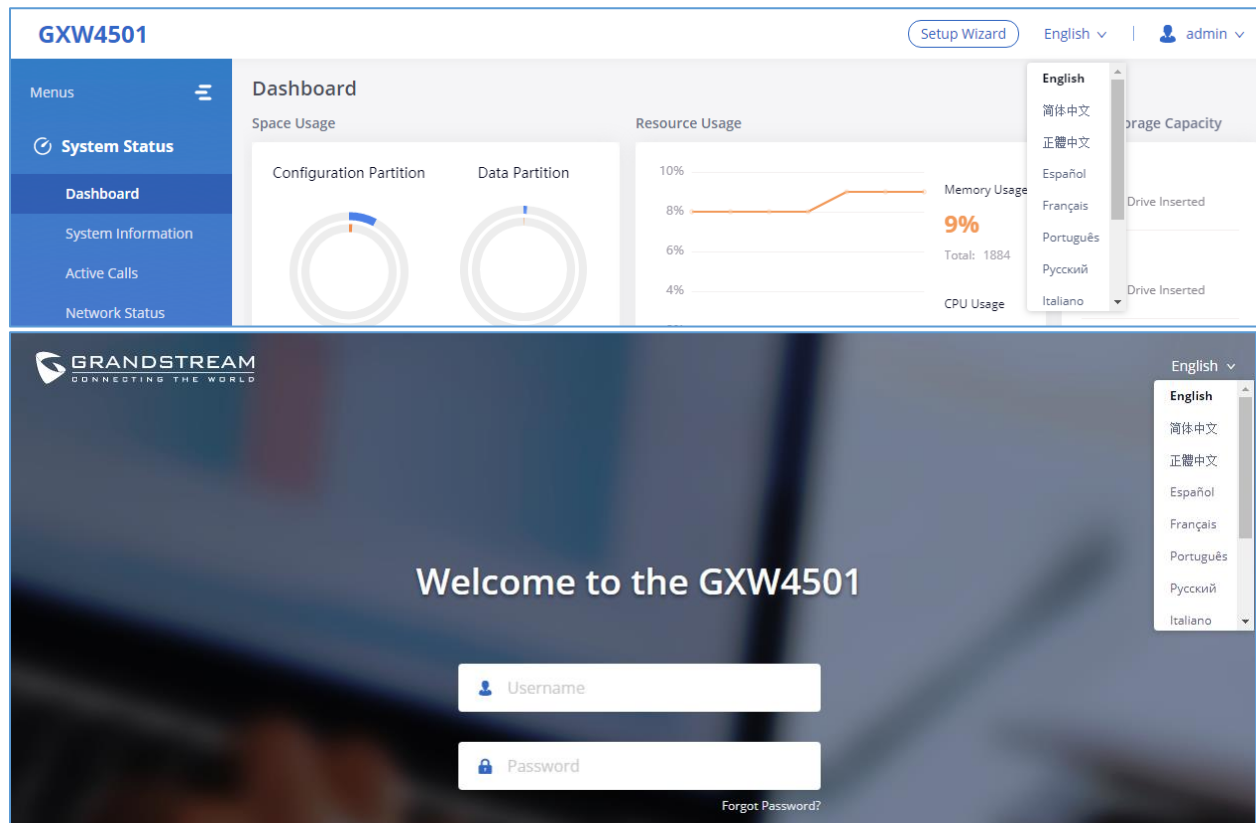


Figure 6: GXW450X Web GUI Languages

Save and Apply Changes

Click on "Save" button after configuring the Web GUI options in one page. After saving all the changes, make sure click on "Apply Changes" button on the upper right of the web page to submit all the changes. If the change requires reboot to take effect, a prompted message will pop up for you to reboot the device.

SYSTEM STATUS

The System Status section is the interface that allows users to check the general information about the GXW450X such as: software and hardware information, space usage, resources usage etc.

Dashboard

The GXW450X monitors the status for Trunks, Digital Channels, Disk capacities etc. It presents administrators the real-time status in different sections under Web GUI → **System Status** → **Dashboard**.

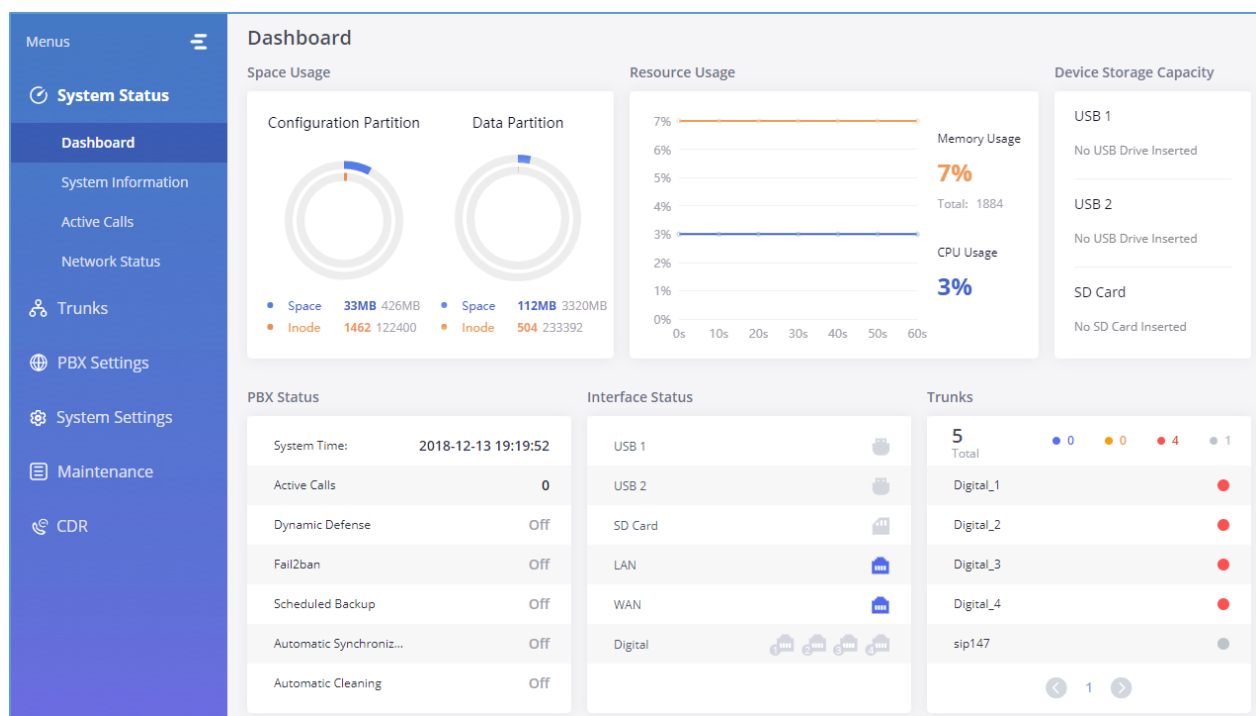


Figure 7: GXW450X Dashboard

Space Usage

Users could access the space usage information from Web GUI → **System Status** → **Dashboard** → **Space Usage**. It shows the available and used space for Space Usage and Inode Usage.

Space Usage includes:

- Configuration partition: This partition contains GXW450X system configuration files and service configuration files.
- Data partition : CDR records, Voice Prompts etc.



Inode Usage includes:

- Configuration partition
- Data partition

Note: Inode is the pointer used for file reference in the system. The system usually has limited resources of pointers.

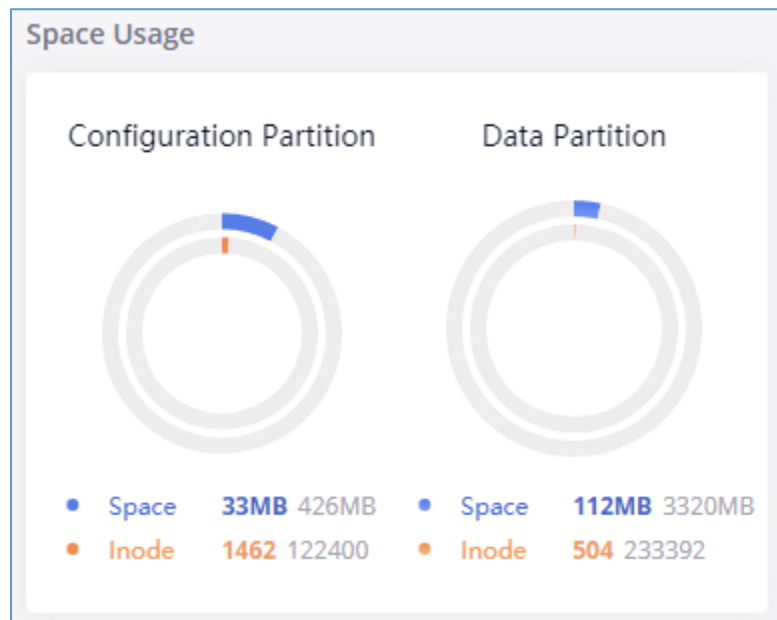


Figure 8: Space Usage

Resource Usage

When configuring and managing the GXW450X, users could access resource usage information to estimate the current usage and allocate the resources accordingly. Under Web GUI → **System Status** → **Dashboard** → **Resource Usage**, the current CPU usage and Memory usage are shown in this chart.

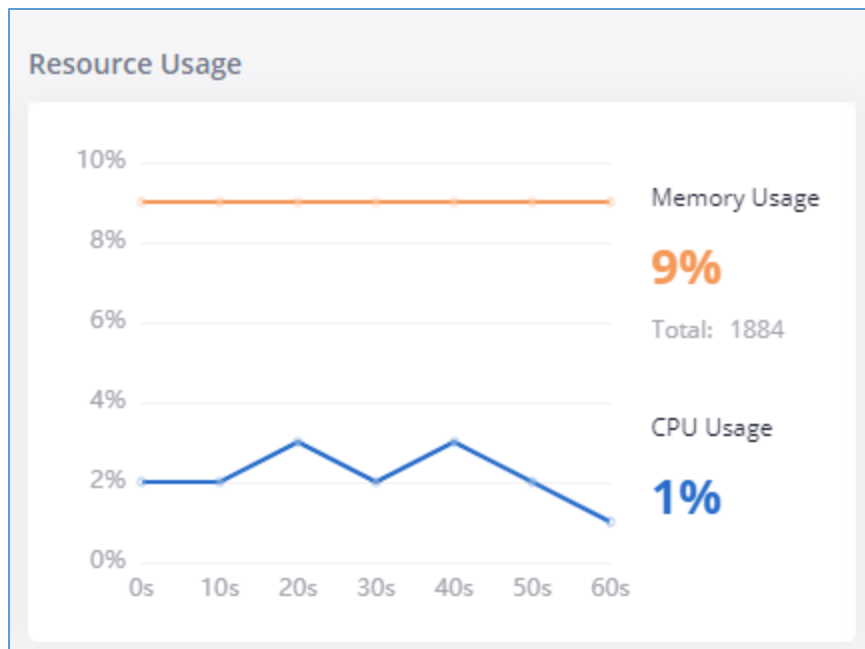


Figure 9: Resource Usage

Disk Capacity

Users could check the external devices capacities from the Dashboard page of the GXW450X under Web GUI → **System Status** → **Dashboard** → **Device Storage Capacity**.

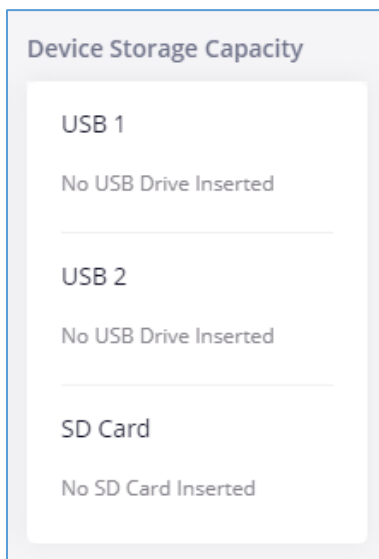


Figure 10: Device Storage Capacity

PBX Status

The PBX status shows the status of some of the gateway GXW450X services. Among the services monitored on the PBX status tab there is: System Time, Active Calls, Schedule backup etc.

PBX Status	
System Time:	2018-12-13 19:44:06
Active Calls	0
Dynamic Defense	Off
Fail2ban	Off
Scheduled Backup	Off
Automatic Synchroniz...	Off
Automatic Cleaning	Off

Figure 11: PBX Status

Interfaces Status

This section displays interface connection status on the GXW450X for USB, SD Card, LAN, WAN, and Digital interfaces.



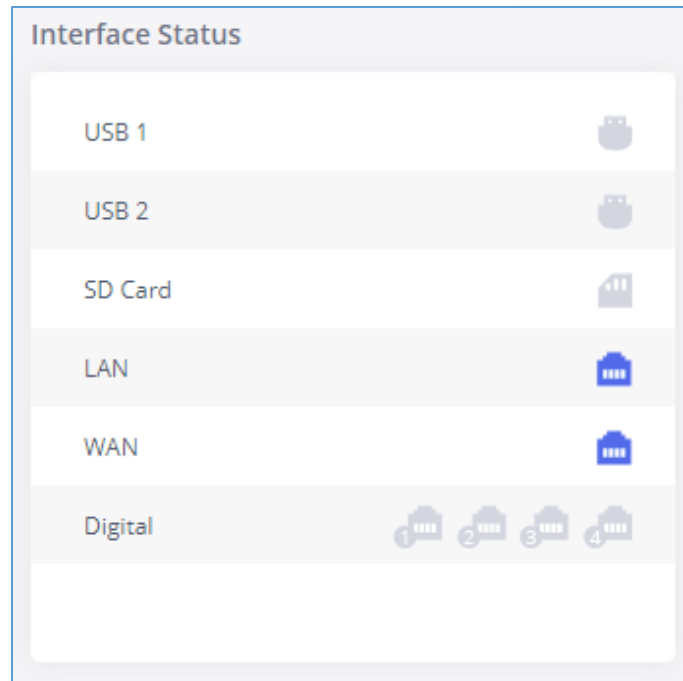


Figure 12: Interface Status

Trunks

Users could see all the configured trunks status in this section.

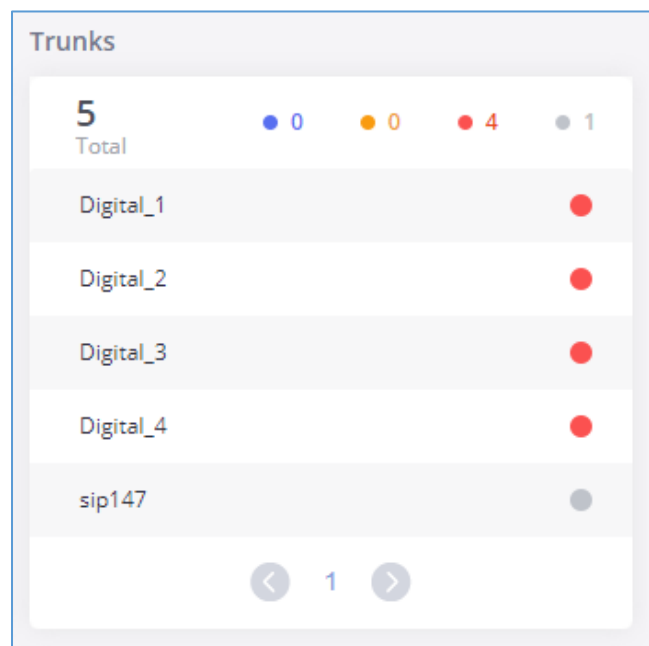


Figure 13: Trunks Status

Four statuses are possible for any trunk configured on the GXW450X:

- Available
- Busy
- Abnormal
- Unmonitored

To visualize the state of each channel of the Digital trunk, users can waver the mouse over the status of the digital trunk as the shown on the figure below:

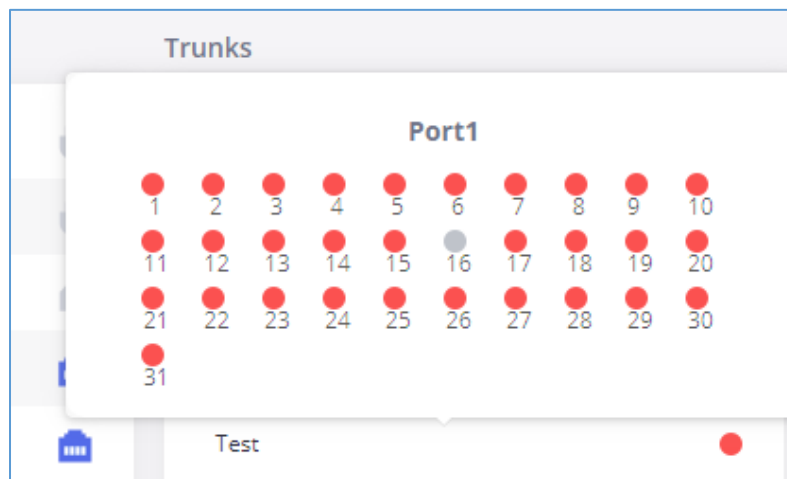


Figure 14: Digital Trunk Channels Status

System Information

The GXW450X system Information can be accessed via Web GUI→**System Status**→**System Information**, which displays the following system information.

General

On this menu, users could check the hardware and software information for the GXW450X. Please see details in the following table.

Table 6: System information→General

System Information	
Model	Product model.
Part Number	Product part number.

System Time	Current system time. The current system time is also available on the upper right of each web page.
Up Time	System up time since the last reboot.
Version Information	
Boot	Boot version.
Core	Core version.
Base	Base version.
Program	Program version. This is the main software release version.
Recovery	Recovery version.

System Information

General
Network

System Information

Model: GXW4501 V1.2A

Part Number: 9660003712A

System Time: 2019-03-29 12:49:05 UTC-04:00

Up Time: 02:29:23

Version Information

Boot: 1.0.0.18

Core: 1.0.0.18

Base: 1.0.0.18

Lang: 1.0.0.18

Program: 1.0.0.18

Recovery: 1.0.0.18

Figure 15: System Information→General

Network

Under Web GUI→**System Status**→**System Information**→**Network**, users could check the network information for the GXW450X. Please see details in the following table.

WAN/LAN	
MAC Address	Global unique ID of device, in HEX format. The MAC address can be found on the label coming with original box and on the label located on the bottom of the device.
IPv4 Address	The IPv4 address attributed to network interface
IPv6 Address	The IPv6 address attributed to the network interface
IPv6 Address Link	The IPv6 address Link attributed to the network interface
Gateway	Default gateway address.
Subnet Mask	Subnet mask address.
DNS Server	DNS server address.

System Information

General
Network

System Information

Model: GXW4501 V1.2A

Part Number: 9660003712A

System Time: 2019-06-11 10:55:40 UTC-04:00

Up Time: 00:00:42

Version Information

Boot: 1.0.0.24

Core: 1.0.0.24

Base: 1.0.0.24

Lang: 1.0.0.24

Program: 1.0.0.24

Recovery: 1.0.0.24

Figure 16: System Information→Network



Active Calls

The active calls on the GXW450X are displayed in Web GUI→**System Status**→**Active Calls** page. Users can monitor call status and hang up active call(s) in real time manner.

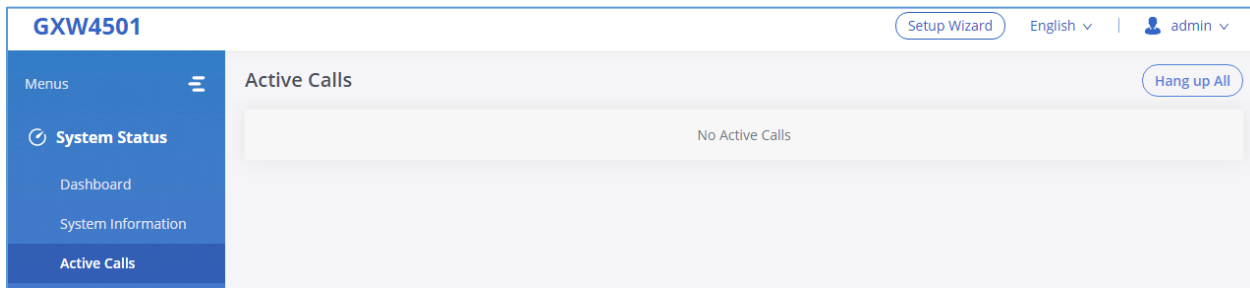


Figure 17: Active Calls

Users can click on “Hang up All” to terminate the all the active calls at once.

Network status

GXW450X supports Network Status to display active internet connections. User can use Network Status to troubleshoot connection issues between GXW450X and other services. This information can be found under Web GUI→**System Status**→**Network Status**, the users can view active Internet connections and the Active Unix Domain Sockets.

Network Status					
Active Connections		Active Unix Domain Sockets			
Proto	Recv-Q	Send-Q	Local-Address	Foreign-Address	State
tcp	0	0	0.0.0.0:8088	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:8888	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:25	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:7777	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:7681	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:7777	127.0.0.1:36727	TIME_WAIT
tcp	0	0	127.0.0.1:7777	127.0.0.1:36728	TIME_WAIT
tcp	0	0	127.0.0.1:7681	127.0.0.1:40182	ESTABLISHED
tcp	0	0	127.0.0.1:40182	127.0.0.1:7681	ESTABLISHED

Figure 18: Active connections



Network Status						
Active Connections		Active Unix Domain Sockets				
Proto	RefCnt	Flags	Type	State	I-Node	
unix	2	[ACC]	SEQPACKET	LISTENING	9226	
unix	9	[]	DGRAM		11548	
unix	2	[ACC]	STREAM	LISTENING	1922	
unix	2	[ACC]	STREAM	LISTENING	10371	
unix	2	[]	DGRAM		10384	
unix	2	[ACC]	STREAM	LISTENING	12486	
unix	2	[ACC]	STREAM	LISTENING	13150	

Figure 19: Active Unix Domain Sockets



SYSTEM SETTINGS

This chapter explains configurations for system-wide parameters on the GXW450X. System settings are under “System Settings” tab on GXW450X Web GUI. System settings include, Network Settings, Security Settings, HTTP Server, Email Settings, Time Settings, OpenVPN® settings and DDNS Settings

HTTP Server

The GXW450X embedded web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow the users to configure the gateway through a Web browser such as Microsoft IE, Mozilla Firefox and Google Chrome. By default, the Gateway can be accessed via HTTPS using Port 8089 (e.g., <https://192.168.1.50:8089>). Users could also change the access protocol and port as preferred under Web GUI→**System Settings**→**HTTP Server**.

Basic Settings	
Redirect From Port 80	Enable or disable redirect from port 80. On the gateway, the default access protocol is HTTPS and the default port number is 8089. When this option is enabled, the access using HTTP with Port 80 will be redirected to HTTPS with Port 8089. The default setting is "Enable".
Protocol Type	Select HTTP or HTTPS. The default setting is "HTTPS". This is also the protocol used for zero config when the end point device downloads the config file from the GXW450X.
Port	Specify port number to access the HTTP server. Default port is 8089.
Enable IP whitelist	If enabled, only the IP address on the permitted IP list will be allowed to access the GXW450X's web GUI.
Permitted IP(s)	Add an IP address to the list of allowed IPs to access GXW450X's web GUI. Ex: 192.168.6.233 / 255.255.255.255
Certificate Settings	
Options	Select the mode to download SSL certificates for web server, two modes are available: <ul style="list-style-type: none"> • Manually Upload certificate: Upload the files while respecting size and format.



	<ul style="list-style-type: none"> • Automatically request certificate: enter domain from which to request the certificate files.
TLS Private Key	<p>Upload private key for the built-in http server.</p> <p>Note: The size of the key file must be under 2MB and the it will be renamed as "private.pem" automatically.</p>
TLS Cert	<p>Upload certificate for the built-in http server and override the existing one.</p> <p>Note: The size of your certificate must be under 2MB. This is the certificate file (*.pem format only) for TLS connection and it will be renamed as "certificate.pem" automatically. It contains private key for the client and signed certificate for the server.</p>
Reset Certificate	<p>Restore the default key and certificate. The web server needs to reload to take effect after certificate restoration.</p>

Network Settings

After successfully connecting the GXW450X to the network for the first time, users could login the Web GUI and go to **System Settings→Network Settings** to configure the network parameters for the device. In this section, all the available network setting options are listed. Select each tab in Web GUI→**System Settings→Network Settings** page to configure IPV4 Settings, IPV6 Settings, 802.1X and Static Routes.

Basic Settings

Please refer to the following tables for basic network configuration parameters on GXW450X.

Table 7: GXW450X Network Settings→Basic Settings

Method	Switch: WAN port interface will be used for uplink connection. LAN port interface will be used as a room for PC connection.
MTU	Specifies the Maximum Transmission Unit. (By default, it's 1492)
IPv4 Address	
Preferred DNS Server	Enter the preferred DNS server address. If Preferred DNS is used, GXW450X will try to use it as Primary DNS server.



WAN (when Method set to “Route”) / LAN (when Method set to “Switch”)	
IP Method	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
If “IP Method” is set to “Static”	
IP Address	Enter the IP address for static IP settings. The default setting is 192.168.0.160
Subnet Mask	Enter the subnet mask address for static IP settings. The default setting is 255.255.0.0.
Gateway IP	Enter the gateway IP address for static IP settings. The default setting is 0.0.0.0
DNS Server 1	Enter the DNS server 1 address for static IP settings.
DNS Server 2	Enter the DNS server 2 address for static IP settings.
If “IP Method” is set to “PPPoE”	
User Name	Enter the user name to connect via PPPoE.
Password	Enter the password to connect via PPPoE.
If “IP Method” is set to “DHCP”, “Static” or “PPPoE”	
Layer 2 QoS 802.1Q/VLAN Tag	Assign the VLAN tag of the layer 2 QoS packets for LAN port. The default value is 0 (no VLAN Tag). The valid range is between 2 and 4094.
Layer 2 QoS 802.1p Priority Value	Assign the priority value of the layer 2 QoS packets for LAN port. The default value is 0. The valid range is between 0 and 7.
LAN (when Method set to “Route”)	
IP Address	Enter the IP address. The default setting is 192.168.2.1
Subnet Mask	Enter the subnet mask address. The default setting is 255.255.255.0.
DHCP Server Enable	Enable or disable DHCP server capability. The default setting is “Yes.”
DNS Server 1	Enter DNS server address 1. The default setting is 8.8.8.8.



DNS Server 2	Enter DNS server address 2. The default setting is 208.67.222.222.
Allow IP Address From	Enter the DHCP IP Pool starting address. The default setting is 192.168.2.100.
Allow IP Address To	Enter the DHCP IP Pool ending address. The default setting is 192.168.2.254.
Default Gateway	Configure the default Gateway assigned by DHCP server.
Default IP Lease Time	Enter the IP lease time (in seconds). The default setting is 43200.
Layer 2 QoS 802.1Q/VLAN Tag	Assign the VLAN tag of the layer 2 QoS packets for LAN port. The default value is 0 (no VLAN Tag). The valid range is between 2 and 4094.
Layer 2 QoS 802.1p Priority Value	Assign the priority value of the layer 2 QoS packets for LAN port. The default value is 0. The valid range is between 0 and 7.
IPv6 Address	
WAN (when "Method" is set to "Route") / LAN (when "Method" is set to "Switch")	
IP Method	Select Auto or Static. The default setting is Auto
If "IP Method" is set to "Static"	
IP Address	Enter the IP address for static IP settings.
IP Prefixlen	Enter the Prefix length. Default is 64
DNS Server 1	Enter the DNS server 1 address for static settings.
DNS Server 2	Enter the DNS server 2 address for static settings.
LAN (when "Method" is set to "Route")	
DHCP Server	<p>Enable or disable DHCP server capability. Available options are:</p> <ul style="list-style-type: none"> • Disable: DHCP Server will be disabled • Auto: Stateless address auto configuration using NDP protocol • DHCPv6: Stateful address autoconfiguration using DHCPv6 protocol. <p>The default setting is "Disable"</p>



If “DHCP Server” is set to “Auto” or “DHCPv6”	
DHCP Prefix	Enter DHCP Prefix when static IP is used. Format: "xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx". Default is “2001:db8:2:2::”
DHCP Prefixlen	Enter the Prefix length. Default is 64
DNS Server 1	Enter DNS server address 1. The default setting is “2001:4860:4860::8888”.
DNS Server 2	Enter DNS server address 2. The default setting is “2001:4860:4860::8844”.
If “DHCP Server” is set to “DHCPv6”	
Allow IP Address From	Enter the DHCP IP Pool starting address. The default setting is “2001:db8:2:2::3000”.
Allow IP Address To	Enter the DHCP IP Pool ending address. The default setting is “2001:db8:2:2::4000”.
Default IP Lease Time	Enter the IP lease time (in seconds). The default setting is 43200.

DHCP Client List

This feature can bind MAC to IP address on the LAN port when GXW450x is set to “Route” mode.

When devices receive IP addresses from GXW450X LAN port, they will be listed on the web UI under **“System Settings → Network Settings → DHCP Client List”** as shown below.

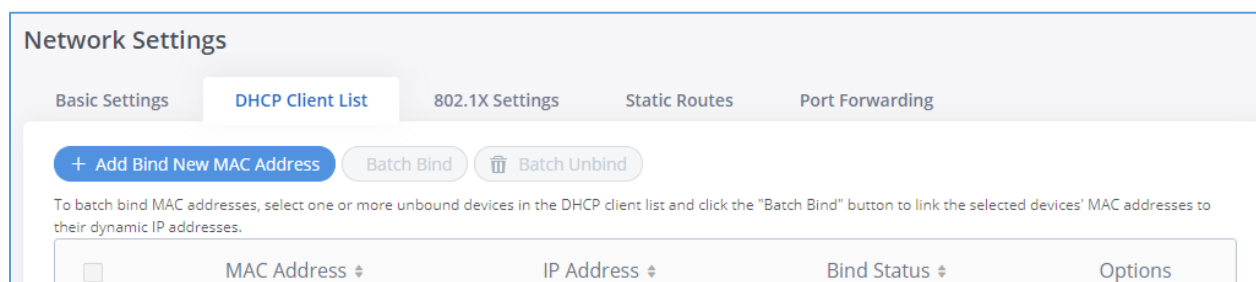


Figure 20: DHCP Client List

User can bind manually a MAC to an IP address by clicking on **+ Add Bind New MAC Address** , the following figure will pop up.

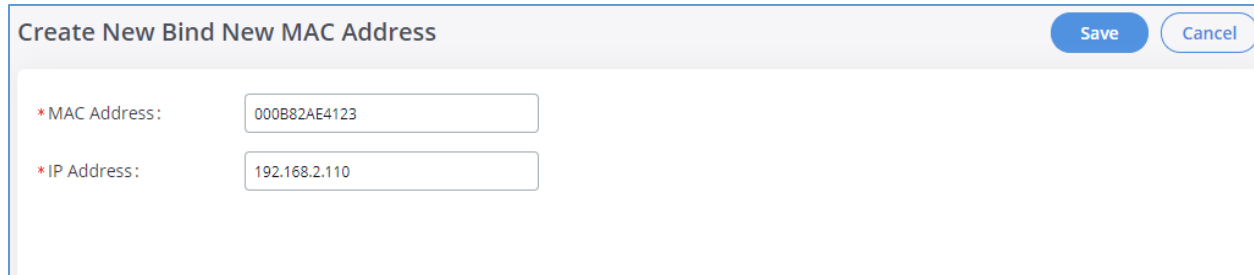
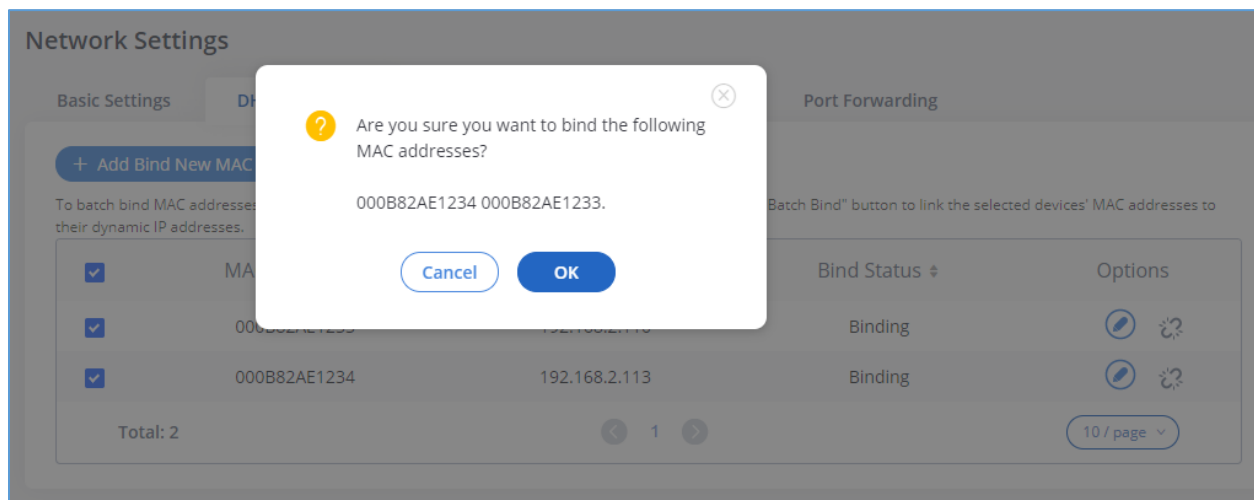


Figure 21: Add Bind New MAC Address Bind

User needs to set the device MAC address and the IP that will be bound to it (the IP address needs to be within the GXW450X DHCP range).

In order to bind a batch of listed MAC addresses, user needs to check first the MAC addresses to bind and click on **Batch Bind** . A confirmation popup will be shown, click **OK** to bind the addresses.



MAC	IP	Bind Status	Options
000B82AE1233	192.168.2.110	Binding	
000B82AE1234	192.168.2.113	Binding	

Figure 22: Batch Add MAC Address Bind

After Clicking “OK” to confirm the binding, the “Bind Status” will change from “Unbind” to “Binding”.

802.1X Settings

IEEE 802.1X is an IEEE standard for port-based network access control. It provides an authentication mechanism to device before the device can access Internet or other LAN resources. The GXW450X supports 802.1X as a supplicant/client to be authenticated. The following diagram and figure show the GXW450X uses 802.1X mode “EAP-MD5” on WAN port as client in the network to access Internet.

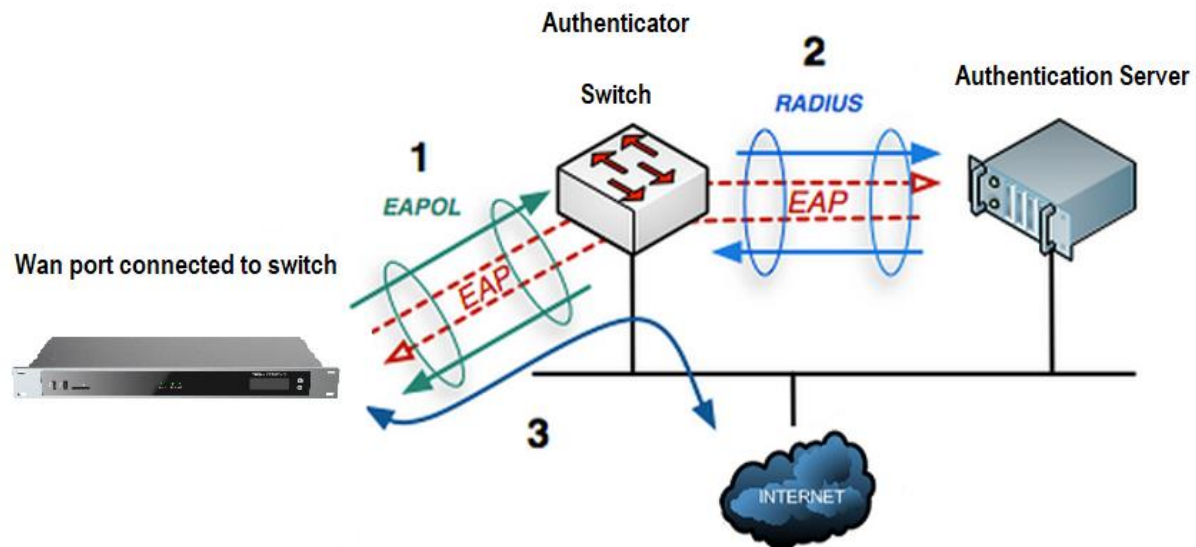


Figure 23: GXW450X Using 802.1X as Client

Network Settings

Basic Settings
DHCP Client List
802.1X Settings
Static Routes
Port Forwarding

WAN

802.1X Mode:

* Identity:

* MD5 Password:

Figure 24: GXW450X using 802.1X EAP-MD5

The following table shows the configuration parameters for 802.1X on GXW450X. Identity and MD5 password are required for authentication, which should be provided by the network administrator obtained from the RADIUS server. If “EAP-TLS” or “EAP-PEAPv0/MSCHAPv2” is used as the 802.1X mode, users will also need to upload 802.1X CA Certificate and 802.1X Client Certificate, which should be also generated from the RADIUS server.

Table 8: GXW450X Network Settings→802.1X

802.1X Mode	Select 802.1X mode. The default setting is "Disable". The supported 802.1X mode are: <ul style="list-style-type: none"> • EAP-MD5 • EAP-TLS • EAP-PEAPv0/MSCHAPv2
Identity	Enter 802.1X mode Identity information.
MD5 Password	Enter 802.1X mode MD5 password information.
802.1X CA Certificate	Upload 802.1X CA certificate. This file will be renamed as "8021x_ca_cert" automatically.
802.1X Client Certificate	Upload 802.1X client certificate with both certificate and private key. This file will be renamed as "8021x_client_cert" automatically.

Static Routes

The GXW450X provides users static routing capability that allows the device to use manually configured routes, rather than information only from dynamic routing or gateway configured in the GXW450X Web GUI→**System Settings**→**Network Settings**→**Basic Settings** to forward traffic. It can be used to define a route when no other routes are available or necessary.

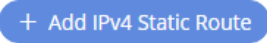
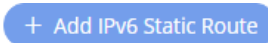


- Click on  to create a new IPv4 static route or click on  to create a new IPv6 static route. The configuration parameters are listed in the table below.
- Once added, users can select  to edit the static route.
- Select  to delete the static route.

Table 9: GXW450X Network Settings→Static Routes

Destination	Configure the destination IPv4 address or the destination IPv6 subnet for the GXW450X to reach using the static route. Example: IPv4 address - 192.168.66.4 IPv6 subnet - 2001:740:D::1/64
Netmask	Configure the subnet mask for the above destination address. If left blank, the default value is 255.255.255.255. Example: 255.255.255.0



Gateway	Configure the IPv4 or IPv6 gateway address so that the GXW450X can reach the destination via this gateway. Gateway address is optional. Example: 192.168.40.5 or 2001:740:D::1
Interface	Specify the network interface on the GXW450X to reach the destination using the static route.

Port Forwarding

The GXW450X network interface supports router functions which provides users the ability to do port forwarding. If the GXW450X is set to “Route” under Web GUI→**System Settings**→**Network Settings**→**Basic Settings: Method**, port forwarding is available for configuration.

The port forwarding configuration is under Web GUI→**System Settings**→**Network Settings**→**Port Forwarding** page. Please see related settings in the table below.

Table 10: GXW450X System Settings → Network Settings→Port Forwarding

WAN Port	Specify the WAN port number or a range of WAN ports. Unlimited number of ports can be configured. Note: When it is set to a range, WAN port and LAN port must be configured with the same range, such as WAN port: 1000-1005 and LAN port: 1000-1005, and access from WAN port will be forwarded to the LAN port with the same port number, for example, WAN port 1000 will be port forwarding to LAN port 1000.
LAN IP	Specify the LAN IP address.
LAN Port	Specify the LAN port number or a range of LAN ports. Note: When it is set to a range, WAN port and LAN port must be configured with the same range, such as WAN port: 1000-1005 and LAN port: 1000-1005, and access from WAN port will be forwarded to the LAN port with the same port number, for example, WAN port 1000 will be port forwarding to LAN port 1000.
Protocol Type	Select protocol type “UDP Only”, “TCP Only” or “TCP/UDP” for the forwarding in the selected port. The default setting is “UDP Only”.



OpenVPN®

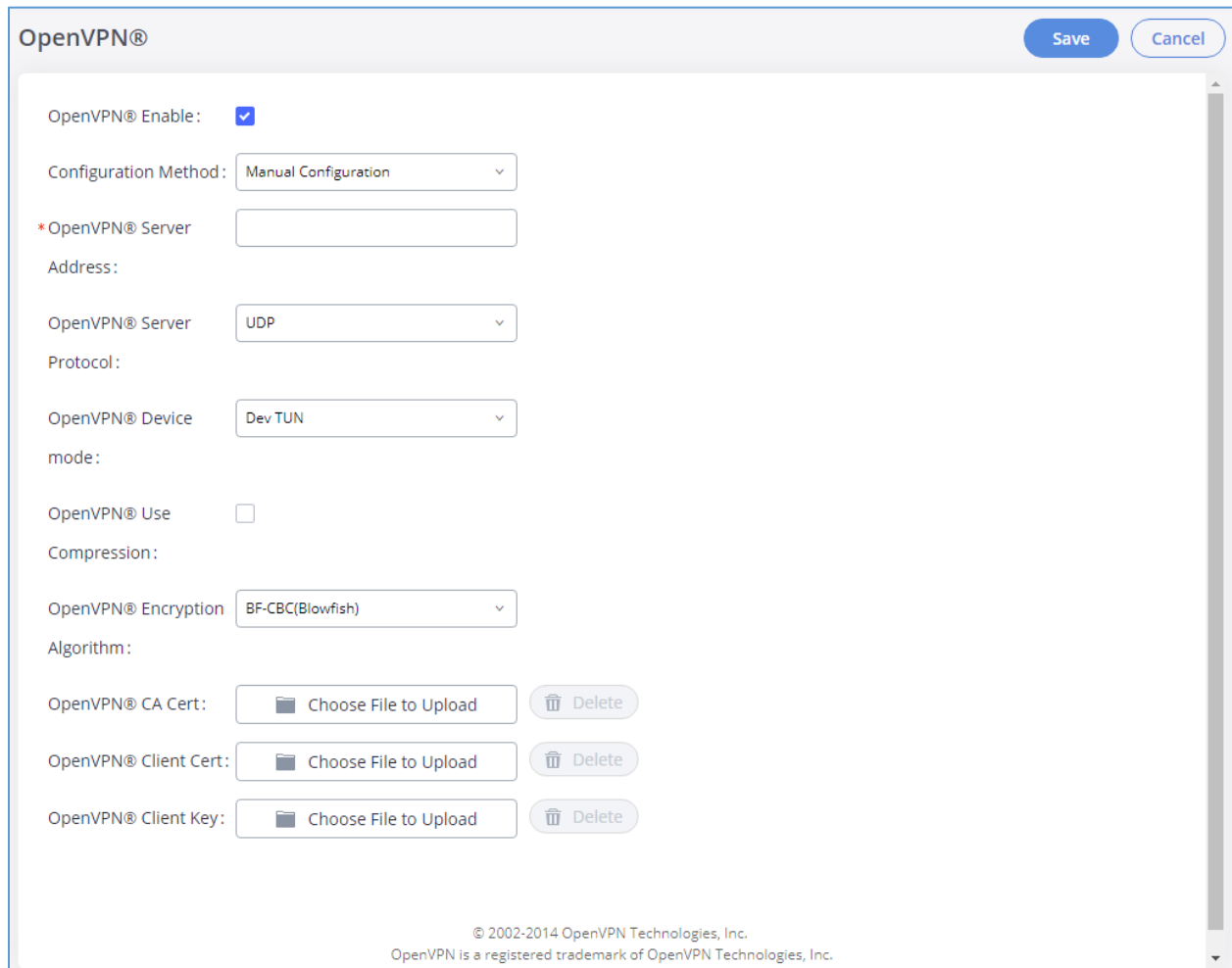
OpenVPN® settings allow the users to configure GXW450X to use VPN features, the following table gives details about the various options in order to configure the GXW450X as OpenVPN Client.

Table 11: GXW450X System Settings→Network Settings→OpenVPN®

OpenVPN® Enable	Enable / Disable the OpenVPN® feature. Default is “Disabled”.
Configuration Method	Select OpenVPN® configuration method. <ul style="list-style-type: none"> • Manual Configuration. • Upload Configuration File.
If “Configuration Method” is set to “Manual Configuration”	
OpenVPN® Server Address	Configures the hostname/IP and port of the server. For example, "192.168.1.2:22" or "2001:0DB8:0000:0000:0000:0000:1428:0000".
OpenVPN® Server Protocol	Select the same protocol that the OpenVPN® server is using, e.g., select UDP if the OpenVPN® is using UDP. Available options: <ul style="list-style-type: none"> • UDP • TCP The default setting is “UDP”.
OpenVPN® Device Mode	Use the same setting as used on the server. <ul style="list-style-type: none"> • Dev TUN: Create a routed IP tunnel. • Dev TAP: Create an Ethernet tunnel. The default setting is “Dev TUN”.
OpenVPN® Use Compression	Compress tunnel packets using the LZO algorithm on the VPN link. Don't enable this unless it is also enabled in the server config file.
OpenVPN® Encryption Algorithm	Please select a cryptographic cipher from drop-down list. Use the same setting that you are using on the server. The default setting is “BF-CBC(Blowfish)”.
OpenVPN® CA Cert	Upload a SSL/TLS root certificate. This file will be renamed as ‘ca.crt’ automatically.
OpenVPN® Client Cert	Upload a client certificate. This file will be renamed as ‘cliend.crt’ automatically.



OpenVPN® Client Key	Upload a client private key. This file will be renamed as 'client.key' automatically.
If “Configuration Method” is set to “Manual Configuration”	
OpenVPN® Configuration File	Upload Configuration file to with OpenVPN® settings. Only file with <i>.conf,.ovpn</i> suffix is accepted for OpenVPN® Configuration File. The file size must be under 2MB.



OpenVPN® Save Cancel

OpenVPN® Enable:

Configuration Method:

*OpenVPN® Server Address:

OpenVPN® Server Protocol:

OpenVPN® Device mode:

OpenVPN® Use Compression:

OpenVPN® Encryption Algorithm:

OpenVPN® CA Cert:

OpenVPN® Client Cert:

OpenVPN® Client Key:

© 2002-2014 OpenVPN Technologies, Inc.
OpenVPN is a registered trademark of OpenVPN Technologies, Inc.

Figure 25: OpenVPN® Feature on the GXW450X

DDNS Settings

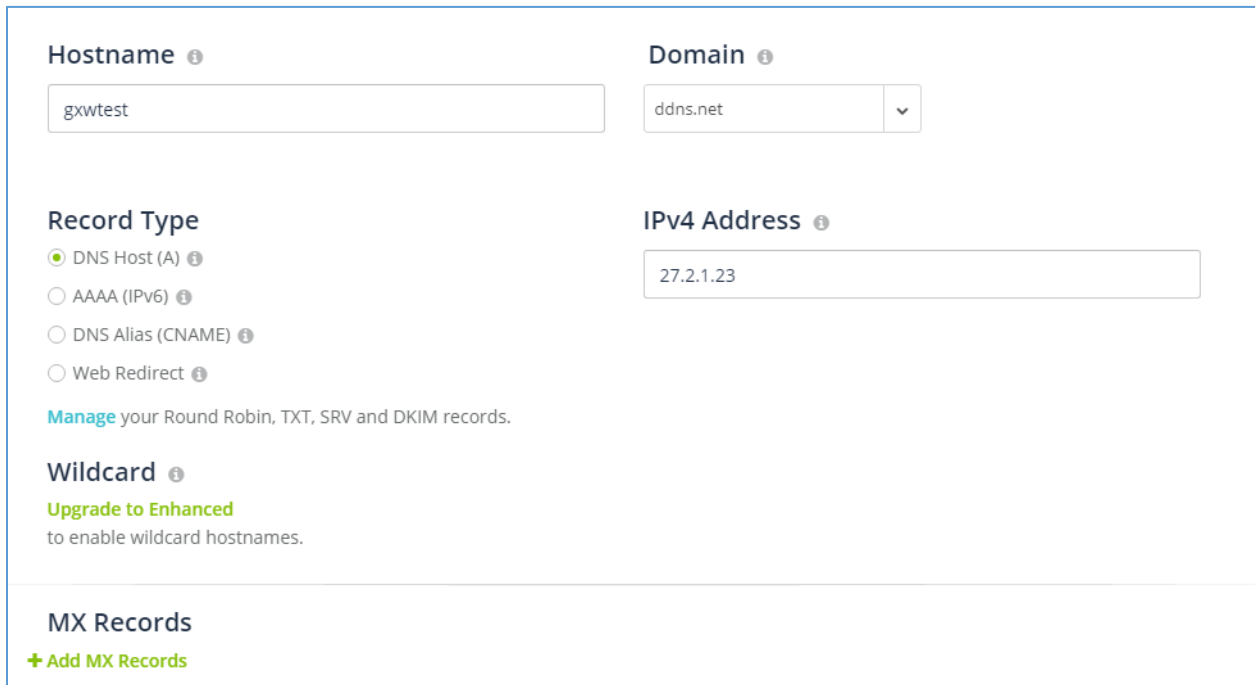
DDNS setting allows user to access GXW450X via domain name instead of IP address.

The GXW450X supports DDNS service from the following DDNS provider:

- dydns.org
- freedns.afraid.org
- zoneedit.com
- noip.com
- oray.net

Here is an example of using noip.com for DDNS.

1. Register domain in DDNS service provider. Please note the GXW450X needs to have public IP access.



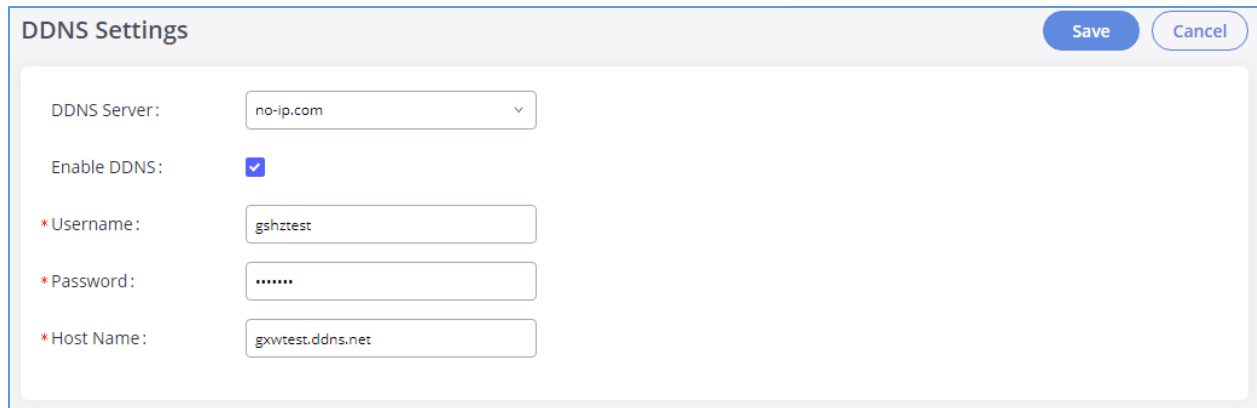
The screenshot shows a web interface for configuring DDNS. It features several input fields and options:

- Hostname**: A text input field containing "gxwtest".
- Domain**: A dropdown menu showing "ddns.net".
- Record Type**: A group of radio buttons with the following options:
 - DNS Host (A)
 - AAAA (IPv6)
 - DNS Alias (CNAME)
 - Web Redirect
- IPv4 Address**: A text input field containing "27.2.1.23".
- Wildcard**: A section with a link "Upgrade to Enhanced" and the text "to enable wildcard hostnames."
- MX Records**: A section with a link "+ Add MX Records".

Figure 26: Register Domain Name on Noip.com

2. On Web GUI → **System Settings** → **Network Settings** → **DDNS Settings**, enable DDNS service and configure username, password and host name.





DDNS Settings Save Cancel

DDNS Server:

Enable DDNS:

* Username:

* Password:

* Host Name:

Figure 27: GXW450X DDNS Settings

3. Now you can use domain name instead of IP address to connect to the GXW450X Web GUI.

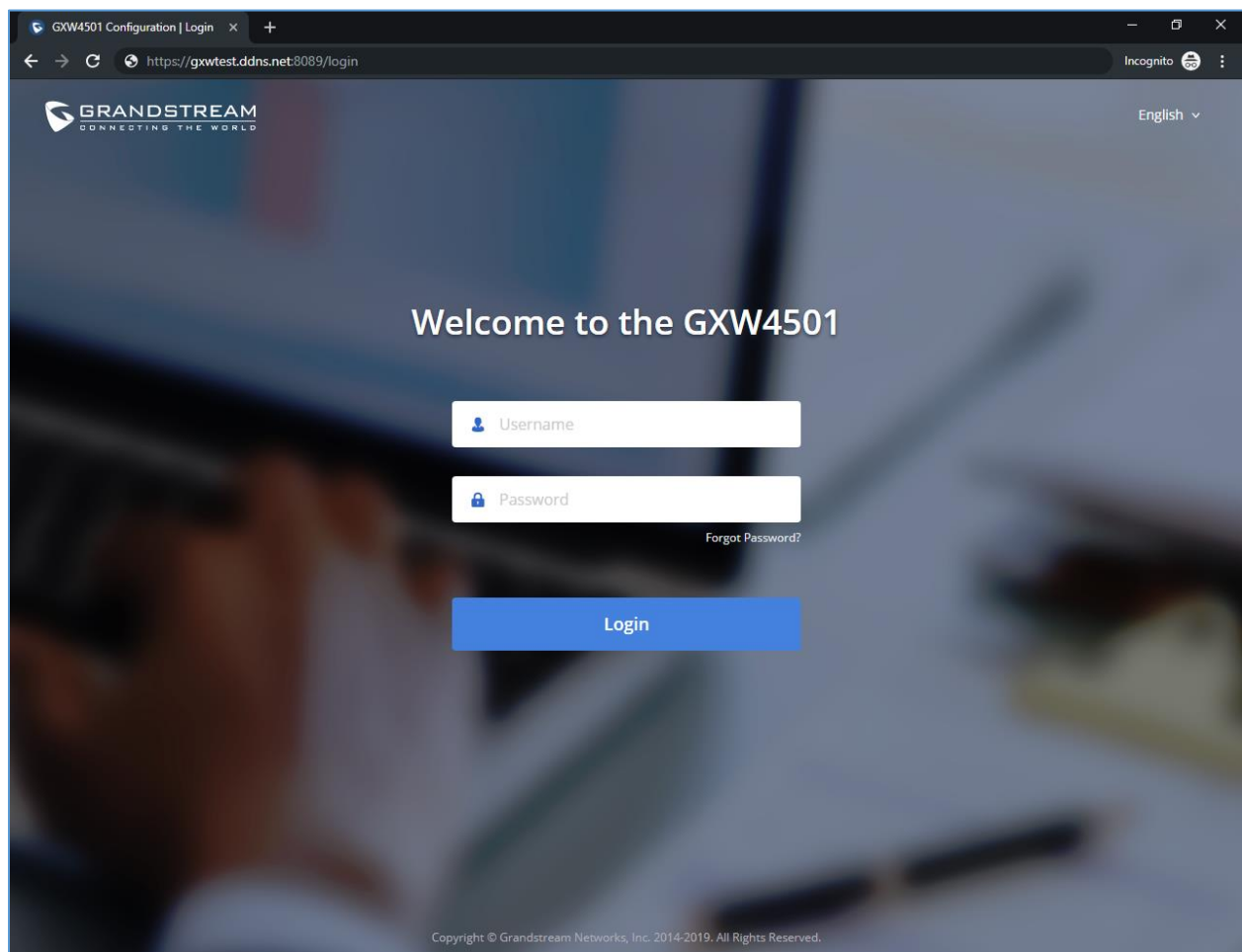


Figure 28: Using Domain Name to Connect to GXW450X

Security Settings

The GXW450X provides users firewall security configurations to prevent certain malicious attack to the GXW450X system. Users could configure to allow, restrict or reject specific traffic through the device for security and bandwidth purpose. The GXW450X also provides Fail2ban feature for authentication errors in SIP REGISTER, INVITE and SUBSCRIBE. To configure firewall settings in the GXW450X, go to Web GUI→**System Settings**→**Security Settings** page.

Static Defense

Under Web GUI→**System Settings**→**Security Settings**→**Static Defense** page, users will see the following information:

- Current service information with port, process and type.
- Custom firewall settings.
- Typical firewall settings.

The following table shows a sample current service status running on the GXW450X.

Table 12: GXW450X Static Defense→Current Service

Port	Process	Type	Port	Process	Type
2000	asterisk	TCP/IPv4	67	dhcpcd	UDP/IPv4
8088	asterisk	TCP/IPv4	69	udpsvd	UDP/IPv4
8888	pbxmid	TCP/IPv4	37178	asterisk	UDP/IPv4
25	master	TCP/IPv4	80	lighttpd	TCP/IPv6
7777	asterisk	TCP/IPv4		master	TCP/IPv6
7681	pbxmid	TCP/IPv4	8089	lighttpd	TCP/IPv6
4520	asterisk	UDP/IPv4	4569	asterisk	UDP/IPv6
4569	asterisk	UDP/IPv4	5060	asterisk	UDP/IPv6
3765	dhcpcd	UDP/IPv4	24539	dhcpcd	UDP/IPv6
5000	asterisk	UDP/IPv4	54411	asterisk	UDP/IPv6
67	udhpcd	UDP/IPv4			



Under "Custom Firewall Settings", users could create new rules to accept, reject or drop certain traffic going through the GXW450X. To create new rule, click on "Create New Rule" button and a new window will pop up for users to specify rule options.

Right next to "Create New Rule" button, there is a checkbox for option "Reject Rules". If it's checked, all the rules will be rejected except the firewall rules listed below. In the firewall rules, only when there is a rule that meets all the following requirements, the option "Reject Rules" will be allowed to check:

- Action: "Accept"
- Type "In"
- Destination port is set to the system login port (e.g., by default 8089)
- Protocol is not UDP

Create New Firewall Rule

* Rule Name:

* Action:

* Type:

* Interface:

* Service:

Source IP Address and Port: :

Destination IP Address and Port: :

* Protocol:







Figure 29: Create New Firewall Rule

Below is a table listing all the firewall rules settings:

Table 13: Firewall Rule Settings

Rule Name	Specify the Firewall rule name to identify the firewall rule.
Action	Select the action for the Firewall to perform. <ul style="list-style-type: none"> • ACCEPT • REJECT • DROP
Type	Select the traffic type. <ul style="list-style-type: none"> • IN If selected, users will need specify to the network interface (for GXW450X) for the incoming traffic. • OUT
Service	Select the service type. <ul style="list-style-type: none"> • FTP • SSH • Telnet • HTTP • Custom If "Custom" is selected, users will need specify Source (IP and port), Destination (IP and port) and Protocol (TCP, UDP or Both) for the service. Please note if the source or the destination field is left blank, it will be used as "Anywhere".

Save the change and click on "Apply" button. Then submit the configuration by clicking on "Apply Changes" on the upper right of the web page. The new rule will be listed at the bottom of the page with sequence number, rule name, action, protocol, type, source, destination and operation. More operations below:

- Click on  to edit the rule.
- Click on  to delete the rule.
- Use the arrows up , down , to the top  or to the bottom  to move the rules up and down.

For typical firewall settings, users could configure the following options on the GXW450X.

Table 14: Firewall Rule Settings

Ping Defense Enable	If enabled, ICMP response will not be allowed for Ping request. The default setting is disabled. To enable or disable it, click on the check box for the LAN or WAN (GXW450X) interface.
SYN-Flood Defense Enable	<p>Allows the GXW450X to handle excessive amounts of SYN packets from one source and keep the web portal accessible. There are two options available and only one of these options may be enabled at one time.</p> <ul style="list-style-type: none"> • eth(0)LAN defends against attacks directed to the LAN IP address of the GXW450X. • eth(1)WAN defends against attacks directed to the WAN IP address of the GXW450X. <p>SYN Flood Defense will limit the amount of SYN packets accepted by the GXW450X from one source to 10 packets per second. Any excess packets from that source will be discarded.</p>
Ping-of-Death Defense Enable	Enable to prevent Ping-of-Death attack to the device. The default setting is disabled. To enable or disable it, click on the check box for the LAN or WAN (GXW450X) interface.

Dynamic Defense

Dynamic defense is supported on the GXW450X series. It can blacklist hosts dynamically when the LAN mode is set to "Route" under Web GUI → **System Settings** → **Network Settings** → **Basic Settings** page. If enabled, the traffic coming into the GXW450X can be monitored, which helps prevent massive connection attempts or brute force attacks to the device. The blacklist can be created and updated by the GXW450X firewall, which will then be displayed in the web page. Please refer to the following table for dynamic defense options on the GXW450X.

Table 15: GXW450X Firewall Dynamic Defense

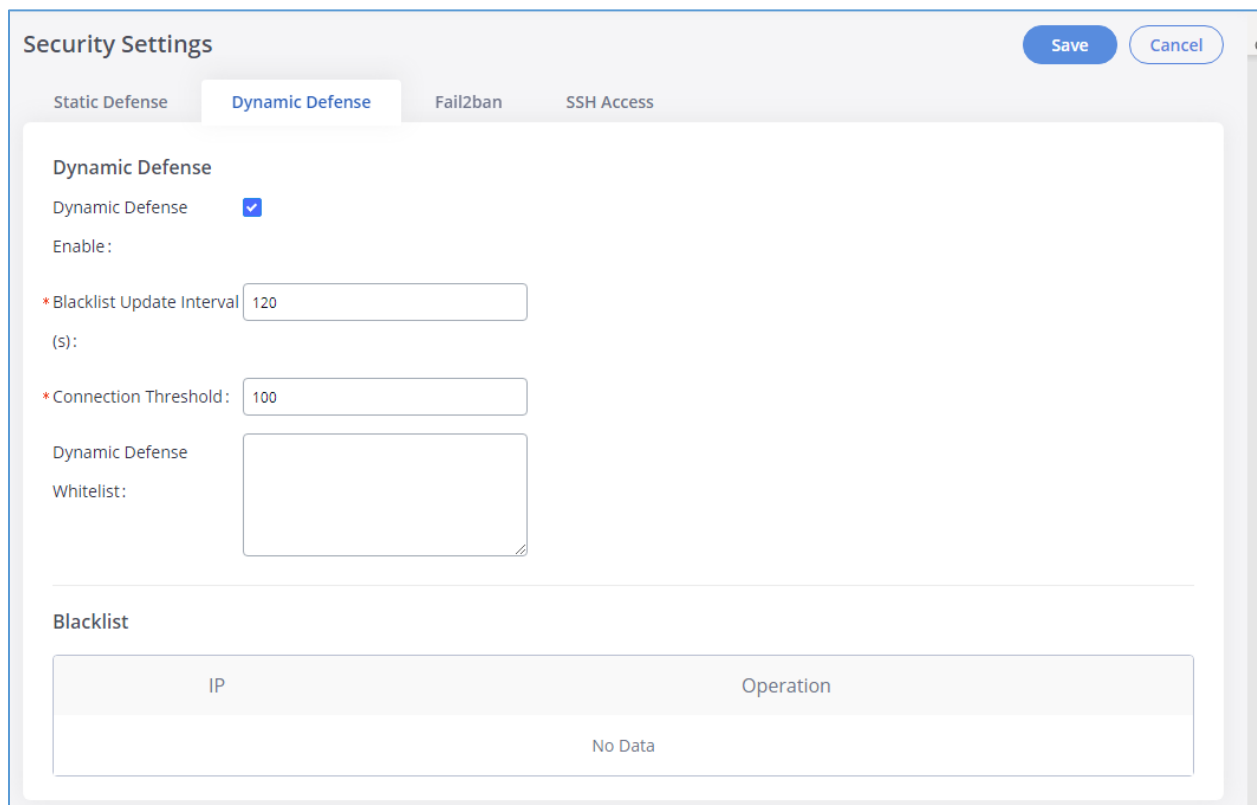
Dynamic Defense Enable	Enable dynamic defense. The default setting is disabled.
Blacklist Update Interval	Configure the blacklist update time interval (in seconds). The default setting is 120.
Connection Threshold	Configure the connection threshold. Once the number of connections from the same host reaches the threshold, it will be added into the blacklist. The default setting is 100.



Dynamic Defense Whitelist	Allowed IPs and ports range, multiple IP addresses and port range. For example: 192.168.2.10- 192.168.2.20 5060:5061
Blacklist	
Black List	Users will be able to view the IPs that have been blocked by GXW450X.

The following figure shows a configuration example:

- If a host at IP address 192.168.2.5 initiates more than 100 TCP connections to the GXW450X, it will be added into GXW450X blacklist. This host 192.168.2.5 will be blocked by the GXW450X for 500 seconds.
- Since IP range 192.168.2.10-192.168.2.20 is in whitelist, if a host initiates more than 20 TCP connections to the GXW450X within 1 minute, it will not be added into GXW450X blacklist. It can still establish TCP connection with the GXW450X.



The screenshot shows the 'Security Settings' configuration page for the GXW450X. The 'Dynamic Defense' tab is selected. The 'Dynamic Defense' section is enabled (checkbox checked). The 'Blacklist Update Interval' is set to 120 seconds, and the 'Connection Threshold' is set to 100. A 'Whitelist' text area is present but empty. Below this is a 'Blacklist' table with columns for 'IP' and 'Operation', which is currently empty and displays 'No Data'.

Figure 30: Dynamic Defense Configuration

Fail2Ban

Fail2Ban feature on the GXW450X provides intrusion detection and prevention for authentication errors in SIP INVITE and SUBSCRIBE. Once the entry is detected within "Max Retry Duration", the GXW450X will act to forbid the host for certain period as defined in "Banned Duration". This feature helps prevent SIP brute force attacks to the gateway system.

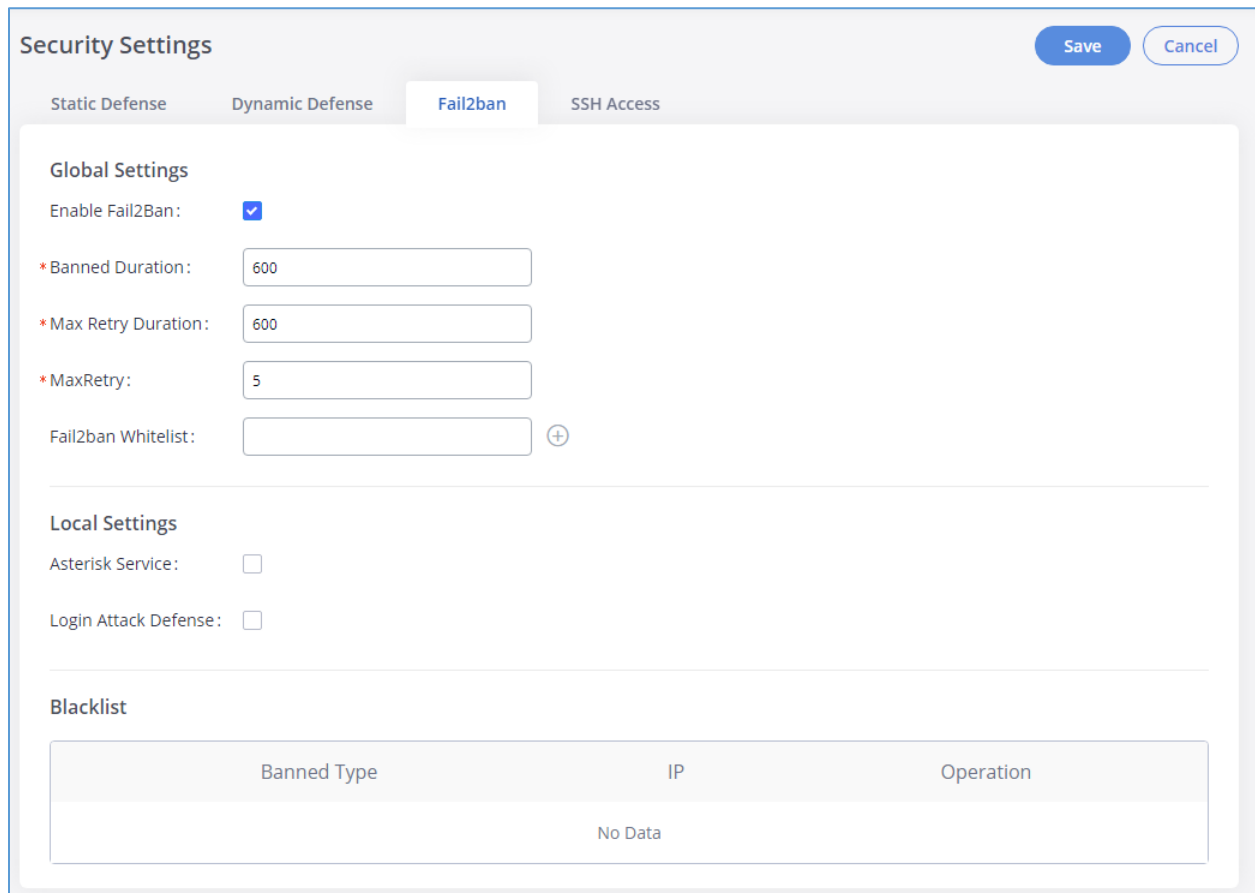


Figure 31: Fail2Ban Settings

Table 16: Fail2Ban Settings

Global Settings	
Enable Fail2Ban	Enable Fail2Ban. The default setting is disabled. Please make sure both "Enable Fail2Ban" and "Asterisk Service" are turned on to use Fail2Ban for SIP authentication on the GXW450X.
Banned Duration	Configure the duration (in seconds) for the detected host to be banned. The default setting is 600. If set to 0, the host will be always banned.



Max Retry Duration	Within this duration (in seconds), if a host exceeds the max times of retry as defined in "MaxRetry", the host will be banned. The default setting is 600.
MaxRetry	Configure the number of authentication failures during "Max Retry Duration" before the host is banned. The default setting is 5.
Fail2Ban Whitelist	Configure IP address, CIDR mask or DNS host in the whitelist. Fail2Ban will not ban the host with matching address in this list. Up to 20 addresses can be added into the list.
Local Settings	
Asterisk Service	Enable Asterisk service for Fail2Ban. The default setting is disabled. Please make sure both "Enable Fail2Ban" and "Asterisk Service" are turned on to use Fail2Ban for SIP authentication on the GXW450X.
Listening Port Number	Configure the listening port number for the service. By default, port 5060 will be used for UDP and TCP, and port 5061 will be used for TLS.
MaxRetry	Configure the number of authentication failures during "Max Retry Duration" before the host is banned. The default setting is 10. Please make sure this option is properly configured as it will override the "MaxRetry" value under "Global Settings".
Login Attack Defense	Enables defense against excessive login attacks to the GXW450X's web GUI. The default setting is disabled.
Listening Port Number	This is the Web GUI listening port number which is configured under System Settings → HTTP Server → Port . The default is 8089.
MaxRetry	When the number of failed login attempts from an IP address exceeds the MaxRetry number, that IP address will be banned from accessing the Web GUI. The default setting is 5
Blacklist	
Black List	Users will be able to view the IPs that have been blocked by GXW450X.



SSH Access

SSH switch is available via Web GUI. User can enable or disable SSH access directly from Web GUI or LCD screen. For web SSH access, please log in GXW450X web interface and go to Web GUI→**System Settings**→**Security Settings**→**SSH Access**. By default, SSH access is disabled for security concerns. It is highly recommended to only enable SSH access for debugging purpose.

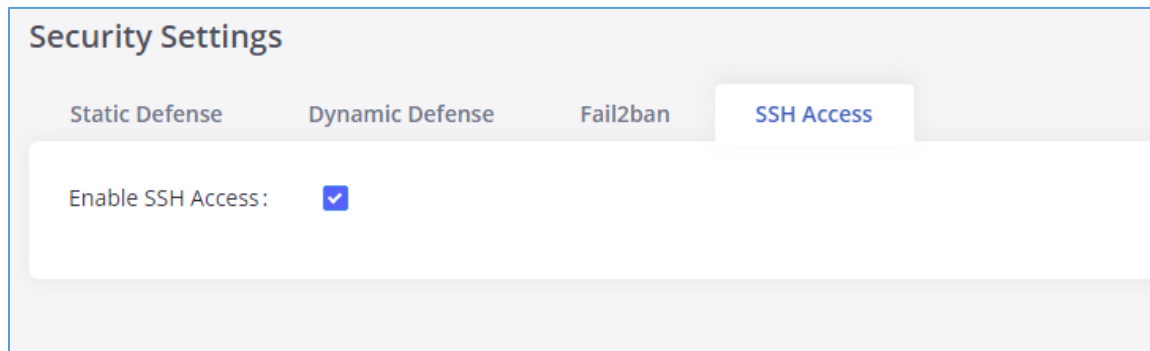


Figure 32:SSH Access

Time Settings

Automatic Date and Time

The current system time on the GXW450X can be found under Web GUI→**System Status**→**Dashboard**→**PBX Status**.

To configure the GXW450X to update time automatically, go to Web GUI→**System Settings**→**Time Settings**→**Automatic Date and Time**.

Time Settings

Automatic Date and Time
Set Date and Time
NTP Server
Office Time
Holiday

Remote NTP Server:

Enable DHCP Option 2:

Enable DHCP Option 42:

Time Zone:

* Self-defined Time Zone:

Figure 33: Automatic Date and Time Settings



Note:

The configurations under Web GUI→**Settings**→**Time Settings**→**Automatic Date and Time** page require reboot to take effect. Please consider configuring Automatic Date and Time related changes when setting up the GXW450X for the first time to avoid service interruption after installation and deployment in production.

Table 17: Automatic Date and Time Settings

Remote NTP Server	Specify the URL or IP address of the NTP server for the GXW450X to synchronize the date and time. The default NTP server is ntp.ipvideotalk.com.
Enable DHCP Option 2	If set to "Yes", the GXW450X can get provisioned for Time Zone from DHCP Option 2 in the local server automatically. The default setting is "Yes".
Enable DHCP Option 42	If set to "Yes", the GXW450X can get provisioned for NTP Server from DHCP Option 42 in the local server automatically. This will override the manually configured NTP Server. The default setting is "Yes".

Time Zone	<p>Select the proper time zone option so the GXW450X can display correct time accordingly.</p> <p>If "Self-Defined Time Zone" is selected, please specify the time zone parameters in "Self-Defined Time Zone" field as described in below option.</p>
Self-Defined Time Zone	<p>If "Self-Defined Time Zone" is selected in "Time Zone" option, users will need define their own time zone following the format below.</p> <p>The syntax is: std offset dst [offset], start [/time], end [/time] Default is set to: MTZ+6MDT+5,M4.1.0,M11.1.0</p> <p>MTZ+6MDT+5</p> <p>This indicates a time zone with 6 hours offset and 1 hour ahead for DST, which is U.S central time. If it is positive (+), the local time zone is west of the Prime Meridian (A.K.A: International or Greenwich Meridian); If it is negative (-), the local time zone is east.</p> <p>M4.1.0,M11.1.0</p> <p>The 1st number indicates Month: 1,2,3..., 12 (for Jan, Feb, ..., Dec). The 2nd number indicates the nth iteration of the weekday: (1st Sunday, 3rd Tuesday...). Normally 1, 2, 3, 4 are used. If 5 is used, it means the last iteration of the weekday. The 3rd number indicates weekday: 0,1,2,...,6 (for Sun, Mon, Tues, ... ,Sat). Therefore, this example is the DST which starts from the First Sunday of April to the 1st Sunday of November.</p>

Set Date and Time

To manually set the time on the GXW450X, go to Web GUI→**System Settings**→**Time Settings**→**Set Date and Time**. The format is YYYY-MM-DD HH:MM:SS.



Time Settings

Automatic Date and Time
Set Date and Time
NTP Server
Office Time
Holiday

Current Date and Time:

Date Format:

Time Format:

Figure 34: Date and Time Manual Configuration

Table 18: Date and Time Manual Settings

Current Date and Time	Manually set up the system time. If the system time is automatically set up successfully, the manually configured value will not take effect.
Date Format	Configure the global date format, the default format is yyyy-mm-dd.
Time Format	Chooses the format that will be used to display the Time, 24-hour format or 12-hour format, the default settings is 24-hour format

 **Note:**

Manual setup of time will take effect immediately after saving and applying changes in the Web GUI. If users would like to reboot the GXW450X and keep the manually setup time setting, please make sure "Remote NTP Server", "Enable DHCP Option 2" and "Enable DHCP Option 42" options under Web GUI→**Settings**→**Time Settings**→**Automatic Date and Time** page are unchecked or set to empty. Otherwise, time auto updating settings in this page will take effect after reboot.

NTP Server

The GXW450X can be used as an NTP server for the NTP clients to synchronize their time with. To configure the GXW450X as the NTP server, set "Enable NTP server" to "Yes" under Web GUI→**System Settings**→**Time Settings**→**NTP Server**. On the client side, point the NTP server address to the GXW450X IP address or host name to use the GXW450X as the NTP server.

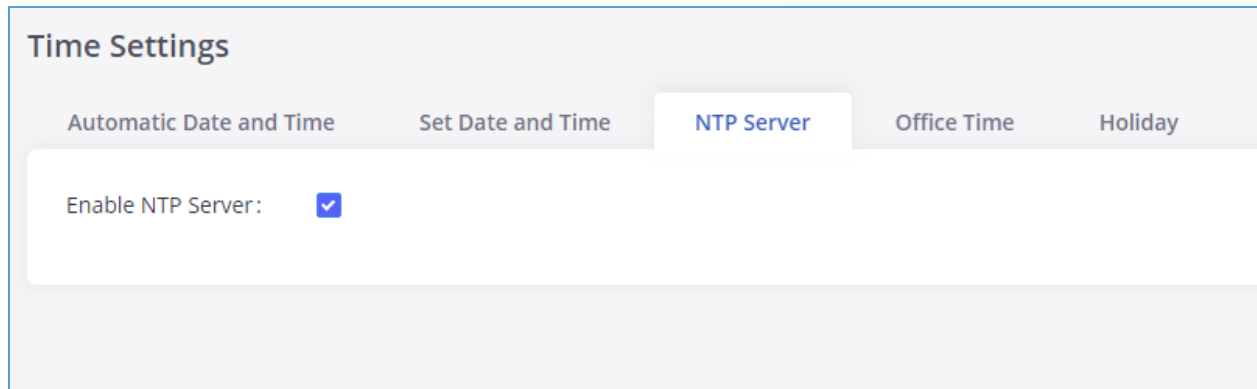


Figure 35: GXW450X NTP Server

Office Time

On the GXW450X, the system administrator can define "office time", which can be used to configure time condition for inbound rule schedule. To configure office time, go to Web GUI→**System Settings**→**Time Settings**→**Office Time**. Click on "Add Office Time" to create an office time.



Create New Office Time

Time: -

Week: Sun Mon Tue Wed
 Thu Fri Sat
 All

Show Advanced Options:

Month: Jan Feb Mar Apr
 May Jun Jul Aug
 Sept Oct Nov Dec
 All

Day: 1 2 3 4
 5 6 7 8
 9 10 11 12
 13 14 15 16
 17 18 19 20
 21 22 23 24
 25 26 27 28
 29 30 31
 All

Figure 36: Add New Office Time

Table 19: Office Time Settings

Time	Configure the start time and end time for office hour.
Week	Select the work days in one week.
Show Advanced Options	Check this option to show advanced options. Once selected, please specify "Month" and "Day" options.
Month	Select the months for office time.
Day	Select the work days in one month.

Select "Time" and the day for the "Week" for the office time. The system administrator can also define month and day of the month as advanced options. Once done, click on "Save" and then "Apply Change" for the office time to take effect. The office time will be listed in the web page as the figure shows below.



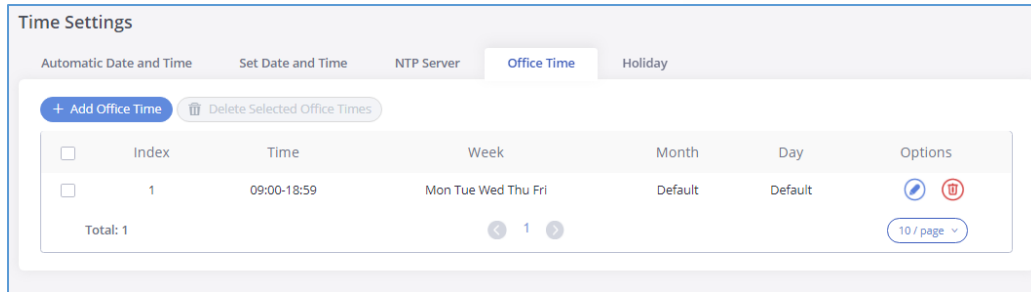




Figure 37: Time Settings→Office Time

- Click on  to edit the office time.
- Click on  to delete the office time.
- Click on "Delete Selected Office Times" to delete multiple selected office times at once.

Holiday

On the GXW450X, the system administrator can define "holiday", which can be used to configure time condition for inbound rule schedule. To configure holiday, go to Web GUI→**System Settings**→**Time Settings**→**Holiday**. Click on "Add Holiday" to create holiday time.

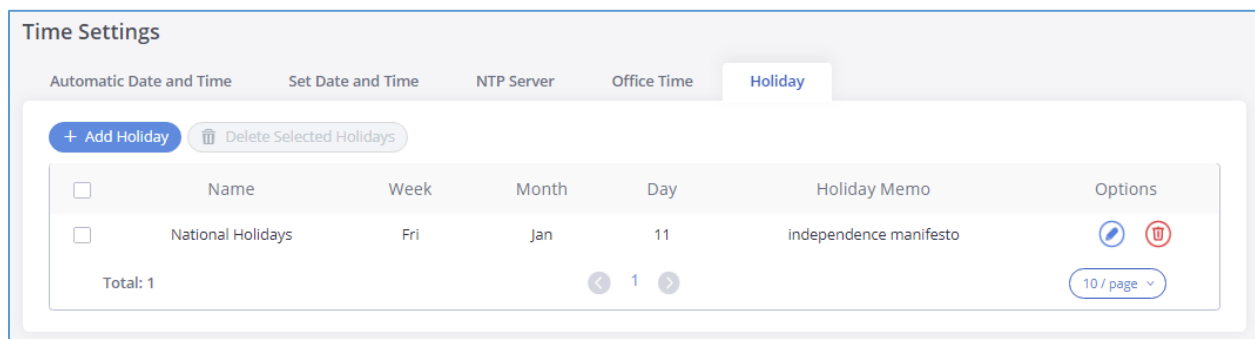
Figure 38: Add a Holiday





Table 20: Holiday Settings

Name	Specify the holiday name to identify this holiday.
Holiday Memo	Create a note for the holiday.
Month	Select the month for the holiday.
Day	Select the day for the holiday.
Show Advanced Options	Check this option to show advanced options. If selected, please specify the days as holiday in one week below.
Week	Select the days as holiday in one week.

Enter holiday "Name" and "Holiday Memo" for the new holiday. Then select "Month" and "Day". The system administrator can also define days in one week as advanced options. Once done, click on "Save" and then "Apply Change" for the holiday to take effect. The holiday will be listed in the web page as the figure shows below.


Figure 39: Time Settings→Holiday

- Click on  to edit the holiday.
- Click on  to delete the holiday.
- Click on "Delete Selected Holidays " to delete multiple selected holidays at once.



Email Settings

Email Settings

The Email application on the GXW450X can be used to send out alert event Emails, retrieve admin password etc. The configuration parameters can be accessed via Web GUI→**System Settings**→**Email Settings**→**Email Settings**.

Table 21: Email Settings

TLS Enable	Enable or disable TLS during transferring/submitted your Email to another SMTP server. The default setting is "Yes".
Type	<p>Select Email type.</p> <ul style="list-style-type: none"> • MTA: Mail Transfer Agent. The Email will be sent from the configured domain. When MTA is selected, there is no need to set up SMTP server for it or no user login is required. However, the Emails sent from MTA might be considered as spam by the target SMTP server. • Client: Submit Emails to the SMTP server. A SMTP server is required, and users need login with correct credentials.
Email Template Sending	Select the email template format to be sent. The "HTML" format is compatible with most mail clients and is recommended. If the mail client does not support the "HTML" format, please select the "Plain Text" format.
Domain	Specify the domain name to be used in the Email when using type "MTA".
SMTP Server	Specify the SMTP server when using type "Client".
Enable SASL Authentication	Enable SASL Authentication. When disabled, GXW450X will not try to use the user name and password for mail client login authentication. Most of the mail server requires login authentication while some others private mail servers allow anonymous login which requires disabling this option to send Email as normal. For Exchange Server, please disable this option.



Username	Username is required when using type "Client". Normally it's the Email address.
Password	Password to login for the above Username (Email address) is required when using type "Client".
POP/POP3 Server Address	Configure the POP/POP3 server address for the configured username Example: pop.gmail.com
POP/POP3 Server Port	Configure the POP/POP3 server port for the configured username Example: 995
Display Name	Specify the display name in the FROM header in the Email.
Sender	Specify the sender's Email address. For example: pbx@example.mycompany.com.

The following figure shows a sample Email setting on the GXW450X, assuming the email is using the default SMTP server of Gmail.



Email Settings

Email Settings
Email Template
Email Send Log

TLS Enable:

Type:

Email Template Sending Format:

*SMTP Server:

*Enable SASL Authentication:

*Username:

*Password:

POP/POP3 Server Address:

POP/POP3 Server Port:

*Display Name:

*Sender:

Figure 40: Email Settings

Once the configuration is finished, click on "Test". In the prompt, fill in a valid Email address to send a test Email to verify the Email settings on the GXW450X.



Email Template

The Email templates on the GXW450X can be used for email notification. The configuration parameters can be accessed via Web GUI→**System Settings**→**Email Settings**→**Email Templates**.



Email Settings

Email Settings **Email Template** Email Send Log




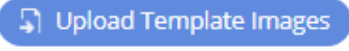


Type	Name	Time	Options
CDR	cdr_template.html	2018-05-24 14:31:23 UTC+08:00	
User Password	password_template.html	2018-05-24 14:31:23 UTC+08:00	
Alert Events	alert_template.html	2018-05-24 14:31:23 UTC+08:00	

Figure 41: Email Templates

- Press on  to upload pictures to be used on email templates.
- Press  to reset all email templates to default ones.
- To configure the email template, click the  button under Options column, and edit the template as desired.



Edit Email Template: Alert Events

*Subject:

*Message in Text Format:

[Device Mac addr: \${MAC}]
 \${WARNING_MSG}

Message in HTML Format:

🔍 **B** **I** **U** **ABE** **X²** **X₂** **A** **👉** **☰** **📄**

Paragraph Sim Sun 16px

[Device Mac addr: \${MAC}]
 \${WARNING_MSG}

Template Variables: \${MAC} : MAC Address
 \${WARNING_MSG} : Warning message

Figure 42: Alert Events Template

- Users can preview mail sample by clicking on .
- Click on in order to restore the default email template.
- Finally, users can click on to upload a custom picture to the email template to display their own logo in the sent mails for example

Email Send Log

Under GXW450X Web GUI→**System Settings**→**Email Settings**→**Email Send Log**, users could search, filter and check whether the Email is sent out successfully or not. This page will also display the corresponding error message if the Email is not sent out successfully.

Email Settings

[Email Settings](#) [Email Template](#) **[Email Send Log](#)**

In MTA mode, you cannot receive SPF authentication. Therefore, even if mail is sent successfully, the return code of 550 will still be returned. Many mail servers will place non-SPF-certified mail into the trash or quarantine mailbox. If the recipient has not received sent mail, please check to see if the sent mail was placed in the recipient's trash or quarantine mailbox.

In Client mode, a 250 return code means that the Email has been sent successfully from the GXW to your proxy mail server. The Email still fails to be sent due to invalid destination address or other reasons. Please login in your configuration mail account and check whether there is System bounce notification to confirm the cause of the failure. Return Code ^

250 Mail sent successfully.

501 Address format parsing error. In MTA mode, if the recipient's email address contains unsupported characters, a 501 message will be returned. Please check if the format of the recipient's email address is correct. In Client mode, some servers also return 501 when the sender and mail accounts do not match. Please correct "Sender" for your "Mail Account".

535 There was a problem with account/password verification in client mode. Please check that "account and password" are configured correctly (individual email servers will return 460).

550 Possible Causes: (1)The recipient's email address does not exist or is in a disabled state. Please check the recipient's email address for errors.
 (2)The number of destination addresses sent by the sender exceeds the maximum daily limit and is temporarily blacklisted. Please decrease the sending frequency or try again the next day.
 (3)The sending IP does not pass the SPF permission detection of the sending domain. Messages sent in MTA mode may still return the error code even if they are sent successfully.

552 The message sent is too large, or the message attachment type is disabled.

553 Sender and mail account inconsistencies. Please configure the "Sender" for your "Mail Account".

554 The message is identified as spam. Please decrease the sending frequency or retry the next day.

none Means no return code. If the "sending result" is deferred, there may be a problem with the mail server configuration, Please check to see if the "server" configuration is correct. If the result is bounced, there may be a problem with the domain name of the recipient's email address. Please check the message's "recipient" to make sure it is correct. If in MTA mode, please make sure that "Domain" is configured to be in the same domain as the recipient.

Show All Logs Delete All Logs Filter ^

Start Time:

End Time:

Receivers:

Send Result:

Return Code:

Email Send Module:

Email Generat ed Time	Email Send Mo dule	Receivers	Last Send Tim e	Last Send Add ress	Send Result	Return Code	Options
No Data							

Figure 43: Email Send Log

Table 22: Email Log Filter

Field	Description
Start Time	Enter the start time for filter
End time	Enter the end time for filter
Receivers	Enter the email recipient, while searching for multiple recipients, please separate them with comma and no spaces.
Send result	Enter the status of the send result to filter with
Return code	Enter the email code to filter with
Email send module	Select the email module to filter with from the drop-down list, which contains: All modules; User password; Alert events; CDR; Test.



TRUNKS

GXW450X is a VoIP Digital Gateway that supports both trunk modes Digital and VoIP to ensure a smooth integration of digital and VoIP communication to connect the legacy telephony infrastructure made up of PRI (E1, T1, J1) to the IP network.

Digital Trunks

The GXW450X supports E1/T1/J1 which are physical connection technologies used in digital network. T1 is the North American standard, J1 is used in Japan, whereas E1 is the European standard. GXW450X supports four signaling protocols: PRI_NET, PRI_CPE, MFC/R2 and SS7. PRI provides a varying number of channels depending on the standards in the country of implementation (E1, T1 or J1); MFC/R2 is a signaling protocol heavily used over E1 trunks; SS7 uses out-of-band signaling, which travels on a separate, dedicated channel rather than within the same channel as the telephone call, providing more efficiency and higher security level when the telephone calls are set up.

To set up digital trunk on the GXW450X:

1. Go to Web GUI→**PBX Settings**→**Interface Settings**→**Digital Hardware** to configure port type and channels.
2. Go to Web GUI→**Trunks**→**Digital Trunks** to add and edit digital trunk.
3. Go to Web GUI→ **Trunks**→**Outbound Routes** and **Inbound Routes** to configure outbound and inbound rule for the digital trunk.

Digital Hardware Configuration

Go to Web GUI→ **PBX Settings**→**Interface Settings**→**Digital Hardware** page and configure the following:



Interface Settings

Digital Hardware

Global Type Settings





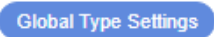








Port	Type	Signaling	Data channel	Options
1	E1	PRI_CPE	16	
2	E1	PRI_CPE	16	
3	E1	PRI_CPE	16	
4	E1	PRI_CPE	16	

Figure 44: Digital Hardware Configuration

- Click on  To change the Span of the Digital ports
- Click on  to edit digital ports. Please see configuration parameters in the tables below:

GXW4504

Menus 

-  System Status
-  Trunks
-  **PBX Settings**
 - SIP Settings
 - RTP Settings
 - Jitter Buffer
- Interface Settings**
-  System Settings
-  Maintenance
-  CDR

Edit Digital Ports: 1

Basic Settings Advanced Settings

Span Type:

Clock:

*Signaling:

Data channel:

LBO:

Coding:

RX Gain:

TX Gain:

Codec:

Play Local RBT:

Framing:

CRC Validation:

Figure 45: Digital Port Configuration



The GXW450X currently supports E1, T1 and J1 digital hardware type. When different signaling is selected for E1, T1 or J1, the settings in basic options and advanced options will be different. The following tables list all the settings to configure digital ports when selecting each signaling.

Table 23: Digital Hardware Configuration Parameters: E1 – PRI_NET/PRI_CPE

Basic Settings	
Clock	<p>All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the gateway system clock will synchronize to it.</p> <ul style="list-style-type: none"> • Master: The port will never be used as a source of timing. This is appropriate when you know far end should always be a slave to you. • Slave: The equipment at the far end of the E1/T1/J1 link is the preferred source of the master clock.
Signaling	<p>Chooses the signaling protocol that will be used on the digital port.</p> <p>PRI: when one end is set to NET, the other end should be set to CPE</p>
Data channel	<p>Chooses the Data Channel for control.</p>
LBO	<p>The line build-out (LBO) is the distance between the operators and the gateway. Please use the default value 0dB unless the distance is long.</p>
Coding	<p>T1:"AMI" or "B8ZS" E1:"AMI" or "HDB3"</p>
RX Gain	<p>Configure the RX gain for the receiving channel of digital port. The valid range is from -24dB to +12dB.</p>
TX Gain	<p>Configure the TX Gain for the transmitting channel of digital port. The valid range is -24dB to +12dB.</p>
Codec	<p>Select alaw or ulaw. If set to default, alaw will be used for E1.</p>
Framing	<p>If span type is E1, the signaling configure as MFC/R2, then framing must configure as "cas"; If span type is E1, the signaling configure as PRI or SS7, then framing must configure as "ccs"; If span type is T1, and the signaling configure as PRI or SS7, then framing can configure as "esf" or "d4"; If span type is J1, and the signaling configure as PRI or SS7, then framing can configure as "esf" or "d4".</p>
CRC Validation	<p>For E1, select whether to use CRC4 or None.</p>



Advanced Settings

Switch Type	<p>Select switch type.</p> <ul style="list-style-type: none"> • EuroISDN: EuroISDN (common in Europe) • NI2: National ISDN type 2 (common in the US) • DMS100: Nortel DMS100 • 4ESS: AT&T 4ESS • 5ESS: Lucent 5ESS • NI1: old national ISDN type 1 • Q.SIG
PRI Dial Plan	<p>This setting is used to specify the type of the callee number. The service provider will usually verify this. The default setting is “unknown”. In some very unusual circumstances, you may need set to “Dynamic” or “Redundant”.</p> <p>Note: When one type is selected, you might not be able to dial another class of numbers. For example, if “National” is configured, you won’t be able to dial local or international numbers.</p>
PRI Local Dial Plan	<p>This setting is used to specify the type of the caller number. The service provider will usually verify this.</p>
International Prefix National Prefix Local Prefix Private Prefix Unknown Prefix	<p>Configure the prefix in PRI Local Dial Plan and PRI Dial Plan for each type.</p>
PRI T310	<p>Configure PRI T310 Timer (in seconds).</p> <p>The default value is 10 seconds.</p>
PRI Indication	<p>Select the PRI Indication.</p> <ul style="list-style-type: none"> • outofband: Use RELEASE, DISCONNECT or other messages with CAUSE to indicate call progress (e.g., cause: unassigned number or user busy). • inband: use in-band tones to play busy or congestion signal to the other side. This is the default setting.



Reset Interval	The interval that restarts idle channels.
PRI Exclusive	This setting is used to set up the ChannelID in SETUP message. If enabled, only the specified B channel can be used. Otherwise, select one of the channels in B channel. If you need override the existing channels selection routine and force all PRI channels to be marked as exclusively selected, please enable it.
Facility Enable	If selected, transmission of facility-based ISDN supplementary services (such as caller name from CPE over facility) will be enabled.
SETUP ACK	When receiving a remote "SETUP" SIP message, and the "Sending Complete" field is not included in it, the gateway will send a "SETUP ACK" to request for more information. This option should be used if a remote device has "SETUP ACK" support issues.
Overlap Dial	Configure this option to send overlap digits. If enabled, SETUP message can include some digits of callee number, and rest of the digits can be sent using INFORMATION message. If disabled, callee number will be sent via SETUP message when all the digits are ready.
NSF	Some switches (AT&T especially) require network specific facility. Currently the supported values are "none", "sdn", "megacom", "tollfreemegacom".

Table 24: Digital Hardware Configuration Parameters: E1 - SS7

Basic Settings	
Clock	<p>All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the gateway system clock will synchronize to it.</p> <ul style="list-style-type: none"> • Master: The port will never be used as a source of timing. This is appropriate when you know far end should always be a slave to you. • Slave: The equipment at the far end of the E1/T1 link is the preferred source of the master clock.
Signaling	<p>Chooses the signaling protocol that will be used on the digital port.</p> <p>PRI: when one end is set to NET, the other end should be set to CPE</p>



Data channel	Chooses the Data Channel for control.
SS7 Variant	Select ITU, ANSI or CHINA.
Originating Point Code	<p>Originating point code is used to identify the node originating the message, always provided by the operator/ISP.</p> <ul style="list-style-type: none"> ITU Format: decimal number. ANSI & CHINA Format: decimal number or XXX-XXX-XXX.
Destination Point Code	<p>Destination point code is the address to send the message to, always be provided by the operator/ISP.</p> <ul style="list-style-type: none"> ITU Format: decimal number. ANSI & CHINA Format: decimal number or XXX-XXX-XXX.
First CIC	<p>When Span Type is E1, ITU & CHINA Range: [0, 4065], ANSI Range: [0, 16353].</p> <p>When Span Type is T1/J1, ITU & CHINA Range: [0, 4072], ANSI Range: [0, 16360].</p>
Assign CIC To D-channel	If set to yes, D-channel will be assigned a CIC. Else, D-channel will not be assigned. By default, it is set to No.
Network Indicator	Network Indicator (NI) should match in nodes, otherwise it might cause issues. Users can select "National", "National Spare", "International", or "International Spare". Usually "National" or "International" is used.
LBO	The line build-out (LBO) is the distance between the operators and the gateway. Please use the default value 0dB unless the distance is long.
Coding	<p>T1:"AMI" or "B8ZS"</p> <p>E1:"AMI" or "HDB3"</p>
RX Gain	Configure the RX gain for the receiving channel of digital port. The valid range is from -24dB to +12dB.
TX Gain	Configure the TX Gain for the transmitting channel of digital port. The valid range is -24dB to +12dB.



Codec	Select alaw or ulaw. If set to default, alaw will be used for E1.
Framing	If span type is E1, the signaling configure as MFC/R2, then framing must configure as "cas"; If span type is E1, the signaling configure as PRI or SS7, then framing must configure as "ccs"; If span type is T1, and the signaling configure as PRI or SS7, then framing can configure as "esf" or "d4"; If span type is J1, and the signaling configure as PRI or SS7, then framing can configure as "esf" or "d4".
CRC Validation	For E1, select whether to use CRC4 or None.
Advanced Settings	
Called Nature of Address Indicator	Indicates the type of the called number. The receiving switch may use this indicator during translations to apply the number's proper dial plan. Users can select "Unknown", "Subscriber", "National", "International" or "Dynamic".
Calling Nature of Address Indicator	Indicates the type of the calling number. The receiving switch may use this indicator during translations to apply the number's proper dial plan. Users can select "Unknown", "Subscriber", "National", "International" or "Dynamic".
International Prefix National Prefix Subscriber Prefix Unknown Prefix	Configure the prefix in Called Nature of Address Indicator and Calling Nature of Address Indicator for each type.

Table 25: Digital Hardware Configuration Parameters: E1 - MFC/R2

Basic Settings	
Clock	All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the gateway system clock will synchronize to it.



	<ul style="list-style-type: none"> • Master: The port will never be used as a source of timing. This is appropriate when you know far end should always be a slave to you. • Slave: The equipment at the far end of the E1/T1 link is the preferred source of the master clock.
Signaling	<p>Chooses the signaling protocol that will be used on the digital port.</p> <p>PRI: when one end is set to NET, the other end should be set to CPE</p>
Data channel	Chooses the Data Channel for control.
Variant	MFC/R2 multinational adaption. GXW450X supports MFC/R2 standards by ITU and MFC/R2 standards in different countries or regions including Argentina, Brazil, China, Czech Republic, Colombia, Ecuador, Indonesia, Mexico, the Philippines and Venezuela.
Category	Defines the Caller Category. Users can choose among the following options: National Subscriber, National Priority Subscriber, International Subscriber, International Priority Subscriber.
Get ANI First	<p>If enabled, the callee side will request the caller to send caller number first and then called number.</p> <p>Note: Options "Get ANI First" and "Skip Category" cannot be enabled at the same time.</p>
LBO	The line build-out (LBO) is the distance between the operators and the gateway. Please use the default value 0dB unless the distance is long.
Coding	<p>T1:"AMI" or "B8ZS"</p> <p>E1:"AMI" or "HDB3"</p>
RX Gain	Configure the RX gain for the receiving channel of digital port. The valid range is from -24dB to +12dB.
TX Gain	Configure the TX Gain for the transmitting channel of digital port. The valid range is -24dB to +12dB.



Framing	If span type is E1, the signaling configure as MFC/R2, then framing must configure as "cas"; If span type is E1, the signaling configure as PRI or SS7, then framing must configure as "ccs"; If span type is T1, and the signaling configure as PRI or SS7, then framing can configure as "esf" or "d4"; If span type is J1, and the signaling configure as PRI or SS7, then framing can configure as "esf" or "d4".
CRC Validation	For E1, select whether to use CRC4 or None.
Advanced Settings	
MF Back Timeout (ms)	MFC/R2 value in milliseconds for MF timeout. Values smaller than 500ms are not recommended. -1 represents default value.
Metering Pulse Timeout (ms)	MFC/R2 value in milliseconds for the metering pulse timeout. Metering pulse is sent by some telcos for some R2 variants during a call presumably for billing purposes to indicate costs. Should not last more than 500ms, -1 represents default value, and for Argentina the default value is 400ms, for others is 0ms.
Allow Collect Calls	Brazil has a special calling party category for collect calls (llamadas por cobrar) instead of using the operator (as in Mexico). The R2 spec in Brazil says a special GB tone should be used to reject collect calls. By default, this is disabled, which means collect calls will be blocked.
Double Answer	Some gateways require a double-answer process to block collect calls. If users have problem blocking collect calls using Group B signals, please try enabling this option.
Accept On Offer	By default, it's enabled. In most of cases, this option should be enabled.
Skip Category	If enabled, the callee side will request the caller to send caller category before sending caller number. Note: "Get ANI First" and "Skip Category" cannot be enabled at the same time.
Charge Calls	Whether or not report to the other end "accept call with charge". This setting has no effect with most telecos. Default setting is enabled (recommended).



Custom Options

Click on “Custom Options” button (on the left top of the configuration dialog) and then user can customize desired tone and timer options accordingly.

Table 26: Digital Hardware Configuration Parameters: T1/J1 - PRI_NET/PRI_CPE

Basic Settings	
Clock	<p>All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the gateway system clock will synchronize to it.</p> <ul style="list-style-type: none"> • Master: The port will never be used as a source of timing. This is appropriate when you know far end should always be a slave to you. • Slave: The equipment at the far end of the E1/T1/J1 link is the preferred source of the master clock.
Signaling	<p>Chooses the signaling protocol that will be used on the digital port.</p> <p>PRI: when one end is set to NET, the other end should be set to CPE</p>
Data channel	Chooses the Data Channel for control.
LBO	The line build-out (LBO) is the distance between the operators and the gateway. Please use the default value 0dB unless the distance is long.
Coding	<p>T1:"AMI" or "B8ZS"</p> <p>E1:"AMI" or "HDB3"</p>
RX Gain	Configure the RX gain for the receiving channel of digital port. The valid range is from -24dB to +12dB.
TX Gain	Configure the TX Gain for the transmitting channel of digital port. The valid range is -24dB to +12dB.
Codec	Select alaw or ulaw. If set to default, ulaw will be used for T1/J1.
Framing	Select “esf” or “d4”. Default setting is esf.
Advanced Settings	
Switch Type	<p>Select switch type.</p> <ul style="list-style-type: none"> • EuroISDN: EuroISDN (common in Europe) • NI2: National ISDN type 2 (common in the US)



	<ul style="list-style-type: none"> • DMS100: Nortel DMS100 • 4ESS: AT&T 4ESS • 5ESS: Lucent 5ESS • NI1: old national ISDN type 1 • Q.SIG
PRI Dial Plan	<p>This setting is used to specify the type of the callee number. The service provider will usually verify this. The default setting is "unknown". In some very unusual circumstances, you may need set to "Dynamic" or "Redundant".</p> <p>Note: When one type is selected, you might not be able to dial another class of numbers. For example, if "National" is configured, you won't be able to dial local or international numbers.</p>
PRI Local Dial Plan	<p>This setting is used to specify the type of the caller number. The service provider will usually verify this.</p>
International Prefix National Prefix Local Prefix Private Prefix Unknown Prefix	<p>Configure the prefix in PRI Local Dial Plan and PRI Dial Plan for each type.</p>
PRI T310	<p>Configure PRI T310 Timer (in seconds). The default value is 10 seconds.</p>
PRI Indication	<p>Select the PRI Indication.</p> <ul style="list-style-type: none"> • outofband: Use RELEASE, DISCONNECT or other messages with CAUSE to indicate call progress (e.g., cause: unassigned number or user busy). • inband: use in-band tones to play busy or congestion signal to the other side. This is the default setting.
Reset Interval	<p>The interval that restarts idle channels.</p>
PRI Exclusive	<p>This setting is used to set up the ChannelID in SETUP message. If enabled, only the specified B channel can be used. Otherwise, select one of the channels in B channel. If you need override the existing channels selection routine and force all PRI channels to be marked as exclusively selected, please enable it.</p>



Facility Enable	If selected, transmission of facility-based ISDN supplementary services (such as caller name from CPE over facility) will be enabled.
SETUP ACK	When receiving a remote "SETUP" SIP message, and the "Sending Complete" field is not included in it, the gateway will send a "SETUP ACK" to request for more information. This option should be used if a remote device has "SETUP ACK" support issues.
Overlap Dial	Configure this option to send overlap digits. If enabled, SETUP message can include some digits of callee number, and rest of the digits can be sent using INFORMATION message. If disabled, callee number will be sent via SETUP message when all the digits are ready.
NSF	Some switches (AT&T especially) require network specific facility. Currently the supported values are "none", "sdn", "megacom", "tollfreemegacom", "accunet".

Table 27: Digital Hardware Configuration Parameters: T1/J1 - SS7

Basic Settings	
Clock	<p>All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the gateway system clock will synchronize to it.</p> <ul style="list-style-type: none"> • Master: The port will never be used as a source of timing. This is appropriate when you know far end should always be a slave to you. • Slave: The equipment at the far end of the E1/T1 link is the preferred source of the master clock.
Signaling	<p>Chooses the signaling protocol that will be used on the digital port.</p> <p>PRI: when one end is set to NET, the other end should be set to CPE</p>
Data channel	Chooses the Data Channel for control.
SS7 Variant	Select ITU, ANSI or CHINA.



Originating Point Code	<p>Originating point code is used to identify the node originating the message, always provided by the operator/ISP.</p> <ul style="list-style-type: none"> • ITU Format: decimal number. • ANSI & CHINA Format: decimal number or XXX-XXX-XXX.
Destination Point Code	<p>Destination point code is the address to send the message to, always be provided by the operator/ISP.</p> <ul style="list-style-type: none"> • ITU Format: decimal number. • ANSI & CHINA Format: decimal number or XXX-XXX-XXX.
First CIC	<p>When Span Type is E1, ITU & CHINA Range: [0, 4065], ANSI Range: [0, 16353].</p> <p>When Span Type is T1/J1, ITU & CHINA Range: [0,4072], ANSI Range: [0, 16360].</p>
Assign CIC to D-Channel	<p>If set to yes, D-channel will be assigned with a CIC. Else, D-channel will not be assigned with a CIC. By default, it is set to No.</p>
Network Indicator	<p>Network Indicator (NI) should match in nodes, otherwise it might cause issues. Users can select "National", "National Spare", "International", or "International Spare". Usually "National" or "International" is used.</p>
LBO	<p>The line build-out (LBO) is the distance between the operators and the gateway. Please use the default value 0dB unless the distance is long.</p>
Coding	<p>T1:"AMI" or "B8ZS"</p> <p>E1:"AMI" or "HDB3"</p>
RX Gain	<p>Configure the RX gain for the receiving channel of digital port. The valid range is from -24dB to +12dB.</p>
TX Gain	<p>Configure the TX Gain for the transmitting channel of digital port. The valid range is -24dB to +12dB.</p>
Codec	<p>Select alaw or ulaw. If set to default, ulaw will be used for T1/J1.</p>
Framing	<p>Select "esf" or "d4". Default setting is esf.</p>

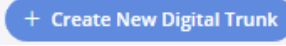




Advanced Settings

Called Nature of Address Indicator	Indicates the type of the called number. The receiving switch may use this indicator during translations to apply the number's proper dial plan. Users can select "Unknown", "Subscriber", "National", "International" or "Dynamic".
Calling Nature of Address Indicator	Indicates the type of the calling number. The receiving switch may use this indicator during translations to apply the number's proper dial plan. Users can select "Unknown", "Subscriber", "National", "International" or "Dynamic".
International Prefix National Prefix Subscriber Prefix Unknown Prefix	Configure the prefix in Called Nature of Address Indicator and Calling Nature of Address Indicator for each type.

Digital Trunk Configuration

After configuring digital hardware, go to Web GUI → **Trunks** → **Digital Trunks**.

- Click on  to add a new digital trunk.
- Click on  to configure detailed parameters for the digital trunk.
- Click on  to delete the digital trunk.

The digital trunk parameters are listed in the table below.

Table 28: Digital Trunk Configuration Parameters

Trunk Name	Configure trunk name to identify the digital trunk.
Port	Configure the digital channel group used by the trunk.
Hide CallerID	Configure to hide outgoing caller ID. The default setting is "No".
Caller ID	Configure the Caller ID. This is the number that the trunk will try to use when making outbound calls. For some providers, it might not be possible to set the CallerID with this option and this option will be ignored.

CallerID Name	Configure the name of the caller.
DAHDI Out Line Selection	<p>This is to implement Digital trunk outbound line selection strategy. Three options are available:</p> <ul style="list-style-type: none"> • Ascend: When the call goes out from this digital trunk, it will always try to use the first idle digital port. The port order that the call will use to go out would be port 1→port 2→port 3→port 4. Every time it will start with port 1 (if it's idle). • Poll: When the call goes out from this digital trunk, it will use the port that is not used last time. And it will always use the port in the order of port 1→2→3→4→1→2→3→4→1→2→3→4→1→2→3→4..., following the last port being used. • Descend: When the call goes out from this digital trunk, it will always try to use the last idle digital port. The port order that the call will use to go out would be port 16→port 10→port 2→port 1. Every time it will start with port 4 (if it's idle). <p>The default setting is "Ascend" mode.</p>
Fax Gateway	<p>Enable/disable Fax Gateway on the digital trunk.</p> <p>If enabled, GXW450X will detect fax tone on digital interface in order to initiate T.38 fax, otherwise, it will be sent in audio as pass-through.</p>

Digital Trunk Troubleshooting

After configuring the digital trunk on the GXW450X as described above, if it doesn't work as expected, users can go to capture signaling trace on the GXW450X Web GUI for troubleshooting purpose.

Depending on the signaling selected for the digital trunk, users can go to following pages to capture trace:

PRI Signaling Trace: Web GUI→**Maintenance**→**Signaling Troubleshooting**→**PRI Signaling Trace**

SS7 Signaling Trace: Web GUI→**Maintenance**→**Signaling Troubleshooting**→**SS7 Signaling Trace**

MFC/R2 Signaling Trace: Web GUI→**Maintenance**→**Signaling Troubleshooting**→**MFC/R2 Signaling Trace**

Users can also capture a **Digital Record Trace** to record the call for other troubleshooting purposes such as audio quality problems and noise.



Below are the steps to capture the trace:

1. Click on "Start" to start capturing trace. The output result shows "Capturing..."
2. Once the test is done, click on "Stop" to stop the trace.
3. Click on "Download" to download the trace.

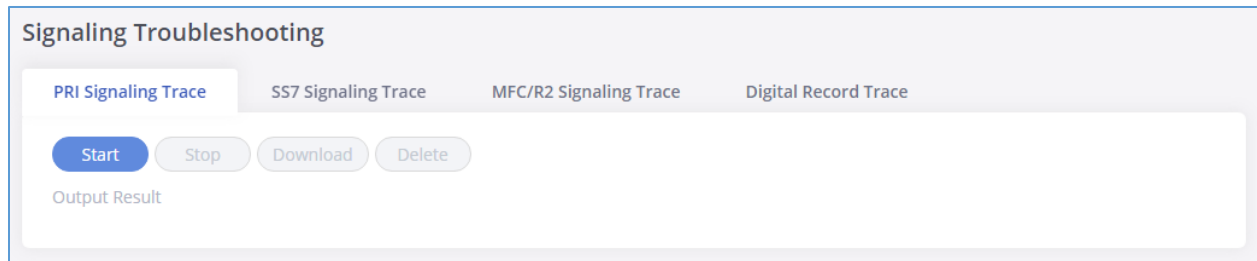


Figure 46: Troubleshooting Digital Trunks

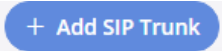


After capturing the trace, users can download it for basic analysis. Or you can contact Grandstream Technical support in the following link for further assistance if the issue is not resolved:

<http://www.grandstream.com/support>

VoIP Trunks

The VoIP trunks allow the GXW450X to be connected over an IP network via SIP protocol to a VoIP provider or to another device that supports the SIP trunks.

VoIP trunks can be configured in GXW450X under Web GUI → **Trunks** → **VoIP Trunks**. Once created, the VoIP trunks will be listed with Provider Name, Type, Hostname/IP, Username and Options to edit/detect the trunk.

- Click on  to add a new VoIP trunk.
- Click on  to configure detailed parameters for the VoIP trunk.
- Click on  to delete the VoIP trunk.

The VoIP trunk options are listed in the table below.

Table 29: Create New SIP Trunk

Type	Select VoIP trunk type to create. <ul style="list-style-type: none"> • Peer SIP Trunk • Register SIP Trunk
Provider Name	Configure a unique label (up to 64 characters) to identify this trunk when listed in outbound rules, inbound rules and etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
NAT	Turn on this setting when the gateway is using public IP and communicating with devices behind NAT. If there is one-way audio issue, usually it is related to NAT configuration or SIP/RTP port support on the firewall.
Disable This Trunk	If checked, the trunk will be disabled. Note: If a current "Register SIP trunk" is disabled, GXW450X will send UNREGISTER message (REGISTER message with expires=0) to the SIP provider.
TEL URI	If the trunk has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and TO header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is disabled.
From Domain	Configure the actual domain name. This can be used to override the "From" Header. For example, "trunk.GXW450X.provider.com" is the From Domain in From Header: sip: 1234567@trunk.GXW450X.provider.com.
Transport	Configure the SIP transport protocol to be used in this trunk. UDP; TCP or TLS. The default setting is "UDP"
If "Type" is set to "Register SIP Trunk"	
Need Registration	Select whether the trunk needs to register on the external server or not when "Register SIP Trunk" type is selected. The default setting is "Yes".
Allow outgoing calls if registration fails	If enabled outgoing calls even if the registration to this trunk fail will still be able to go through. Note that if we uncheck "Need Registration" option, this option will be ignored. The default setting is "Yes".



Username	Enter the username to register to the trunk from the provider.
Password	Enter the password to register to the trunk from the provider.
AuthID	Enter the Authentication ID to register to the trunk from the provider.


After creating the SIP Trunk user can click on  to edit the trunk and have detailed parameters to configure. Below is a table of the Basic and advanced parameters of a SIP trunk.

Table 30: VoIP Trunk Configuration Parameters – Register SIP Trunk

Basic Settings	
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules and etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
NAT	Turn on this option when the gateway is using public IP and communicating with devices behind NAT. If there is one-way audio issue, usually it's related to NAT configuration or SIP/RTP port configuration on the firewall.
Disable This Trunk	If selected, the trunk will be disabled. Note: If a current SIP trunk is disabled, GXW450X will send UNREGISTER message (REGISTER message with expires=0) to the SIP provider.
TEL URI	If the trunk has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and TO header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is disabled.
From Domain	Configure the actual domain name. This can be used to override the "From" Header. For example, "trunk.GXW450X.provider.com" is the From Domain in From Header: sip:1234567@trunk.GXW450X.provider.com.
Transport	Configure the SIP transport protocol to be used in this trunk. <ul style="list-style-type: none"> • UDP • TCP • TLS The default setting is "UDP".



Need Registration	Select whether the trunk needs to register on the external server or not when "Register SIP Trunk" type is selected. The default setting is "Yes".
Allow outgoing calls if registration fails	If enabled outgoing calls even if the registration to this trunk fail will still be able to go through. Note that if we uncheck "Need Registration" option, this option will be ignored. The default setting is "Yes".
Username	Enter the username to register to the trunk from the provider.
Password	Enter the password to register to the trunk from the provider.
AuthID	Enter the Authentication ID to register to the trunk from the provider.
Advanced Settings	
Codec Preference	Select audio codec for the VoIP trunk. The available codecs are: PCMU, PCMA, G.726, G.729, iLBC, G.722, AAL2-G.726-32, G.723, OPUS
Send PAI Header	If checked, the INVITE message sent from the trunk will contain PAI (P-Asserted-Identity) Header. Default is unchecked.
PAI Header	The user and name of the PAI header. It is formatted as "name<number>" or "<number>" or "number"; if null, use the CID according to the priority.
Passthrough PAI Header	If enabled and "Send PAI Header" is disabled, PAI headers will be preserved as calls pass through the GXW450X.
Outbound Proxy Support	Enable to send outbound signal to the proxy instead of the devices directly. The default setting is "unchecked".
DID Mode	Configure where to get the destination ID of an incoming SIP call, from SIP Request-line or To-header. The default is set to "Request-line".
DTMF Mode	<p>Configure the default DTMF mode when sending DTMF on this trunk.</p> <ul style="list-style-type: none"> • Default: The global setting of DTMF mode will be used. The global setting for DTMF Mode setting is under Web GUI→PBX Settings→SIP Settings→ToS. • RFC2833: Send DTMF using RFC2833. • Info: Send DTMF using SIP INFO message. • Inband: Send DTMF using inband audio. This requires 64-bit codec, i.e., PCMU and PCMA. • Auto: Send DTMF using RFC2833 if offered. Otherwise, inband.
Enable Heartbeat Detection	If enabled, the GXW450X will regularly send SIP OPTIONS to the device to check if the device is still online. The default setting is "No".



Heartbeat Frequency	When "Enable Heartbeat Detection" option is set to "Yes", configure the interval (in seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. The default setting is 60 seconds.
Maximum Number of Call Lines	The maximum number of concurrent calls using the trunk. The default settings 0, which means no limit.
SRTP	<p>Enable SRTP for the VoIP trunk to use</p> <ul style="list-style-type: none"> • Disabled • Enabled but not forced • Enabled and forced <p>The default setting is "Disabled".</p> <p>It uses SDP Security Description to exchange key. Please refer to SDES: https://tools.ietf.org/html/rfc4568</p> <p>SRTP: https://www.ietf.org/rfc/rfc3711.txt</p>

Table 31: VoIP Trunk Configuration Parameters – Peer SIP Trunk

Basic Settings	
Provider Name	Configure a unique label to identify this trunk when listed in outbound rules, inbound rules and etc.
Host Name	Configure the IP address or URL for the VoIP provider's server of the trunk.
NAT	Turn on this option when the gateway is using public IP and communicating with devices behind NAT. If there is one-way audio issue, usually it's related to NAT configuration or SIP/RTP port configuration on the firewall.
Disable This Trunk	If selected, the trunk will be disabled.
TEL URI	If the trunk has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and TO header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is disabled.
From Domain	<p>Configure the actual domain name. This can be used to override the "From" Header.</p> <p>For example, "trunk.GXW450X.provider.com" is the From Domain in From Header: sip:1234567@trunk.GXW450X.provider.com.</p>



Transport	<p>Configure the SIP transport protocol to be used in this trunk.</p> <ul style="list-style-type: none"> • UDP • TCP • TLS <p>The default setting is "UDP".</p>
Advanced Settings	
Codec Preference	Select audio codec for the VoIP trunk. The available codecs are: PCMU, PCMA, G.726, G.729, iLBC, G.722, AAL2-G.726-32, G.723, OPUS.
Send PAI Header	If checked, the INVITE message sent from the trunk will contain PAI (P-Asserted-Identity) Header. Default is unchecked.
PAI Header	The user and name of the PAI header. It is formatted as "name<number>" or "<number>" or "number"; if null, use the CID according to the priority.
Passthrough PAI Header	If enabled and "Send PAI Header" is disabled, PAI headers will be preserved as calls pass through the GXW450X.
Outbound Proxy Support	Enable to send outbound signal to the proxy instead of the devices directly. The default setting is "unchecked".
DID Mode	Configure where to get the destination ID of an incoming SIP call, from SIP Request-line or To-header. The default is set to "Request-line".
DTMF Mode	<p>Configure the default DTMF mode when sending DTMF on this trunk.</p> <ul style="list-style-type: none"> • Default: The global setting of DTMF mode will be used. The global setting for DTMF Mode setting is under Web GUI→PBX Settings→SIP Settings→ToS. • RFC2833: Send DTMF using RFC2833. • Info: Send DTMF using SIP INFO message. • Inband: Send DTMF using inband audio. This requires 64-bit codec, i.e., PCMU and PCMA. • Auto: Send DTMF using RFC2833 if offered. Otherwise, inband.
Enable Heartbeat Detection	If enabled, the GXW450X will regularly send SIP OPTIONS to the device to check if the device is still online. The default setting is "No".
Heartbeat Frequency	When "Enable Heartbeat Detection" option is set to "Yes", configure the interval (in seconds) of the SIP OPTIONS message sent to the device to check if the device is still online. The default setting is 60 seconds.






Maximum Number of Call Lines	The maximum number of concurrent calls using the trunk. The default settings 0, which means no limit.
SRTP	Enable SRTP for the VoIP trunk to use <ul style="list-style-type: none"> • Disabled • Enabled but not forced • Enabled and forced” The default setting is "Disabled". It uses SDP Security Description to exchange key. Please refer to SDES: https://tools.ietf.org/html/rfc4568 SRTP: https://www.ietf.org/rfc/rfc3711.txt

Outbound Routes

An outbound route is a set of rules defined by privileges and patterns that the gateway uses to decide the numbers that can go out through the trunk, who has the right to use the trunk and trunk to use for an outbound call.

To create an outbound route, Go to Web GUI → **Trunks** → **Outbound Routes**.

- Click on  to add a new outbound route.
- Click on  to edit the outbound route.
- Click on  to delete the outbound route.

On the GXW450X, the outbound route priority is based on “Best matching pattern”. For example, the GXW450X has outbound route A with pattern 1xxx and outbound route B with pattern 10xx configured. When dialing 1000 for outbound call, outbound route B will always be used first. This is because pattern 10xx is a better match than pattern 1xxx. Only when there are multiple outbound routes with the same pattern configured, the GXW450X will use the first pattern matched.








Sequence	Outbound Rule Name	Pattern	Options
1	TO_TEST	_X.	 
Total: 1		 1 	10 / page 

Figure 47: Create Outbound Route

Calling Rule Name	Configure the name of the calling rule (e.g., local, long-distance, and etc). Letters, digits, _ and - are allowed.
Pattern	<ul style="list-style-type: none"> All patterns are prefixed with the "_". Special characters: <ul style="list-style-type: none"> X: Any Digit from 0-9. Z: Any Digit from 1-9. N: Any Digit from 2-9. .": Wildcard. Match one or more characters. "!": Wildcard. Match zero or more characters immediately. <p>Example: [12345-9] - Any digit from 1 to 9.</p> <p>Notes:</p> <ul style="list-style-type: none"> Multiple patterns can be used. Each pattern should be entered in new line. <u>Example:</u> <pre>_X. _NNXXNXXXXX _818X.</pre>
Main Trunk	
Trunk	Select the trunk for this outbound rule.
Strip	Allows the user to specify the number of digits that will be stripped from the beginning of the dialed string before the call is placed via the selected trunk.



	<p><u>Example:</u></p> <p>The users will dial 9 as the first digit of a long-distance calls. However, 9 should not be sent out via digital lines and the PSTN line. In this case, 1 digit should be stripped before the call is placed.</p>
Prepend	<p>Specify the digits to be prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.</p>
Failover Trunk	
Trunk	<p>Failover trunks can be used to make sure that a call goes through an alternate route, when the primary trunk is busy or down. If "Use Failover Trunk" is enabled and "Failover trunk" is defined, the calls that cannot be placed via the regular trunk may have a secondary trunk to go through.</p> <p>GXW450X support up to 10 failover trunks.</p> <p><u>Example:</u> The user's primary trunk is a VoIP trunk and the user would like to use the PSTN when the VoIP trunk is not available. The PSTN trunk can be configured as the failover trunk of the VoIP trunk.</p>
Strip	<p>Allows the user to specify the number of digits that will be stripped from the beginning of the dialed string before the call is placed via the selected trunk.</p> <p><u>Example:</u></p> <p>The users will dial 9 as the first digit of a long-distance calls. However, 9 should not be sent out via digital lines and the PSTN line. In this case, 1 digit should be stripped before the call is placed.</p>
Prepend	<p>Specify the digits to be prepended before the call is placed via the trunk. Those digits will be prepended after the dialing number is stripped.</p>
Time Condition	
Time Condition Mode	<p>Use Main Trunk or Failover Trunk: Use the Main Trunk and its settings during the configured time conditions. If the main trunk is unavailable, the Failover Trunk and its settings will be used instead.</p> <p>Use Specific Trunks: Use specific trunks during the configured time conditions. The Strip and Prepend settings of the Main Trunk will be used. If a trunk is unavailable during its time condition, no failover trunks will be used.</p>



Time Condition


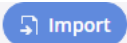



Users could customize holiday time, office time or a specified time to allow the outbound route to be used.

Inbound Routes

When a call comes into the GXW450X from the outside, it will usually arrive along with information about the telephone number that was dialed (also known as the "DID") and the Caller ID of the person who called.

The Inbound Routes is used to tell the system what to do with calls that come into the GXW450X on any trunk based on the patten of the DID and the caller ID of the person who called.

Inbound routes can be configured via Web GUI → **Trunks** → **Inbound Routes**.

- Click on  button to add a new inbound route.
- Click on  To import inbound routes.
- Click on  to export inbound routes.
- Click on  to edit the inbound route.
- Click on  to delete the inbound route

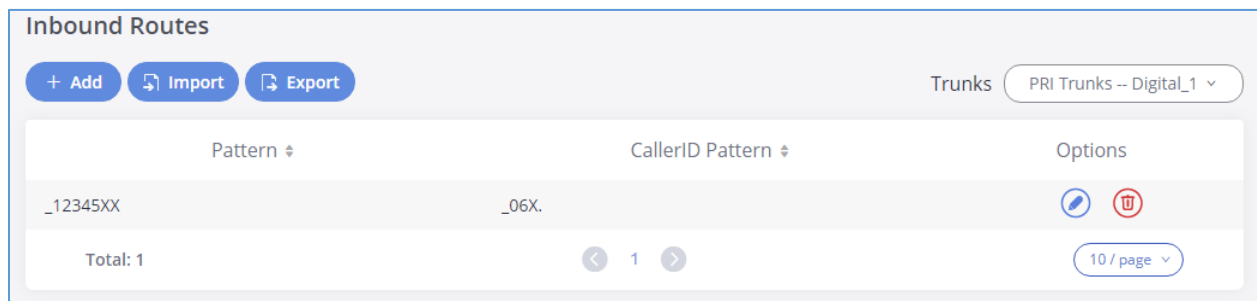


Figure 48: Create Inbound Routes

Inbound Route Configuration

Table 32: Inbound Rule Configuration Parameters

Trunks	Select the trunk to configure the inbound rule.
Pattern	<ul style="list-style-type: none"> • All patterns are prefixed with the "_". • Special characters:

X: Any Digit from 0-9.

Z: Any Digit from 1-9.

N: Any Digit from 2-9.

.": Wildcard. Match one or more characters.

!": Wildcard. Match zero or more characters immediately.

Example: [12345-9] - Any digit from 1 to 9.

Notes:

- Multiple patterns can be used. Each pattern should be entered in new line.
- Example:

Pattern	CallerID Pattern
_X.	1000
_NNXXNXXXXX	1001
_818X.	

CallerID Pattern

All patterns are prefixed by "_" character, but please do not enter more than one "_" at the beginning. In patterns, some characters have special meanings:

[12345-9] ... Any digit in the brackets. In this example, 1,2,3,4,5,6,7,8,9 are allowed.

N ... Any digit from 2-9.

. ... Wildcard, matching one or more characters.

! ... Wildcard, matching zero or more characters immediately.

X ... Any digit from 0-9.

Z ... Any digit from 1-9.

- ... Hyphen is to connect characters and it will be ignored.

[] Contain special characters ([x], [n], [z]) represent letters x, n, z.

Inbound Route: Import/Export Inbound Route

Users can import and export inbound routes to quickly set up inbound routing on a GXW450X or to back up an existing configuration. An exported inbound route configuration can be directly imported without needing any manual modifications.



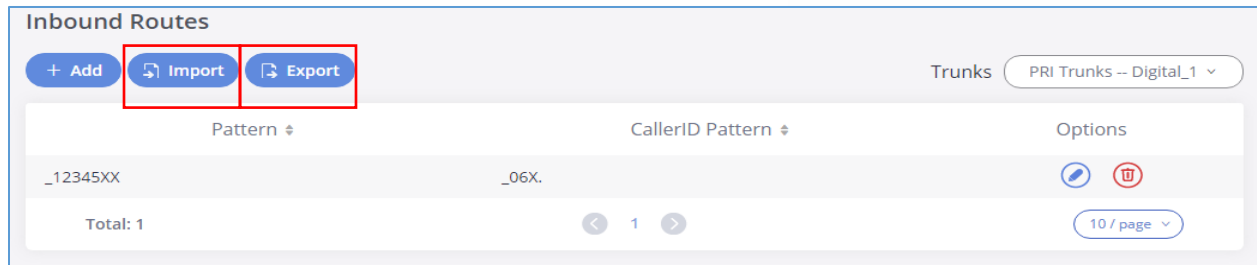


Figure 49: Import/Export Inbound Route

The imported file should be on CSV format and using UTF-8 encoding, the imported file should contain below columns, and each column should be separated by a comma (It is recommended to use Notepad++ for the imported file creation):

- Pattern: Always prefixed with _
- CallerID Pattern: Always prefixed with _



PBX SETTINGS

This section describes internal options that haven't been mentioned in previous sections yet. The settings in this section can be applied globally to the GXW450X, including general configurations, jitter buffer, RTP settings and hardware config. The options can be accessed via Web GUI→**PBX Settings**→**General Settings**.

SIP Settings

The GXW450X SIP global settings can be accessed via Web GUI→**PBX Settings**→**SIP Settings**.

General

On this page users can define the Binding UDP Port for SIP protocol and Enable 486 to Failover Trunk.

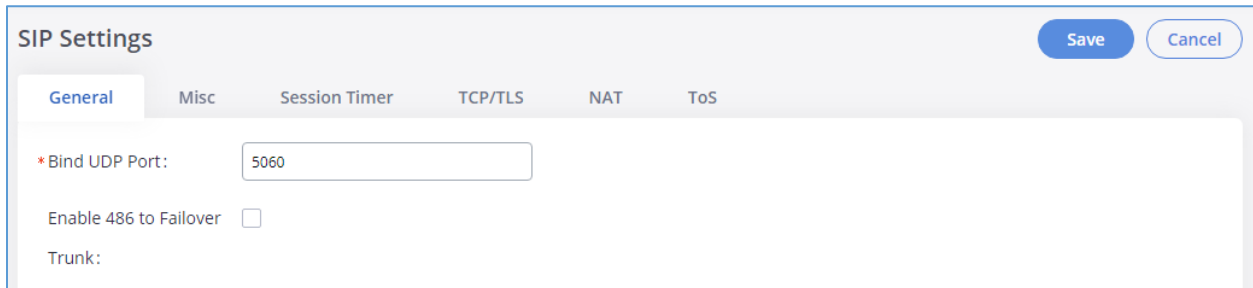


Figure 50: SIP Settings - General

Table 33: SIP Settings - General

Bind UDP Port	Configure binding UDP port for SIP. The default setting is "5060".
Enable 486 to Failover Trunk	Reroutes failed outbound calls that receive a 486 response through the failover trunk to retry the call. If disabled, calls that receive a 486 response will be terminated. The default setting is "unchecked".

Misc

On this Web page users can define the DNS mode used by the GXW450X and Outbound SIP Registrations.



SIP Settings

General **Misc** Session Timer TCP/TLS NAT ToS

Outbound SIP Registrations

* Register Timeout:

* Register Attempts:

DNS

DNS mode:

Figure 51: SIP Settings/Misc

Table 34: SIP Settings - Misc

Outbound SIP Registrations	
Register Timeout	Configures the register retry timeout (in seconds). The default setting is 20.
Register Attempts	Configure the number of registration attempts before giving up. 0 means continuously trying until the registration request is accepted. The default setting is "0".
DNS	
DNS mode	Selects DNS mode. Available options: <ul style="list-style-type: none"> • A&AAAA • A • AAAA The default setting is "A&AAAA" Note: This setting only affects the DNS queries that occurs when making calls.

Session Timer

Table 35: SIP Settings/Session Timer

Force Timer	If checked, always request and run session timer. Default is "unchecked".
Timer	If checked, run session timer only when requested by another UA. Default is "checked".
Session Expire	Configure the maximum session refresh interval (in seconds). The default setting is 1800.
Min SE	Configure the minimum session refresh interval (in seconds). The default setting is 90.

TCP and TLS

Table 36: SIP Settings/TCP and TLS

TCP Enable	Configure to allow incoming TCP connections with the GXW450X. The default setting is "No".
TCP Bind IPv4 Address	Configure the IP address for TCP server to bind to. 0.0.0.0 means binding to all interfaces. The port number is optional. If not specified, 5060 will be used. The default setting is "0.0.0.0:5060"
TCP Bind IPv6 Address	Configure the IPv6 address for TCP server to bind to. "[::]" means bind to all interfaces. The port number is optional with the default being 5060. For example, [2001:0DB8:0000:0000:0000:1428:0000]:5060. The default setting is "[::]:5060".
TLS Enable	Configure to allow incoming TLS connections with the GXW450X. The default setting is "No".
TLS Bind IPv4 Address	Configure the IP address for TLS server to bind to. 0.0.0.0 means binding to all interfaces. The port number is optional. If not specified, 5061 will be used. The default setting is "0.0.0.0:5061". Note: The IP address must match the common name (hostname) in the certificate. Please do not bind a TLS socket to multiple IP addresses. For details on how to construct a certificate for SIP, please refer to the following document: http://tools.ietf.org/html/draft-ietf-sip-domain-certs



TLS Bind IPv6 Address	Configure the IPv6 address for TLS server to bind to. "[::]" means bind to all interfaces. The port number is optional with default being 5061. For example, [2001:0DB8:0000:0000:0000:1428:0000]:5061. Note: The IP address must match the common name (host name) in the certificate so that the TLS socket won't bind to multiple IP addresses. The default setting is "[::]:5061".
TLS Do Not Verify	If enabled, the TLS server's certificate won't be verified when acting as a client. The default setting is "Yes".
TLS Self-Signed CA	This is the CA certificate if the TLS server being connected to requires self-signed certificate, including server's public key. This file will be renamed as "TLS.ca" automatically. Note: The size of the uploaded ca file must be under 2MB.
TLS Cert	This is the Certificate file (*.pem format only) used for TLS connections. It contains private key for client and signed certificate for the server. This file will be renamed as "TLS.pem" automatically. Note: The size of the uploaded certificate file must be under 2MB.
TLS Key	The size of a private key must be under 2MB. This is the private key (*.key format only) for TLS connections. This file will be renamed as "TLS.key" automatically.
TLS CA Cert	This file must be named with the CA subject name hash value. It contains CA's (Certificate Authority) public key, which is used to verify the accessed servers. Note: The size of the uploaded CA certificate file must be under 2MB.
TLS CA List	Display a list of files under the CA Cert directory.



Note:

The configuration in this section requires system reboot to take effect.



NAT

Table 37: NAT Settings

External Host	Configure a static IP address and port (optional) used in outbound SIP messages if the GXW450X is behind NAT. If it is a host name, it will only be looked up once.
Use IP address in SDP	If enabled, the SDP connection will use the IP address resolved from the external host. The default setting is "enabled".
External UDP Port	Configure the externally mapped UDP port when the GXW450X is behind a static NAT or PAT. The default setting is "5060".
External TCP Port	Configure the externally mapped TCP port when the GXW450X is behind a static NAT or PAT. The default setting is "5060".
External TLS Port	Configures the externally mapped TLS port when GXW450X is behind a static NAT or PAT. The default setting is "5061".
Local Network Address	<p>Adds a list of network addresses that are considered inside of the NAT network. Multiple entries are allowed. If not configured, the external IP address will not be set correctly.</p> <p>A sample configuration could be as follows:</p> <pre>192.168.0.0/16</pre>

ToS

Table 38: ToS Settings

ToS For SIP	Configure the Type of Service for SIP packets. The default setting is None.
ToS For RTP Audio	Configure the Type of Service for RTP audio packets. The default setting is None.
Send Compact SIP Headers	<p>If enabled, compact SIP headers will be sent. The default setting is "No".</p> <p>Note: This change requires a system reboot to take effect.</p>
Enable Relaxed DTMF	Select to enable relaxed DTMF handling. The default setting is "No".
DTMF Mode	<p>Configures the default mode for sending DTMF.</p> <ul style="list-style-type: none"> • RFC2833: DTMF is transmitted as audio in the RTP stream but is encoded separately from the audio stream.



	<ul style="list-style-type: none"> • Inband: DTMF is transmitted as audio and is included in the audio stream. Requires alaw/ulaw codecs. • SIP INFO: DTMF is transmitted through a separate network connection from the media streams. • Auto: DTMF mode will be negotiated with the remote peer. RFC2833 will be used by default unless the remote peer does not support it. <p>The default setting is "RFC2833".</p>
RTP Timeout	Configure the timeout in seconds. When the call is in talking status, if there is no RTP activity after the timeout, the call will be terminated. The default setting is 90 seconds.
RTP Hold Timeout	Configure the timeout in seconds. When the call is on hold, if there is no RTP activity after the timeout, the call will be terminated. This value must be larger than "RTP Timeout". The default setting is 100 seconds.
RTP Keep-alive	Configure the interval (in seconds) that a RTP Keepalive packet will be sent on an SDP connection. The default setting is 0 (no RTP Keepalive).
Default Incoming/Outgoing Registration Time	Configure the default duration (in seconds) of incoming/outgoing registration. The default setting is 120.
100rel	<p>Configure the 100rel setting on GXW450X.</p> <ul style="list-style-type: none"> • No: Unsupported. • Yes: Supported. • Required: Forced to support. <p>The default setting is "Yes".</p>
Trust Remote Party ID	Configure whether the Remote-Party-ID should be trusted. The default setting is "No".
Send Remote Party ID	Configure whether the Remote-Party-ID should be sent or not. The default setting is "No".
Generate In-Band Ringing	<p>Configure whether the GXW450X should generate inband ringing or not.</p> <ul style="list-style-type: none"> • Yes: The GXW450X will send 180 Ringing followed by 183 Session Progress and in-band audio.



	<ul style="list-style-type: none"> • No: The GXW450X will send 180 Ringing if 183 Session Progress has not been sent yet. If audio path is established already with 183 then send in-band ringing. • Never: Whenever ringing occurs, the GXW450X will send 180 Ringing as long as 200OK has not been set yet. <p>The default setting is "Never".</p>
Server User Agent	Configure the user agent string for the GXW450X.
Default Incoming/Outgoing Registration Time	Configure the default duration (in seconds) of incoming and outgoing registration. The default setting is 120 seconds.

RTP Settings

RTP Settings

Table 39: RTP Settings

RTP Start	Configure the RTP port starting number. The default setting is 10000.
RTP End	Configure the RTP port ending address. The default setting is 20000.
Strict RTP	Configure to enable or disable strict RTP protection. If enabled, RTP packets that do not come from the source of the RTP stream will be dropped. The default setting is "Disable".
RTP Checksums	Configure to enable or disable RTP Checksums on RTP traffic. The default setting is "Disable".

Payload Type Settings

The GXW450X payload type for audio codecs can be configured here.

Table 40: Payload Type Configuration

AAL2-G.726	Configure payload type for ADPCM (G.726, 32kbps, AAL2 codeword packing). The valid range is between 96 and 127. The default setting is 112.
DTMF	Configure payload type for DTMF. The valid range is between 96 and 127. The default setting is 101.
G.721 Compatible	Configure to enable/disable G.721 compatible. The default setting is Yes.



G.726	Configure the payload type for G.726 if "G.721 Compatible" is disabled. The default setting is 111.
iLBC	Configure the payload type for iLBC. The valid range is between 96 and 127. The default setting is 97.
OPUS	Configure the payload type for OPUS. The valid range is between 96 and 127. The default setting is 123.

- Click on **Default All** to set the values of the payload parameters to the factory default values
- While configuring the payload values users can Click on **Reset All** to reset the values to the last saved values on the gateway.

Voice Prompt

The GXW450X supports multiple languages in Web GUI as well as system voice prompt. The following languages are currently supported in system voice prompt:

English (United States), British English, Arabic, Chinese, Dutch, French, German, Greek, Hebrew, Italian, Polish, Portuguese, Russian, Spanish, Catalan, Swedish, Czech and Turkish.

English (United States) and Chinese voice prompts are built in with the GXW450X already. The other languages provided by Grandstream can be downloaded and installed from the GXW450X Web GUI directly. Additionally, users could customize their own voice prompts, package them and upload to the GXW450X.

Language settings for voice prompt can be accessed under Web GUI → **PBX Settings** → **Voice Prompt** → **Language**.

Download and Install Voice Prompt Package

To download and install voice prompt package in different languages from GXW450X Web GUI, click on **Check Prompt List** button.



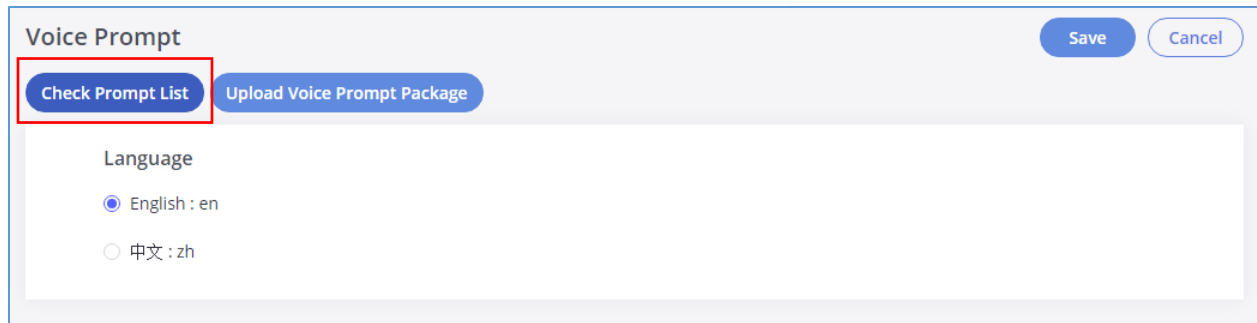


Figure 52: Language Settings for Voice Prompt

A new dialog window of voice prompt package list will be displayed. Users can see the version number (latest version available V.S. current installed version), package size and options to upgrade or download the language

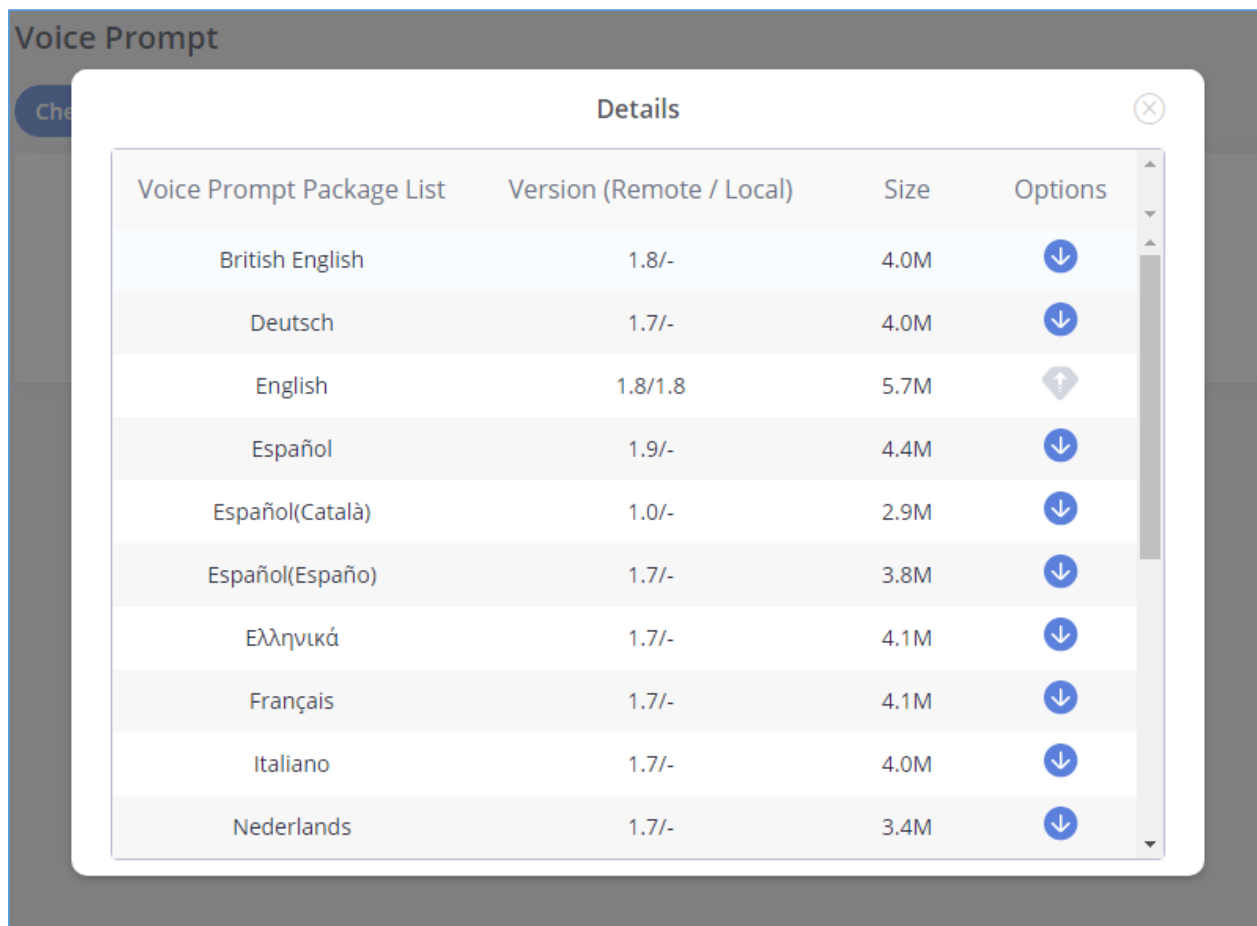



Figure 53: Voice Prompt Package List

Click on  to download the language to the GXW450X. The installation will be automatically started once the downloading is finished.



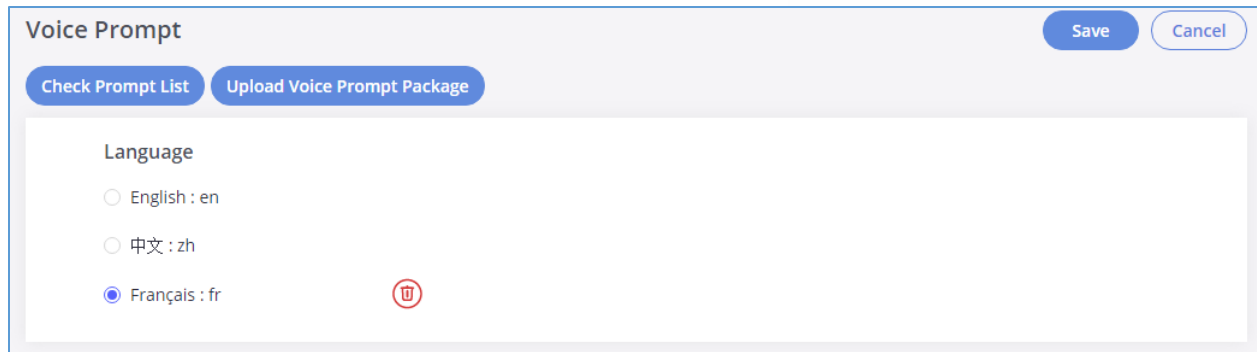
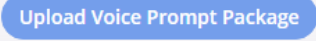


Figure 54: New Voice Prompt Language Added

A new language option will be displayed after successfully installed. Users then could select it to apply in the GXW450X system voice prompt or delete it from the GXW450X

Manual Upload of Prompt Package

Users can upload the prompt package manually to the GXW450X. Users can create their own prompt package for different languages and use them as the default voice prompts.

To upload the voice prompt to the GXW450X, press the  button and brows the prompt package.

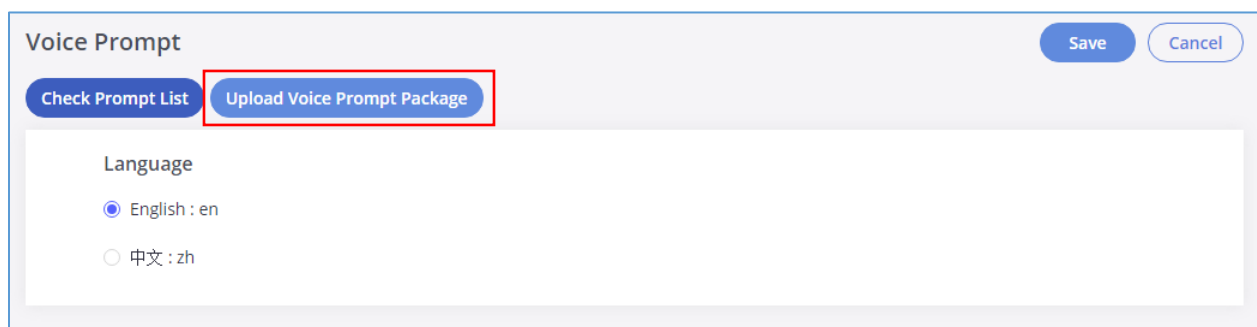


Figure 55: Upload Voice prompt Package

Note: The prompt package should be in tar.bz2, tar.gz, tar.Z, tgz, tar, bz2, zip or gz format.

Jitter Buffer

A jitter buffer is used at the receiving equipment to store incoming RTP packets, re-align them in terms of timing and check they are in the correct order. If some arrive slightly out-of-sequence then, provided it is large enough, the jitter buffer can put them back into the right sequence. However, for this to work the receiving device must delay the audio very slightly while it checks and reassembles the packet stream.



Below are the Jitter buffer Settings to control the size of the buffer and its implementation mode:

Table 41: Jitter Buffer Settings

Enable Jitter Buffer	Select to enable jitter buffer on the sending side of the SIP channel. The default setting is "No".
Jitter Buffer Size	Configure the time (in ms) to buffer. This is the jitter buffer size used in "Fixed" jitter buffer or used as the initial time for "adaptive" jitter buffer. The default setting is 100.
Implementation	<p>Configure the jitter buffer implementation on the sending side of a SIP channel. The default setting is "Fixed".</p> <ul style="list-style-type: none"> • Fixed The size is always equal to the value of "Max Jitter Buffer". • Adaptive The size is adjusted automatically and the maximum value equals to the value of "Max Jitter Buffer".
Max Jitter Buffer	Configure the maximum time (in ms) to buffer for "Adaptive" jitter buffer implementation or used as the jitter buffer size for "Fixed" jitter buffer implementation. The default setting is 100.

Interface Settings

The GXW450X supports E1/T1/J1 which are physical connection technologies used in digital network. T1 is the North American standard, J1 is used in Japan, whereas E1 is the European standard. GXW450X supports four signaling protocols: PRI_NET, PRI_CPE, MFC/R2 and SS7. PRI provides a varying number of channels depending on the standards in the country of implementation (E1, T1 or J1); MFC/R2 is a signaling protocol heavily used over E1 trunks; SS7 uses out-of-band signaling, which travels on a separate, dedicated channel rather than within the same channel as the telephone call, providing more efficiency and higher security level when the telephone calls are set up.

The interface settings page allows to configure digital hardware parameters. For more details, refer to **[Digital Hardware Configuration]** section.



MAINTENANCE

The Maintenance section lists different tools to help troubleshooting the issues that might be encountered while using the GXW450X alongside a set of options to manage users, control web GUI access, upgrade the firmware, backup the configuration, take ethernet and Digital traces ...etc.

User Management

User management is on Web GUI → **Maintenance** → **User Management** page. User could create multiple accounts for different administrators to log in the GXW450X Web GUI.

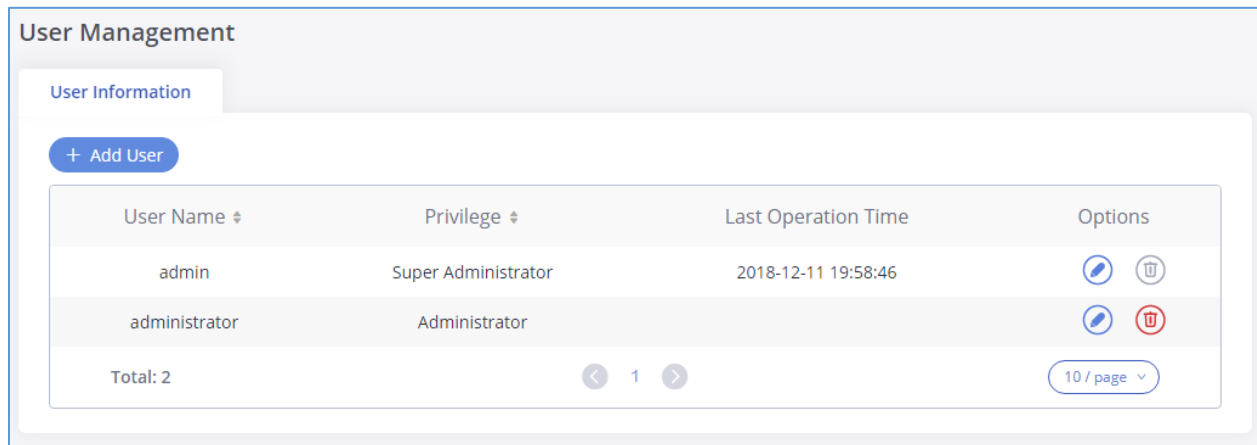
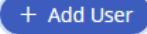


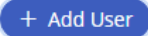


Figure 56: User Management Page Display

- Click on  To add a user
- Click on  to edit the user
- Click on  to delete the user

When logged in as Super Admin, click on  to create a new account for Web GUI user. The following dialog will prompt. Configure the parameters as shown in below table.



Create New User Information

* User Name: <input type="text"/>	Privilege: <input type="text" value="Administrator"/>
* User Password: <input type="text"/>	Department: <input type="text"/>
Fax: <input type="text"/>	Email Address: <input type="text"/>
First Name: <input type="text"/>	Last Name: <input type="text"/>
Home Number: <input type="text"/>	Mobile Phone Number: <input type="text"/>

Figure 57: Create New User

Table 42: Create New User Information

User Name	Configures a username to identify the user which will be required in Web GUI login. Letters, digits and underscore are allowed in the user name.
Privilege	This is the role of the Web GUI user. Currently only “Admin” is supported when Super Admin creates a new user.
User Password	Configures a password for this user which will be required in Web GUI login. Letters, digits and underscore are allowed.
Department	Enters the necessary information to keep a record for this user.
Fax	
Email Address	
First Name	
Last Name	
Home Number	
Mobile Phone Number	

Change Information

Change Password

Follow the steps below to change the Web GUI access password.

1. Go to Web GUI→**Maintenance**→**Change Information** page.
2. Enter the old password first.



3. Enter the new password and retype the new password to confirm. The new password has to be at least 4 characters. The maximum length of the password is 16 characters.
4. Configure the Email Address that is used when login credentials are lost.
5. Click on “Save” and the user will be automatically logged out.
6. Once the web page comes back to the login page again, enter the username “admin” and the new password to login.

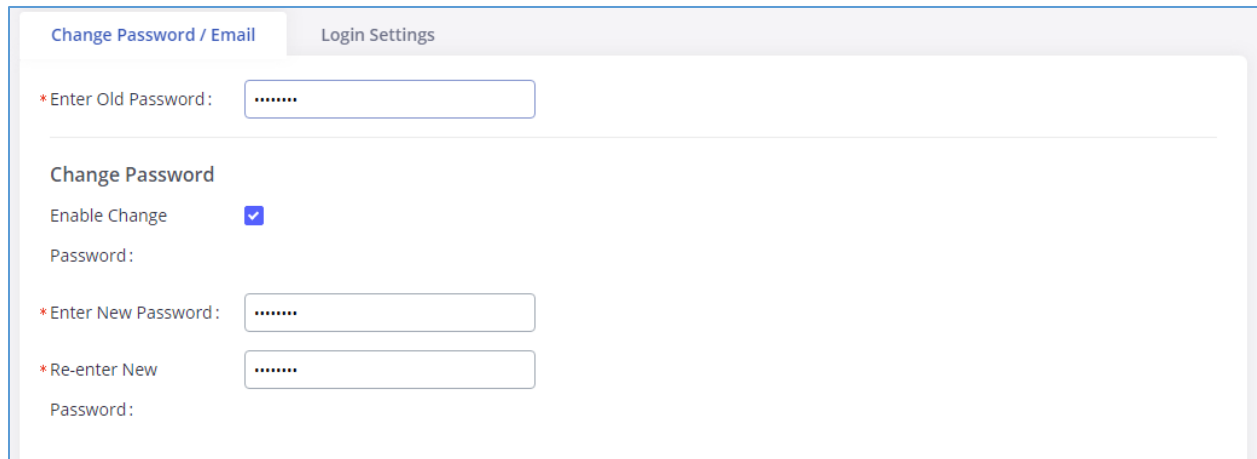


Figure 58: Change Password

Table 43: Change Password Parameters

Enter Old Password	Enter the old Password for GXW450X
Enable Change Password	When enabled, the fields to enter the new password will be displayed
Enter New Password	Enter the New Password for GXW450X
Re-enter New Password	Retype the New Password for GXW450X

Change Binding Email

GXW450X allows user to configure binding email in case login password is lost. GXW450X login credential will be sent to the designated email address. The feature can be found under Web GUI→Maintenance→Change Information→Change Binding Email.



Change Binding Email

Email Address: [Email Template](#)

Figure 59: Change Binding Email

Login Settings

After the user logs in the GXW450X Web GUI, the user will be automatically logged out after certain timeout, or he/she can be banned for a specific period if the login timeout is exceeded. Those values can be specified under GXW450X web GUI→**Maintenance**→**Change Information**→**Login Settings** page.

The “**User Login Timeout**” value is in minute and the default setting is 10 minutes. If the user doesn’t make any operation on Web GUI within the timeout, the user will be logged out automatically. After that, the Web GUI will be redirected to the login page and the user will need to enter username and password to log in. If set to 0, there is no timeout for the Web GUI login session and the user will not be automatically logged out.

“**Maximum number of login attempts**” can prevent the GXW450X from brute force decryption, if this number is exceeded user IP address will be banned from accessing the GXW for a period based on user configuration, the default value is 5.

“**User ban period**” specify the period in minutes an IP will be banned from accessing the GXW if the User max number of try login is exceeded, the default value is 5.

“**Login Banned User List**” show the list of IPs’ banned from the GXW.

“**Login White List**” User can add a list of IPs’ to avoid the above restriction, thus, they can exceed the User max number of try login.

Change Information

Change Password / Email
Login Settings

* User Login Timeout:

* Maximum number of login attempts:

* User ban period:

Login Banned User List

IP Address ↕	User Name ↕	Banned Time ↕	Options
No Data			

Login Whitelist

The IP addresses in the Login Whitelist will not be restricted. This option doesn't support network segment format.

IP Address ↕	Options
No Data	

Figure 60: Login Timeout Settings

Operation Log

The admin has the authority to view operation logs on GXW450X Web GUI → **Maintenance** → **Operation Log** page. Operation logs list the operations done by all the Web GUI users, for example, Web GUI login, creating trunk, creating outbound rule etc. There are 7 columns to record the operation details “Date”, “User Name”, “IP Address”, “Results”, “Page Operation”, “Specific Operation” and “Remark”.


Operation Log						
Delete Search Result (s)		Delete All Logs		Filter ▾		
Date ↕	User Name ↕	IP Address ↕	Results ↕	Page Operation ↕	Specific Operation ↕	Remark ↕
2018-12-12 02:17:02	admin	172.16.1.62	Operation successful	downloadFile	type: syslog. ⓘ	Click to modify notes.
2018-12-12 02:16:55	admin	172.16.1.62	Operation successful	Login: Login	User Name: admin. ⓘ	Click to modify notes.
2018-12-12 02:16:48	admin	172.16.1.62	Wrong account or password!	Login: Login	User Name: admin. ⓘ	Click to modify notes.
2018-12-12 02:16:46	admin	172.16.1.62	Wrong account or password!	Login: Login	User Name: admin. ⓘ	Click to modify notes.
2018-12-12 02:16:41	admin	172.16.1.62	Wrong account or password!	Login: Login	User Name: admin. ⓘ	Click to modify notes.
2018-12-11 23:06:34	admin	41.250.164.94	Operation successful	Login: Login	User Name: admin. ⓘ	Click to modify notes.
2018-12-11 22:51:17	admin	41.250.164.94	Operation successful	Login: Login	User Name: admin. ⓘ	Click to modify notes.
2018-12-11 22:50:59	admin	41.250.164.94	Operation successful	Logout: Logout	User Name: undefined. ⓘ	Click to modify notes.
2018-12-11 22:41:13	admin	41.250.164.94	Operation successful	Login: Login	User Name: admin. ⓘ	Click to modify notes.
2018-12-11 22:40:57	admin	41.250.164.94	Operation successful	Extensions: Update User Information	User Name: admin. ⓘ	Click to modify notes.
Total: 181		 1 2 3 4 5 ... 19			10 / page ▾	


Figure 61: Operation Logs



The operation log can be sorted and filtered for easy access. Click on the header of each column to sort. For example, clicking on “Date” will sort the logs according to operation date and time. Clicking on “Date” again will reverse the order.

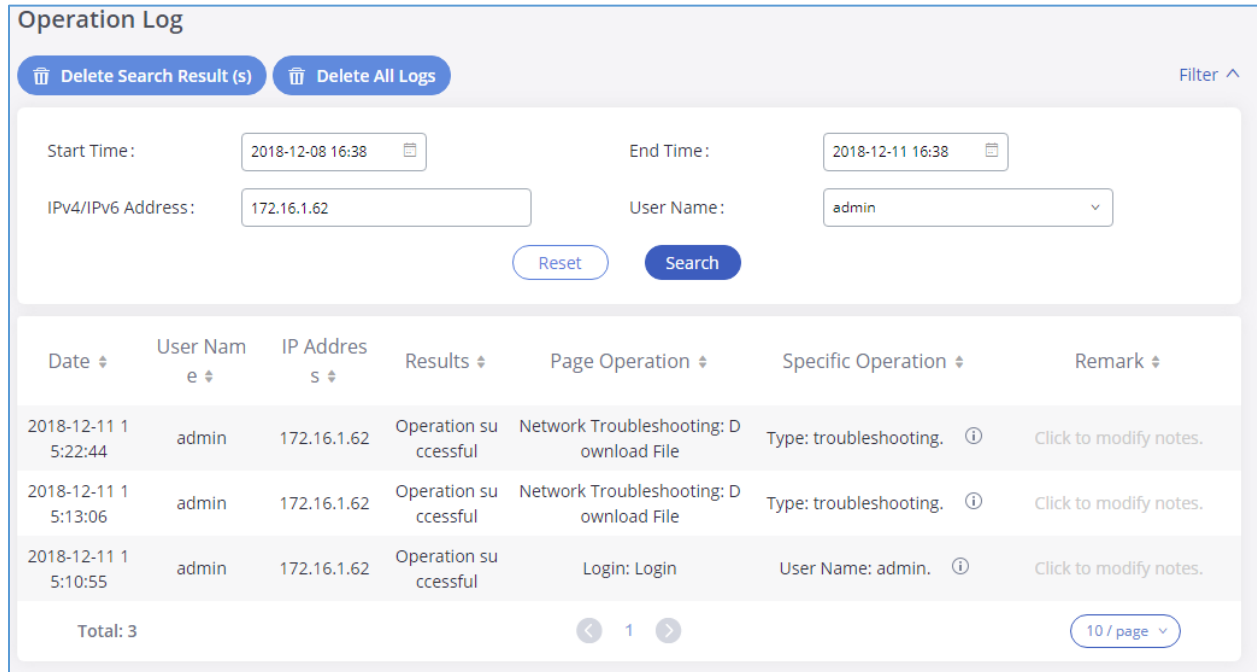
Table 44: Operation Log Column Header

Date	The date and time when the operation is executed.
User Name	The username of the user who performed the operation.
IP Address	The IP address from which the operation is made.
Results	The result of the operation.
Page Operation	The page where the operation is made. For example, login, logout, delete user, create trunk and etc.

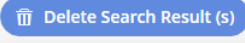
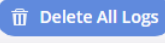


Specific Operation	Click on  to view the options and values configured by this operation.
Remark	Allows users to add notes and remarks to each operation

Users could also filter the operation logs by time condition, IP address and/or username. To use the filter, click on  and configure the conditions then click on .






Operation Log



Filter ^

Start Time:
 End Time:

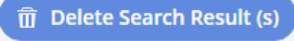

IPv4/IPv6 Address:
 User Name:

Date	User Name	IP Address	Results	Page Operation	Specific Operation	Remark
2018-12-11 15:22:44	admin	172.16.1.62	Operation successful	Network Troubleshooting: Download File	Type: troubleshooting. 	Click to modify notes.
2018-12-11 15:13:06	admin	172.16.1.62	Operation successful	Network Troubleshooting: Download File	Type: troubleshooting. 	Click to modify notes.
2018-12-11 15:10:55	admin	172.16.1.62	Operation successful	Login: Login	User Name: admin. 	Click to modify notes.

Total: 3 10 / page

Figure 62: Operation Logs Filter

The above figure shows an example that operations made by user “admin” on device with IP 172.16.1.62 from 2018-12-08 16:38 to 2018-12-11 16:38 are filtered out and displayed.

To delete operation logs, users can perform filtering first and then click on  to delete the filtered result of operation logs. Or users can click on  to delete all operation logs at once.

Syslog

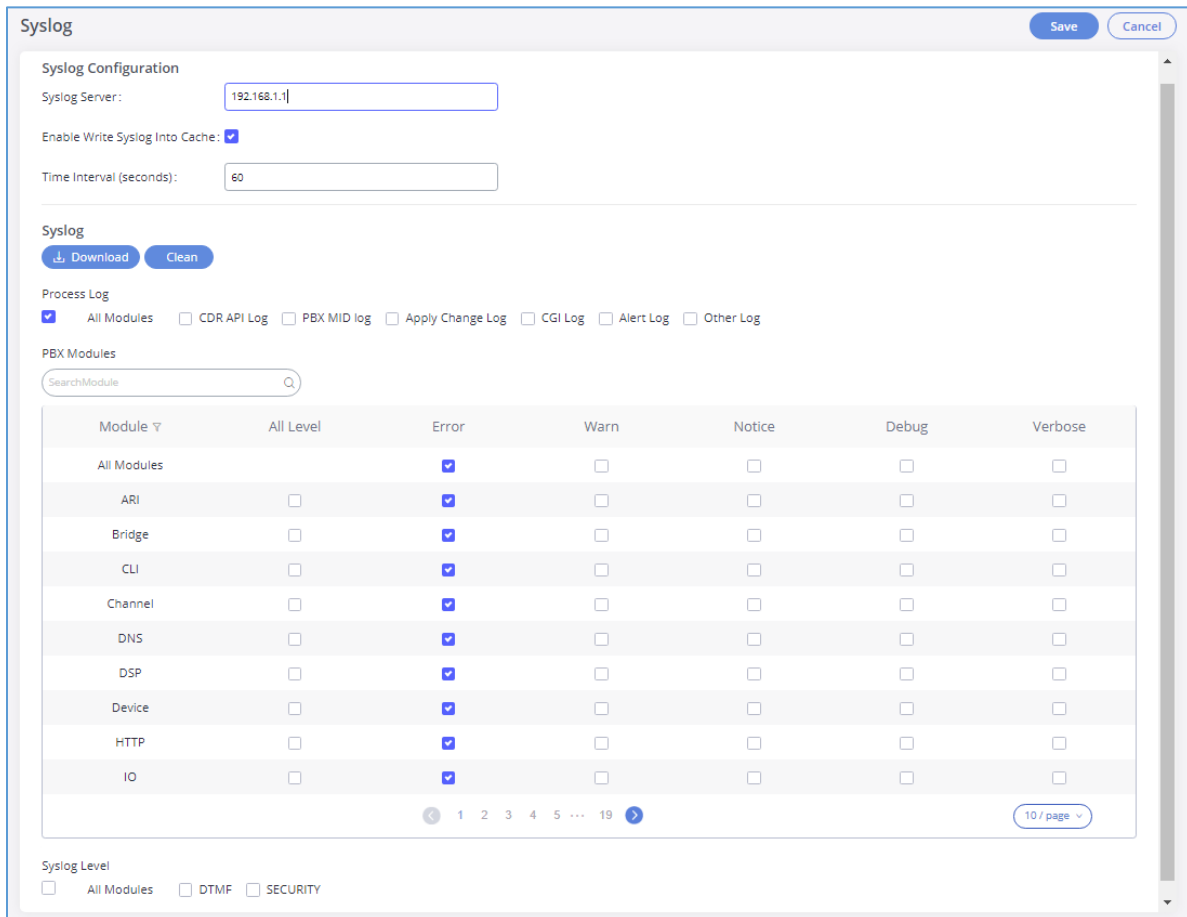
On the GXW450X, users could dump the syslog information to a remote server under Web GUI → **Maintenance** → **Syslog**. Enter the syslog server hostname or IP address and select the module/level for the syslog information.



The default syslog level for all modules is "error", which is recommended in your GXW450X settings because it can be helpful to locate the issues when errors happen.

Some typical modules for GXW450X functions are as follows and users can turn on "notice" and "verb" levels besides "error" level.

- **pbx:** This module is related to general PBX functions.
- **pjsip:** This module is related to SIP calls.
- **chan_dahdi:** This module is related to digital calls (E1/T1/J1).



The screenshot shows the Syslog Configuration window with the following settings:

- Syslog Server: 192.168.1.1
- Enable Write Syslog Into Cache:
- Time Interval (seconds): 60
- Buttons: Download, Clean
- Process Log: All Modules, CDR API Log, PBX MID log, Apply Change Log, CGI Log, Alert Log, Other Log
- PBX Modules: SearchModule

Module ▾	All Level	Error	Warn	Notice	Debug	Verbose
All Modules	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ARI	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bridge	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CLI	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Channel	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DNS	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DSP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Device	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HTTP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IO	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Page: 10 / page

Syslog Level: All Modules, DTMF, SECURITY

Figure 63: Syslog Settings

Note:

Syslog is usually for debugging and troubleshooting purpose. Turning on all levels for all syslog modules is not recommended for daily usage. Too many syslog prints might cause traffic and affect system performance.

The reserved size for Syslog entries on the cache memory of the GXW is 50M, once this sized is reached the GXW will clean up 2M of the oldest Syslog entries to allow to save new logs.

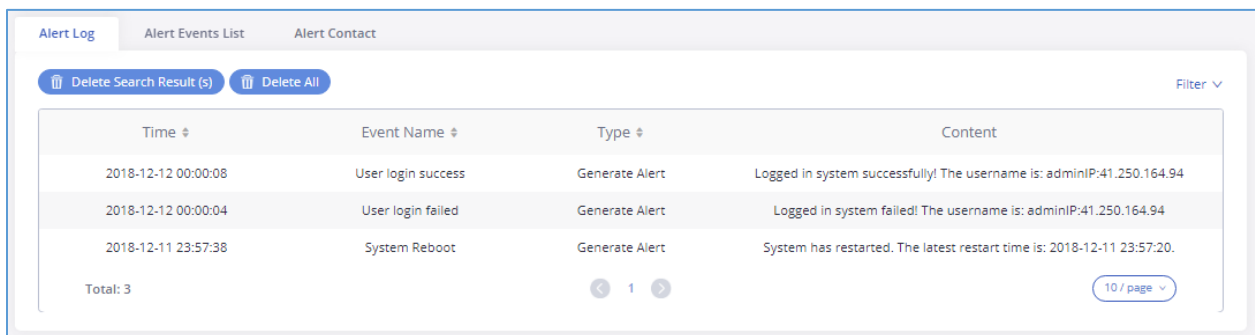


System Events

The GXW450X can monitor important system events, log the alerts and send Email notifications to the system administrator.

Alert Log

Under Web GUI→**Maintenance**→**System Events**→**Alert Log**, system messages are listed when the alert is triggered for the configured system events. The following picture shows “**User Login Successes**”, “**User Login Failed**” and “**System Reboot**” alert log.

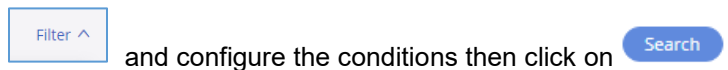
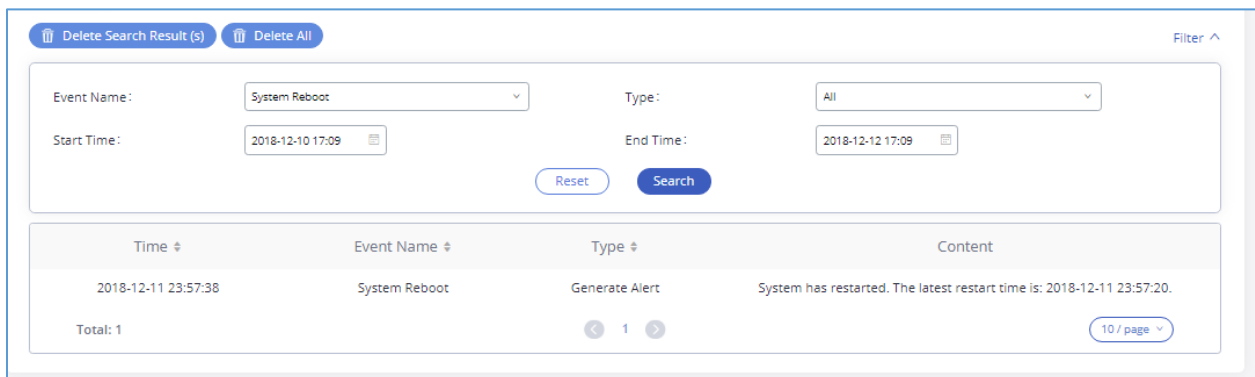


Time	Event Name	Type	Content
2018-12-12 00:00:08	User login success	Generate Alert	Logged in system successfully! The username is: adminIP:41.250.164.94
2018-12-12 00:00:04	User login failed	Generate Alert	Logged in system failed! The username is: adminIP:41.250.164.94
2018-12-11 23:57:38	System Reboot	Generate Alert	System has restarted. The latest restart time is: 2018-12-11 23:57:20.

Total: 3

Figure 64: System Events→Alert Log

Users could also filter the Alert Logs by time condition, Event Name and/or Type. To use the filter, click on

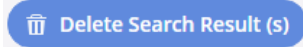
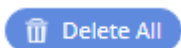



Time	Event Name	Type	Content
2018-12-11 23:57:38	System Reboot	Generate Alert	System has restarted. The latest restart time is: 2018-12-11 23:57:20.

Total: 1

Figure 65: Alert Log Filter

The above figure shows an example of a System reboot Alerts logged on 2018-12-11 23:57 displayed using the filter Event name System Reboot.

To delete alert logs, users can perform filtering first and then click on  to delete the filtered result of operation logs. Or users can click on  to delete all alert logs at once.




Alert Events List

The system alert events list can be found under Web GUI→**Maintenance**→**System Events**→**Alert Events**.

The following event are currently supported on the GXW450X which will have an alert, and/or an Email generated if occurred:

- **Disk Usage**
- **Modify Super Admin Password**
- **Memory Usage**
- **System Reboot**
- **System Update**
- **System Crash**
- **Register SIP trunk failed**
- **Restore Config**
- **User Login Success**
- **User Login Failed**
- **SIP Outgoing Call through Trunk Failure**
- **Fail2ban Blocking**
- **SIP Peer Trunk Status**
- **User Login Banned**
- **External Disk Usage**
- **The CDR database is corrupted**

Click on  to configure the parameters for each event

1. Disk Usage

Alert Settings: Disk Usage

*Detect Cycle :	<input style="width: 90%;" type="text" value="10"/>	<input style="width: 90%;" type="text" value="minute(s)"/>
*Alert Threshold :	<input style="width: 90%;" type="text" value="80"/>	%

Figure 66: System Events→Alert Events Lists: Disk Usage

- **Detect Cycle:** The GXW450X will perform the internal disk usage detection based on this cycle. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.
- **Alert Threshold:** If the detected value exceeds the threshold (in percentage), the GXW450X system will send the alert.

2. External Disk Usage

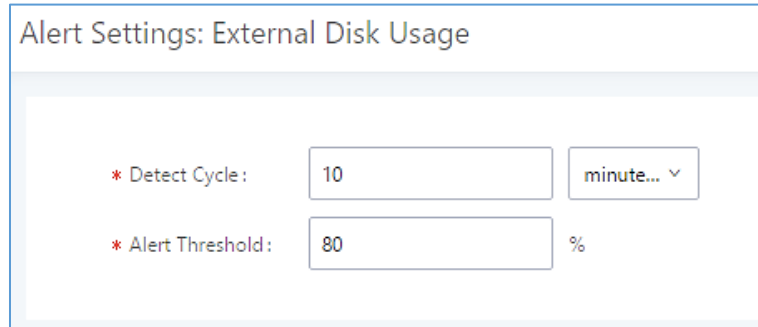


Figure 67: System Events→Alert Events Lists: External Disk Usage

- **Detect Cycle:** The GXW450X will perform the External disk usage detection based on this cycle. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.
- **Alert Threshold:** If the detected value exceeds the threshold (in percentage), the GXW450X system will send the alert.

3. Memory Usage

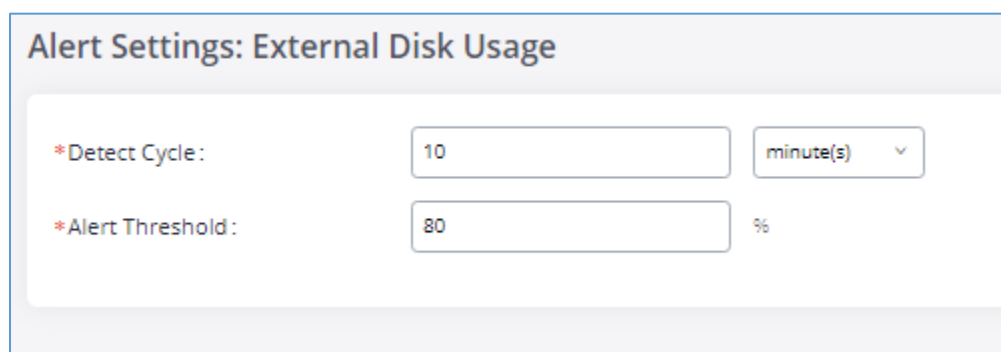


Figure 68: System Events→Alert Events Lists: Memory Usage

- **Detect Cycle:** The GXW450X will perform the memory usage detection based on this cycle. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.



- **Alert Threshold:** If the detected value exceeds the threshold (in percentage), the GXW450X system will send the alert.

4. System Crash

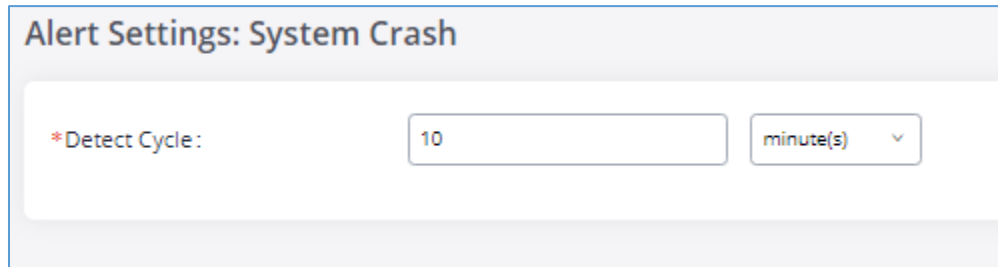



Figure 69: System Events→Alert Events Lists: System Crash

- **Detect Cycle:** The GXW450X will detect the event at each cycle based on the specified time. Users can enter the number and then select second(s)/minute(s)/hour(s)/day(s) to configure the cycle.

Click on the switch  to turn on/off the alert and Email notification for the event. Users could also select the checkbox for each event and then click on button "Alert On", "Alert Off", "Email Notification On", "Email Notification Off" to control the alert and Email notification configuration.

Alert Contact

Users could add administrator's Email address under Web GUI→**Maintenance**→**System Events**→**Alert Contact** to send the alert notification to. Up to 10 Email addresses can be added.



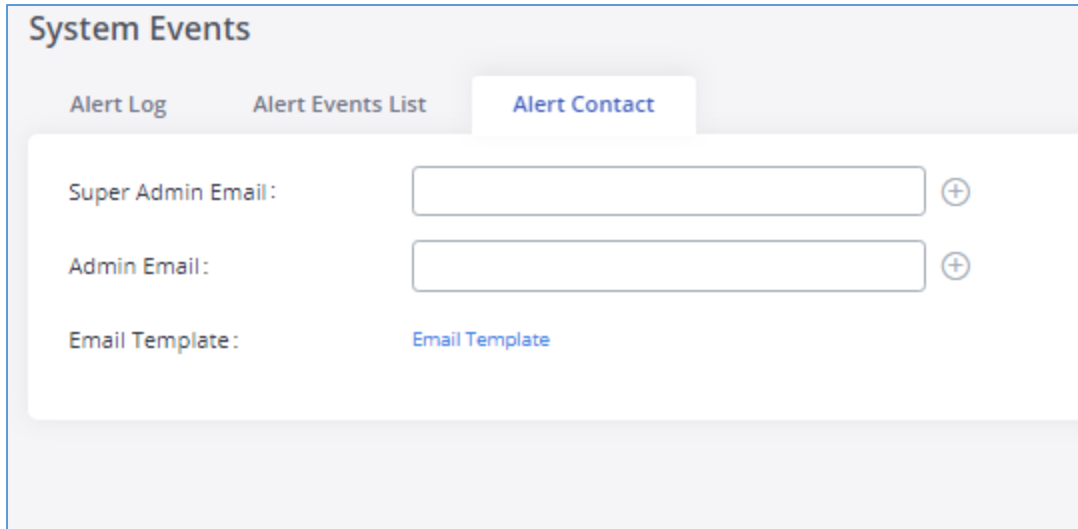


Figure 70: Alert Contact

Upgrade

The GXW450X can be upgraded to a new firmware version remotely or locally. This section describes how to upgrade your GXW450X via network or local upload.

Upgrading via Network

The GXW450X can be upgraded via TFTP/HTTP/HTTPS by configuring the URL/IP Address for the TFTP/HTTP/HTTPS server and selecting a download method. Configure a valid URL for TFTP, HTTP or HTTPS; the server name can be FQDN or IP address.

The upgrading configuration can be accessed via Web GUI→**Maintenance**→**Upgrade**.



Upgrade Via :	<input type="text" value="HTTP"/>
Firmware Server Path :	<input type="text" value="fw.ipvideotalk.com/gs"/>
Firmware File Prefix :	<input type="text"/>
Firmware File Suffix :	<input type="text"/>
HTTP/HTTPS Username :	<input type="text"/>
HTTP/HTTPS Password :	<input type="text"/>

Figure 71: Network Upgrade

Table 45: Network Upgrade Configuration

Upgrade Via	Allow users to choose the firmware upgrade method: TFTP, HTTP or HTTPS.
Firmware Server Path	Configures firmware server path. For example, firmware.grandstream.com
Firmware File Prefix	If configured, only the firmware with the matching encrypted prefix will be downloaded.
Firmware File Suffix	If configured, only the firmware with the matching encrypted postfix will be downloaded.
HTTP/HTTPS User Name	The user name for the HTTP/HTTPS server.
HTTP/HTTPS Password	The password for the HTTP/HTTPS server.


Please follow the steps below to upgrade the firmware remotely.

1. Enter the firmware server path under Web GUI→**Maintenance**→**Upgrade**.
2. Click on "Save". Then reboot the device to start the upgrading process.
3. Please be patient during the upgrading process. Once done, a reboot message will be displayed in the LCD.
4. Manually reboot the GXW450X when it's appropriate to avoid immediate service interruption. After it boots up, log in the Web GUI to check the firmware version.



Upgrading via Local Upload

If there is no HTTP/TFTP server, users could also upload the firmware to the GXW450X directly via Web GUI. Please follow the steps below to upload firmware locally.

1. Download the latest GXW450X firmware file from the following link and save it in your PC:
<http://www.grandstream.com/support/firmware>
2. Log in the Web GUI as administrator in the PC.
3. Go to Web GUI→**Maintenance**→**Upgrade**, upload the firmware file by clicking on  and select the firmware file from your PC. The default firmware file name is *gxw4500fw.bin*

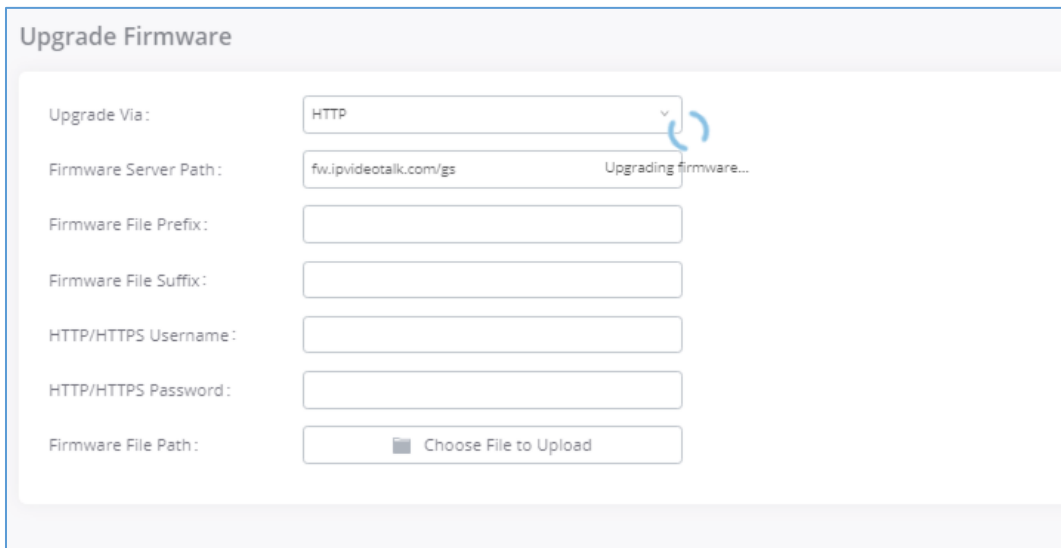


Figure 72: Upgrading Firmware Files

4. Wait until the upgrading process is successful and a window will be popped up in the Web GUI requesting to confirm the reboot of the GXW450X for the changes to take effect.
5. Click on "OK" to reboot the GXW450X and check the firmware version after it boots up.

Notes:

- Please do not interrupt or power cycle the GXW450X during upgrading process.
- The firmware file name allows the use of the special characters besides the following restricted characters: # \$ ^ & * + () [] / ; ' | , < > ?



Upgrading via a Local Server

Users can download a free TFTP, FTP or HTTP server and conduct a local firmware upgrade. A free window version TFTP server is available for download from:

http://www.solarwinds.com/products/freetools/free_tftp_server.aspx

<http://tftpd32.jounin.net>

Please check our website at <http://www.grandstream.com/support/firmware> for latest firmware.

Instructions for local firmware upgrade via TFTP:

1. Unzip the firmware files and put all of them in the root directory of the TFTP server;
2. Connect the PC running the TFTP server and the GXW450X to the same LAN segment;
3. Launch the TFTP server and go to the File menu→Configure→Security to change the TFTP server's default setting from "Receive Only" to "Transmit Only" for the firmware upgrade;
4. Start the TFTP server and configure the TFTP server in the GXW450X web configuration interface;
5. Configure the Firmware Server Path to the IP address of the PC;
6. Update the changes and reboot the GXW450X.

End users can also choose to download a free HTTP server from <http://httpd.apache.org/> or use Microsoft IIS web server.

No Local Firmware Server

For users that would like to use remote upgrading without a local TFTP/FTP/HTTP server, Grandstream offers a NAT-friendly HTTP server. This enables users to download the latest software upgrades for the gateway via this server. Please refer to the following webpage for the firmware server path to use:

<http://www.grandstream.com/support/firmware>

Backup

The GXW450X configuration can be backed up locally or via network. The backup file will be used to restore the configuration on GXW450X when necessary.



Backup/Restore

Users could backup the GXW450X configurations for restore purpose under Web GUI→**Maintenance**→**Backup**→**Backup/Restore**. Click on **Add Backup** to create a new backup. Then the following dialog will show:

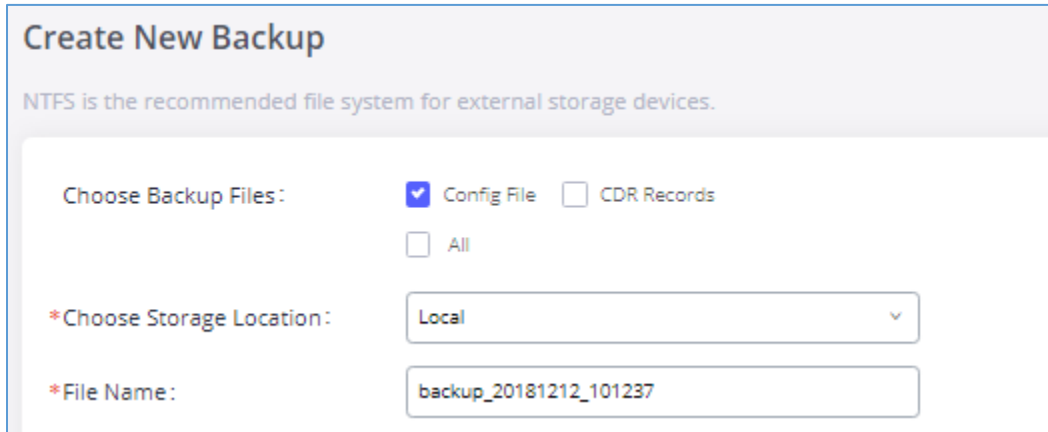





Figure 73: Create New Backup

1. Choose the files to be included in the backup.
2. Choose where to store the backup file: USB Disk, SD Card or Local.
3. Name the backup file.
4. Click on "Backup" to start backup.

Once the backup is done, the list of the backups will be displayed with date and time in the web page. Users can download , restore , or delete  it from the GXW450X internal storage or the external device.

Click on **Upload Backup File** to upload backup file from the local device to GXW450X. The uploaded backup file will also be displayed in the web page and can be used to restore the GXW450X.



Backup/Restore
Data Sync

Backup Configuration

Add Backup
Schedule Backup
Upload Backup File

List of Previous Configuration Backups

Delete Selected Backup File (s)

<input type="checkbox"/>	Name ↕	Date ↕	Size ↕	Options
<input type="checkbox"/>	backup_20181212_105534.tar	2018-12-12 18:01:20 UTC+08:00	4.83 MB	↓ ↺ 🗑
Total: 1		⏪ 1 ⏩		10 / page

Scheduled Backup Log

Clean

Figure 74: Backup / Restore

The Schedule Backup option allows GXW450X to perform automatically backup on the user specified time. Scheduled backup files can only be stored in USB / SD card / SFTP server. Users can set backup time from 0-23 and how frequent the backup will be performed.



Schedule Backup

NTFS is the recommended file system for external storage devices.

Enable Scheduled

Backup:

Choose Backup Files: Config File CDR Records
 All

Choose Storage: SFTP Server

Location:

*Account:

Password:

*Server Address:

Destination Directory:

*Backup Time:

*Backup Frequency:

+ Test Connection

Figure 75: Schedule Backup

Data Sync

Besides local backup, users could backup the voice records and/or CDR in a daily basis to a remote server via SFTP protocol automatically under Web GUI→**Maintenance**→**Backup**→**Data Sync**.

The client account supports special characters such as @ or “.”. This change allows user to use email address as SFTP accounts. It allows users as well to specify the destination directory on SFTP server for backup file. If the directory doesn't exist on the destination, GXW450X will create the directory automatically.



Backup

Backup/Restore
Data Sync

Use SFTP to automatically sync CDR, recordings, voicemail, CDR, and fax every day.

Data Sync Configuration

Enable Data Sync:

Choose Data Sync Files: CDR Records Recording Files

Account:

Password: 👁

Server Address:

Destination Directory:

Sync Time:

+ Test Connection
+ Synchronize All Data

Data Sync Log

Clean

Figure 76: Data Sync

Table 46: Data Sync Configuration



Enable Data Sync	Enable the auto backup function. This option is disabled by default
Choose Data Sync Files	Choose the files to sync
Account	Enter the Account name on the SFTP backup server.
Password	Enter the Password associate with the Account on the SFTP backup server.
Server Address	Enter the SFTP server address.
Destination Directory	Specify the directory in SFTP server to keep the backup file. Format: 'xxx/xxx/xxx', If this directory does not exist, GXW will create this directory automatically.
Sync Time	Enter 0-23 to specify the backup hour of the day.

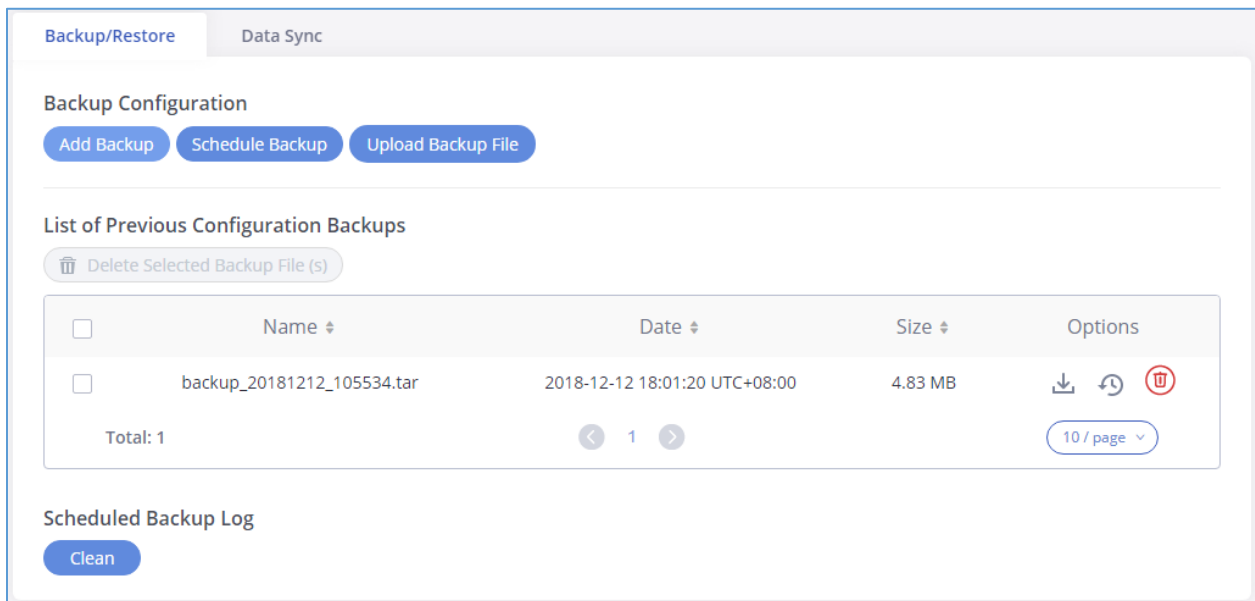
Before saving the configuration, users could click on "Test Connection". The GXW450X will then try connecting the server to make sure the server is up and accessible for the GXW450X.

Save the changes and all the backup logs will be listed on the web page.

Restore Configuration from Backup File

To restore the configuration on the GXW450X from a backup file, users could go to Web GUI→Maintenance→Backup→Backup/Restore.

- A list of previous configuration backups is displayed on the web page. Users could click on  of the desired backup file and it will be restored to the GXW450X.
- If users have other backup files on PC to restore on the GXW450X, click on "Upload Backup File" first and select it from local PC to upload on the GXW450X. Once the uploading is done, this backup file will be displayed in the list of previous configuration backups for restore purpose. Click on  to restore from the backup file.
- User could also restore using the backup file saved in SD card or USB device plugged into the GXW450X.



The screenshot shows the 'Backup/Restore' section of the web interface. It includes buttons for 'Add Backup', 'Schedule Backup', and 'Upload Backup File'. Below these is a 'List of Previous Configuration Backups' section with a 'Delete Selected Backup File (s)' button. A table lists the backups with columns for Name, Date, Size, and Options. The table contains one entry: 'backup_20181212_105534.tar' with a date of '2018-12-12 18:01:20 UTC+08:00' and a size of '4.83 MB'. The Options column for this entry contains icons for download, refresh, and delete. At the bottom of the table, there is a 'Total: 1' indicator, pagination controls showing '1' of 1 page, and a '10 / page' dropdown menu. Below the table is a 'Scheduled Backup Log' section with a 'Clean' button.




<input type="checkbox"/>	Name ↕	Date ↕	Size ↕	Options
<input type="checkbox"/>	backup_20181212_105534.tar	2018-12-12 18:01:20 UTC+08:00	4.83 MB	  

Figure 77: Restore GXW450X from Backup File

Note:

Backup file must be in tar format and contain letters, digits or special characters -_. File size must be less than 10MB.



System Cleanup/Reset

Reset & Reboot

Users could perform reset and reboot under Web GUI→**Maintenance**→**System Cleanup/Reset**→**Reset & Reboot**. To factory reset the device, select the mode type first. There are two different types for reset.

- **User Data:** The data such as CDR Records Operation Logs Core file etc.
- **All:** Restore the device to factory default settings for both User Data and User Configuration.

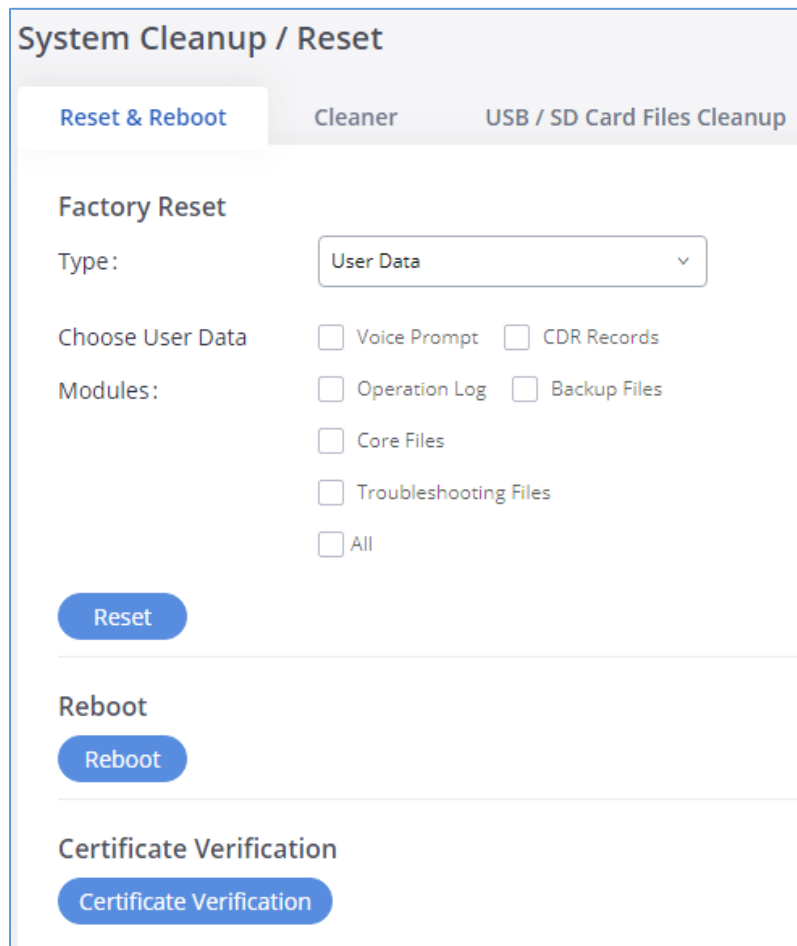


Figure 78: Reset and Reboot

- Press **Reset** to factory reset the GXW450X.
- Press **Reboot** to reboot the unit.
- Press **Certificate Verification** to validate certificate chain for the server's certificate.



Cleaner

Users could configure to clean the Call Detail Report/Voice Records/Voice Mails/FAX automatically under Web GUI → **Maintenance** → **System Cleanup/Reset** → **Cleaner**.

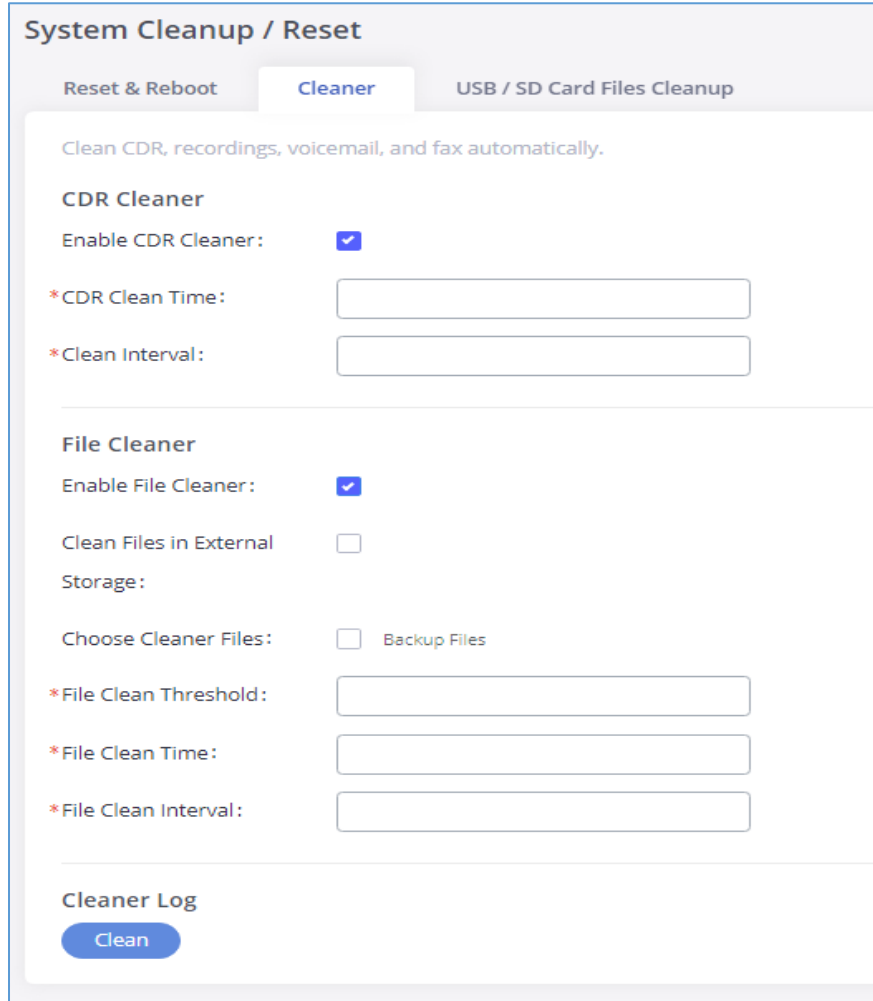


Figure 79: Cleaner

Table 47: Cleaner Configuration

CDR Cleaner	
Enable CDR Cleaner	Enable the CDR Cleaner function.
CDR Clean Time	Enter 0-23 to specify the hour of the day to clean up CDR.
Clean Interval	Enter 1-30 to specify the day of the month to clean up CDR.
File Cleaner	
Enable File Cleaner	Enter the Voice Records Cleaner function.

Clean Files in External Device	If enabled the files in external device (USB/SD card) will be atomically cleaned up as configured.
Choose Cleaner File	Select the files for system automatic clean.
File Clean Threshold	Specify the threshold of local storage usage from 0 to 99 (in percentage).
File Clean Time	Enter 0-23 to specify the hour of the day to clean up the files.
File Clean Interval	Enter 1-30 to specify the day of the month to clean up the files.
Cleaner Log	Press Clean “button” to clean cleaner log.

Note: All the cleaner logs will be listed on the bottom of the page.

USB/SD Card Files Cleanup

Users could manage the content of the external drives, USB and /or SD card, manually from the Web GUI under **Maintenance**→**System Cleanup/Reset** →**USB / SD Card Files Cleanup**.

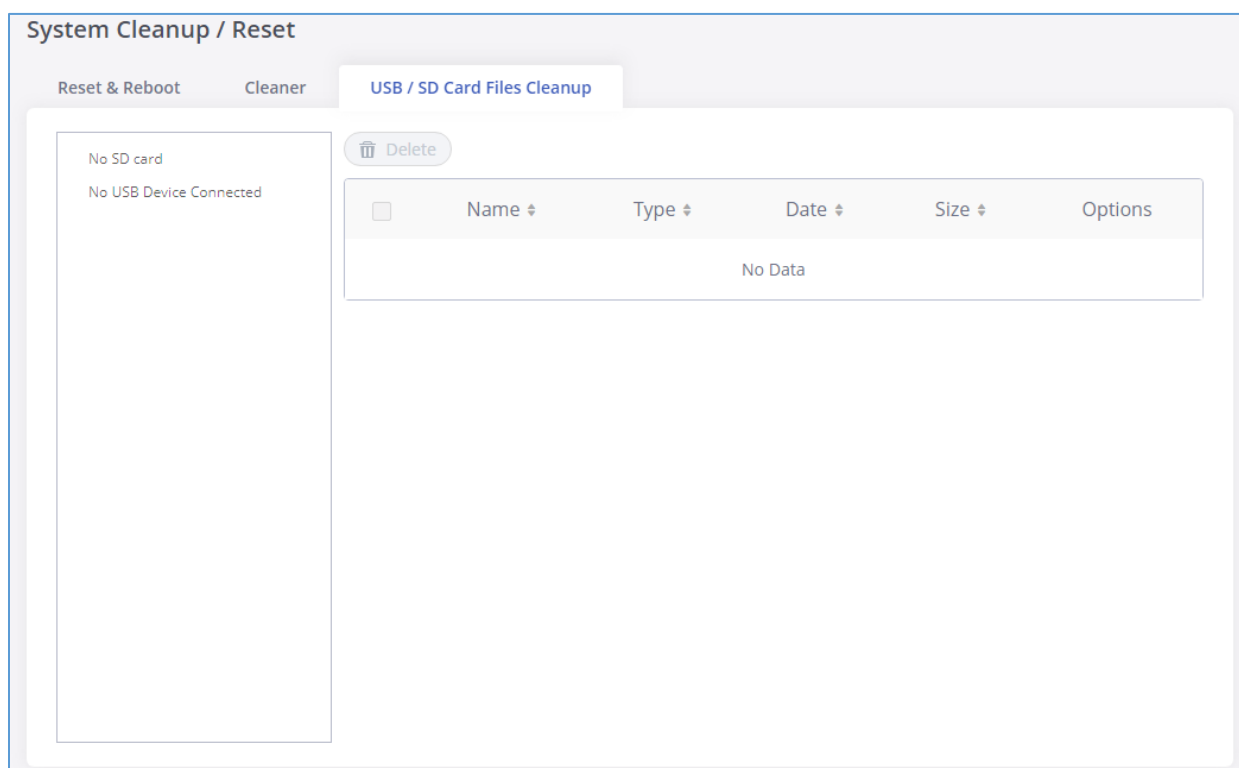


Figure 80: SB/SD Card Files Cleanup

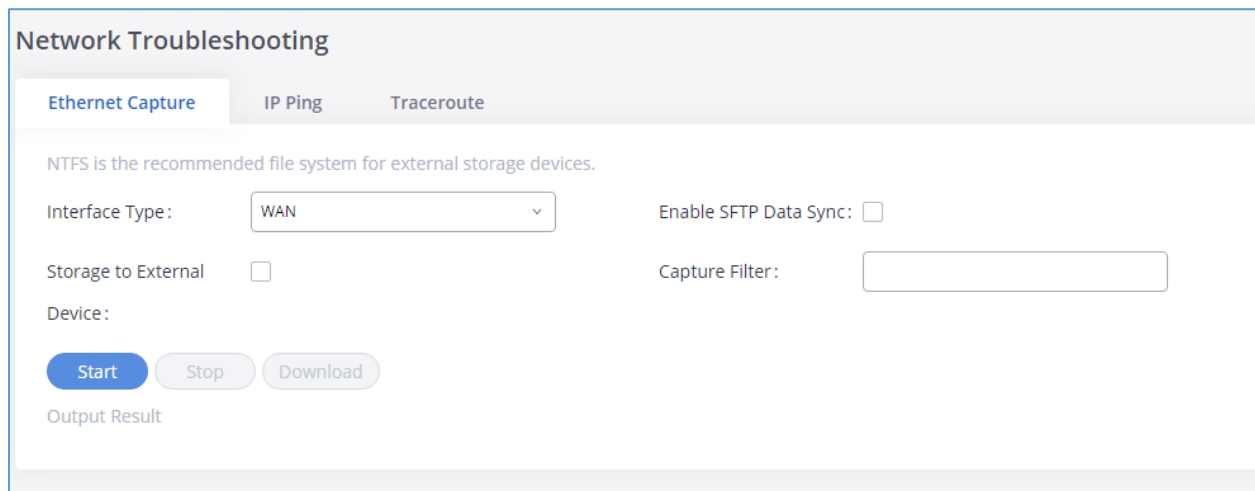
In this Web page users could navigate through the paths and the directories of the USB and/or the SD card and select the files and folders to clean up.

Network Troubleshooting

On the GXW450X, users could capture traces, ping remote host and traceroute remote host for troubleshooting purpose under Web GUI→**Maintenance**→**Network Troubleshooting**.

Ethernet Capture

An ethernet trace can be captured for troubleshooting purposes related to network issues, the SIP flow etc. The captured trace can be downloaded for analysis. Instructions or result will be displayed in the Web GUI output result.



The screenshot shows the 'Network Troubleshooting' web interface. It has three tabs: 'Ethernet Capture' (selected), 'IP Ping', and 'Traceroute'. Below the tabs, there is a note: 'NTFS is the recommended file system for external storage devices.' The configuration area includes:

- 'Interface Type': A dropdown menu currently set to 'WAN'.
- 'Enable SFTP Data Sync': An unchecked checkbox.
- 'Storage to External': An unchecked checkbox.
- 'Capture Filter': An empty text input field.
- 'Device': A label with no input field.
- Three buttons: 'Start' (blue), 'Stop' (grey), and 'Download' (grey).
- 'Output Result': A label for the results area.

Figure 81: Ethernet Capture

Table 48: Ethernet Capture Parameters

Interface Type	Select the network interface to monitor. <ul style="list-style-type: none"> • WAN • LAN • Both Default is "WAN".
Enable SFTP Data Sync	Check this box to save the capture files in the SFTP server. Please make sure the configuration of data synchronization works in advance.
Storage to External Device	Check this box to activate storage of the capture either on the USB or SD Card.
Capture Filter	Enter the filter to obtain the specific types of traffic, such as (host, src, dst, net, proto...).

Start	Click to start the trace.
Stop	Click to stop the trace.
Download	Click to download the trace if trace is stored locally.

The output result is in .pcap format. Therefore, users could specify the capture filter as used in general network traffic capture tool (host, src, dst, net, protocol, port, port range) before starting capturing the trace.

IP Ping

Enter the Target Host using either a host name or an IP address. Then press "Start" button. The output result will dynamically be displayed in the window below.

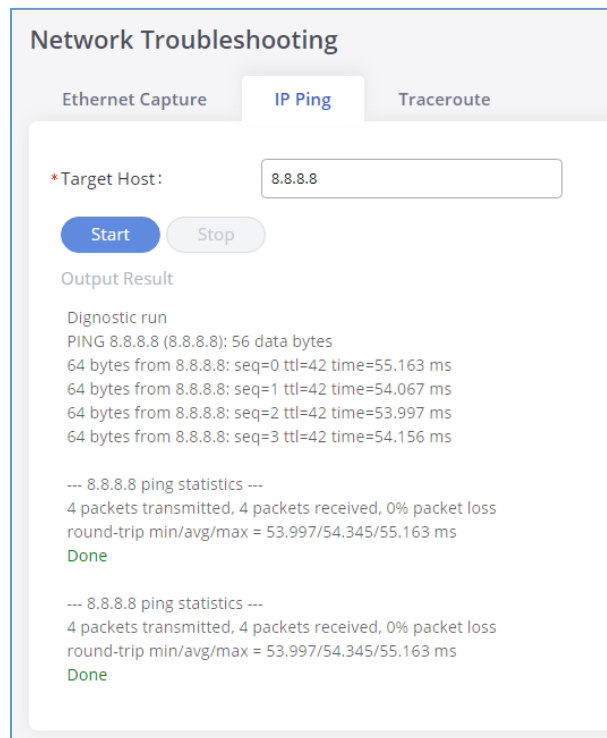


Figure 82: IP Ping

Traceroute

Enter the target host in host name or IP address. Then press "Start" button. The output result will dynamically be displayed in the window below.

Network Troubleshooting

Ethernet Capture
IP Ping
Traceroute

*Target Host:

Start
Stop

Output Result

```

Dignostic run
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 46 byte packets
1 * *
Done
          
```

Figure 83: Traceroute

Signaling Troubleshooting

Please refer to [Digital Trunk Troubleshooting] section.

Service Check

Enable Service Check to periodically check the GXW450X responsiveness. Check Cycle is configurable in seconds and the default setting is 60 sec. Check Times is the maximum number of failed checks before restart the GXW450X. The default setting is 3. If there is no response from GXW450X after 3 attempts (default) to check, current status will be stored and GXW450X will be restarted.

Service Check

Toggle Service Check:

* Check Cycle:

* Check times:


Figure 84: Service Check



CDR (CALL DETAIL RECORD)

CDR (Call Detail Record) is a data record generated by the PBX that contains attributes specific to a single instance of phone call handled by the PBX. It has several data fields to provide detailed description for the call, such as phone number of the calling party, phone number of the receiving party, start time, call duration, etc.

CDR Filter

On the GXW450X, the CDR can be accessed under Web GUI→**CDR**→**CDR**. Users could filter the call report by clicking on  and specifying the date range and criteria, depending on how the users would like to include the logs to the report. Click on "Search" button to display the generated report.

CDR

By default, this page displays the CDR entries from the current month. Use the "Filter" button to specify a time range.

Delete All Delete Search Result (s) Download All Records Download Search Result (s)

Filter ^

Automatic Download

Caller Number: <input style="width: 90%;" type="text"/>	Callee Number: <input style="width: 90%;" type="text"/>
Source Trunk Name: <input style="width: 90%;" type="text"/>	Destination Trunk Name: <input style="width: 90%;" type="text"/>
Time: <input style="width: 45%;" type="text" value="2018-11-13 10:58"/> - <input style="width: 45%;" type="text" value="2018-12-14 10:57"/>	
Status: <input type="checkbox"/> Answered <input type="checkbox"/> No Answer <input type="checkbox"/> Busy <input type="checkbox"/> Failed	
Reset Search	

Status	Call from	Call to	Start Time	Call Time	Talk Time
	"3100" 3100 [Trunk: Digital_1]	21007 [Trunk: sip147]	2018-11-13 18:52:14	14:09:17	14:09:15
	"3100" 3100 [Trunk: Digital_1]	21006 [Trunk: sip147]	2018-11-13 18:51:52	0:00:09	0:00:05
	"3100" 3100 [Trunk: Digital_1]	21007 [Trunk: sip147]	2018-11-13 18:51:03	0:00:36	0:00:22

Figure 85: CDR Filter

Table 49: CDR Filter parameters

Caller Number	You can specify a caller number or set caller number with a pattern (. match zero or more characters only appears in the end. X match any digit from 0-9, case-insensitive, repeatable, only appears in the end. If the pattern string contains "." in the end, "X" must appear before ".").
----------------------	--



	<p><u>For Example:</u></p> <ul style="list-style-type: none"> • X: It will filter out CDR records where a caller number is of ranges from 0 to 9. • XXXX: It will filter out CDR records where a caller number has 4 digits. • 3XXX: It will filter out CDR records where a caller number has a leading digit 3 and length of 4 digits. • 3.: It will filter out CDR records where a caller number has a leading digit 3.
Callee Number	Enter the caller name to filter the CDR report. CDR with the matching caller name will be filtered out.
Source Trunk Name	Select source trunk(s) and the CDR of calls going through inbound the trunk(s) will be filtered out.
Destination Trunk Name	Select destination trunk(s) and the CDR of calls going outbound through the trunk(s) will be filtered out.
Time	Specify the start time and the end time to filter the CDR report. Click on the calendar icon on the right and the calendar will show for users to select the exact date and time.
Status	<p>Filter with the call status, the available statuses are the following:</p> <ul style="list-style-type: none"> • Answered • No Answer • Busy • Failed

The call report will display as the following figure shows.






Status ↕	Call from ↕	Call to ↕	Start Time ↕	Call Time ↕	Talk Time ↕
	"3100" 3100 [Trunk: Digital_1]	21007 [Trunk: sip147]	2018-11-13 18:52:14	14:09:17	14:09:15
	"3100" 3100 [Trunk: Digital_1]	21006 [Trunk: sip147]	2018-11-13 18:51:52	0:00:09	0:00:05
	"3100" 3100 [Trunk: Digital_1]	21007 [Trunk: sip147]	2018-11-13 18:51:03	0:00:36	0:00:22
	"1007" 1007 [Trunk: sip147]	41000 [Trunk: Digital_1]	2018-11-13 15:29:57	0:00:26	0:00:07
	"1007" 1007 [Trunk: sip147]	41000 [Trunk: Digital_1]	2018-11-13 15:28:31	0:00:08	0:00:00

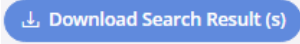
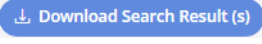
Figure 86: Call Report

The CDR report has the following data fields:

- **Status**
Answered, Busy, No answer or Failed.
- **Call From**
Example format: "3100" 3100 [Trunk: Digital_1]
- **Call To**
Example format: 21007 [Trunk: sip147]
- **Start Time**
Example Format: 2018-11-13 18:52:14
- **Call Time**
Example Format: 0:00:08
- **Talk Time**
Example Format: 0:00:07

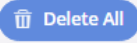
CDR Report Operations

After applying the filter, Users could perform the following operations on the CDR report:


- **Sort by data field**
Click on the header of the data field column to sort the report according to an ascending or descending order. Clicking on the same header again to reverse the order.
- **Download the search result**
Click on  to export the records filtered out to a .csv file.
- **Delete search result**
On the bottom of the page, click on  button to remove CDR records that appear on search results.



- **Delete all records**

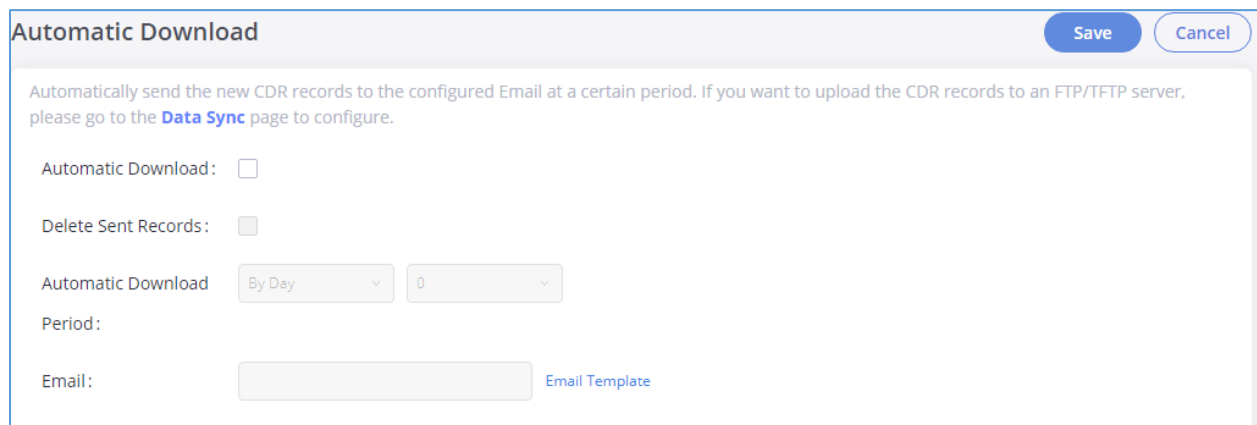
Click on  button to remove all the call report information.

- **Download all records.**

Click on  to export all the records to a .csv file.

Automatic Download

User could configure the GXW450X to automatically download the CDR records and send the records to an Email address. Click on “Automatic Download Settings” and configure the parameters in the dialog below.



The dialog box titled "Automatic Download" has a "Save" button and a "Cancel" button. The text inside reads: "Automatically send the new CDR records to the configured Email at a certain period. If you want to upload the CDR records to an FTP/TFTP server, please go to the [Data Sync](#) page to configure."

Fields in the dialog:

- Automatic Download:
- Delete Sent Records:
- Automatic Download: By Day (dropdown) | 0 (dropdown)
- Period: (empty field)
- Email: (text input field) | [Email Template](#)

Figure 87: Automatic CDR Download

To receive CDR record automatically from Email, check “Enable” and select a time period “By Day” “By Week” or “By Month”, select Hour of the day as well for the automatic download period. Make sure you have entered an Email or multiple email addresses where to receive the CDR records.

Note: Users have the option to delete the sent records “**Delete Sent Records**”.

CDR Report Data Fields

The CSV CDR report file downloaded will have the following data fields.

Table 50: CDR Report Data Fields

Field	Type	Description	Access
Account Code	String	An account code associated with the Party A channel.	r/w
Caller Number	String	The Caller ID number.	r
Callee Number	String	The destination number.	r
Context	String	The context of the call.	r
CallerID	String	The caller ID.	r
Source Channel	String	The name of the source channel.	r
Dest Channel	String	The name of the destination channel.	r
Lastapp	String	The last application the Party A channel executed.	r
Lastdata	String	The application data for the last application the Party A channel executed.	r
Start time	Date/time	The time the CDR was created.	r
Answer Time	Date/time	The time when Party A was answered, or when the bridge between a Party A and a Party B was created.	r
End time	Date/time	The time when the CDR was finished. This occurs when either party hangs up, or when the bridge between the parties is broken.	r
Call time	Integer	The time in seconds from start time until end time.	r
Talk time	Integer	The time in seconds from answer time until end time.	r
Disposition	Enum	The final known disposition of the CDR record. The possible values are: "ANSWERED", "NO ANSWER, CONGESTION, FAILED and BUSY.	r
Amaflags	Enum	A flag specified on the Party A channel. The possible values are: "OMIT, BILLING and DOCUMENTATION.	r/w
Uniqueid	String	A unique identifier for the Party A channel	r
Userfield	String	A user defined field set on the channels. If set on both the Party A and Party B channel, the userfields of both are concatenated and separated by a comma.	r/w
Dest Channel Extension	String	The destination extension of the call	r
Caller Name	String	The name of the caller	r



Answer by	String	The extension to be called	r
Session	String	A numeric value that, combined with uniqueid and linkedid, can be used to uniquely identify a single CDR record	r
Action Owner	String	The party that made the call	r
Action Type	String	The action type of the call	r
Source Trunk Name	String	The inbound route trunk name	r
Dest Trunk Name	String	The outbound route trunk name	r

Example of a CDR report Data fields:

- **Account code:** --
- **Caller Number:** 1008
- **Callee number:** 1006
- **Context:** did-out
- **Caller ID:** "" <1008>
- **Source Channel:** DAHDI/i1-1-1
- **Dest Channel:** PJSIP/trunk_5-00000000
- **Lastapp:** Dial
- **Lastdata:** PJSIP/1006@trunk_5,,b(callee-handler^s^1)
- **Start time:** 11/13/2018 3:01:28 PM
- **Answer time:** 11/13/2018 3:01:31 PM
- **End time:** 11/13/2018 3:01:50 PM
- **Call time:** 22 (in seconds)
- **Talk Time:** 18
- **Disposition:** ANSWERED
- **Amaflags:** DOCUMENTATION
- **UniqueID:** 1542092488
- **Userfield:** External
- **Dest channel extension:** trunk_5
- **Caller name:** -
- **Answer by:** trunk_5
- **Session:** 1542092488529109-1008
- **Action owner:** 1008
- **Action type:** DIAL.
- **Source Trunk name:** Digital_1



- **Dest Trunk name:** sip147



EXPERIENCING THE GXW450X SERIES DIGITAL GATEWAY

Please visit our website: <http://www.grandstream.com> to receive the most up- to-date updates on firmware releases, additional features, FAQs, documentation and news on new products.

We encourage you to browse our [product related documentation](#), [FAQs](#) and [User and Developer Forum](#) for answers to your general questions. If you have purchased our products through a Grandstream Certified Partner or Reseller, please contact them directly for immediate support.

Our technical support staff is trained and ready to answer all your questions. Contact a technical support member or [submit a trouble ticket online](#) to receive in-depth support.

Thank you again for purchasing Grandstream GXW450X IP PBX appliance, it will be sure to bring convenience and color to both your business and personal life.

*** Asterisk is a Registered Trademark of Digium, Inc.**

