Grandstream Networks, Inc.

GXW4500 series

1, 2 or 4 T1/E1/J1 Interfaces

Digital VoIP Gateway

User Manual

COPYRIGHT

The latest electronic version of this guide is available for download here:
http://www.grandstream.com/support

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 GXW4500 adaptor complies with FCC/CE and various safety standards. The GXW4500 power adaptor is compliant with UL standard. Only use the universal power adapter provided with the GXW4500 package. The manufacturer's warranty does not cover damages to the device caused by unsupported power adaptors

Table of Contents

Table of Tables

Table of Figures

GNU GPL INFORMATION

GXW4500 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 GXW4500 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 1.0.0.6

- This is the initial version.

WELCOME

Thank you for purchasing the Grandstream GXW4500 Digital VoIP Gateway. The GXW4500 offers an easy to manage, easy to configure IP communications solution for any business with virtual and/or branch locations. The GXW4500 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 GXW4500 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 GXW4500 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 GXW4500 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 GXW4500 OVERVIEW

The GXW4500 series are E1/T1/J1 Digital VoIP Gateways that allow digital PSTN and ISDN trunks to be integrated with VoIP networks. By connecting the GXW4500 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 GXW4500 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 GXW4500:

Table 1: GXW4500 Features Highlights

GXW4500 	• 1,2 or 4 Software configurable E1/T1/J1 ports • Support of PRI, SS7and 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 • Automated provisioning by HTTP/TFTP with XML config files • Support of multi-language voice prompt • Supports up to 120 concurrent calls

GXW4500 Technical Specifications

The following table resumes all the technical specifications including the protocols/standards supported, voice codecs, languages and upgrade/provisioning settings for the GXW4500

Table 2: GXW4500 Technical Specifications

Interfaces	
T1/E1/J1 Interface	1/2/4 RJ45 ports, supporting up to 30/60/120 simultaneous VoIP calls
Network Interface	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 & video 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, HDLC, HDLC-ETH, 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/1.5A
Temperature and Humidity	Operating: 32 - 113ºF / 0 ~ 45ºC, Humidity 10 - 90% (non-condensing) Storage: 14 - 140ºF / -10 ~ 60ºC, 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 GXW4500.

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

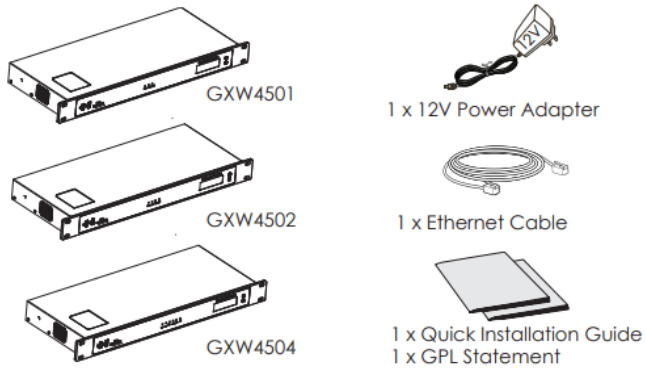


Figure 1: GXW4500 Package Contents

Connecting the GXW4500

Connecting the GXW4500 gateway is easy. Follow these steps to connect your GXW4500 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 GXW4500; 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 GXW4500. 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 GXW4500; connect the other end into the T1/E1/J1 wall jack.
4. Wait for the GXW4500 to boot up. The front LCD display will show the GXW4500 hardware information when the boot process is completed.
5. Once the GXW4500 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.

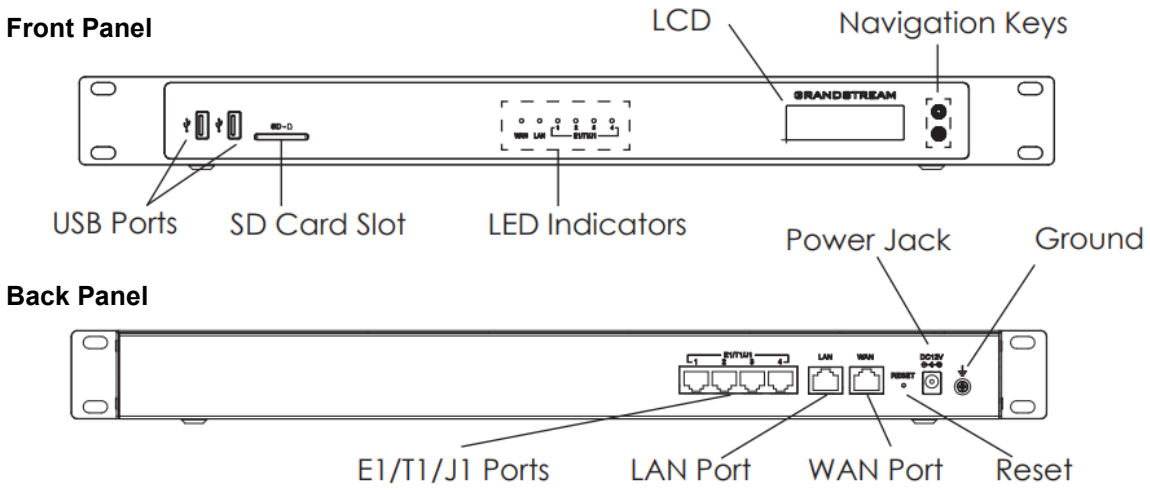


Figure 2: Diagram of GXW4504 Back and Front Panel

Table 3: Definitions of the GXW4500 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 GXW4500 Keypad Menu

The keypad menu of the GXW4500 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	• **Critical Events** • **Other Events**
Device Info	• **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	• **LAN Mode**: DHCP, Static IP or PPPoE • **LAN IP**: IP address • **LAN Subnet Mask**
Network Menu	• **LAN Mode**: Select LAN mode as DHCP, Static IP or PPPoE • **Static Routes Reset**: Click to reset the static route setting
Factory Menu	• **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

	the test, reboot the device manually and the device will display the correct time. • **Hardware Testing** Select "Test DSP" to perform DSP test on the device. 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.
Default Password	Showing the default Web login password. Once the password was changed, this menu will not show again.
Web Info	• **Protocol**: Web access protocol. HTTP or HTTPS. By default, it's HTTPS • **Port**: Web access port number. By default, it's 8089
SSH Switch	• **Enable SSH:** Enable SSH access. • **Disable SSH:** Disable SSH access. By default, the SSH access is disabled.

Use the LED Indicators

The GXW4500 has LED indicators in the front to display connection status. The following table shows the status definitions.

Table 5: GXW4500 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 GXW4500 via Web GUI

Web GUI Access

The GXW4500 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.

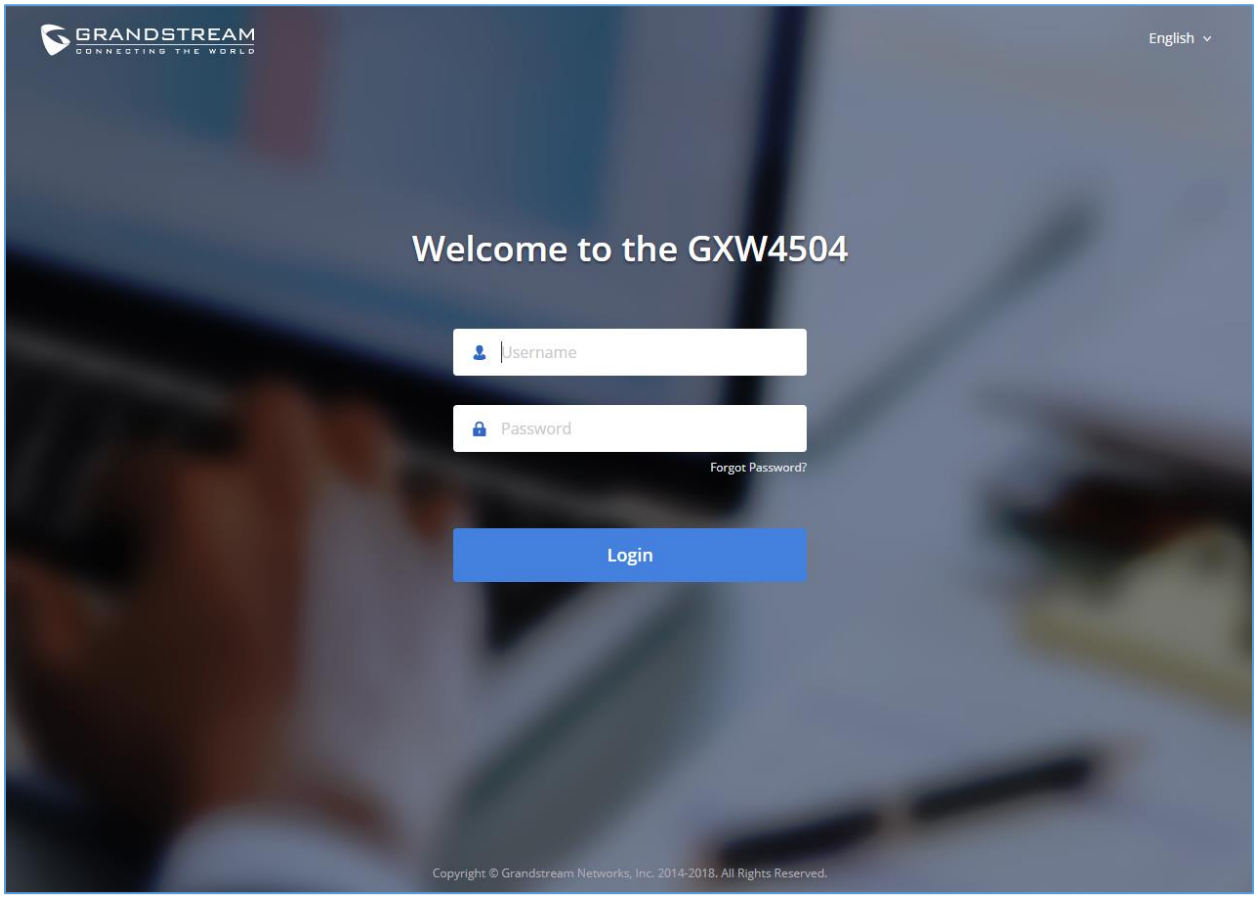


Figure 3: GXW4500 Web Gui Login Page

To access the Web GUI:

1. Connect the computer to the same network as the GXW4500.
2. Ensure the GXW4500 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 GXW4500).

Setup Wizard

When the user logs in the GXW4500 Web GUI for the first time, a setup wizard will provide guidance to set up basic configuration. Configurations in setup wizard include: Network settings, Time zone and Trunk/routes.

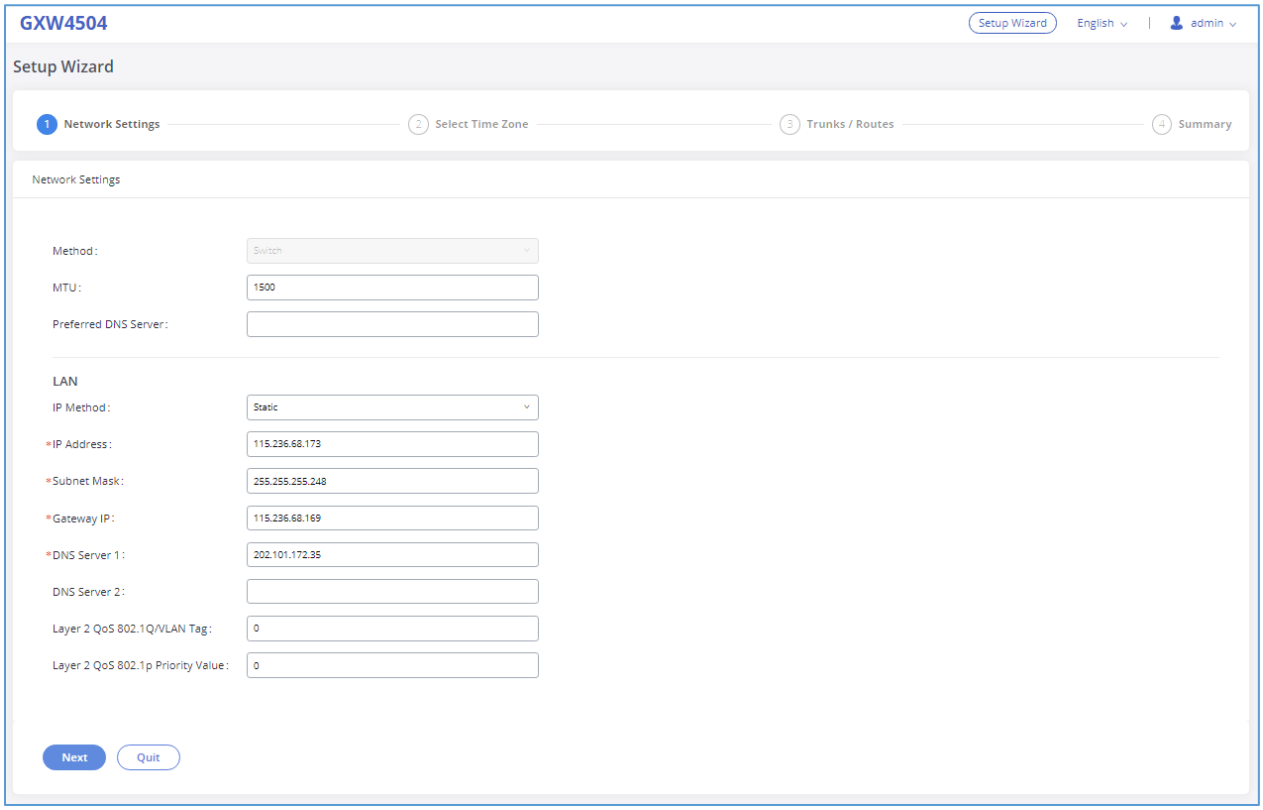


Figure 4: GXW4500 Setup Wizard

Web GUI Configurations

There are six main sections in the Web GUI for users to view the Gateway status, configure and manage the GXW4500.

- **System Status**: Displays GXW4500 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 GXW4500 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.

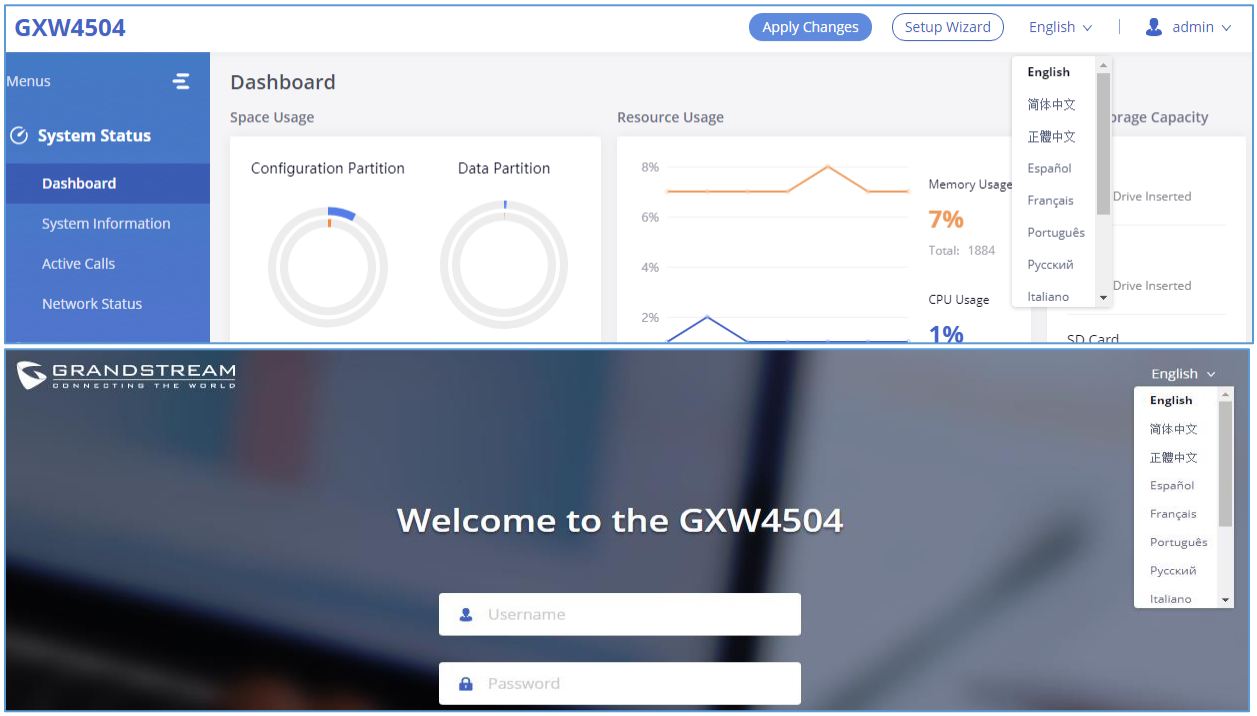


Figure 5: GXW4500 Web GUI Languages

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 GXW4500 such us: software and hardware information, space usage, resources usage etc.

Dashboard

The GXW4500 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**.

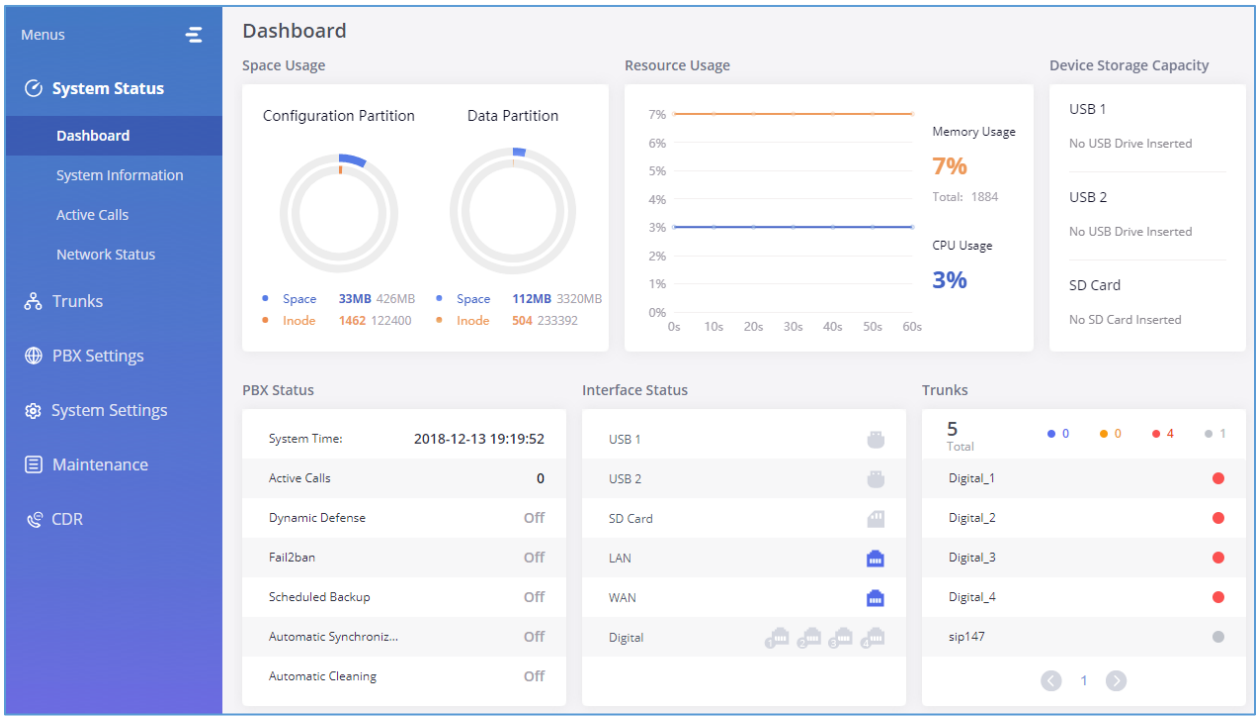


Figure 6: GXW4500 Dashboard

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 GXW4500 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.

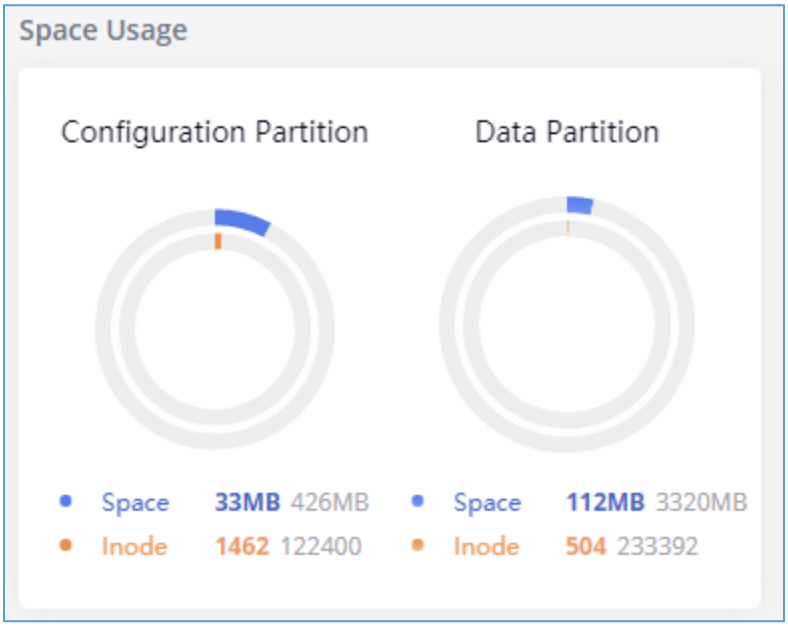


Figure 7: Space Usage

Resource Usage

When configuring and managing the GXW4500, 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.

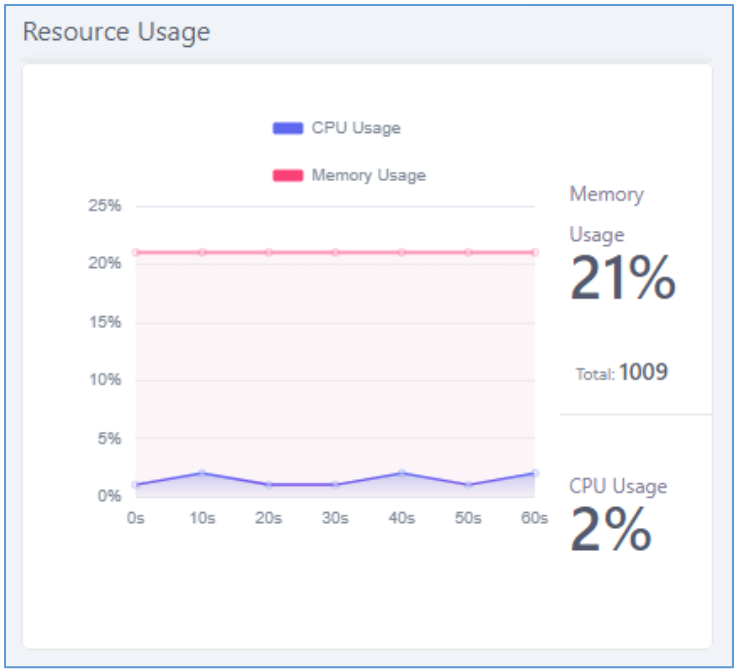


Figure 8: Resource Usage

Disk Capacity

Users could check the external devices capacities from the Dashboard page of the GXW4500 under Web GUI→**System Status→Dashboard →Device Storage Capacity.**

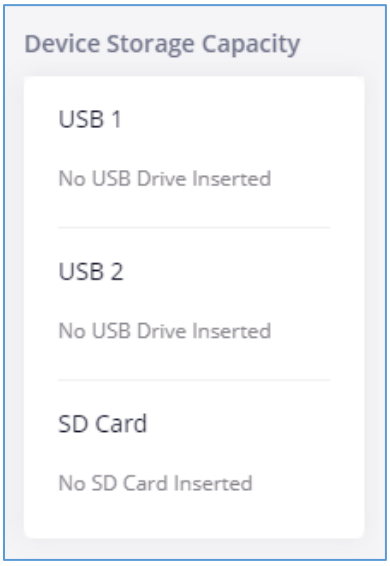


Figure 9: Device Storage Capacity

PBX Status

The PBX status shows the status of some of the gateway GXW4500 services. Among the services monitored on the PBX status tab there is: System Time, Active Calls, Schedule backup etc.

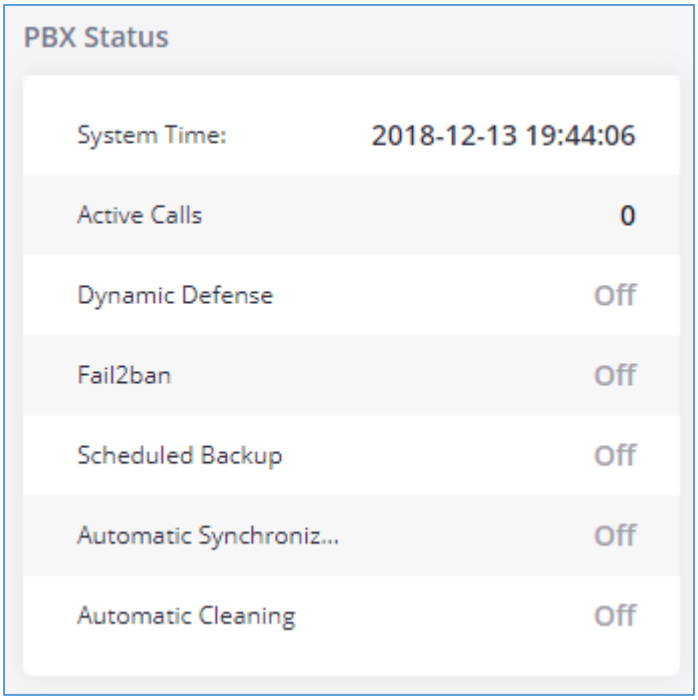


Figure 10: PBX Status

Interfaces Status

This section displays interface connection status on the GXW4500 for USB, SD Card, LAN, WAN, and Digital interfaces.

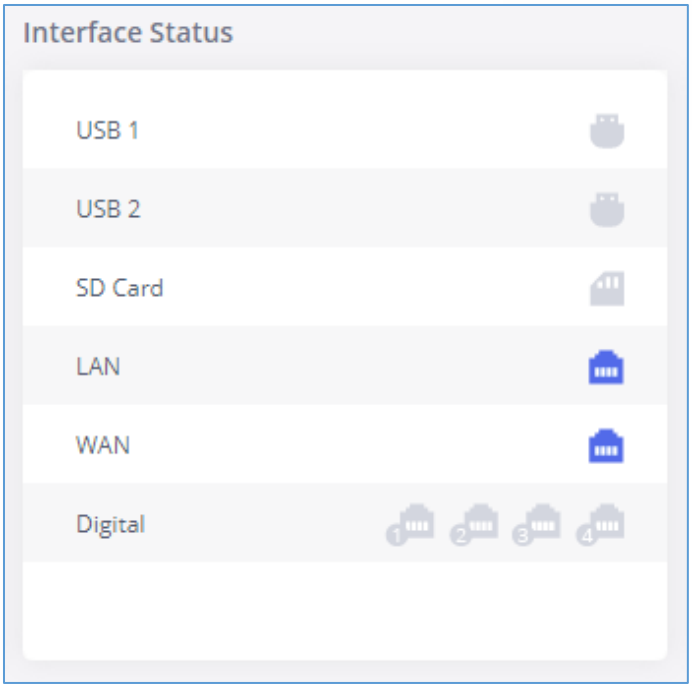


Figure 11: Interface Status

Trunks

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

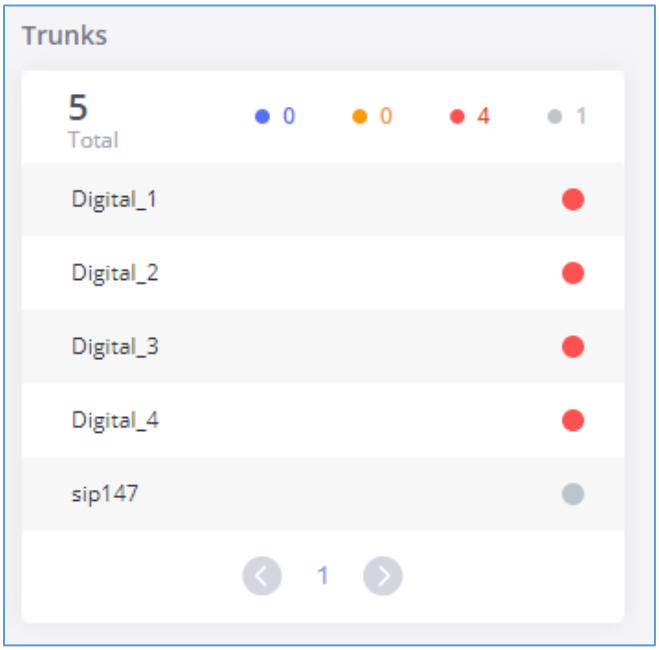


Figure 12: Trunks Status

Four statuses are possible for any trunk configured on the GXW4500:

- 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:

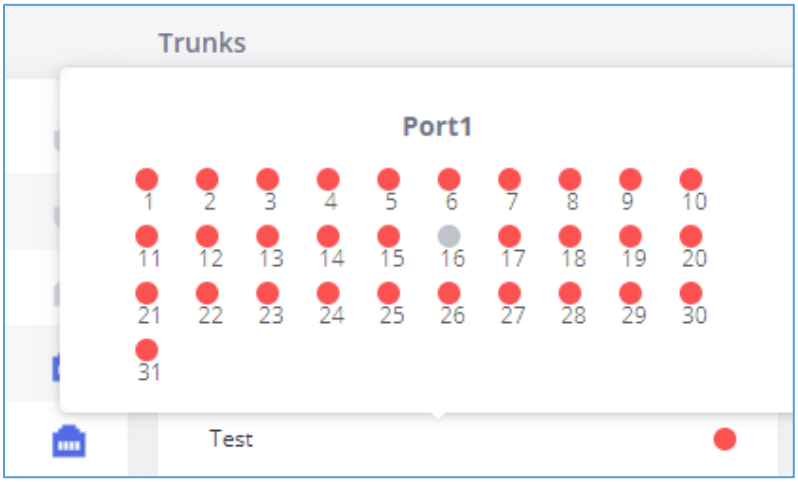


Figure 13: Digital Trunk Channels Status

System Information

The GXW4500 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 GXW4500. 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.

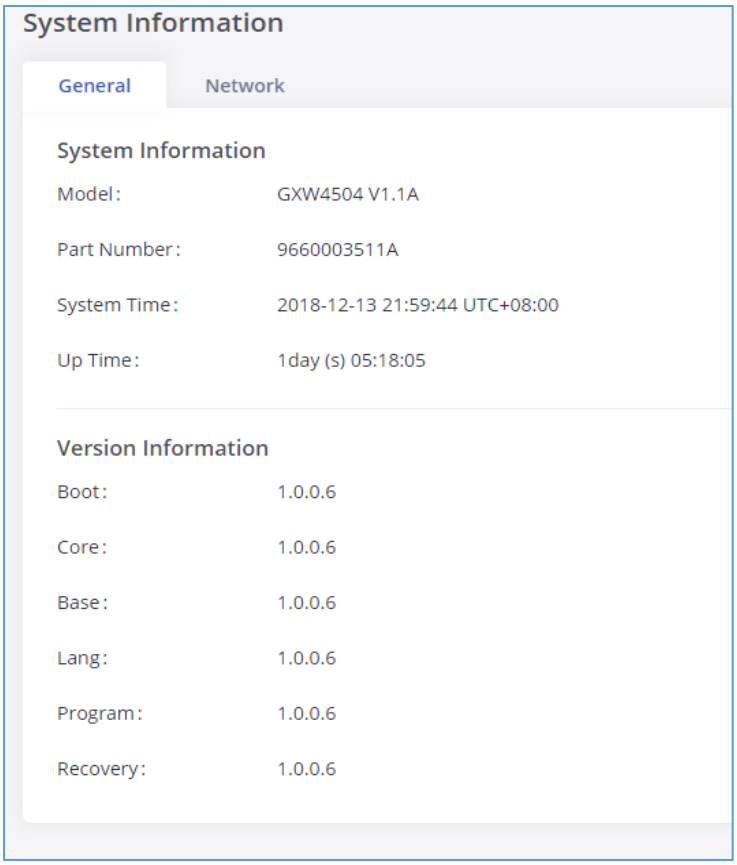


Figure 14: System Information→General

Network

Under Web GUI→**System Status→System Information→Network**, users could check the network information for the GXW4500. 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.

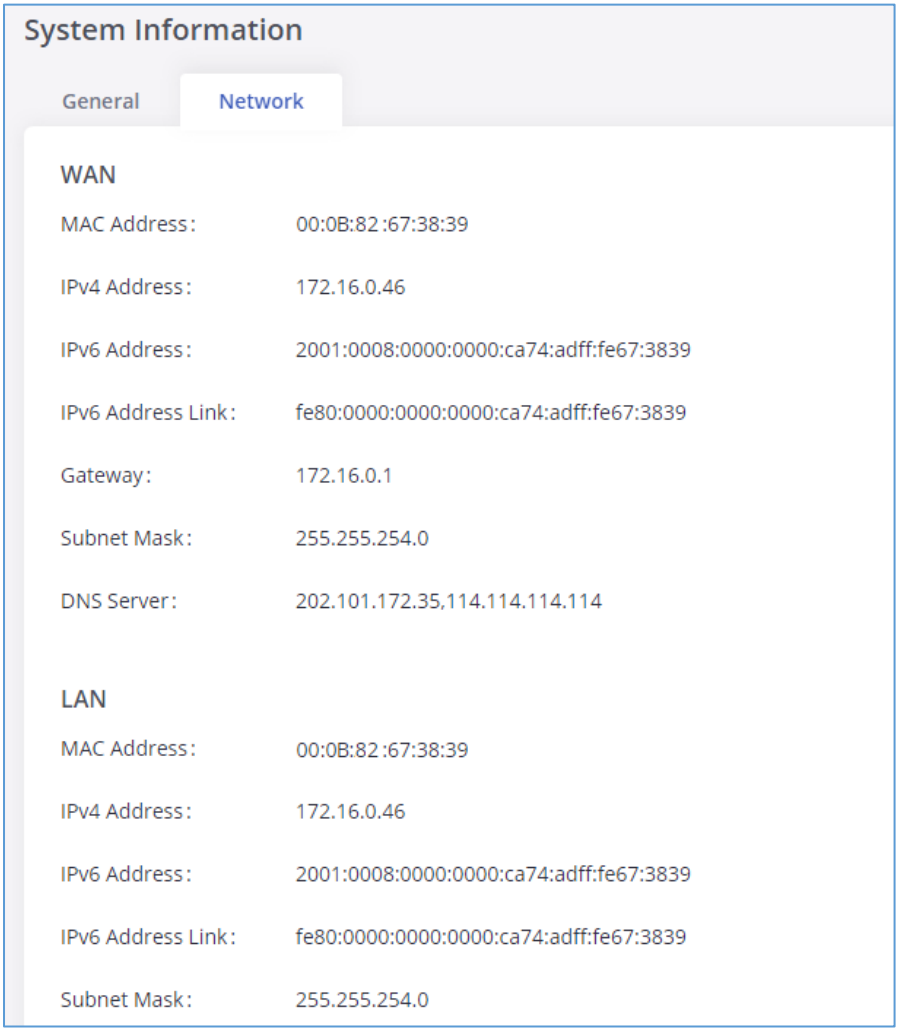


Figure 15: System Information→Network

Active Calls

The active calls on the GXW4500 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.

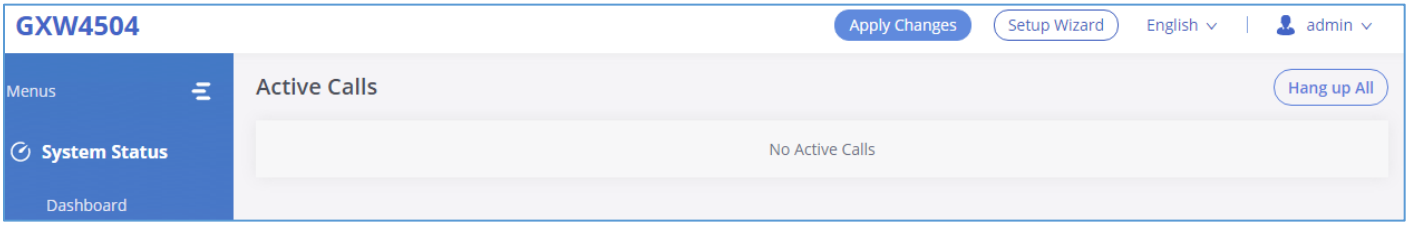
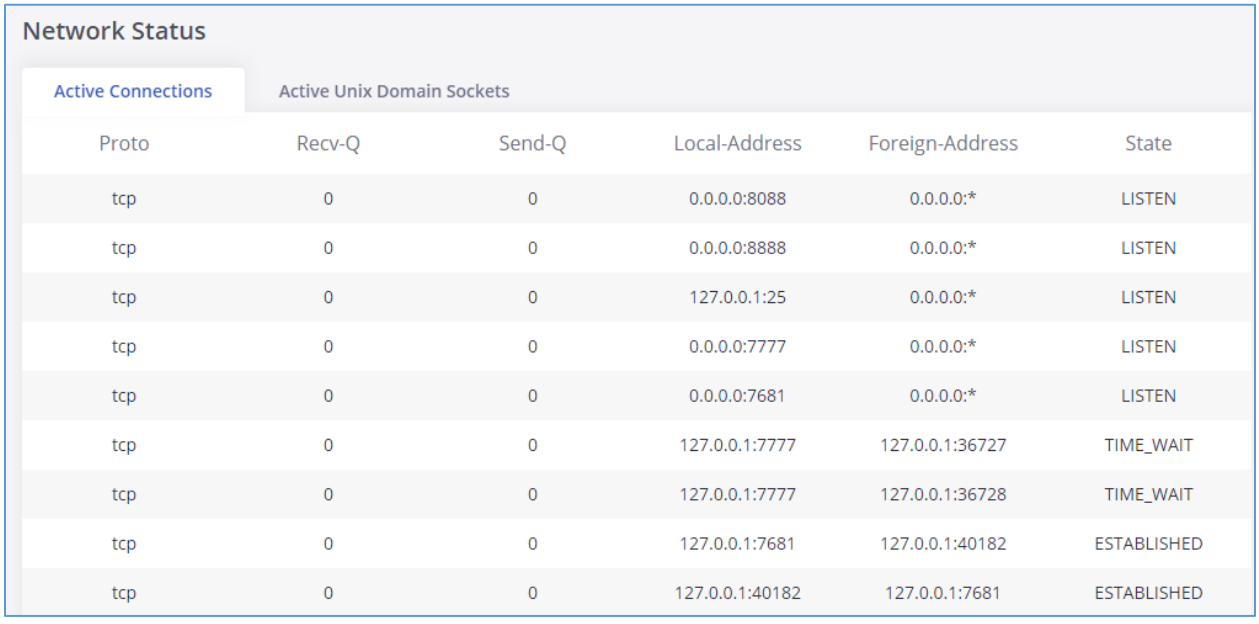


Figure 16: Active Calls

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

Network status

GXW4500 supports Network Status to display active internet connections. User can use Network Status to troubleshoot connection issues between GXW4500 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.



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 17: Active connections

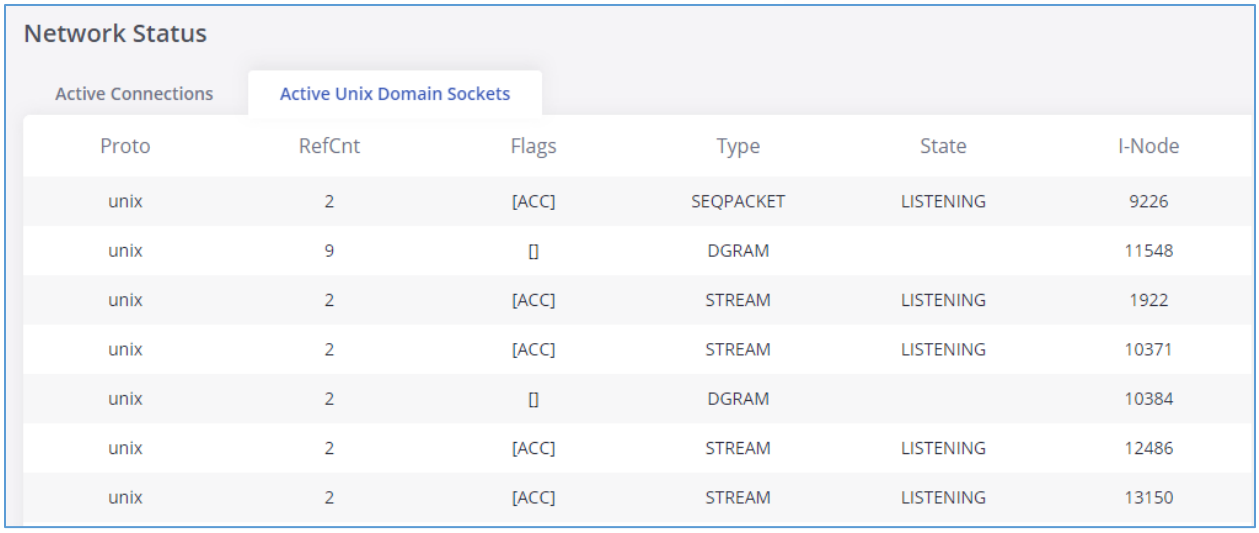


Figure 18: Active Unix Domain Sockets

SYSTEM SETTINGS

This chapter explains configurations for system-wide parameters on the GXW4500. System settings are under “System Settings” tab on GXW4500 Web GUI. System settings include, Network Settings, Security Settings, HTTP Server, Email Settings, Time Settings, OpenVPN® settings and DDNS Settings

HTTP Server

The GXW4500 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 GXW4500.
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 GXW4500’s web GUI.
Permitted IP(s)	Add an IP address to the list of allowed IPs to access GXW4500’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: • **Manually Upload certificate**: Upload the files while respecting size and format.

	• **Automatically request certificate**: enter domain from which to request the certificate files.
TLS Private Key	Upload private key for the built-in http server. **Note:** The size of the key file must be under 2MB and the it will be renamed as "private.pem" automatically.
TLS Cert	Upload certificate for the built-in http server and override the existing one. **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.
Reset Certificate	Restore the default key and certificate. The web server needs to reload to take effect after certificate restoration.

Network Settings

After successfully connecting the GXW4500 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 GXW4500.

Table 7: GXW4500 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, its 1500)
IPv4 Address	
Preferred DNS Server	Enter the preferred DNS server address. If Preferred DNS is used, GXW4500 will try to use it as Primary DNS server.

LAN	
IP Method	Select DHCP, Static IP, or PPPoE. The default setting is DHCP.
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. The default setting is 0.0.0.0.
DNS Server 2	Enter the DNS server 2 address for static IP settings.
User Name	Enter the user name to connect via PPPoE.
Password	Enter the password to connect via 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.
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.
IPv6 Address	
LAN	
IP Method	Select Auto or Static. The default setting is Auto
IP Address	Enter the IP address for static IP settings.
IP Prefixlen	Enter the Prefix length for static settings. 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.

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 GXW4500 supports 802.1X as a supplicant/client to be authenticated. The following diagram and figure show the GXW4500 uses 802.1X mode "EAP-MD5" on WAN port as client in the network to access Internet.

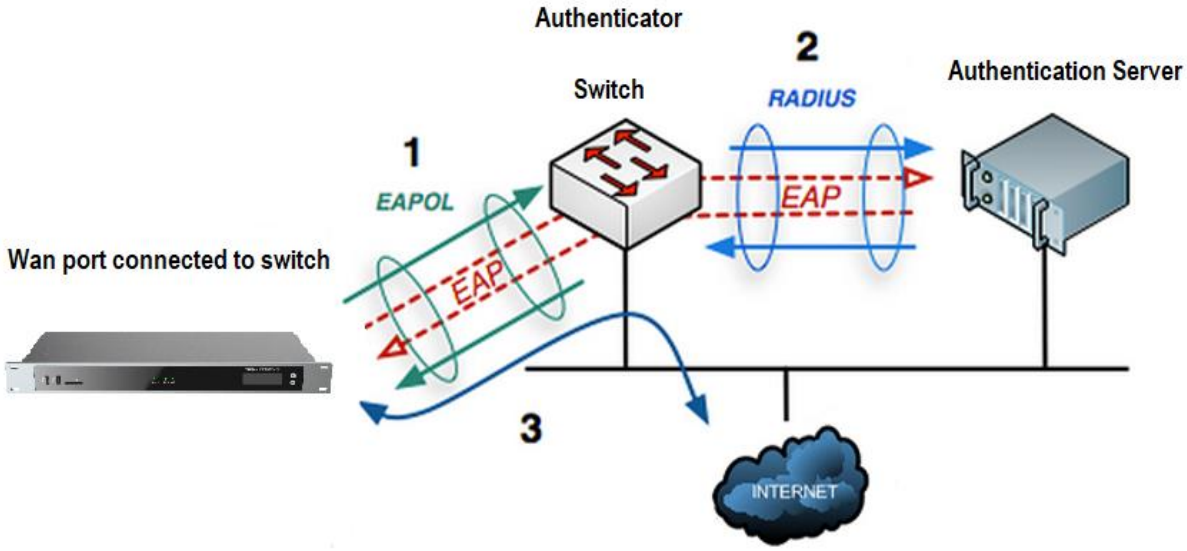


Figure 19: GXW4500 Using 802.1X as Client

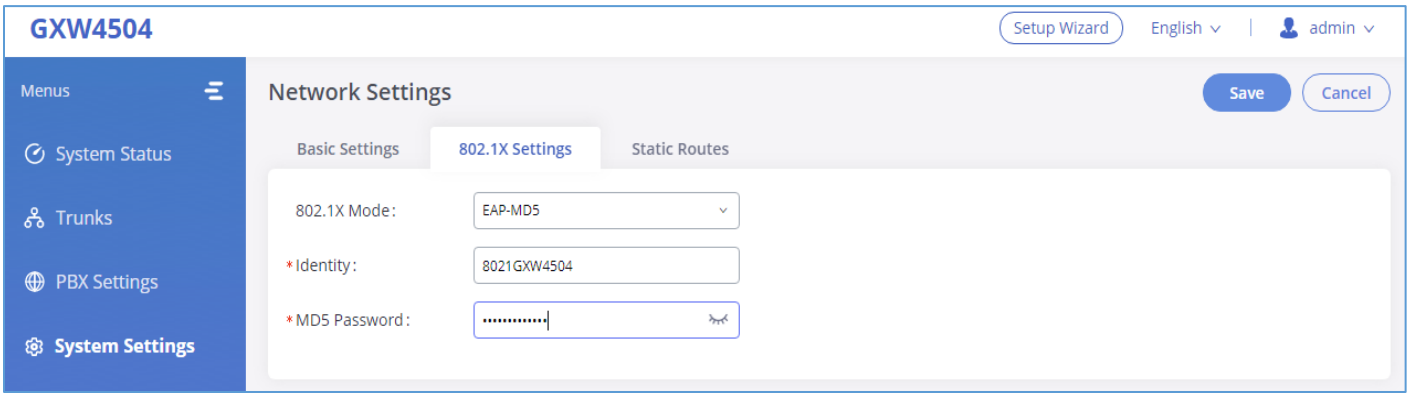


Figure 20: GXW4500 using 802.1X EAP-MD5

The following table shows the configuration parameters for 802.1X on GXW4500. 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: GXW4500 Network Settings→802.1X

802.1X Mode	Select 802.1X mode. The default setting is "Disable". The supported 802.1X mode are: • 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 GXW4500 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 GXW4500 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: GXW4500 Network Settings→Static Routes

Destination	Configure the destination IPv4 address or the destination IPv6 subnet for the GXW4500 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 GXW4500 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 GXW4500 to reach the destination using the static route.

OpenVPN®

OpenVPN® settings allow the users to configure GXW4500 to use VPN features, the following table gives details about the various options in order to configure the GXW4500 as OpenVPN Client.

Table 10: GXW4500 System Settings→Network Settings→OpenVPN®

OpenVPN® Enable	Enable / Disable the OpenVPN feature.
OpenVPN® Server	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.
OpenVPN® Device Mode	Use the same setting as used on the server. **Dev TUN:** Create a routed IP tunnel. **Dev TAP:** Create an Ethernet tunnel.
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. Use the same setting that you are using on the server.
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.

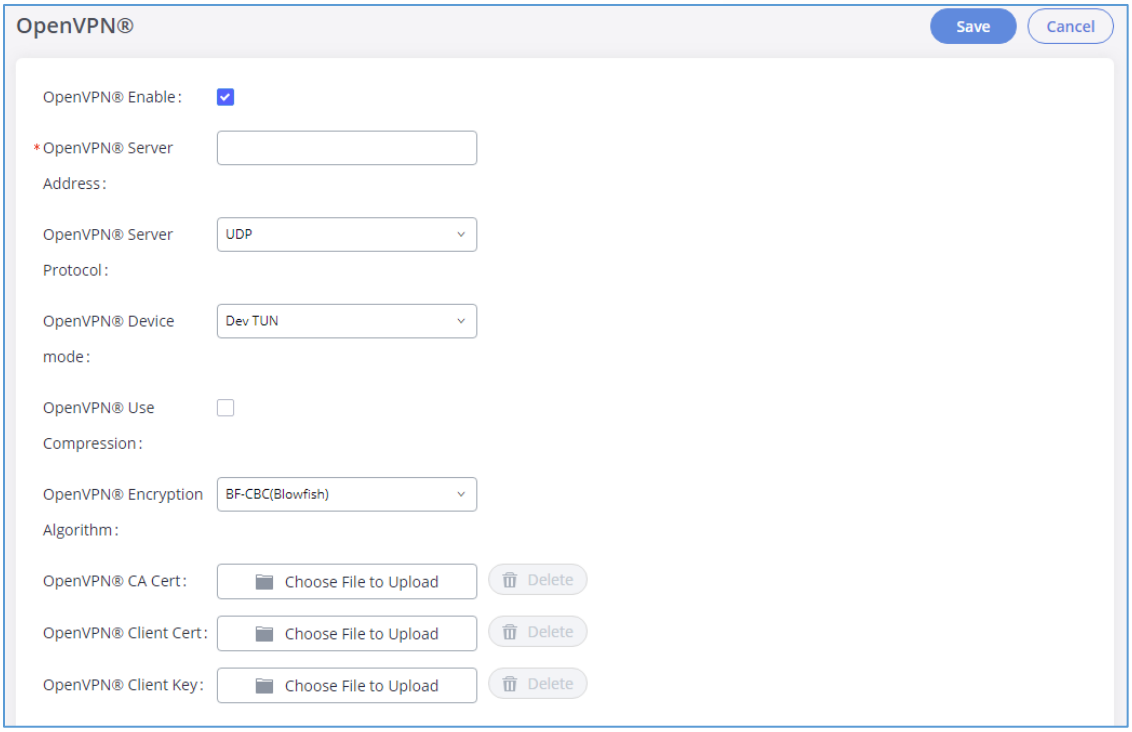


Figure 21: OpenVPN® Feature on the GXW4500

DDNS Settings

DDNS setting allows user to access GXW4500 via domain name instead of IP address.
The GXW4500 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 GXW4500 needs to have public IP access.

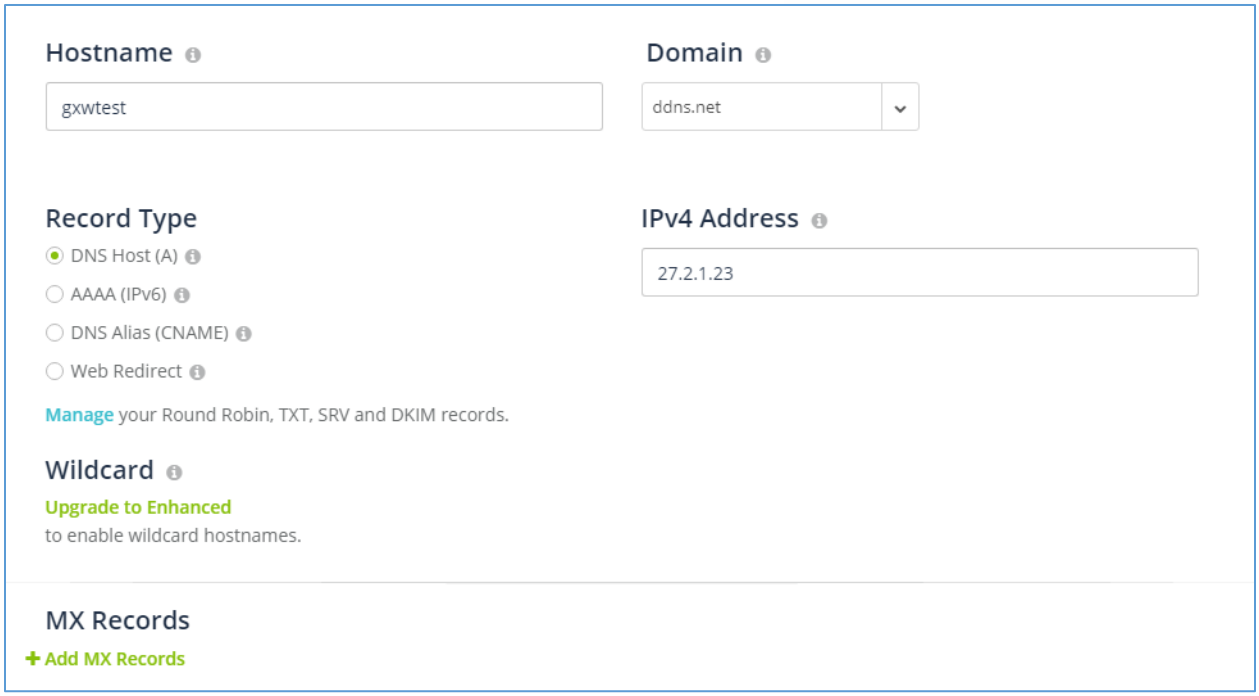


Figure 22: Register Domain Name on Noip.com

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

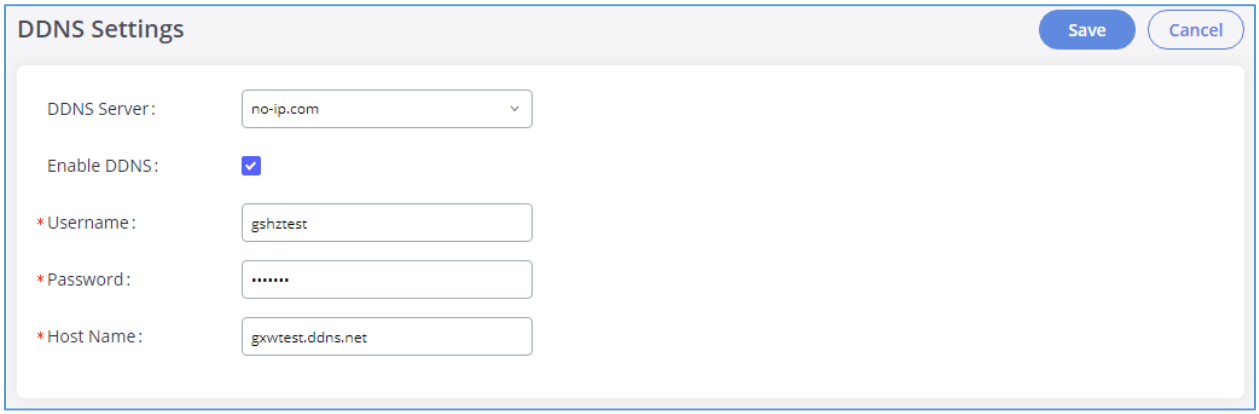


Figure 23: GXW4500 DDNS Settings

3. Now you can use domain name instead of IP address to connect to the GXW4500 Web GUI.

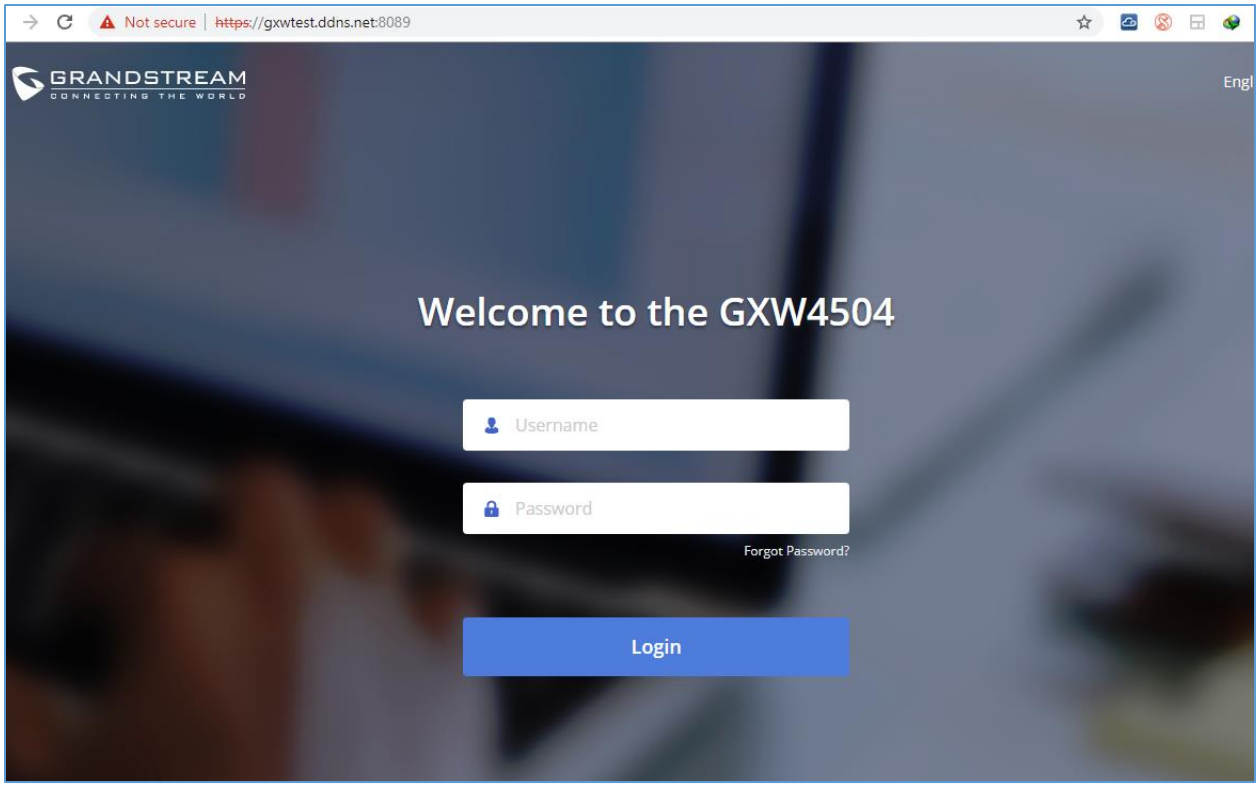


Figure 24: Using Domaine Name to Connect to GXW4500

Security Settings

The GXW4500 provides users firewall security configurations to prevent certain malicious attack to the GXW4500 system. Users could configure to allow, restrict or reject specific traffic through the device for security and bandwidth purpose. The GXW4500 also provides Fail2ban feature for authentication errors in SIP REGISTER, INVITE and SUBSCRIBE. To configure firewall settings in the GXW4500, 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 GXW4500.

Table 11: GXW4500 Static Defense→Current Service

Port	Process	Type
8088	asterisk	TCP/IPv4
25	master	TCP/IPv4
7777	Asterisk	TCP/IPv4
7681	pbxmid	TCP/IPv4
4520	asterisk	UDP/IPv4
4569	asterisk	UDP/IPv4
5000	asterisk	UDP/IPv4
67	udhcpd	UDP/IPv4
69	udpsvd	UDP/IPv4
80	lighttpd	TCP/IPv6
8888	pbxmid	TCP/IPv6
8089	lighttpd	TCP/IPv6
4569	asterisk	UDP/IPv6

Under "Custom Firewall Settings", users could create new rules to accept, reject or drop certain traffic going through the GXW4500. 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

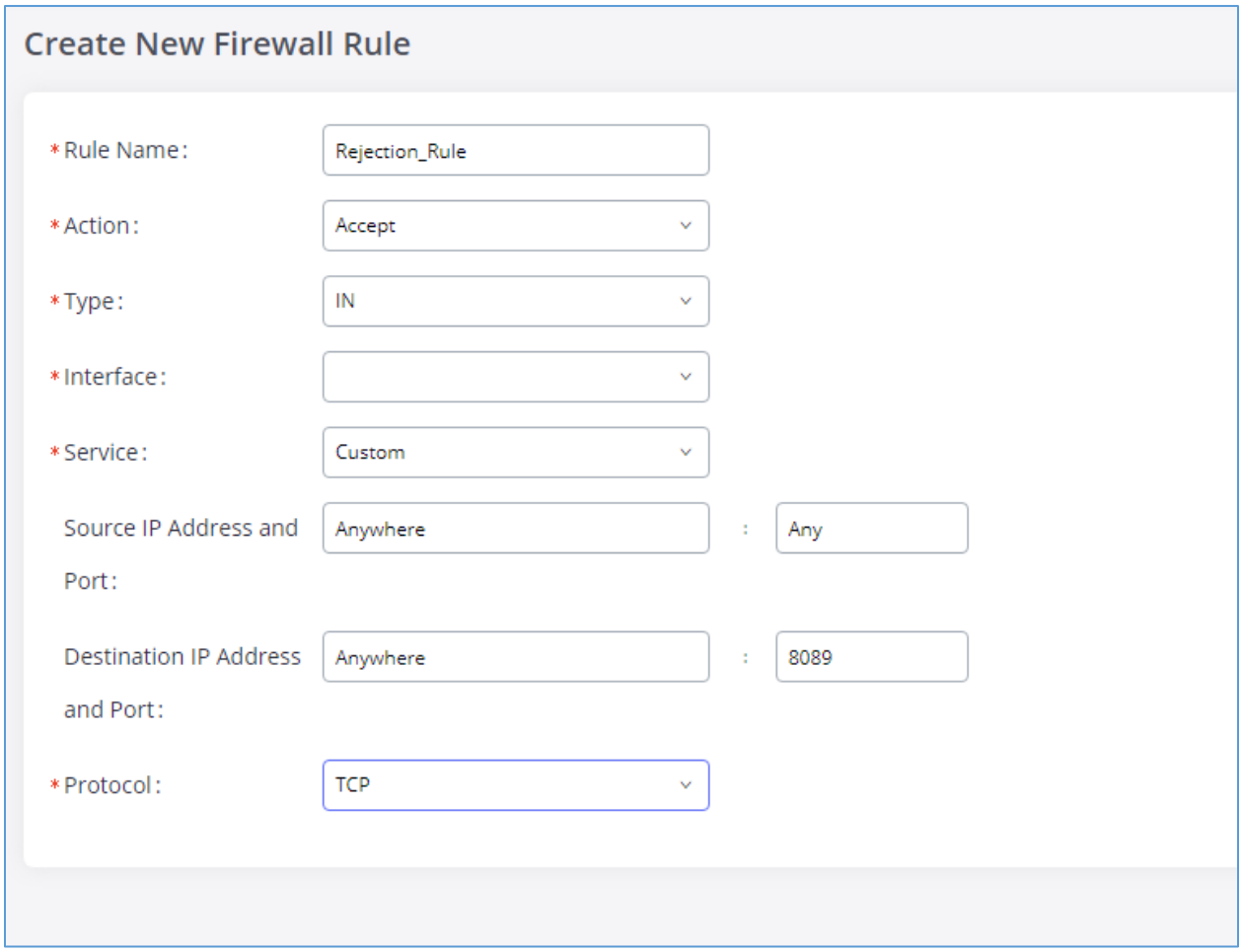


Figure 25: Create New Firewall Rule

Below is a table listing all the firewall rules settings:

Table 12: Firewall Rule Settings

Rule Name	Specify the Firewall rule name to identify the firewall rule.
Action	Select the action for the Firewall to perform. • ACCEPT • REJECT • DROP

Type	Select the traffic type. • **IN** If selected, users will need specify to the network interface (for GXW4500) for the incoming traffic. • **OUT**
Service	Select the service type. • **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 GXW4500.

Table 13: 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 (GXW4500) interface.
SYN-Flood Defense Enable	Allows the GXW4500 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.

	• eth(0)LAN defends against attacks directed to the LAN IP address of the GXW4500. • eth(1)WAN defends against attacks directed to the WAN IP address of the GXW4500. SYN Flood Defense will limit the amount of SYN packets accepted by the GXW4500 from one source to 10 packets per second. Any excess packets from that source will be discarded.
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 (GXW4500) interface.

Dynamic Defense

Dynamic defense is supported on the GXW4500 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 GXW4500 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 GXW4500 firewall, which will then be displayed in the web page. Please refer to the following table for dynamic defense options on the GXW4500.

Table 14: GXW4500 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***

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 GXW4500, it will be added into GXW4500 blacklist. This host 192.168.2.5 will be blocked by the GXW4500 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 GXW4500 within 1 minute, it will not be added into GXW4500 blacklist. It can still establish TCP connection with the GXW4500.

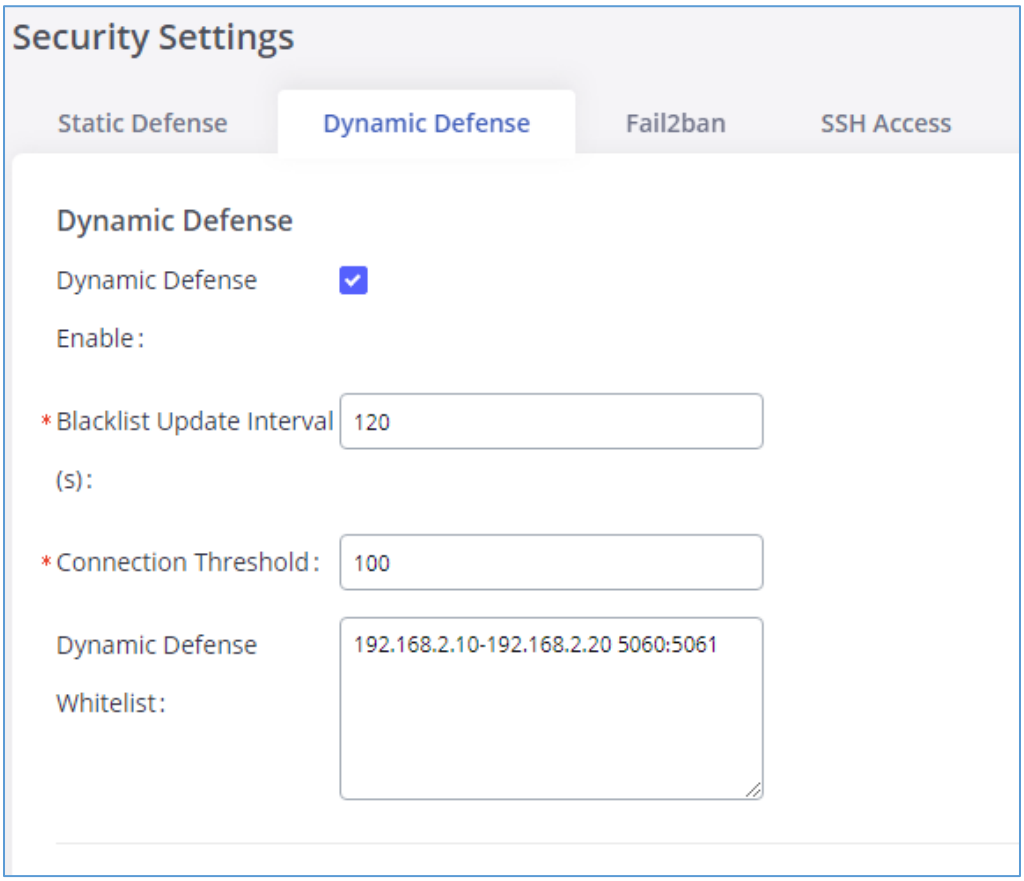


Figure 26: Dynamic Defense Configuration

Fail2Ban

Fail2Ban feature on the GXW4500 provides intrusion detection and prevention for authentication errors in SIP INVITE and SUBSCRIBE. Once the entry is detected within "Max Retry Duration", the GXW4500 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.

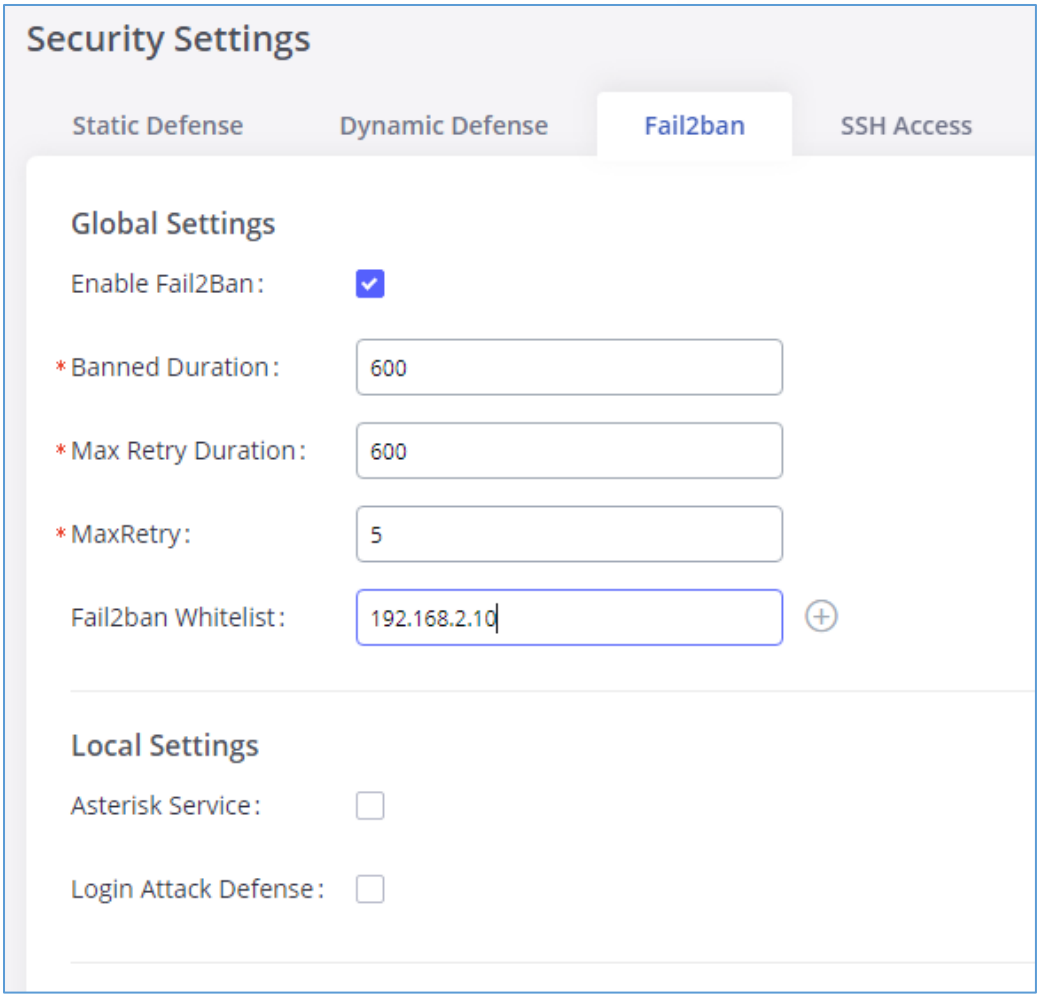


Figure 27: Fail2Ban Settings

Table 15: 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 GXW4500.
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 GXW4500.
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 GXW4500'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 GXW4500.

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 GXW4500 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.

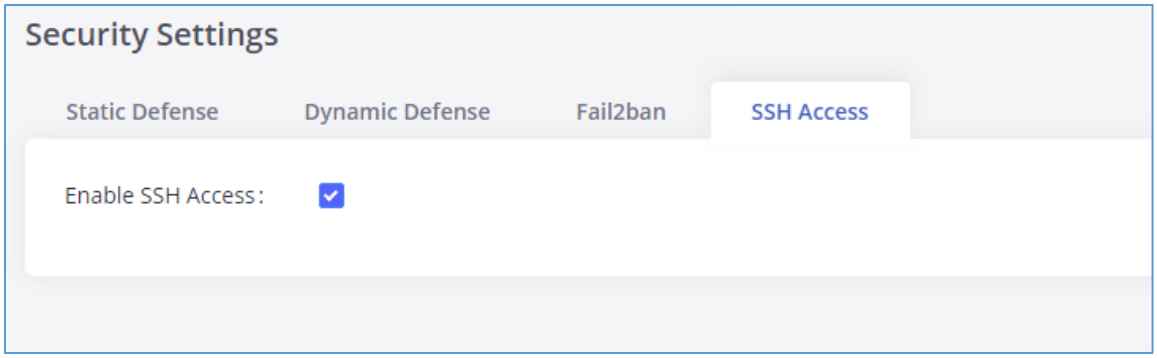


Figure 28:SSH Access

Time Settings

Automatic Date and Time

The current system time on the GXW4500 can be found under Web GUI→**System Status→Dashboard→PBX Status**.

To configure the GXW4500 to update time automatically, go to Web GUI→**System Settings→Time Settings→Automatic Date and Time**.

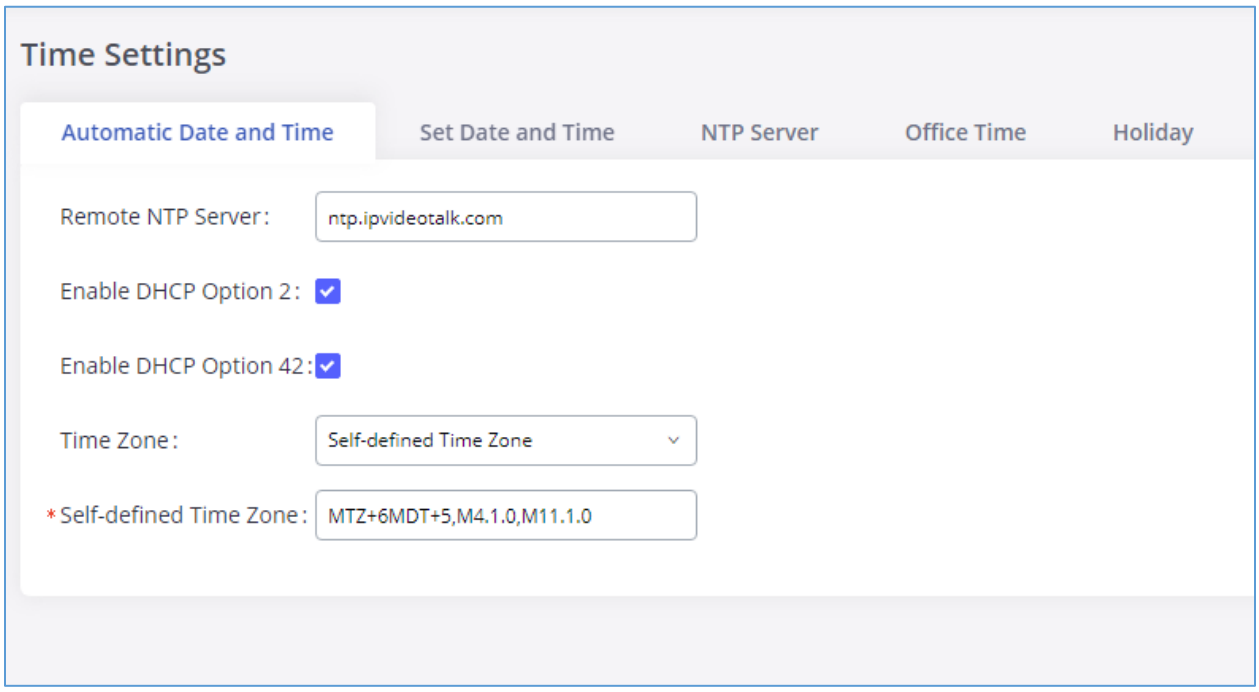


Figure 29: Automatic Date and Time Settings

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 GXW4500 for the first time to avoid service interruption after installation and deployment in production.

Table 16: Automatic Date and Time Settings

Remote NTP Server	Specify the URL or IP address of the NTP server for the GXW4500 to synchronize the date and time. The default NTP server is ntp.ipvideotalk.com.
Enable DHCP Option 2	If set to "Yes", the GXW4500 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 GXW4500 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	Select the proper time zone option so the GXW4500 can display correct time accordingly. If "Self-Defined Tome Zone" is selected, please specify the time zone parameters in "Self-Defined Time Zone" field as described in below option.
Self-Defined Time Zone	If "Self-Defined Time Zone" is selected in "Time Zone" option, users will need define their own time zone following the format below. The syntax is: std offset dst [offset], start [/time], end [/time] Default is set to: MTZ+6MDT+5,M4.1.0,M11.1.0 **MTZ+6MDT+5** 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.

	M4.1.0,M11.1.0 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.

Set Date and Time

To manually set the time on the GXW4500, go to Web GUI→**System Settings→Time Settings→Set Date and Time**. The format is YYYY-MM-DD HH:MM:SS.

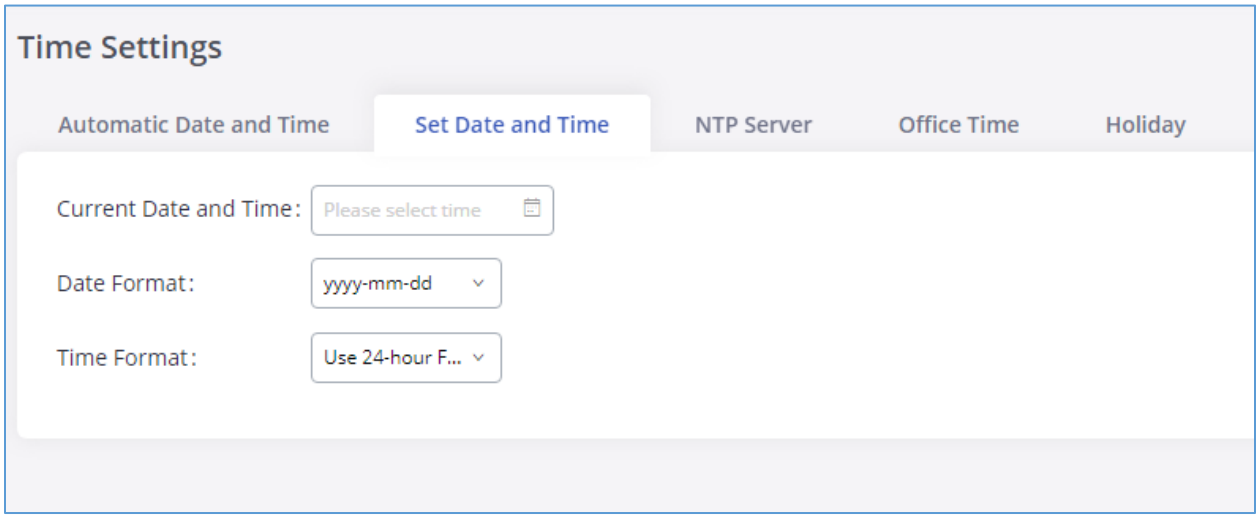


Figure 30: Date and Time Manual Configuration

Table 17: 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 GXW4500 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 GXW4500 can be used as an NTP server for the NTP clients to synchronize their time with. To configure the GXW4500 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 GXW4500 IP address or host name to use the GXW4500 as the NTP server.

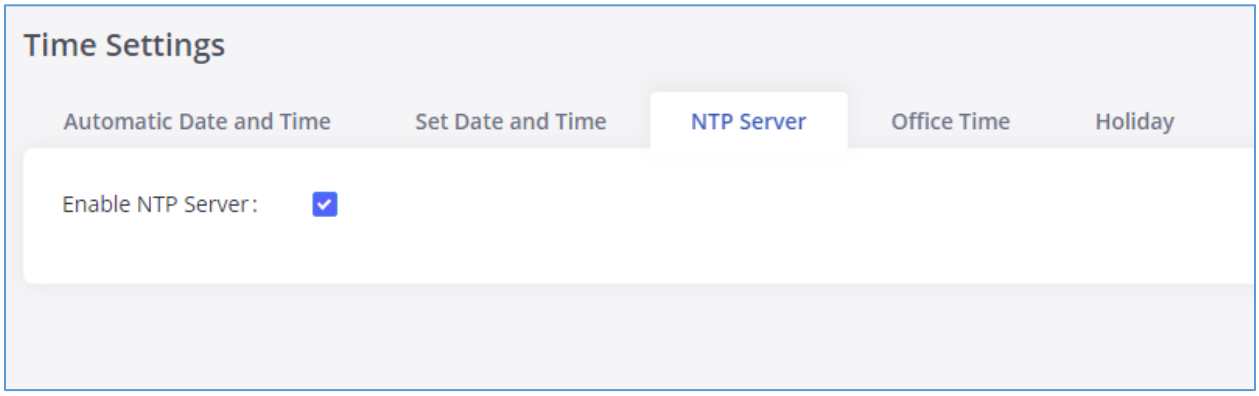


Figure 31: GXW4500 NTP Server

Office Time

On the GXW4500, 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.

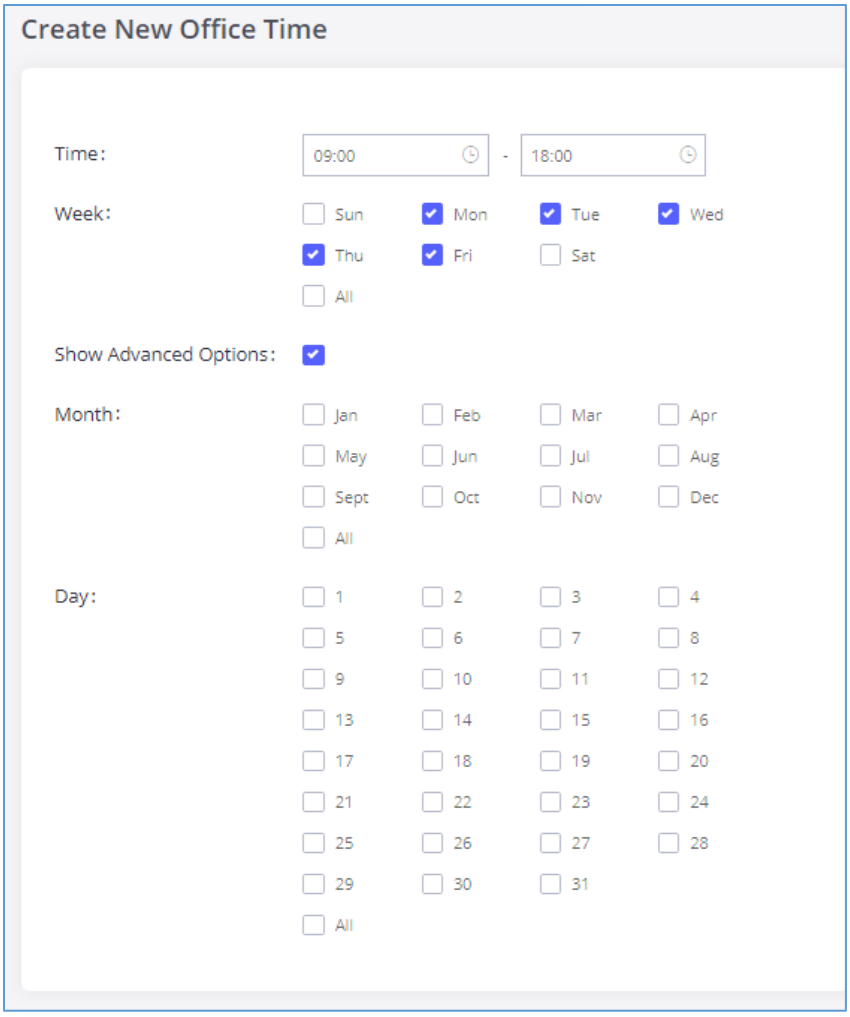


Figure 32: Add New Office Time

Table 18: 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.

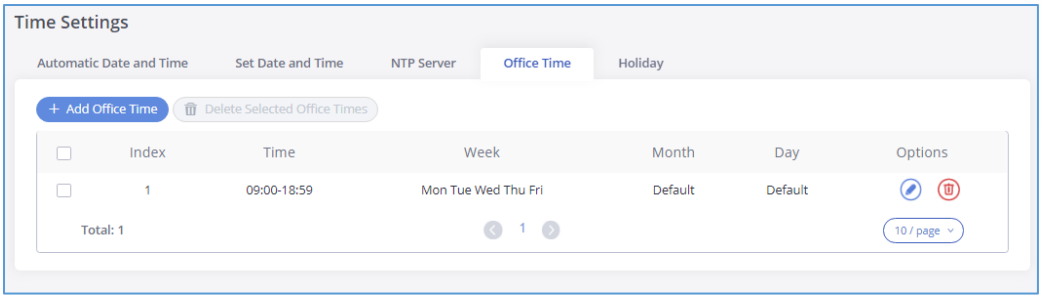


Figure 33: Time Settings→Office Time

- 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 GXW4500, 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.

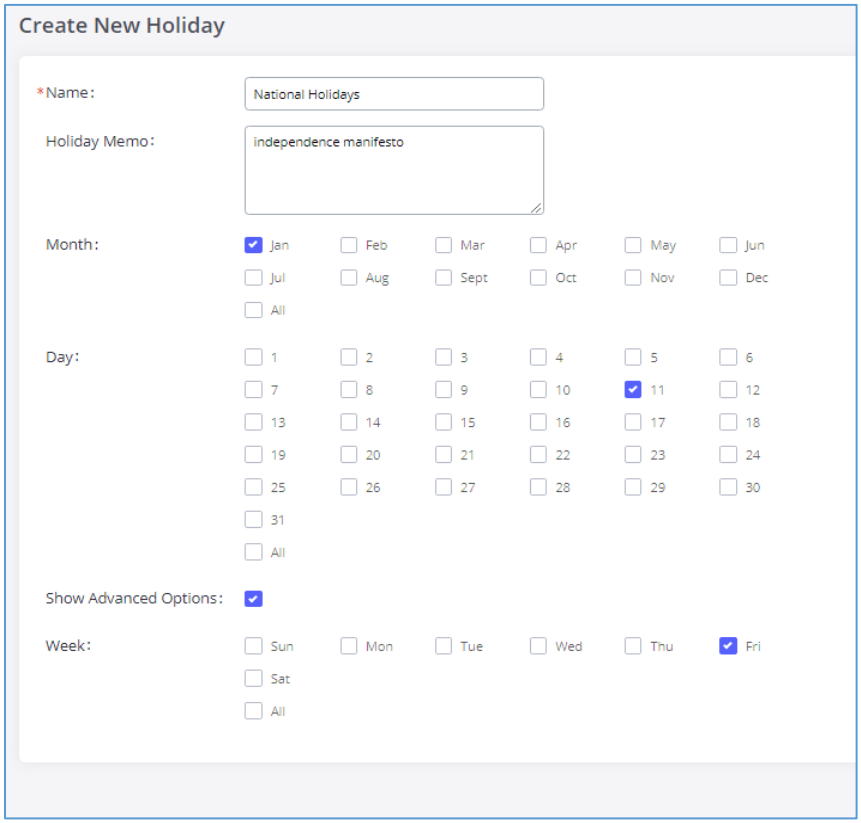


Figure 34: Add a Holiday

Table 19: 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.

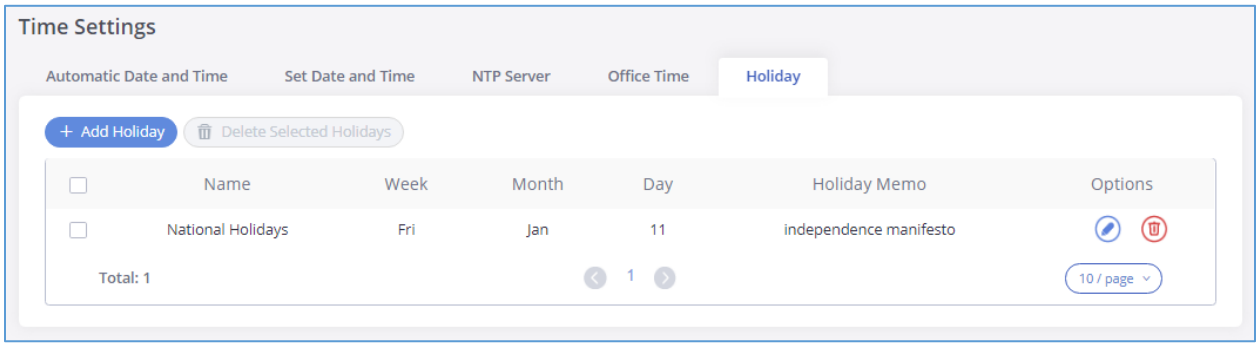


Figure 35: Time Settings→Holiday

- 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 GXW4500 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 20: Email Settings

TLS Enable	Enable or disable TLS during transferring/submitting your Email to another SMTP server. The default setting is "Yes".
Type	Select Email type. • **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, GXW4500 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 GXW4500, assuming the email is using the default SMTP server of Gmail.

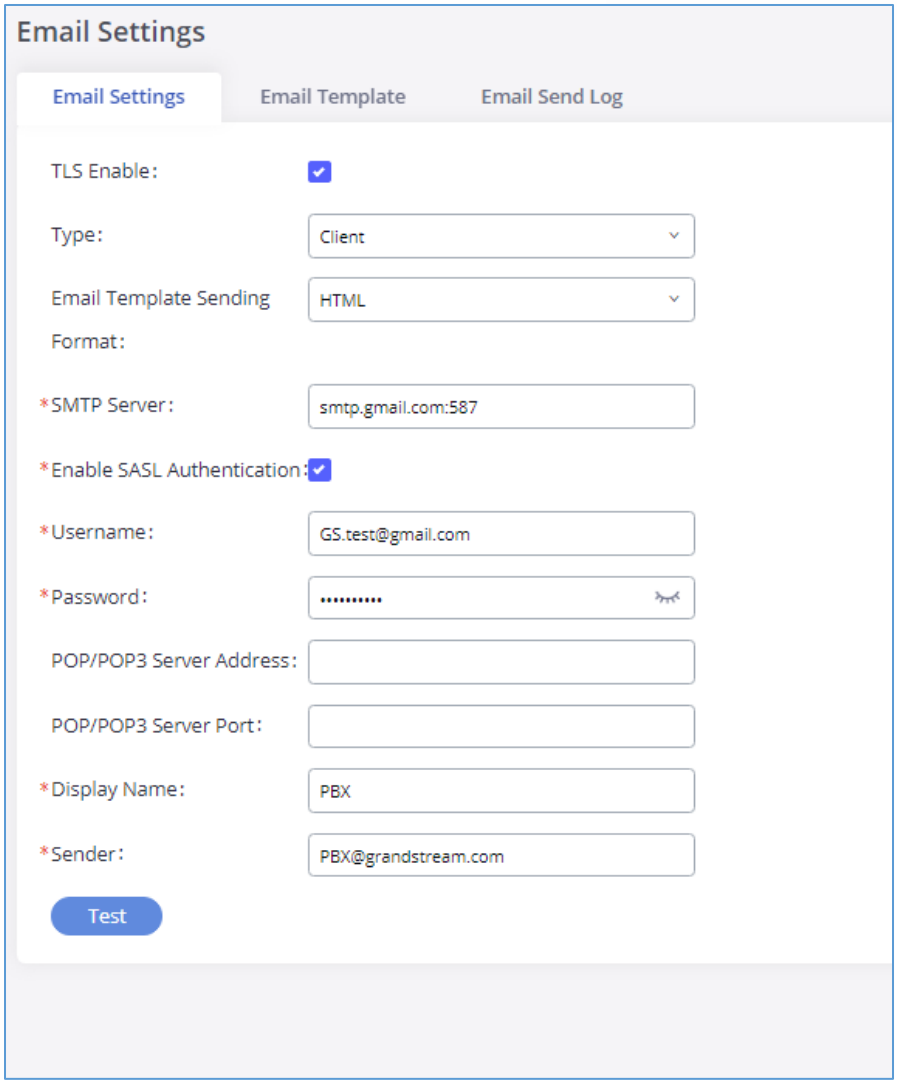


Figure 36: Email Settings

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 GXW4500.

Email Template

The Email templates on the GXW4500 can be used for email notification. The configuration parameters can be accessed via Web GUI→**System Settings**→**Email Settings**→**Email Templates**.

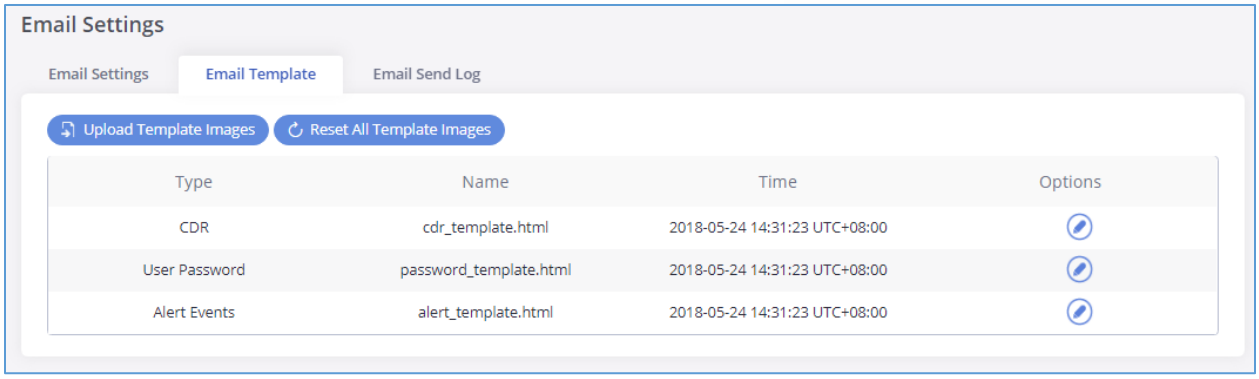


Figure 37: Email Templates

- Press on Upload Template Images to upload pictures to be used on email templates.
- Press Reset All Template Images 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.

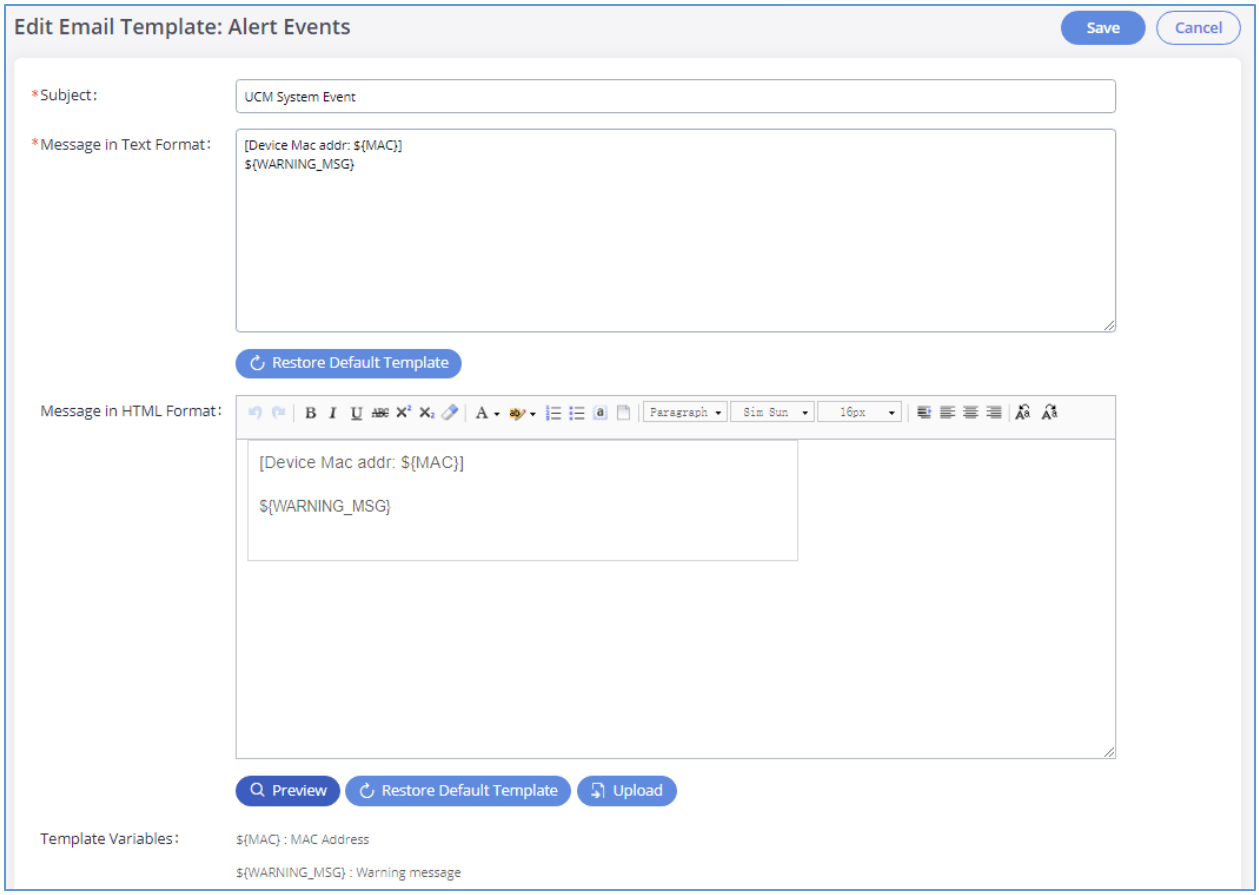


Figure 38: Alert Events Template

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

Email Send Log

Under GXW4500 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.

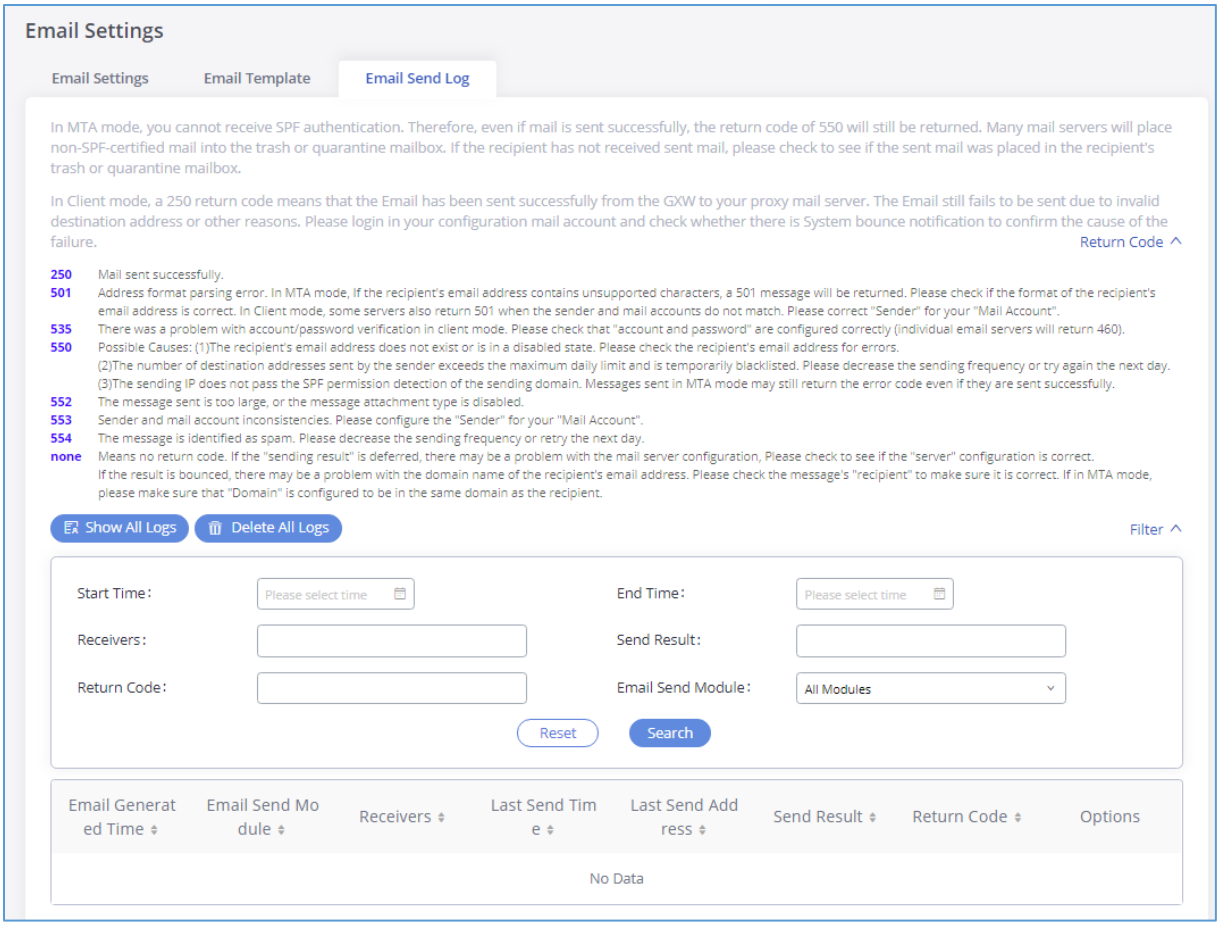


Figure 39: Email Send Log

Table 21: 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 then 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

GXW4500 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 GXW4500 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. GXW4500 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 GXW4500:

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:

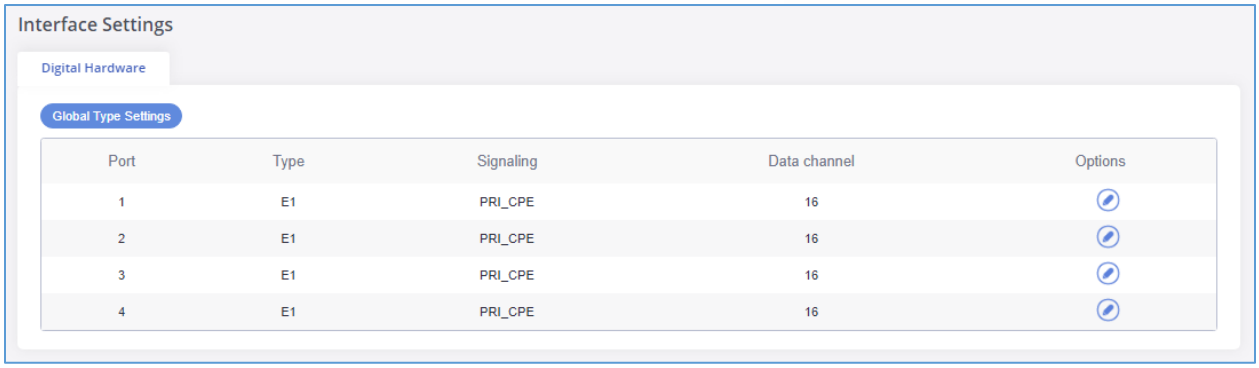


Figure 40: Digital Hardware Configuration

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

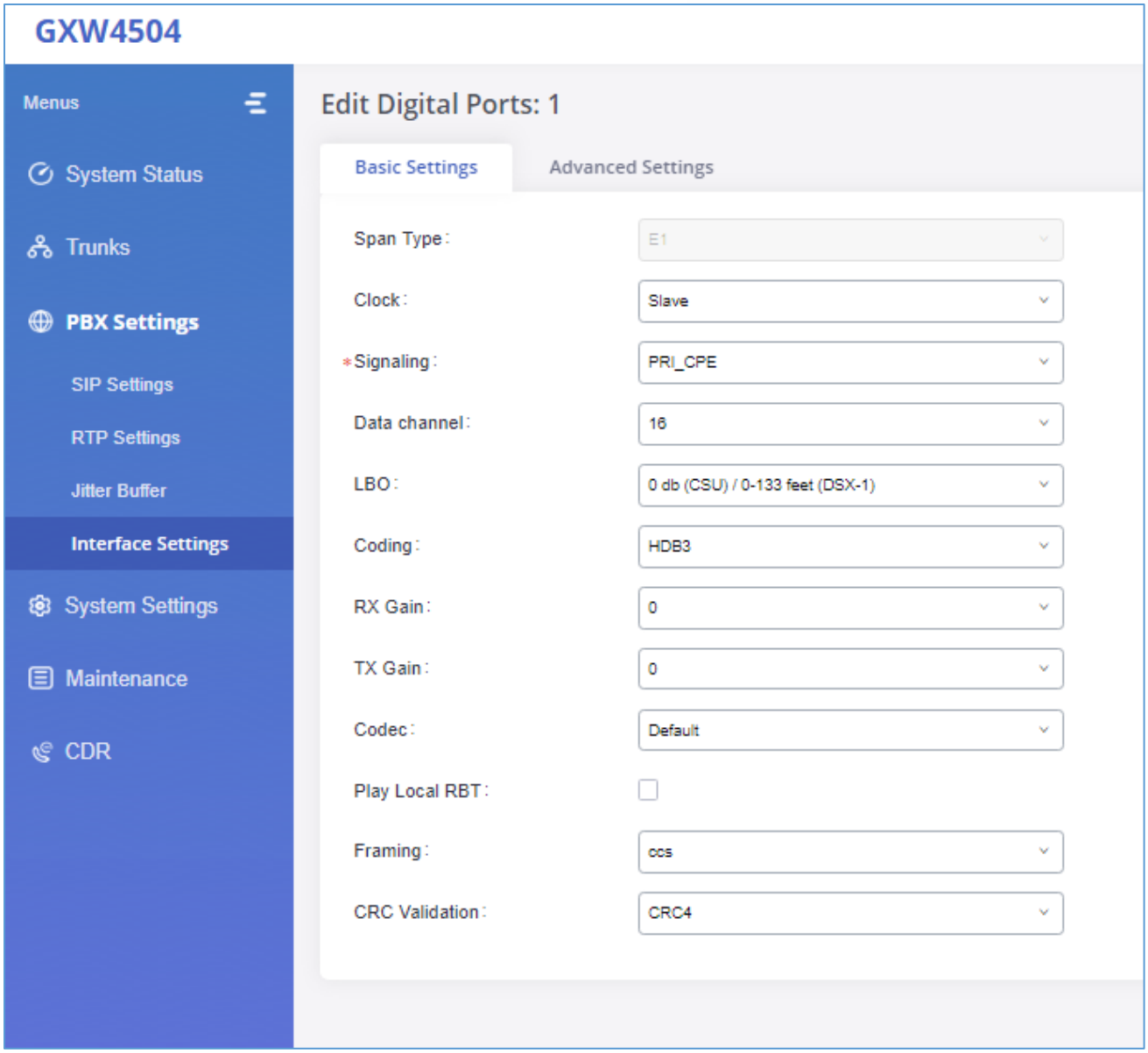


Figure 41: Digital Port Configuration

The GXW4500 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 22: Digital Hardware Configuration Parameters: E1 – PRI_NET/PRI_CPE

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. • **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	Chooses the signaling protocol that will be used on the digital port. PRI: when one end is set to NET, the other end should be set to CPE
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	T1:"AMI" or "B8ZS" E1:"AMI" or "HDB3"
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.
Play Local RBT	This configured whether to play the ringback tone from local GXW4500 or not. If enabled, the local GXW4500 will play ringback tone to the caller. Otherwise, the caller will listen to the tone from peer device. The default setting is disabled.
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	
Switch Type	Select switch type. • **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	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". **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.
PRI Local Dial Plan	This setting is used to specify the type of the caller number. The service provider will usually verify this.
International Prefix **National Prefix** **Local Prefix** **Private Prefix** **Unknown Prefix**	Configure the prefix in PRI Local Dial Plan and PRI Dial Plan for each type.
PRI T310	Configure PRI T310 Timer (in seconds). The default value is 10 seconds.
PRI Indication	Select the PRI Indication. • **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 ChannelD 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 23: Digital Hardware Configuration Parameters: E1 - SS7

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. • **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	Chooses the signaling protocol that will be used on the digital port. PRI: when one end is set to NET, the other end should be set to CPE
Data channel	Chooses the Data Channel for control.
SS7 Variant	Select ITU, ANSI or CHINA.

Originating Point Code	Originating point code is used to identify the node originating the message, always provided by the operator/ISP. • ITU Format: decimal number. • ANSI & CHINA Format: decimal number or XXX-XXX-XXX.
Destination Point Code	Destination point code is the address to send the message to, always be provided by the operator/ISP. • ITU Format: decimal number. • ANSI & CHINA Format: decimal number or XXX-XXX-XXX.
First CIC	When Span Type is E1, ITU & CHINA Range: [0, 4065], ANSI Range: [0, 16353]. When Span Type is T1/J1, ITU & CHINA Range: [0, 4072], ANSI Range: [0, 16360].
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	T1:"AMI" or "B8ZS" E1:"AMI" or "HDB3"
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 24: 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. • **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	Chooses the signaling protocol that will be used on the digital port. PRI: when one end is set to NET, the other end should be set to CPE
Data channel	Chooses the Data Channel for control.
Variant	MFC/R2 multinational adaption. GXW4500 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	If enabled, the callee side will request the caller to send caller number first and then called number. **Note:** Options "Get ANI First" and "Skip Category" cannot be enabled at the same time.
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	T1:"AMI" or "B8ZS" E1:"AMI" or "HDB3"
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.
Play Local RBT	This configured whether to play the ringback tone from local GXW4500 or not. If enabled, the local GXW4500 will play ringback tone to the caller. Otherwise, the caller will listen to the tone from peer device. The default setting is disabled.

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 25: Digital Hardware Configuration Parameters: T1/J1 - PRI_NET/PRI_CPE

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. • **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	Chooses the signaling protocol that will be used on the digital port. PRI: when one end is set to NET, the other end should be set to CPE
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	T1:"AMI" or "B8ZS" E1:"AMI" or "HDB3"
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.
Play Local RBT	This configured whether to play the ringback tone from local GXW4500 or not. If enabled, the local GXW4500 will play ringback tone to the caller. Otherwise, the caller will listen to the tone from peer device. The default setting is disabled.
Framing	Select “esf” or “d4”. Default setting is esf.

Advanced Settings	
Switch Type	Select switch type. • **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	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". **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.
PRI Local Dial Plan	This setting is used to specify the type of the caller number. The service provider will usually verify this.
International Prefix **National Prefix** **Local Prefix** **Private Prefix** **Unknown Prefix**	Configure the prefix in PRI Local Dial Plan and PRI Dial Plan for each type.
PRI T310	Configure PRI T310 Timer (in seconds). The default value is 10 seconds.
PRI Indication	Select the PRI Indication. • **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", "accunet".

Table 26: Digital Hardware Configuration Parameters: T1/J1 - SS7

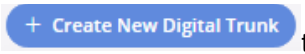
Basic Settings	
Clock	All E1/T1/J1 spans generate a clock signal on their transmit side. The parameter determines whether the clock signal from the far end of the E1/T1/J1 is used as the master source of clock timing. If the far end is used as the master, the gateway system clock will synchronize to it. • **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	Chooses the signaling protocol that will be used on the digital port. PRI: when one end is set to NET, the other end should be set to CPE

Data channel	Chooses the Data Channel for control.
SS7 Variant	Select ITU, ANSI or CHINA.
Originating Point Code	Originating point code is used to identify the node originating the message, always provided by the operator/ISP. • ITU Format: decimal number. • ANSI & CHINA Format: decimal number or XXX-XXX-XXX.
Destination Point Code	Destination point code is the address to send the message to, always be provided by the operator/ISP. • ITU Format: decimal number. • ANSI & CHINA Format: decimal number or XXX-XXX-XXX.
First CIC	When Span Type is E1, ITU & CHINA Range: [0, 4065], ANSI Range: [0, 16353]. When Span Type is T1/J1, ITU & CHINA Range: [0,4072], ANSI Range: [0, 16360].
Assign CIC to D-Channel	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.
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	T1:"AMI" or "B8ZS" E1:"AMI" or "HDB3"
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	
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 27: 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	This is to implement Digital trunk outbound line selection strategy. Three options are available: • **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…, 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). The default setting is "Ascend" mode.

Digital Trunk Troubleshooting

After configuring the digital trunk on the GXW4500 as described above, if it doesn't work as expected, users can go to capture signaling trace on the GXW4500 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.

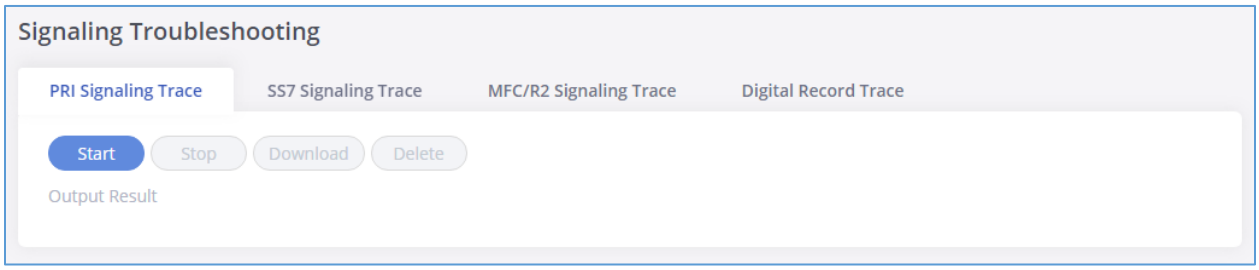


Figure 42: Troubleshooting Digital Trunks

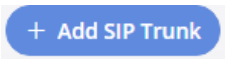
After capturing the trace, users can download it for basic analysis. Or you can contact Grandstream Technical support in the following link for further assistance if the issue is not resolved:

http://www.grandstream.com/support

VoIP Trunks

The VoIP trunks allow the GXW4500 to be connected over an IP network via SIP protocol to a VoIP provider or to another device that supports the SIP trunking.

VoIP trunks can be configured in GXW4500 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 28: Create New 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 SIP trunk is disabled, GXW4500 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.
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. **Important Note:** When making outgoing calls, the following priority order rule will be used to determine which CallerID will be set before sending out the call: From user (Register Trunk Only) → CID from inbound call (***Keep Original CID*** Enabled) → Trunk Username/CallerID (***Keep Trunk CID*** Enabled) → DOD→ Trunk Username/CallerID (***Keep Trunk CID*** Disabled) → Global Outbound CID.
CallerID Name	Configure the name of the caller.
From Domain	Configure the actual domain name. This can be used to override the "From" Header. For example, "trunk.GXW4500.provider.com" is the From Domain in From Header: sip: 1234567@trunk.GXW4500.provider.com.
Transport	Configure the SIP transport protocol to be used in this trunk. UDP; TCP or TLS. The default setting is "UDP"

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 29: SIP Trunk Configuration Parameters

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, GXW4500 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.
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.
From Domain	Configure the actual domain name. This can be used to override the "From" Header. For example, "trunk.GXW4500.provider.com" is the From Domain in From Header: sip:1234567@trunk.GXW4500.provider.com.
Transport	Configure the SIP transport protocol to be used in this trunk. The default setting is "UDP". • UDP • TCP • TLS

Advanced Settings	
Codec Preference	Select audio and video codec for the VoIP trunk. The available codecs are: PCMU, PCMA, GSM, AAL2-G.726-32, G.726, G.722, G.729, G.723, OPUS, ILBC, ADPCM, H.264, H.265, H.263, H.263p.
Send PPI Header	If checked, the invite message sent to trunks will contain PPI (P-Preferred-Identity) Header.
Send PAI Header	If checked, the invite message sent to trunks will contain PAI (P-Asserted-Identity) Header. It is not possible to send both PPI and PAI Headers.
Passthrough PAI Header	If enabled and "Send PAI Header" is disabled, PAI headers will be preserved as calls pass through the gateway.
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	Configure the default DTMF mode when sending DTMF on this trunk. • **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 GXW4500 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. The default setting is "No".

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

On the GXW4500, the outbound route priority is based on “Best matching pattern”. For example, the GXW4500 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 GXW4500 will use the first pattern matched.

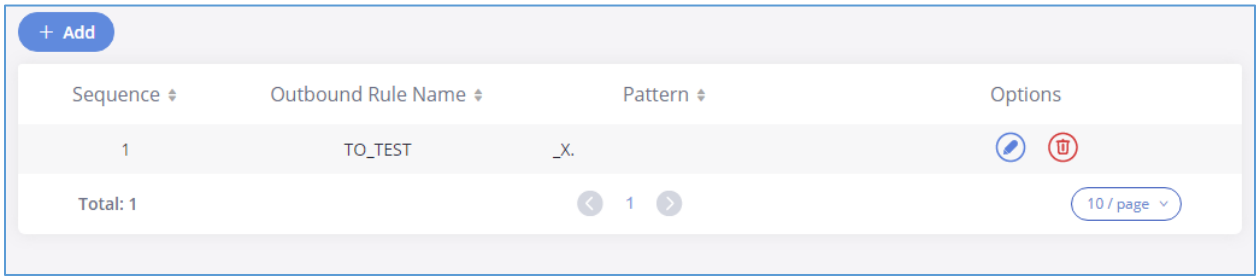


Figure 43: Create Outbound Route

Calling Rule Name	Configure the name of the calling rule (e.g., local, long-distance, and etc). Letters, digits, _ and - are allowed.
Pattern	• 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. ▪ Users can add comments to the end of patterns to better organize and keep track of complex rules by typing "**/***" and "***/**" before and after each comment respectively. ▪ Example: _X. _NNXXNXXXXX /* 10-digit long distance */ _818X. /* Any number with leading 818 */
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. Example: 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.
Prepend	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.
Use Failover Trunk	
Trunk	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.

	GXW4500 support up to 10 failover trunks. Example: 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.
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. Example: 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.
Prepend	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.
Time Condition	
Time Condition Mode	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. 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.
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 GXW4500 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 GXW4500 on any trunk based on the patter 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 + Add button to add a new inbound route.
- Click on Import To import inbound routes.
- Click on Export to export inbound routes.
- Click on to edit the inbound route.
- Click on to delete the inbound route

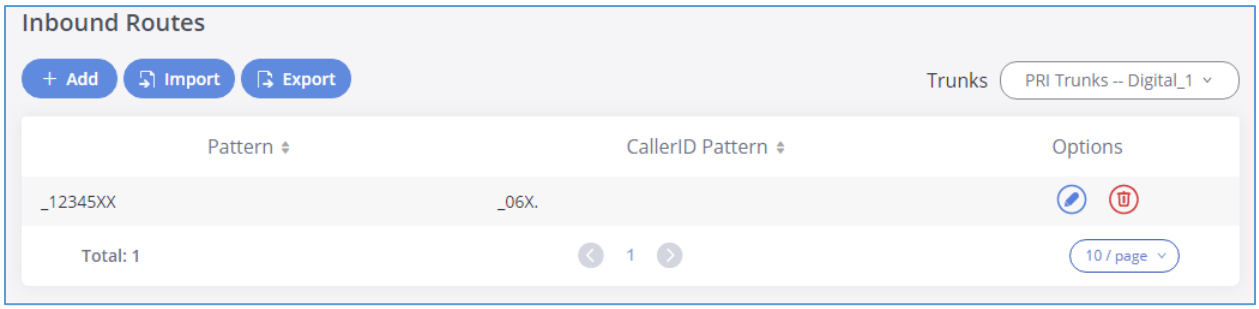


Figure 44: Create Inbound Routes

Inbound Route Configuration

Table 30: Inbound Rule Configuration Parameters

Trunks	Select the trunk to configure the inbound rule.
Pattern	• 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.

<table>
<tr><td></td><td>

Users can add comments to the end of patterns to better organize and keep track of complex rules by typing “/*” and “*/” before and after each comment respectively.
Example:
<table>
<tr><th>Pattern</th><th>CallerID Pattern</th></tr>
<tr><td>_X.
_NNXXNXXXXX /* 10-digit long distance */
_818X. /* Any number with leading 818 */</td><td>1000
1001</td></tr>
</table>

</td></tr>
<tr><td>CallerID Pattern</td><td>All patterns are prefixed by "_" character, but please do not enter more than one "_" at the beginning. All patterns can add comments, such as "_pattren /* comment */". 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.</td></tr>
</table>

Inbound Route: Import/Export Inbound Route

Users can import and export inbound routes to quickly set up inbound routing on a GXW4500 or to back up an existing configuration. An exported inbound route configuration can be directly imported without needing any manual modifications.

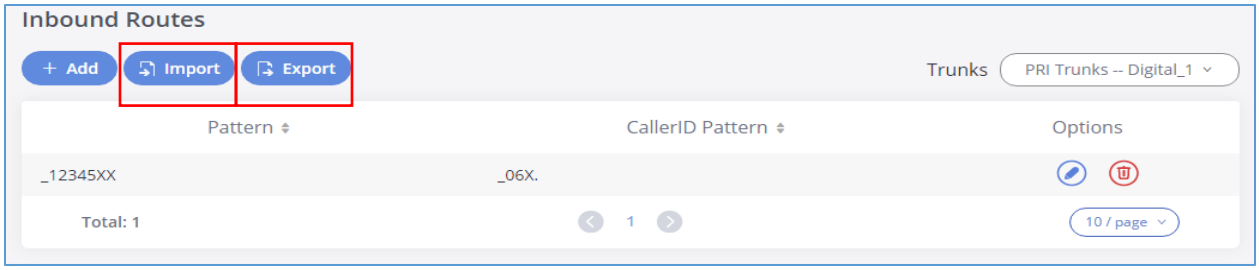


Figure 45: Import/Export Inbound Route

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 GXW4500, 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 GXW4500 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. The default port used is 5060

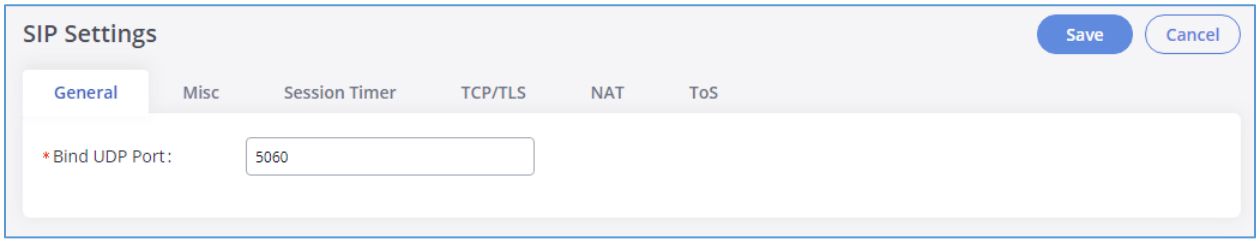


Figure 46: SIP Settings/General

Misc

On this Web page users can define the DNS mode used by the GXW4500. This setting only affects the DNS queries that occurs when making calls.

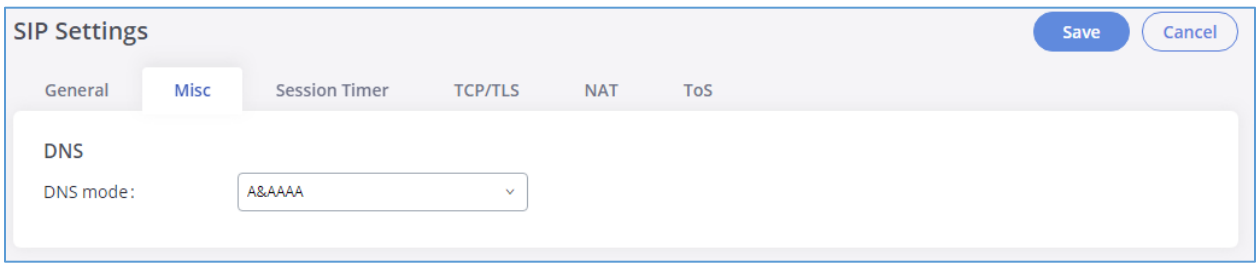


Figure 47: SIP Settings/Misc

Session Timer

Table 31: SIP Settings/Session Timer

Force Timer	If checked, always request and run session timer.
Timer	If checked, run session timer only when requested by another UA.
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 32: SIP Settings/TCP and TLS

TCP Enable	Configure to allow incoming TCP connections with the GXW4500. 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.
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, [2001:0DB8:0000:0000:0000:0000:1428:0000]:5060.
TLS Enable	Configure to allow incoming TLS connections with the GXW4500. 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. **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, [2001:0DB8:0000:0000:0000:0000:1428:0000]: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.
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 33: NAT Settings

External Host	Configure a static IP address and port (optional) used in outbound SIP messages if the GXW4500 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.
External UDP Port	Configure the externally mapped UDP port when the GXW4500 is behind a static NAT or PAT.
External TCP Port	Configure the externally mapped TCP port when the GXW4500 is behind a static NAT or PAT.
External TLS Port	Configures the externally mapped TLS port when GXW4500 is behind a static NAT or PAT.
Local Network Address	Specify 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. A sample configuration could be as follows: 192.168.0.0/16

ToS

Table 34: 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.
Default Incoming/Outgoing Registration Time	Configure the default duration (in seconds) of incoming/outgoing registration. The default setting is 120.
Send Compact SIP Headers	If enabled, compact SIP headers will be sent. The default setting is "No".
Enable Relaxed DTMF	Select to enable relaxed DTMF handling. The default setting is "No".

DTMF Mode	Select DTMF mode to send DTMF. The default setting is RFC2833. If "Info" is selected, SIP INFO message will be used. If "Inband" is selected, 64-kbit codec PCMU and PCMA are required. When "Auto" is selected, "RFC2833" will be used if offered, otherwise "Inband" will be used. The default setting is "RFC2833".
100rel	Configure the 100rel setting on GXW4500. The default setting is “Yes”.
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	Configure whether the GXW4500 should generate inband ringing or not. The default setting is "Never". • **Yes:** The GXW4500 will send 180 Ringing followed by 183 Session Progress and in-band audio. • **No:** The GXW4500 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 GXW4500 will send 180 Ringing as long as 200OK has not been set yet. Inband ringing will not be generated even the end point device is not working properly.
Server User Agent	Configure the user agent string for the GXW4500.

RTP Settings

RTP Settings

Table 35: 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".
ICE Support	Configure whether to support ICE, ICE is the integrated use of STUN and TURN structure to provide reliable VoIP or video calls and media transmission, via a SIP request/ response model or multiple candidate endpoints exchanging IP addresses and ports, such as private addresses and TURN server address. It is enabled by default.
STUN Server	Configure STUN server address, STUN protocol is a Client / Server – is also a Request / Response protocol, where it is used to check the connectivity between the two terminals, such as maintaining NAT binding entries keep alive agreement. The default STUN Server is stun.ipvideotalk.com Valid format: **[(hostname | IP-address) [':' port]** The default port number is 3478 if not specified.
TURN Server	Configure TURN server address. TURN is an enhanced version of the STUN protocol and is dedicated to the processing of symmetric NAT problems.
TURN Server Name	Configure turn server account name.
TURN Server Password	Configure turn server account password.

Payload Type Settings

The GXW4500 payload type for audio codecs can be configured here.

Table 36: Payload Type Configuration

AAL2-G.726	Configure payload type for ADPCM (G.726, 32kbps, AAL2 codeword packing). The default setting is 112.
DTMF	Configured payload type for DTMF. 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 default setting is 97.

- 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 GXW4500 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 GXW4500 already. The other languages provided by Grandstream can be downloaded and installed from the GXW4500 Web GUI directly. Additionally, users could customize their own voice prompts, package them and upload to the GXW4500.

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 GXW4500 Web GUI, click on Check Prompt List button.

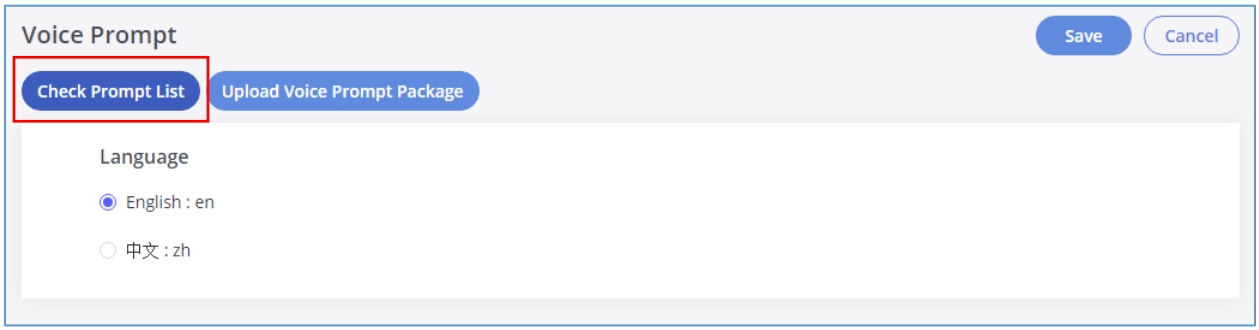


Figure 48: Language Settings for Voice Prompt

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

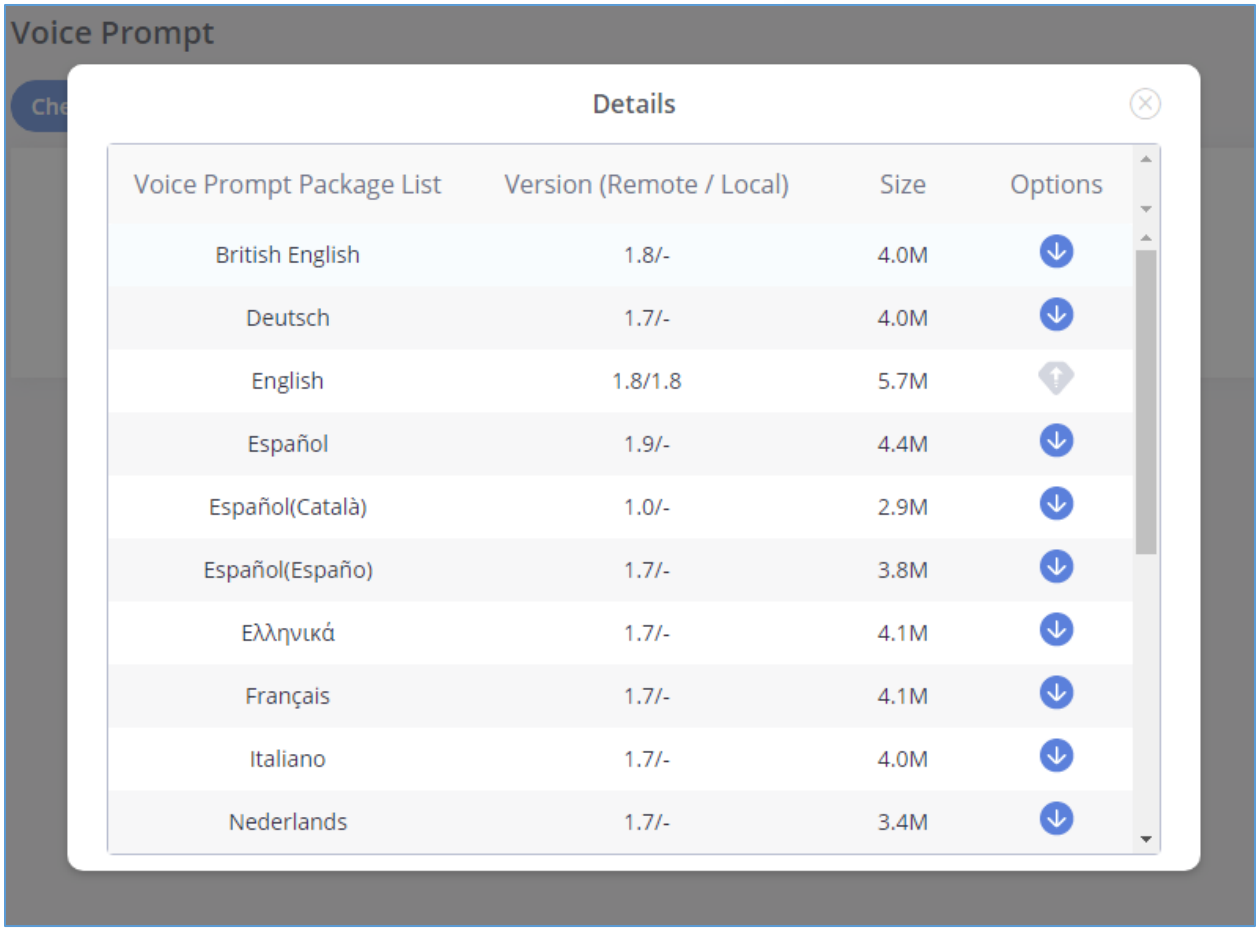


Figure 49: Voice Prompt Package List

Click on to download the language to the GXW4500. The installation will be automatically started once the downloading is finished.

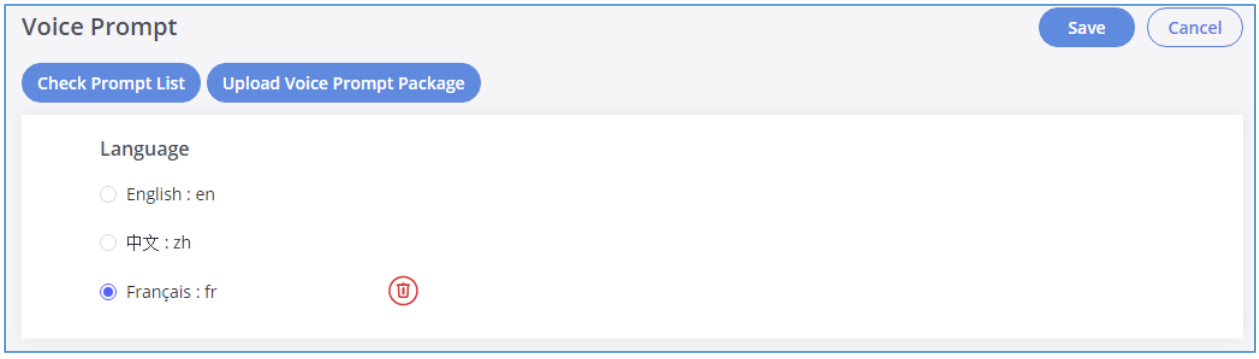


Figure 50: New Voice Prompt Language Added

A new language option will be displayed after successfully installed. Users then could select it to apply in the GXW4500 system voice prompt or delete it from the GXW4500

Manual Upload of Prompt Package

Users can upload the prompt package manually to the GXW4500. 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 GXW4500, press the Upload Voice Prompt Package button and brows the prompt package.

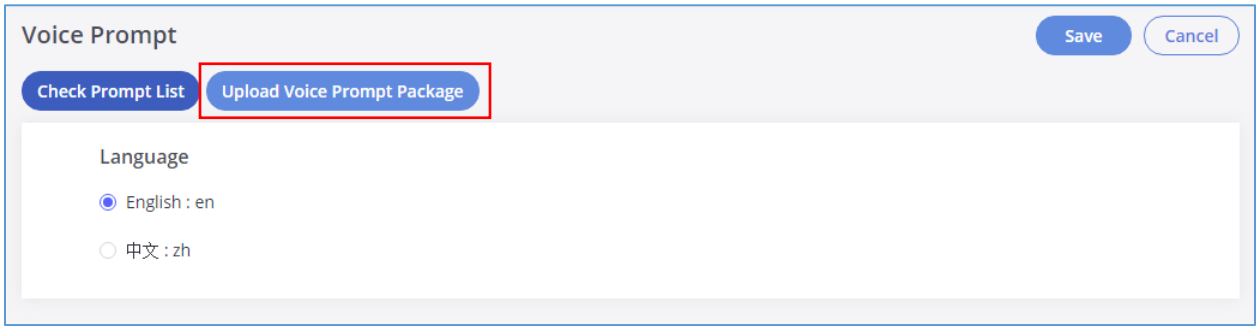


Figure 51: Upload Voice prompt Package

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 37: Jitter Buffer Settings

SIP Jitter Buffer	
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	Configure the jitter buffer implementation on the sending side of a SIP channel. The default setting is "Fixed". • **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 200.

MAINTENANCE

The Maintenance section lists different tools to help troubleshooting the issues that might be encountered while using the GXW4500 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 GXW4500 Web GUI.

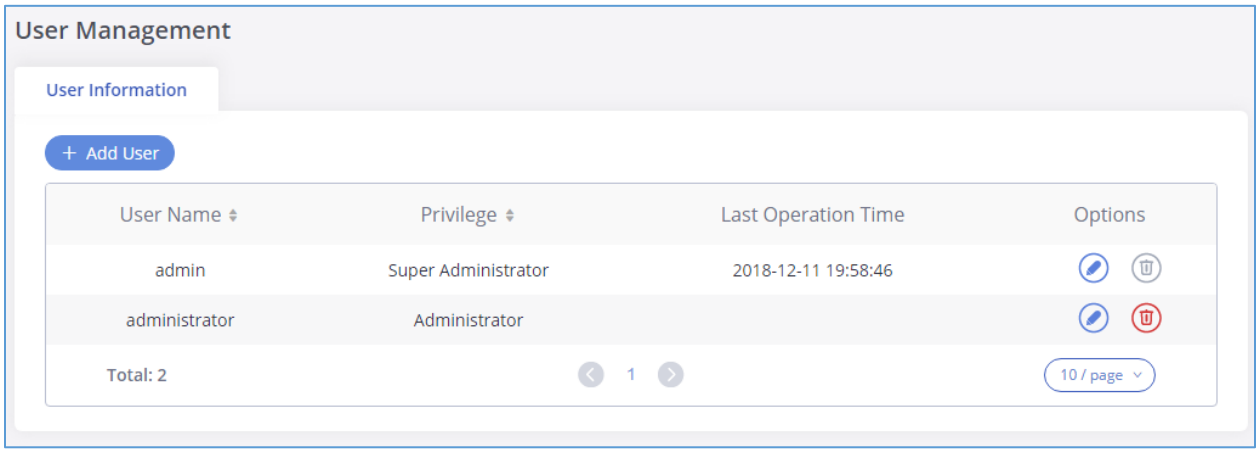


Figure 52: User Management Page Display

- Click on + Add User To add a user
- Click on to edit the user
- Click on to delete the user

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

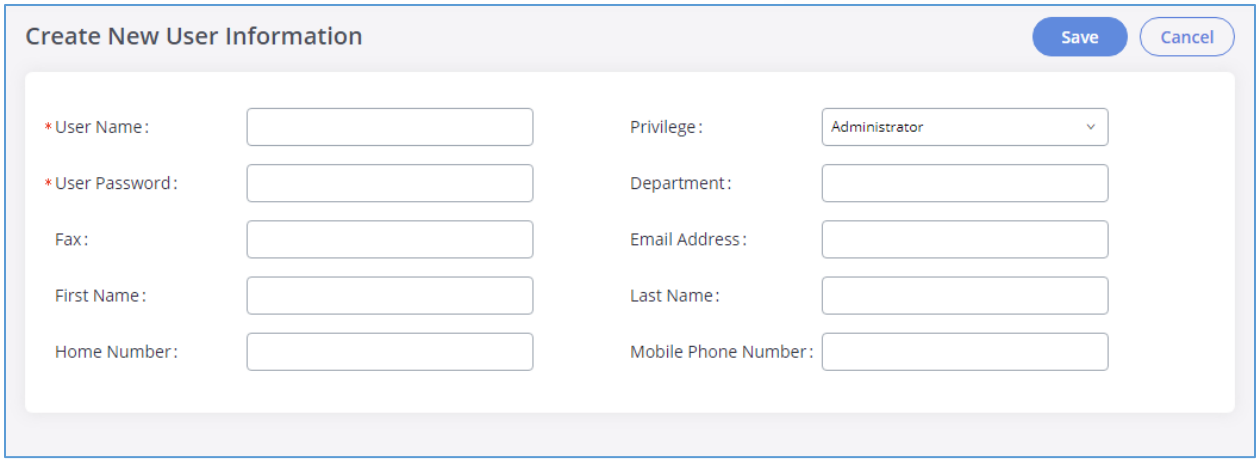


Figure 53: Create New User

Table 38: 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

After logging in the Web GUI for the first time, it is highly recommended for users to change the default password “admin” to a more complicated password for security purposes. 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.

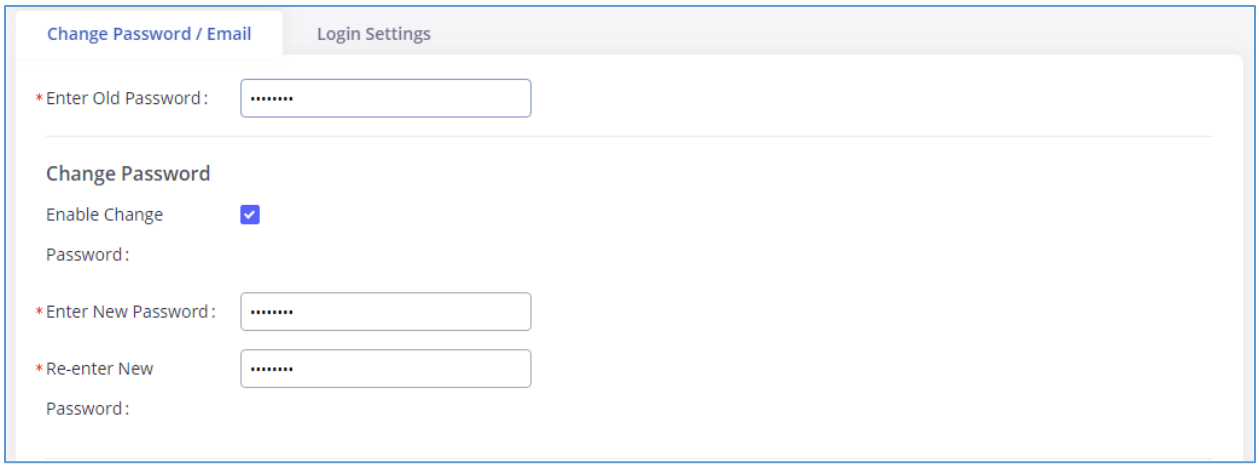


Figure 54: Change Password

Table 39: Change Password Parameters

Enter Old Password	Enter the old Password for GXW4500
Enable Change Password	When enabled, the fields to enter the new password will be displayed
Enter New Password	Enter the New Password for GXW4500
Re-enter New Password	Retype the New Password for GXW4500

Change Binding Email

GXW4500 allows user to configure binding email in case login password is lost. GXW4500 login credential will be sent to the designated email address. The feature can be found under Web GUI→**Maintenance→Change Information→Change Binding Email**.

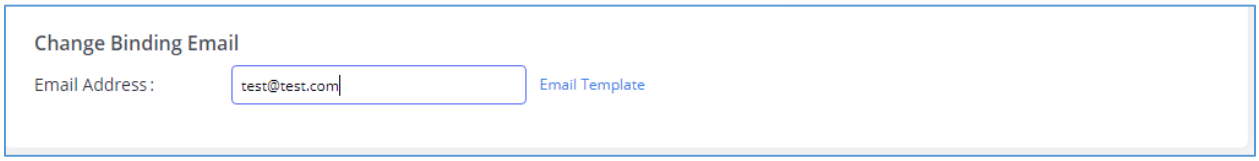


Figure 55: Change Binding Email

Login Settings

After the user logs in the GXW4500 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 GXW4500 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 GXW4500 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.

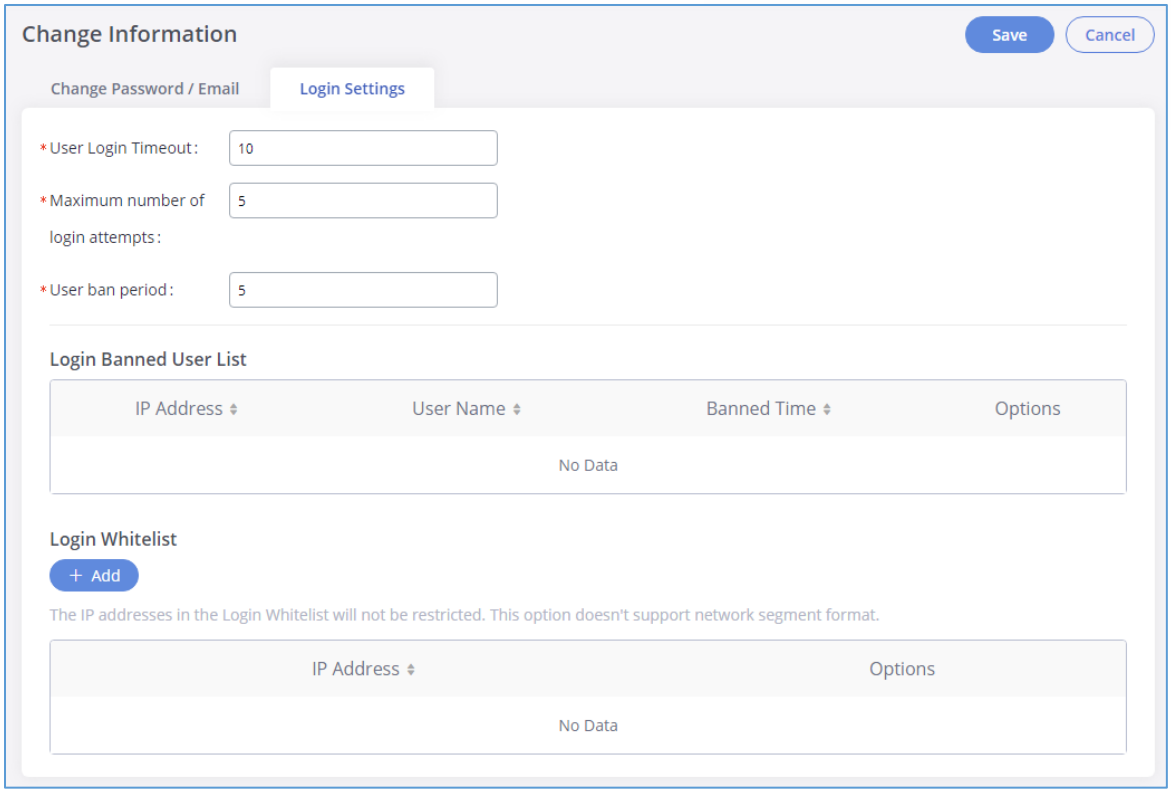


Figure 56: Login Timeout Settings

Operation Log

The admin has the authority to view operation logs on GXW4500 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”.

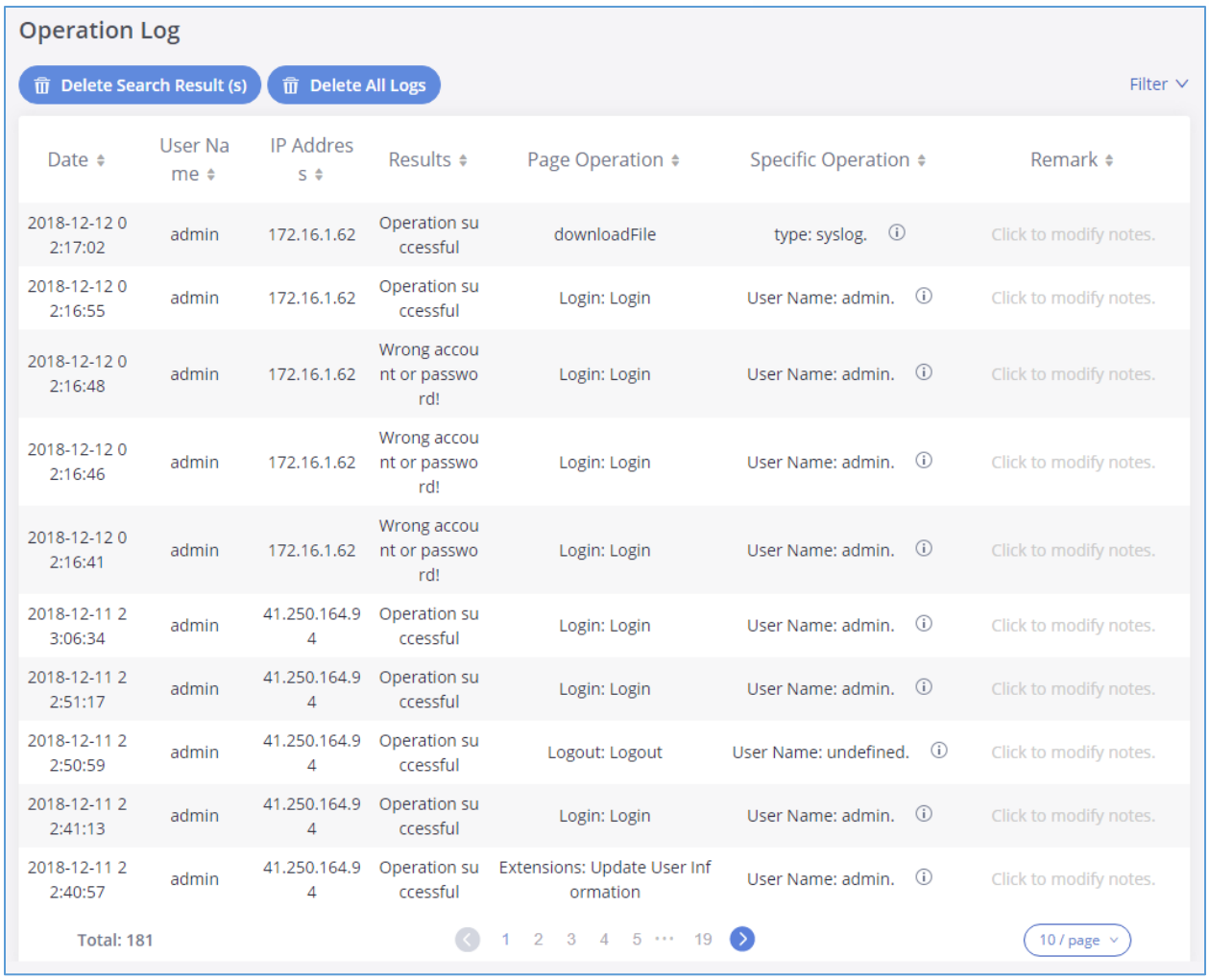


Figure 57: Operation Logs

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 40: 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 Filter and configure the conditions then click on Search.

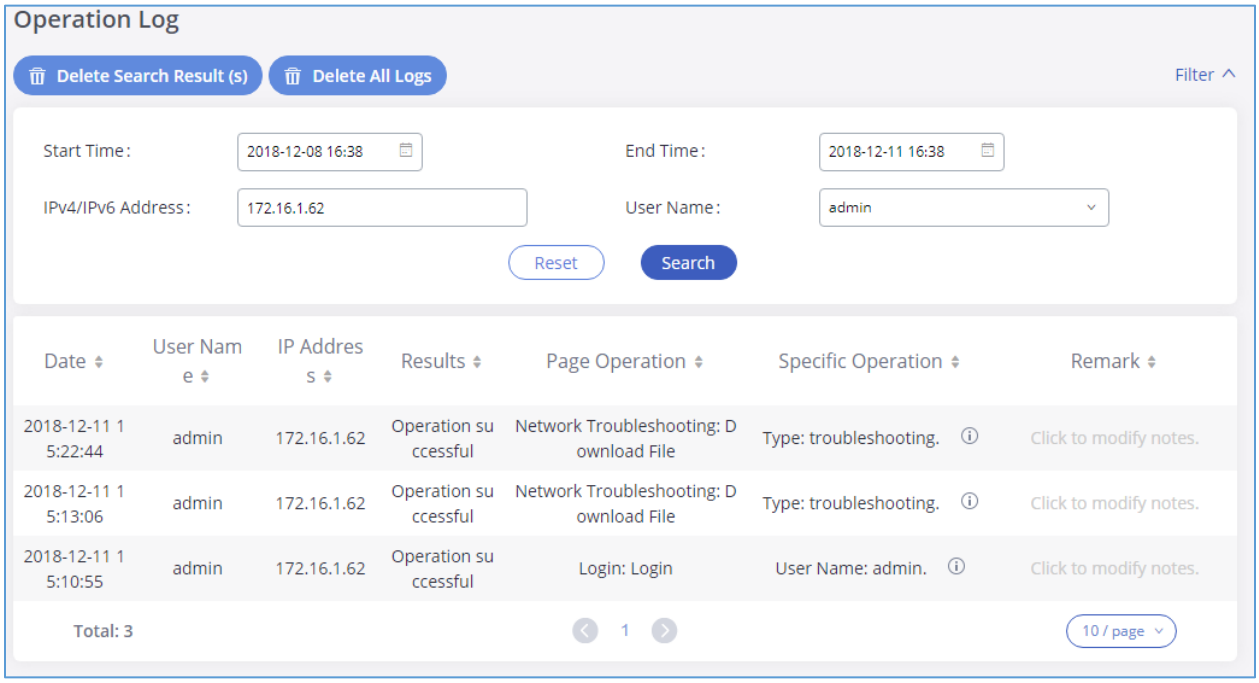


Figure 58: Operation Logs Filter

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 Delete Search Result (s) to delete the filtered result of operation logs. Or users can click on Delete All Logs to delete all operation logs at once.

Syslog

On the GXW4500, 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 GXW4500 settings because it can be helpful to locate the issues when errors happen.

Some typical modules for GXW4500 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).

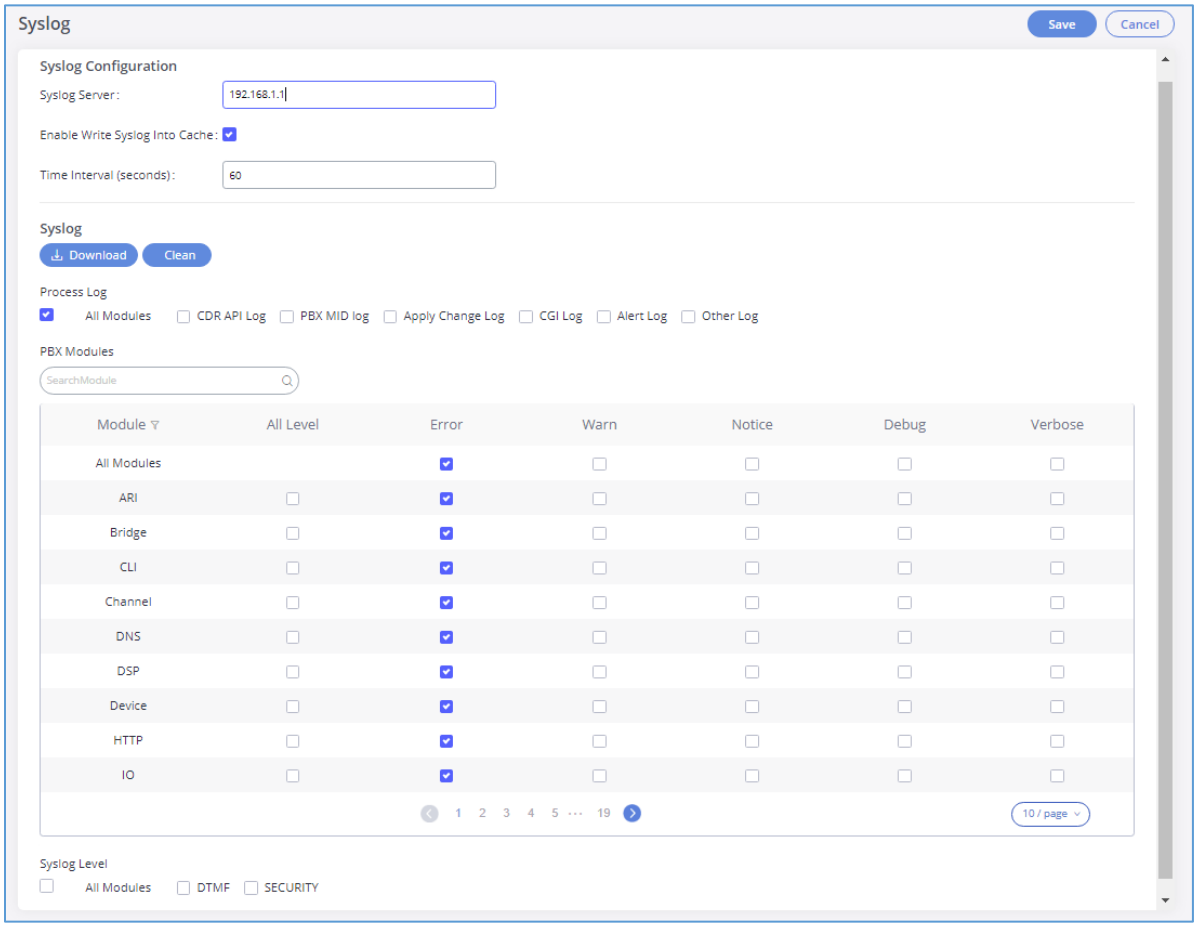


Figure 59: Syslog Settings

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 GXW4500 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.

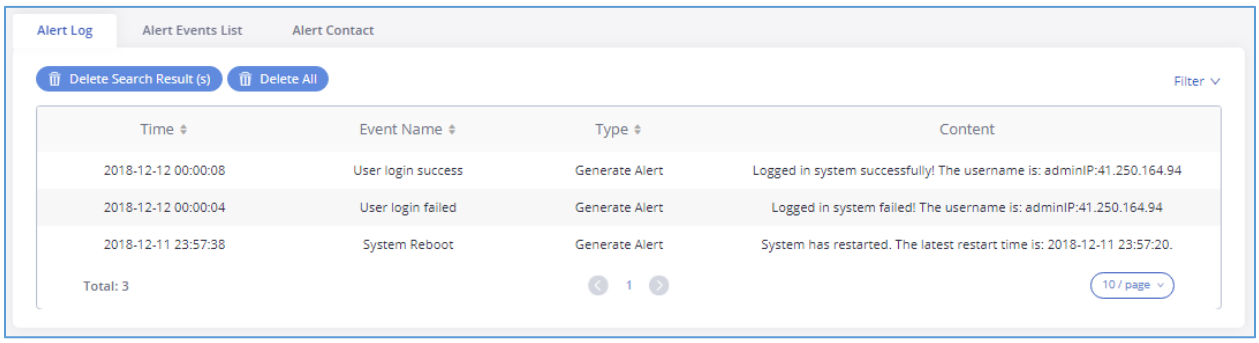


Figure 60: System Events→Alert Log

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

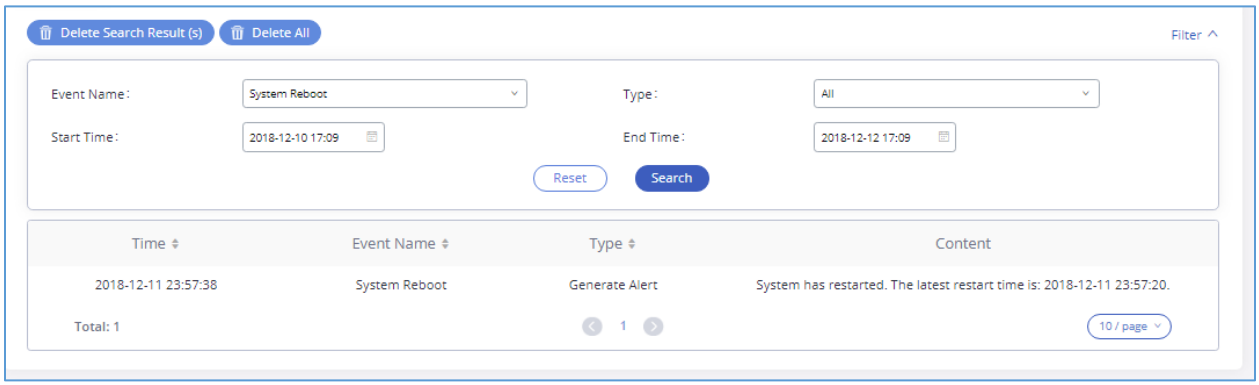


Figure 61: Alert Log Filter

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 Delete Search Result (s) to delete the filtered result of operation logs. Or users can click on Delete All 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 GXW4500 which will have an alert, and/or an Email generated if occurred:

- ***Disk Usage***
- ***Modify Admin Password***
- ***Memory Usage***
- ***System Reboot***
- ***System Update***
- ***System Crash***
- ***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

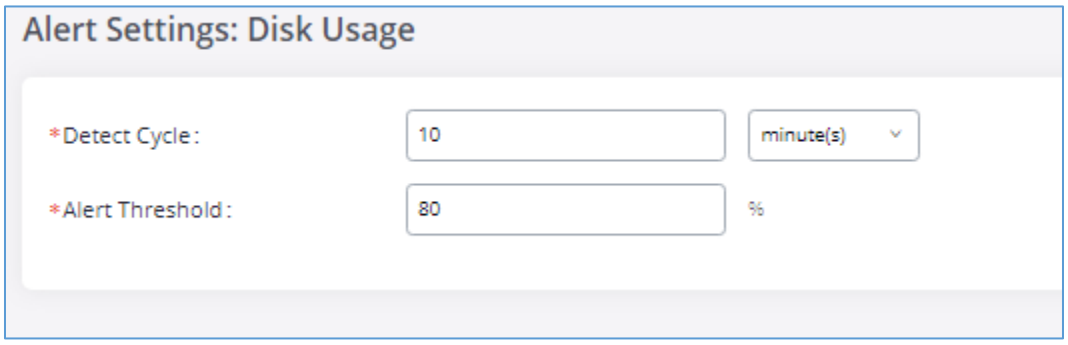


Figure 62: System Events→Alert Events Lists: Disk Usage

- **Detect Cycle**: The GXW4500 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 GXW4500 system will send the alert.

2. External Disk Usage

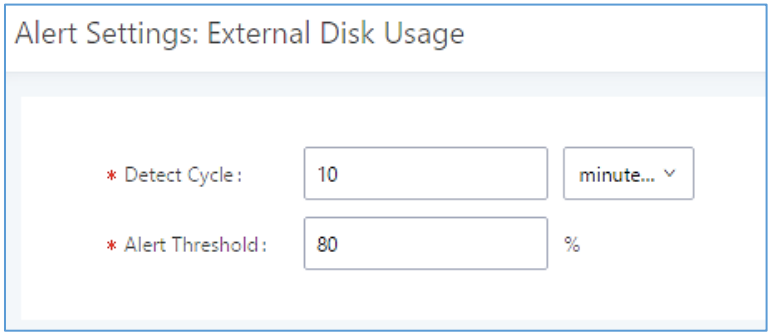


Figure 63: System Events→Alert Events Lists: External Disk Usage

- **Detect Cycle**: The GXW4500 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 GXW4500 system will send the alert.

3. Memory Usage

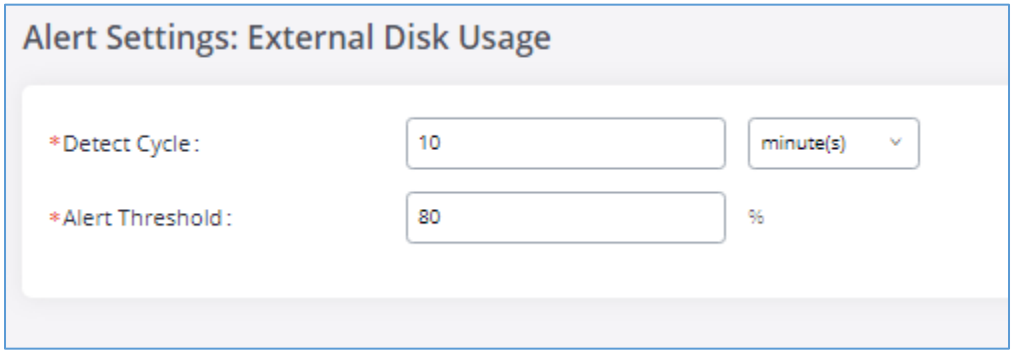


Figure 64: System Events→Alert Events Lists: Memory Usage

- **Detect Cycle**: The GXW4500 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 GXW4500 system will send the alert.

4. System Crash

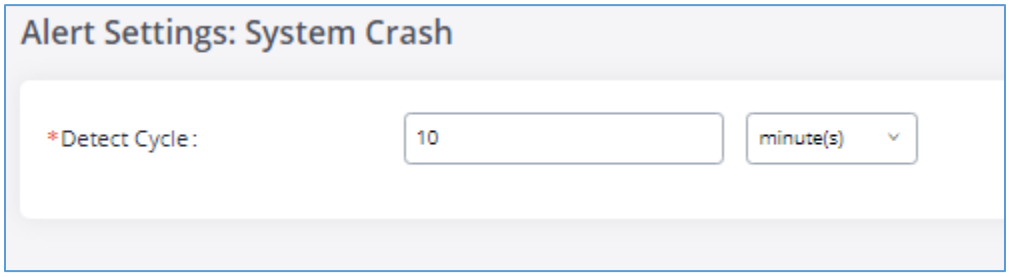


Figure 65: System Events→Alert Events Lists: System Crash

- **Detect Cycle**: The GXW4500 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.

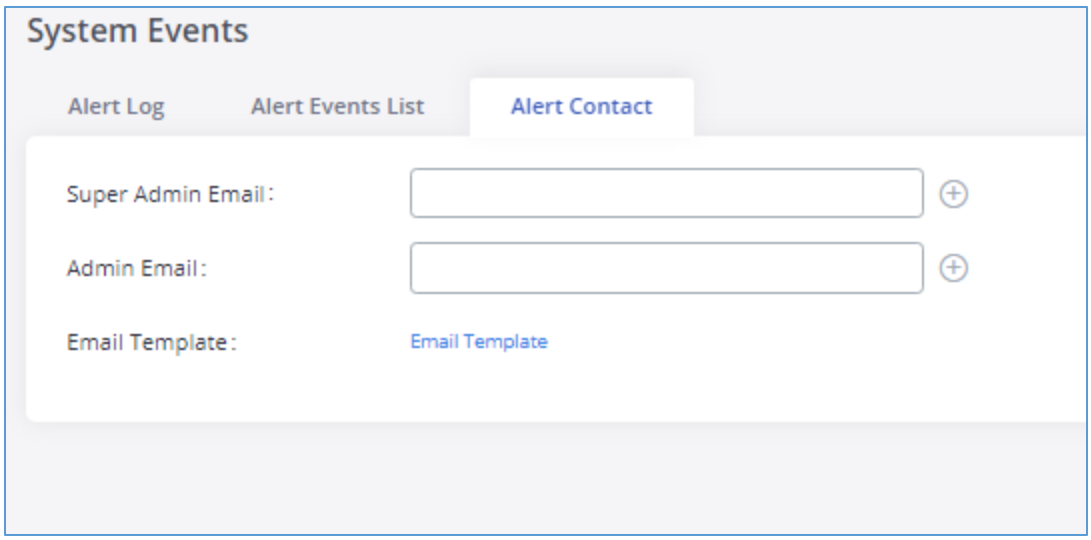


Figure 66: Alert Contact

Upgrade

The GXW4500 can be upgraded to a new firmware version remotely or locally. This section describes how to upgrade your GXW4500 via network or local upload.

Upgrading via Network

The GXW4500 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**.

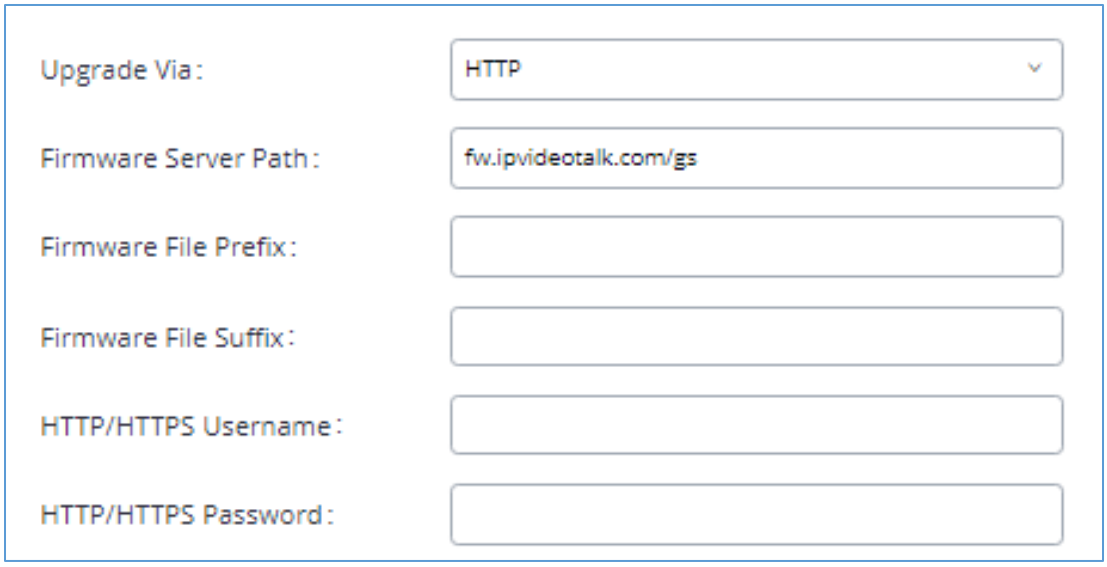


Figure 67: Network Upgrade

Table 41: 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 GXW4500 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 GXW4500 directly via Web GUI. Please follow the steps below to upload firmware locally.

1. Download the latest GXW4500 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 Choose File to Upload and select the firmware file from your PC. The default firmware file name is gxw4500fw.bin

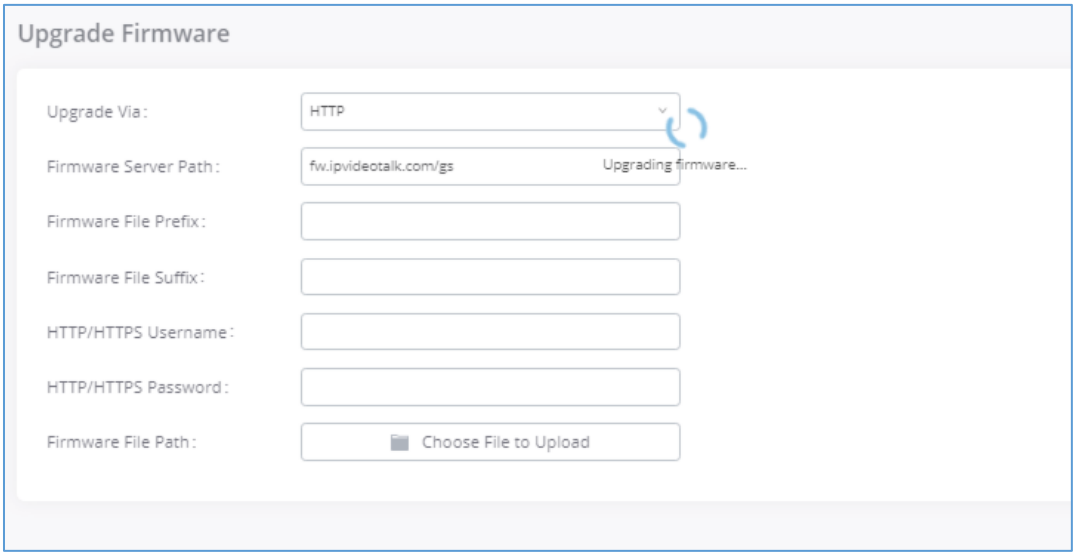


Figure 68: Upgrading Firmware Files

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 GXW4500 for the changes to take effect.

5. Click on "OK" to reboot the GXW4500 and check the firmware version after it boots up.

⚠ **Notes:**

- Please do not interrupt or power cycle the GXW4500 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 GXW4500 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 GXW4500 web configuration interface;
5. Configure the Firmware Server Path to the IP address of the PC;
6. Update the changes and reboot the GXW4500.

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 GXW4500 configuration can be backed up locally or via network. The backup file will be used to restore the configuration on GXW4500 when necessary.

Backup/Restore

Users could backup the GXW4500 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:

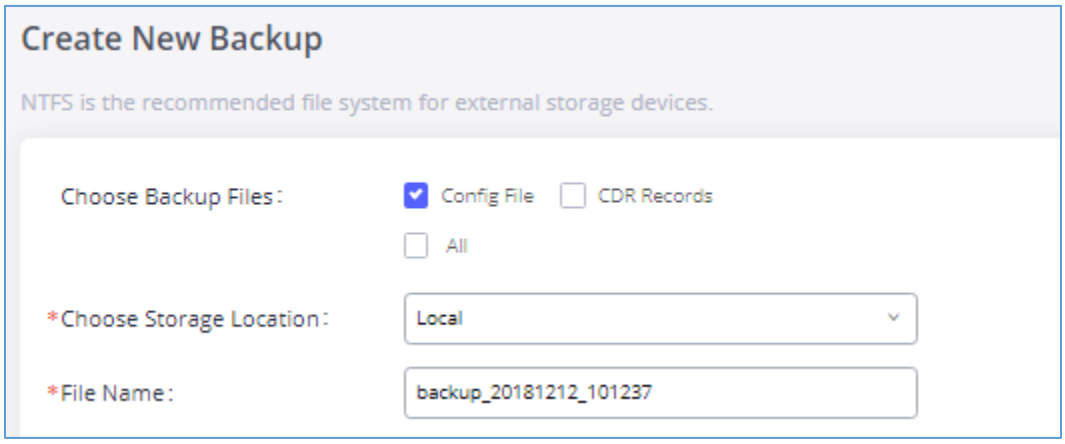


Figure 69: Create New Backup

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 GXW4500 internal storage or the external device. Click on Upload Backup File to upload backup file from the local device to GXW4500. The uploaded backup file will also be displayed in the web page and can be used to restore the GXW4500.

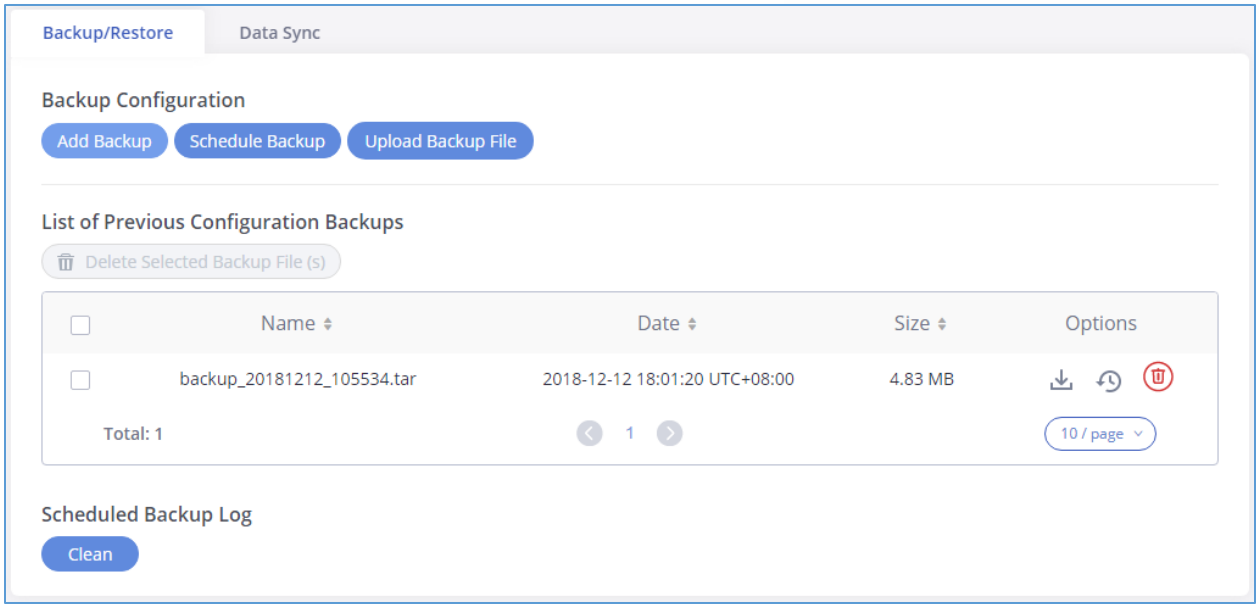


Figure 70: Backup / Restore

The Schedule Backup option allows GXW4500 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.

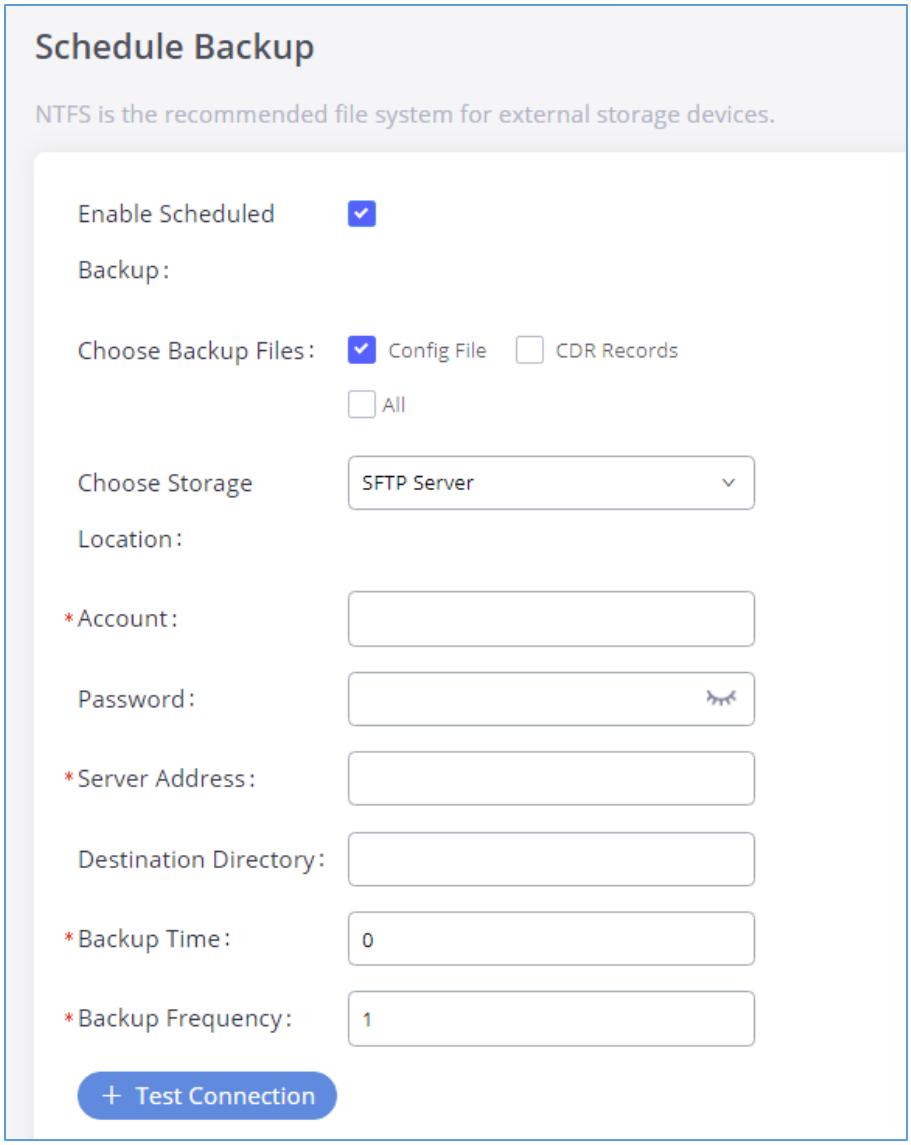


Figure 71: Schedule Backup

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, GXW4500 will create the directory automatically.

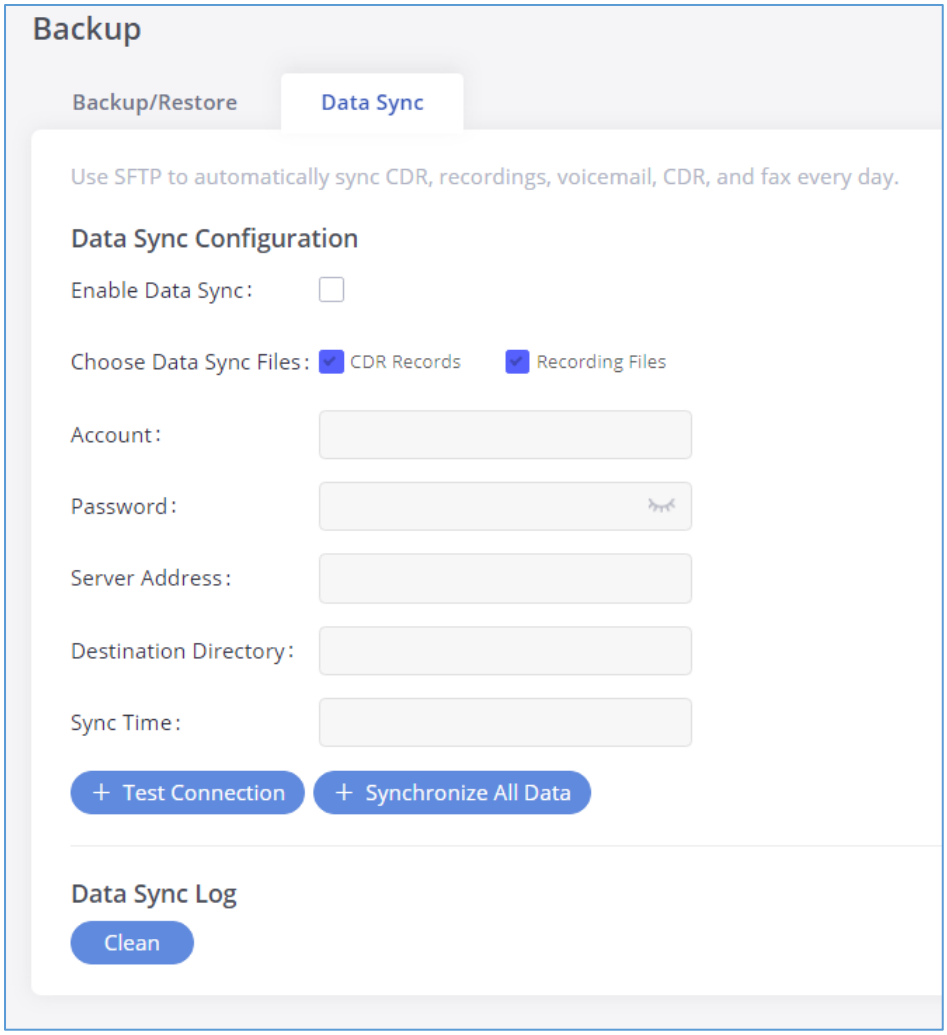


Figure 72: Data Sync

Table 42: 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 GXW4500 will then try connecting the server to make sure the server is up and accessible for the GXW4500.

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 GXW4500 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 GXW4500.
- If users have other backup files on PC to restore on the GXW4500, click on "Upload Backup File" first and select it from local PC to upload on the GXW4500. 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 GXW4500.

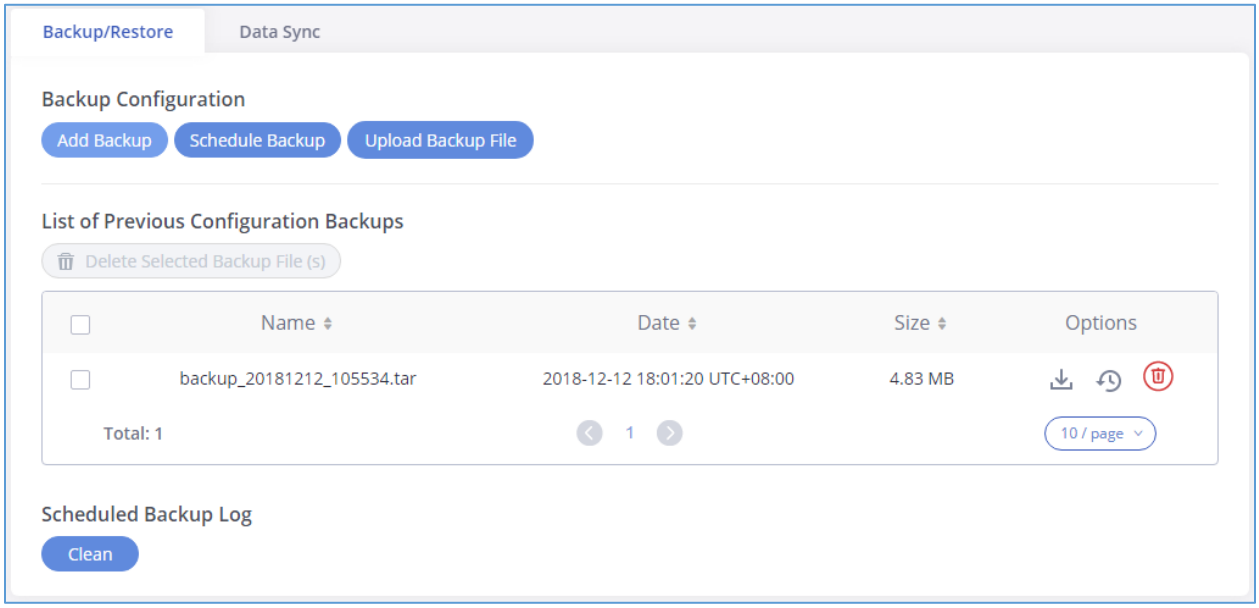


Figure 73: Restore GXW4500 from Backup File

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 and Reboot

Users could perform reset and reboot under Web GUI→**Maintenance→System Cleanup/Reset→Reset and 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.

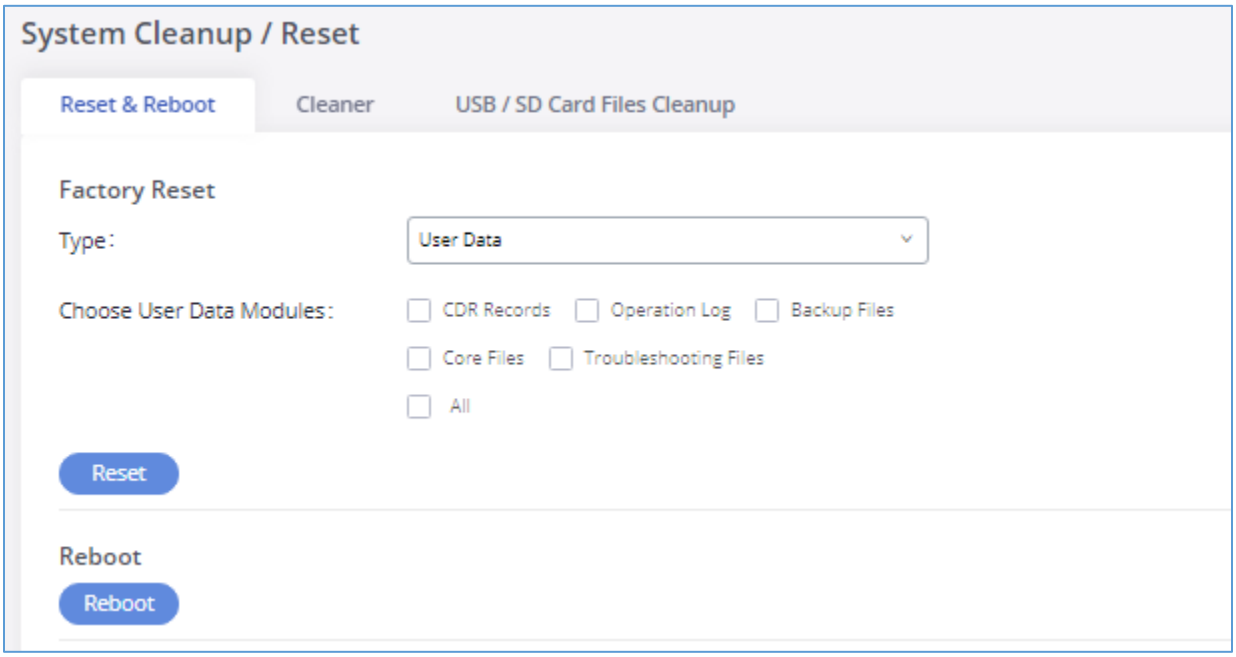


Figure 74: Reset and Reboot

Cleaner

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

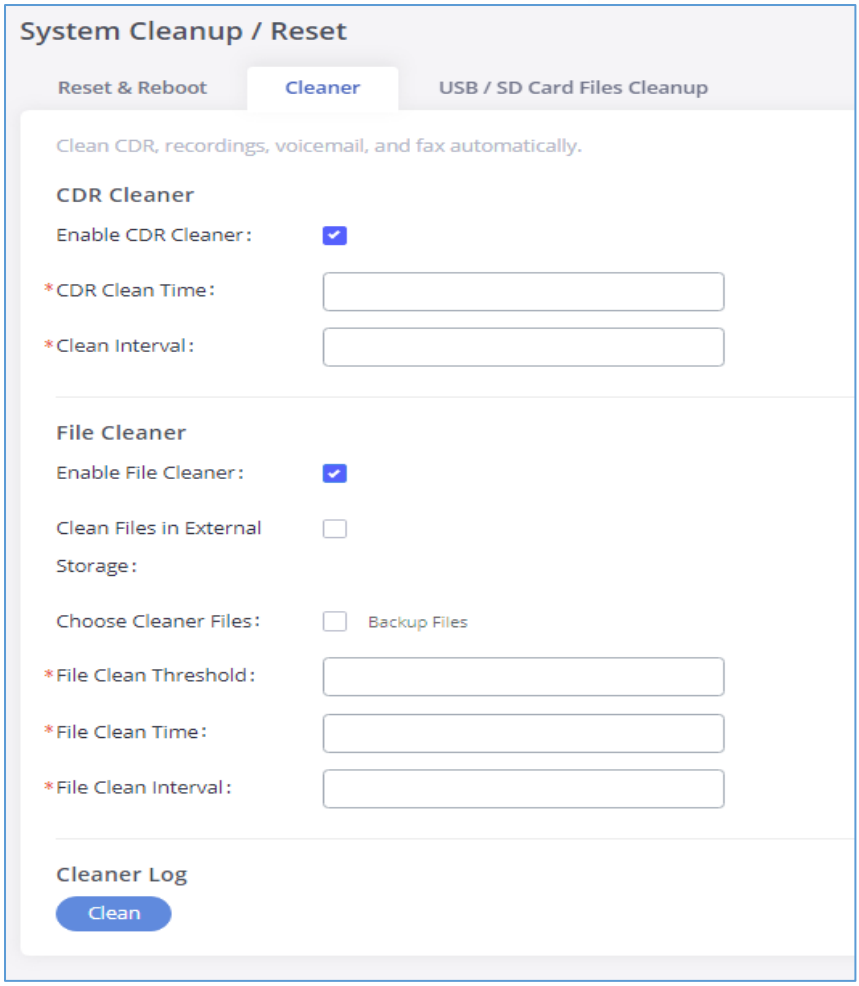


Figure 75: Cleaner

Table 43: 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**.

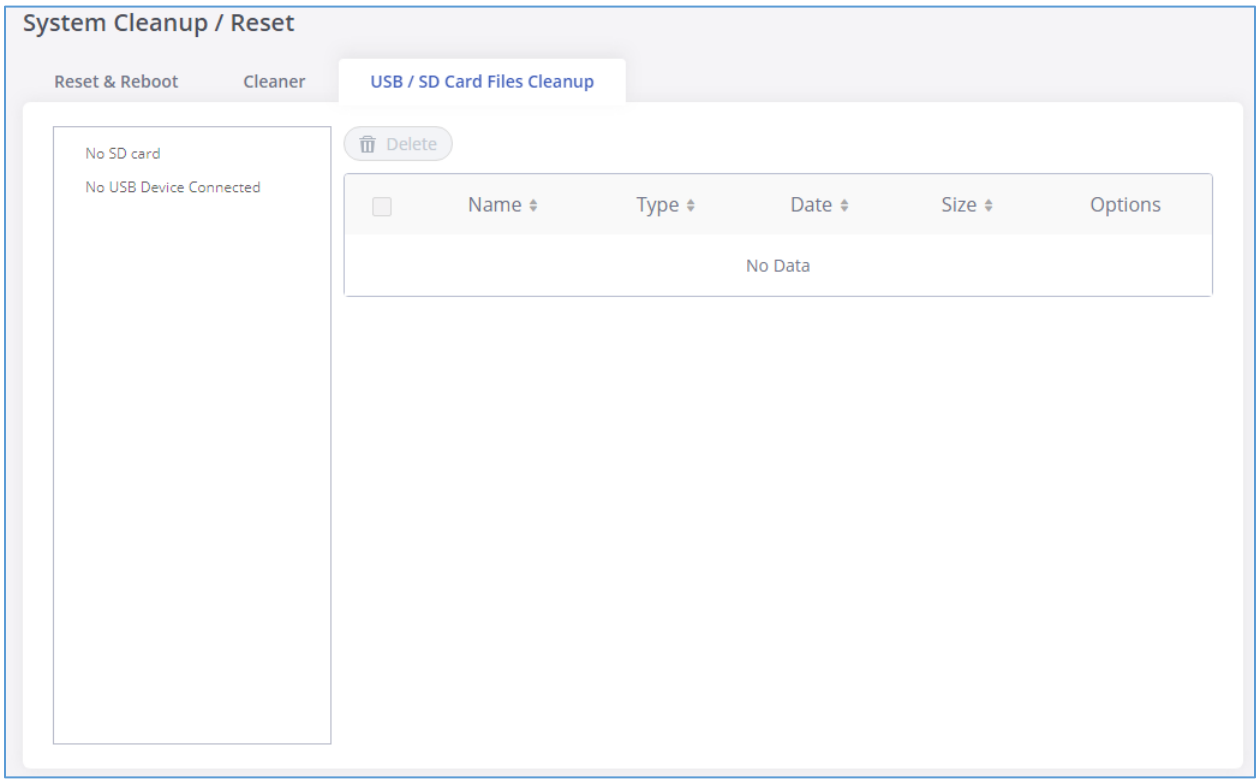


Figure 76: SB/SD Card Files Cleanup

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 GXW4500, 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.

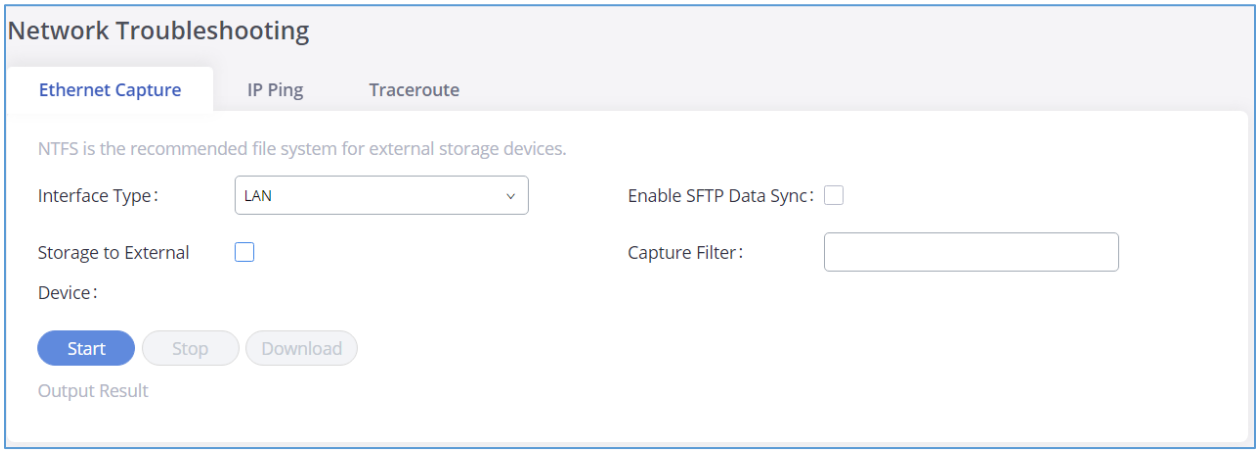


Figure 77: Ethernet Capture

Table 44: Ethernet Capture Parameters

Interface Type	Select the network interface to monitor.
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.

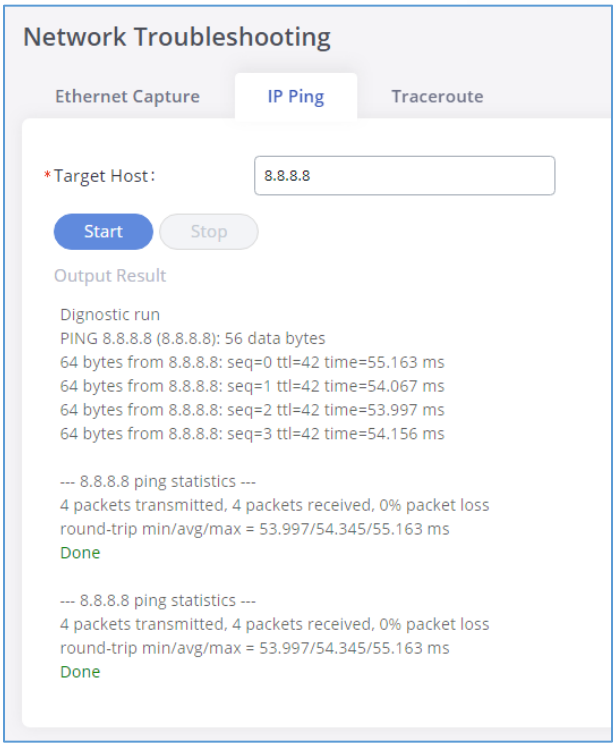


Figure 78: IP Ping

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.

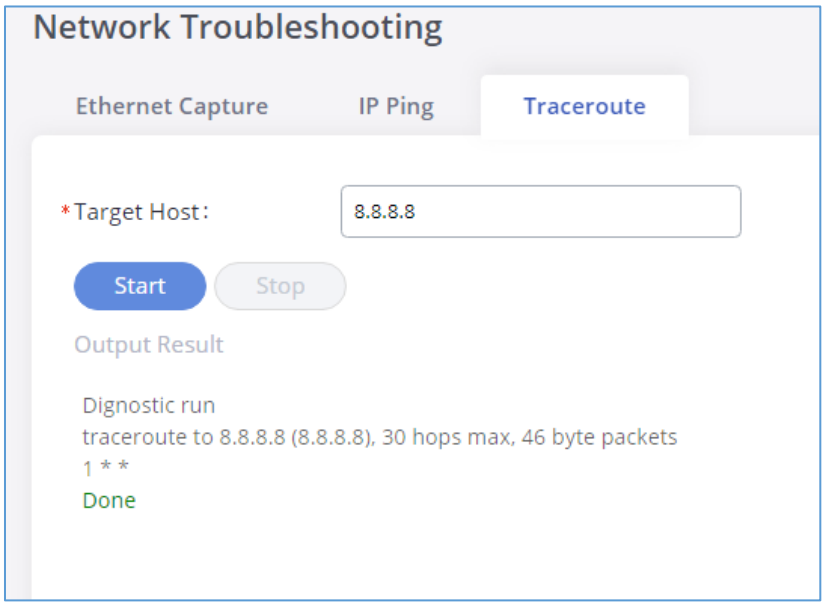


Figure 79: Traceroute

Service Check

Enable Service Check to periodically check the GXW4500 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 GXW4500. The default setting is 3. If there is no response from GXW4500 after 3 attempts (default) to check, current status will be stored and GXW4500 will be restarted.

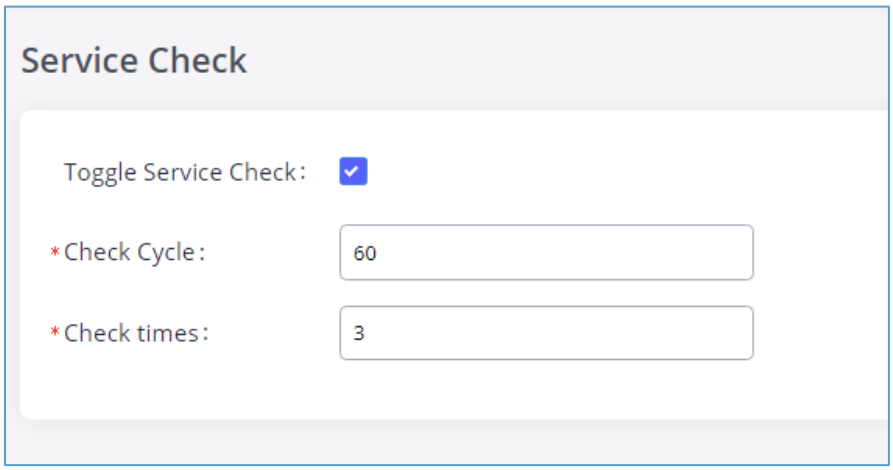


Figure 80: Service Check

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 GXW4500, the CDR can be accessed under Web GUI→**CDR→CDR**. Users could filter the call report by clicking on Filter 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.

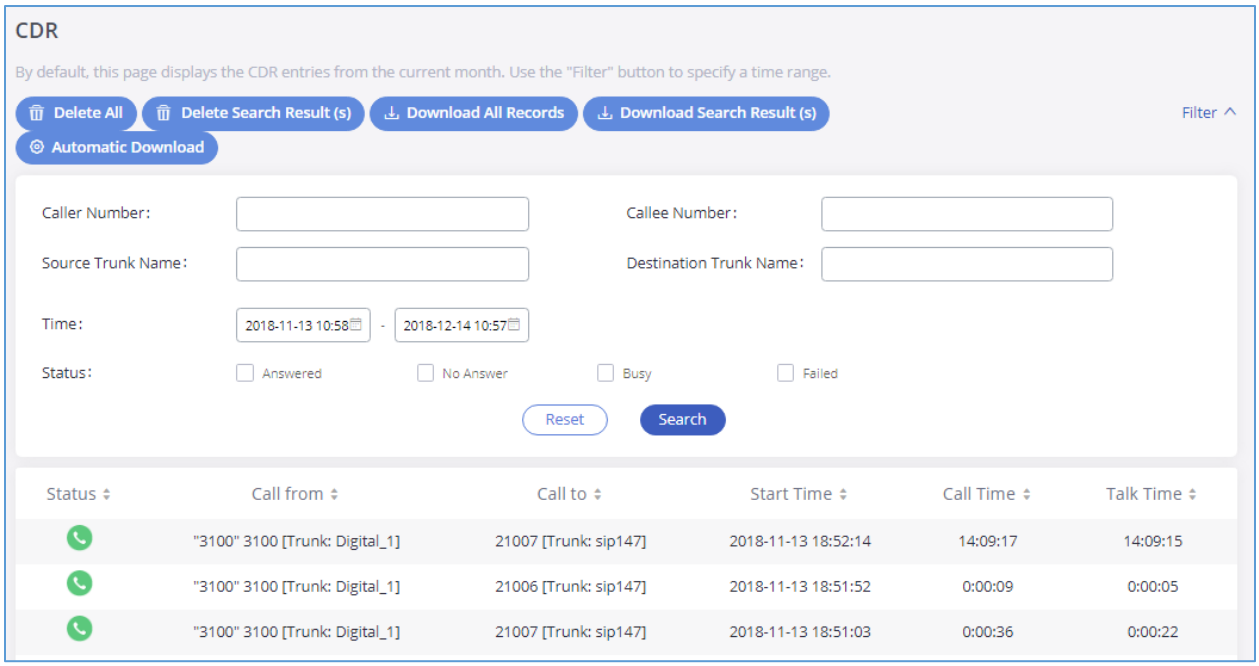


Figure 81: CDR Filter

Table 45: 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 ".".).

	For Example: • **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	Filter with the call status, the available statuses are the following: • 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

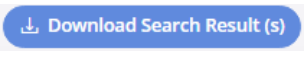
Figure 82: Call Report

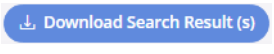
The CDR report has the following data fields:

- **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 Delete All button to remove all the call report information.

- **Download all records**.

  Click on Download All Records to export all the records to a .csv file.

Automatic Download

User could configure the GXW4500 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.

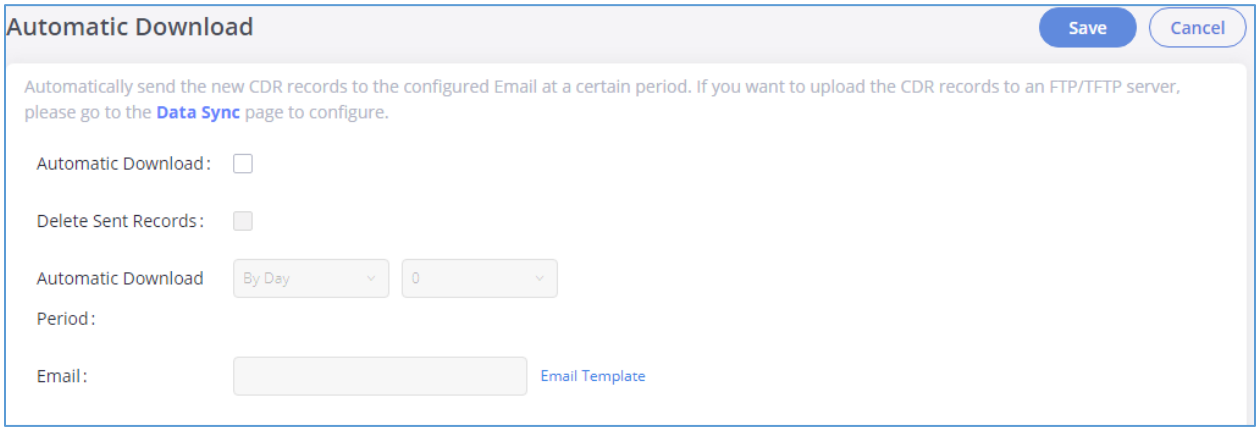


Figure 83: Automatic CDR Download

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

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 DOCMENTATION.	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	Sting	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 GXW4500 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 GXW4500 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.***