Grandstream Networks, Inc.

GVC3220

Ultra HD Multimedia Conferencing System

Administration Guide

COPYRIGHT

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.

WARNING

Please do not use a different power adaptor with devices as it may cause damage to the products and void the manufacturer warranty.

CE Authentication

BE	BG	CZ	DK	DE	EE	IE	EL	LI
ES	FR	HR	IT	CY	LV	LT	LU	CH
HU	MT	NL	AT	PL	PT	RO	SI	TR
SK	FI	SE	NO	IS	UK	UK(NI)		

In the UK and EU member states, operation of 5150-5350 MHz is restricted to indoor use only.

Hereby, Grandstream Networks, Inc. declares that the radio equipment GVC3220 is in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address:

https://www.grandstream.com/support/resources/

GVC3220 Administration Guide
Version 1.0.1.35

.GNU GPL INFORMATION

GVC3220 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: https://www.grandstream.com/sites/default/files/Resources/gvc32xx-gpl.tar.gz

GVC3220 Administration Guide
Version 1.0.1.35

Table of Contents

GVC3220 Administration Guide
Version 1.0.1.35

Table of Tables

Table of Figures

GVC3220 Administration Guide
Version 1.0.1.35

DOCUMENT PURPOSE

This document describes how to configure the GVC3220 via the device LCD menu and web UI menu to fully manipulate the supported features. The intended audiences of this document are device administrators.

To learn the basic functions of the GVC3220, please visit https://www.grandstream.com/support to download the latest "GVC3220 User Guide".

This guide covers following topics:

- Product Overview
- GVC3220 Web GUI Settings
- Firmware Update
- Factory Reset
- Experiencing the GVC3220

CHANGE LOG

This section documents significant changes from previous versions of the GVC3220 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 1.0.1.35

- Added TR-069 and GDMS support. [System Settings/ TR-069]

- Added Pick up distance setting for GMD [GMD Pickup Distance]

- Added Screen sharing when web is not logged in. [Share Screen]

- Added Camera mirroring. [Camera Mirroring]

- Added new meeting schedule interface on web UI. [Call/Schedule]

- Added IPVT Image Size and Video Bit Rate. [Account/IPVideoTalk/Codec Settings]

- Added Wi-Fi Country Code. [Country Code]

- Added LDAP Search Field Filter. [App/LDAP Contacts]

Firmware Version 1.0.1.27

- No Major Changes.

Firmware Version 1.0.1.24

- This is the initial version.

WELCOME

Thank you for purchasing Grandstream GVC3220 Android™ Video Conferencing System. This document introduces the LCD settings, web UI settings and advanced configurations of GVC3220. To learn the basic configuration and how to use GVC3220, please visit https://www.grandstream.com/support to download the latest "GVC3220 User Guide".

The GVC3220 is a revolutionary video conferencing system that provides an interactive and immersive video conferencing environment to increase collaboration and productivity. This SIP-based GVC3220 allows the user to connect their video conferencing solutions with any 3rd-party SIP or H.323 video conferencing platform. Additionally, since the GVC3220 is based on an Android 9.0 operating system. Users will elevate their experience with its 4K Full-HD video, up to 5-way 1080P video conferences, screen-sharing capabilities, Integrated Wi-Fi, Bluetooth and more.

The GVC series supports Grandstream's IPVideoTalk Video and Web Conferencing platform.
This paid subscription-based service allows users to turn any meeting hosted on any GVC device into an online meeting that can be joined seamlessly from a web browser or GVC. Turn any physical room into a virtual, online meeting place to offer your customers the tools they need to be successful, no matter where they are.

PRODUCT OVERVIEW

Table 1: GVC3220 Technical Specifications

Specification	Description
Protocols/ Standards	SIP RFC3261, H.323, BFCP, TIP, RTP/RTCP, HTTP/HTTPS, ARP, ICMP, DNS (A record, SRV, NAPTR), DHCP, PPPoE, SSH, TFTP, NTP, STUN, SIMPLE, LLDP-MED, LDAP, TR-069, 802.1x, TLS, SRTP, TCP/IP/UDP, IPv6, OpenVPN®
MCU	up to 5-way 1080P@30fps conference, 9-way 720P@30fps conference
Camera	1/2.5", 8 Megapixel CMOS, 4k 30fps or 1080p 60fps output
Lens	12x optical zoom, +/-30° tilt, +/-170° pan, 70.1°~7.4°(W) field of view, 40.7°~4.2°(T) field of view
Network Interface	1 x RJ45 10/ 100/ 1000 Mbps port
Wi-Fi	Integrated dual-band 802.11 a/b/g/n/ac (2.4GHz & 5GHz), supports Wi-Fi Multimedia
Bluetooth	Integrated Bluetooth
Video Outputs	1x HDMI 2.0 up to 4k with CEC，1x HDMI 1.4 up to 1080p
Video Input	1x HDMI 1.4 up to 1080p
MIC/Speaker	Support external Bluetooth or 2.4G microphone, 1 built-in speaker
Audio Inputs/Outputs	1x Line in/out ,1x Media
Remote Control	Bluetooth & Infrared remote control with multi-touch touchpad
Auxiliary Ports	1x USB 3.0, 1x USB 2.0, 1x SD, 1x Reset
Voice Codecs	Support for G.711μ/a, G.722 (wide-band), G.726-32, iLBC, Opus, G.722.1, G.722.1C, G729A/B, in-band and out-of-band DTMF (In audio, RFC2833, SIP INFO)
Video Codecs	H.264 BP/MP/HP, video resolution up to 1080P, frame rate up to 30fps, bit rate up to 4Mbps
Portrait Video Resolution	4K from 1Mbps to 8Mbps, 1080P from 1Mbps to 4Mbps, 720P from 512Kbps to 2Mbps
Content Video Resolution	Input: 720P, 1080P (HDMI) Encoding: 800×600, 1024×768, 1280×1024, 1280×720, 1920×1080 Output: 720P, 1080P
Dual-Stream	BFCP, people video (up to 4K@30fps) + content video (up to 1080P@15fps)
Audio Features	AEC, ANS, AGC, PLC, CNG/VAD

Video Features	FEC, dynamic display layout, picture-in-picture, picture-outside-picture.
Video Conferencing Service Platform	SIP, H.323, Grandstream IPVideoTalk, Bluejeans and Zoom
Telephony Features	Hold, mute, downloadable phone book (XML, LDAP), call waiting, call history, flexible dial plan, server redundancy & fail-over
Sample Applications	Microsoft Teams, Skype or Skype for Business, Zoom, YouTube, mobile phone data import/export via Bluetooth, etc. API/SDK available for advanced custom application development.
Application Deployment	Allow various Android operating system 9.0 compliant applications to be developed, downloaded, and run in the embedded device with provisioning control
QoS	Layer 2 QoS (802.1Q, 802.1p) and Layer 3 (ToS, DiffServ, MPLS) QoS
Security	User and administrator level passwords, MD5 and MD5-sess based authentication, 256-bit AES encrypted configuration file, TLS, 128/256-bit SRTP, HTTPS, 802.1x media access control
Multi-Language	English, Chinese, German, Italian, French, Spanish, Portuguese, Russian.
Upgrade/ Provisioning	Firmware upgrade via TFTP / HTTP / HTTPS or local HTTP upload, mass provisioning using TR-069 or AES encrypted XML configuration file. Detect U disk /SD card system version upgrade automatically.
Power & Green Energy Efficiency	Universal power adapter: Input: 100~240Vac 50~60Hz Output: 48V/1.35A(64.8W)
Package Content	GVC3220 video conference system, GMD1208 wireless microphone, remote control, 4 AAA batteries, universal power supply, network cable (2 meters), HDMI cables (1x 5 meters, 2x 1.5 meters), lens cleaning cloth, bracket, quick installation guide.
Temperature and Humidity	Operation: 0°C to 40°C, Storage: -10°C to 60°C, Humidity: 10% to 90% (Non-condensing)
Compliance	Broadsoft FCC: Part15 Class B; Part 15 Subpart C 15.247; Part 15 Subpart E 15.407; MPE. CE: EN 55032; EN 55035; EN 61000-3-2; EN 61000-3-3; EN 62368-1; EN 301 489-1; EN 301 489-17; EN 300 328; EN 301 893; EN 62311. RCM: AS/NZS CISPR32; AS/NZS 4268; AS/NZS 62368.1. IC: ICES-003; RSS-GEN; RSS-247; RSS-102(MPE). HDMI/EAC/REACH/ROHS/WEEE

Safety Compliances

GVC3220 complies with FCC/CE and various safety standards. GVC3220 power adapter is compliant with the UL standard. Use the universal power adapter provided with GVC3220 package only. The manufacturer's warranty does not cover damages to the device caused by unsupported power adapters.

Warranty

If GVC3220 is purchased from a reseller, please contact the company where the device is purchased for replacement, repair, or refund. If the device is purchased directly from Grandstream, please contact Grandstream Support for an RMA (Return Materials Authorization) number before the product is returned. Grandstream reserves the right to remedy warranty policy without prior notification.

GVC3220 WEB GUI SETTINGS

GVC3220 embedded Web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow users to configure the application device through a Web browser such as Mozilla Firefox, Google Chrome™, etc.

Accessing GVC3220 Web GUI
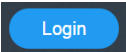
The IP address of the GVC3220 will show on the top status bar of the connected display device (e.g., TV) via HDMI

To access GVC3220 Web GUI:

1. Connect the computer to the same network as GVC3220
2. Make sure GVC3220 is turned on and shows its IP address on the connected display screen.
3. Open a Web browser on your computer.
4. Enter GVC3220's IP address in the address bar of the browser, e.g.: http://192.168.124.111.
5. Enter the administrator's login and password to access the Web Configuration Menu. The default administrator username is "admin" and the default random password can be found at the back sticker on the GVC3220. The default end user username and password are "user" and "123". The user can select English or other languages in the drop-down menu of language.

Figure 1: GVC3220 Web GUI - Login

6. Click "Login" [Login] to access the configurations in web UI.

Saving Changes

When changing any settings on the web UI, always submit them by pressing the "Save" button on the bottom of the page, and then clicking the "Apply" button on the top of the page to apply the configuration

Definitions

This section describes the options in the GVC3220 Web GUI. As mentioned in the previous section, you can log in as an administrator or a normal user.

- **Call**

  Users could initiate conference and control conference from Web GUI. Manage contacts, schedule conference, and manage call history.
- **Account**

  SIP, IPVideoTalk, H323, Video Conf Service Platform.
- **Call Features**

  General Settings, Call Settings, Site Name, Audio Control, Video settings.
- **Network Settings**

  Ethernet Settings, Wi-Fi Settings, OpenVPN Settings, Advanced Network Settings.
- **System Settings**

  Power Manager, Time & Language, TR-069, Security Settings, Peripheral
- **Device Control**

  Preset Settings, Camera Control, Remote Control.
- **App**

  LDAP contacts, BroadSoft Directories, Recording Management, Third Party Application.
- **Maintenance**

  Upgrade, and Troubleshooting.
- **Status**

  Account Status, Interface Status, Network Status, System Info and Remote control status.

The following table shows the web pages accessible by end user and administrator.

Table 2: GVC3220 Web Access

User Type	Username	Default Password	Accessible Web Pages
End User	User	123	- Call - Account - System Settings - Device Control - App - Maintenance - Status

Administrator	Admin	Can be found at the back sticker	All pages

Toolbar

The web UI tool bar is on the upper right corner of the web UI page.
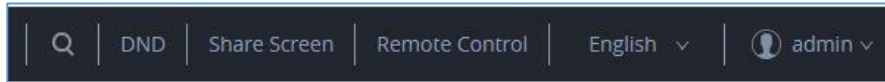
Figure 2: Web UI Tool Bar

- **DND**
  Turn on/off DND mode. Once enabled, the DND text will turn into red in web UI. The LCD for GVC3220 display will shows DND indication on the top of the screen and all incoming calls will be rejected.
- **Share Screen**
  HTTPS is required for sharing screen. Go to "System Settings - Security Settings - Web/SSH Access" to set access mode.
  Note: Starting firmware 1.0.1.35, "Share Screen" is available on the web UI without login.
  1. Click on "Share Screen"
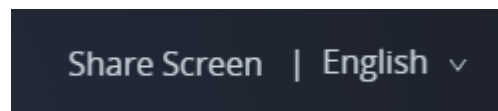
  2. A prompt will ask to enter the code and press "Turn on Sharing".
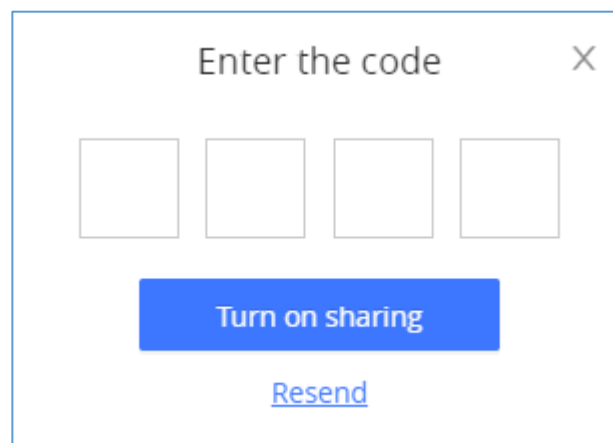
Figure 3: Share Screen – Enter the code

The code is automatically generated and will displayed on the connected TV.
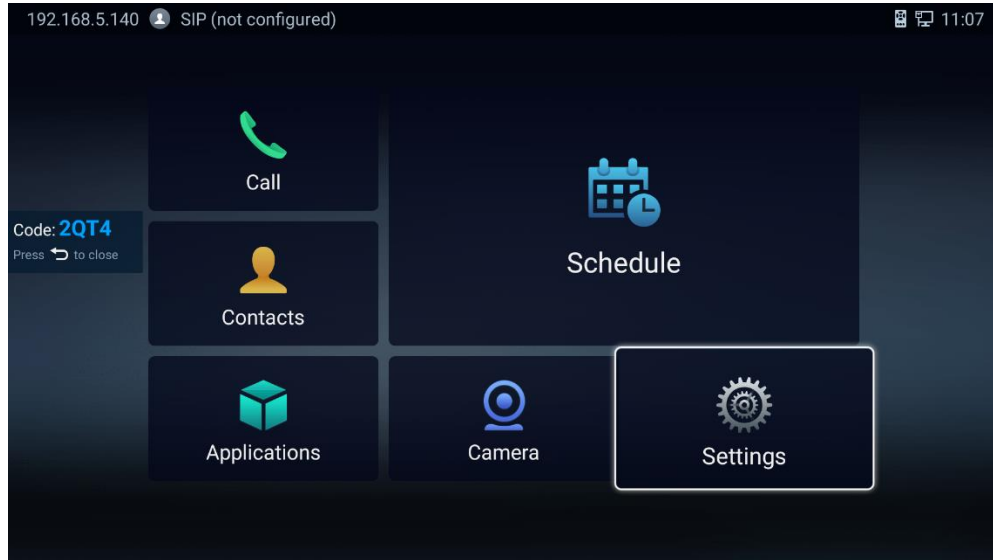
Figure 4: Share Screen Code

3. Select the screen to share and press "Share" button.
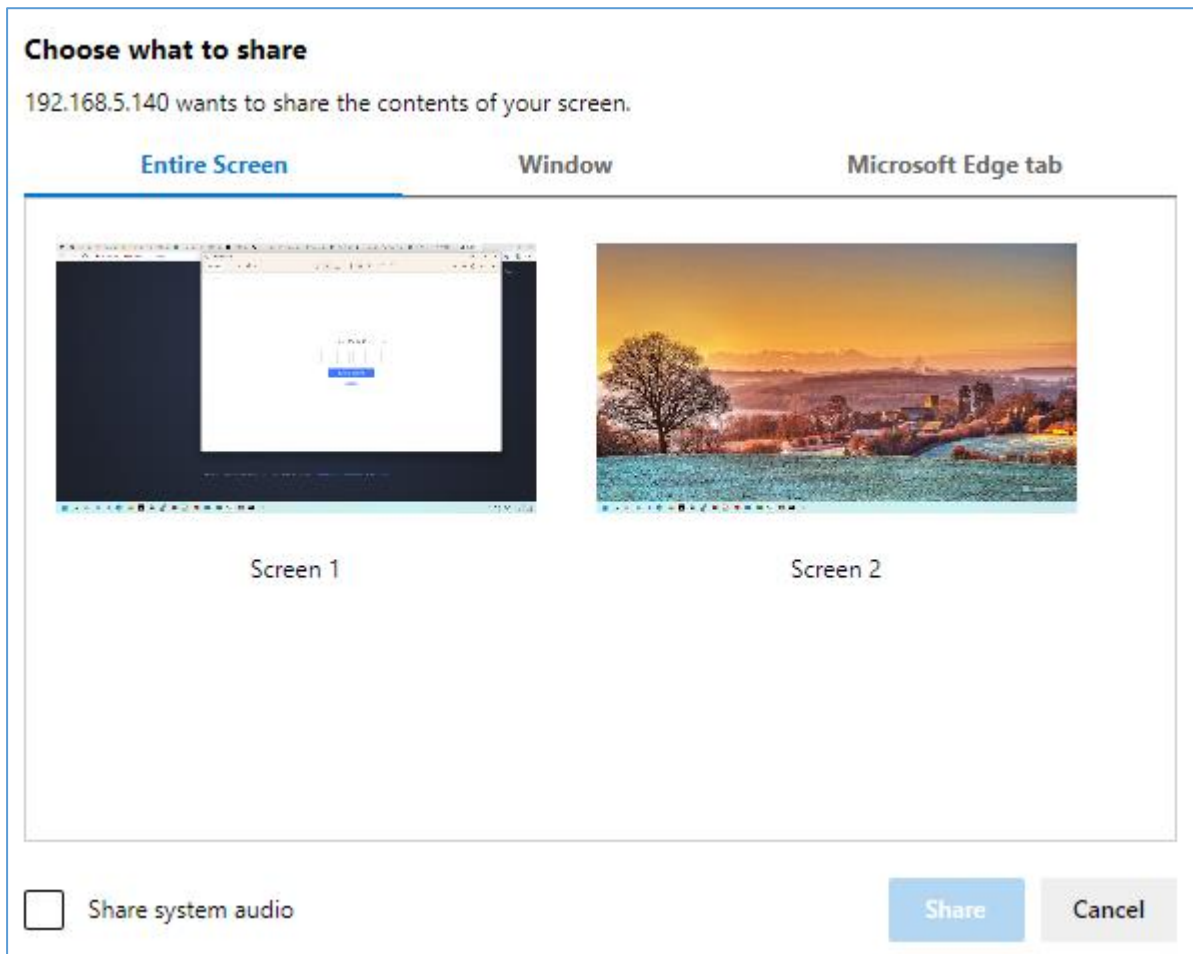
Figure 5: Share Screen – Select the screen to share

- **Remote Control**

  Click to bring up virtual remote control panel.
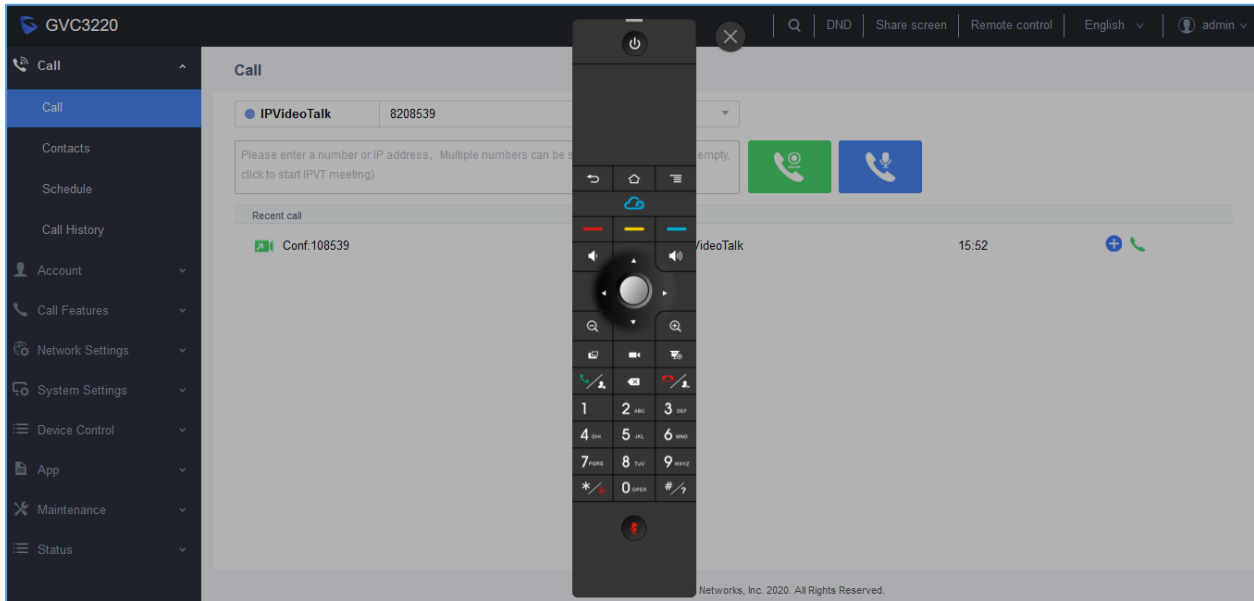
Figure 6: Web UI Virtual Remote Control

- **English**

  Select the display language for the web UI.

- **Logout**

  Log out from the web UI.

Call

Call listing section includes: Call, Contacts, Schedule, and Call History.

Call/Contacts

- **Contacts**

Users could use contacts page from GVC3220 Web UI→**Call**→**Contacts** to manage contacts entries.

Click on "New Contact" to add a new contact entry manually.
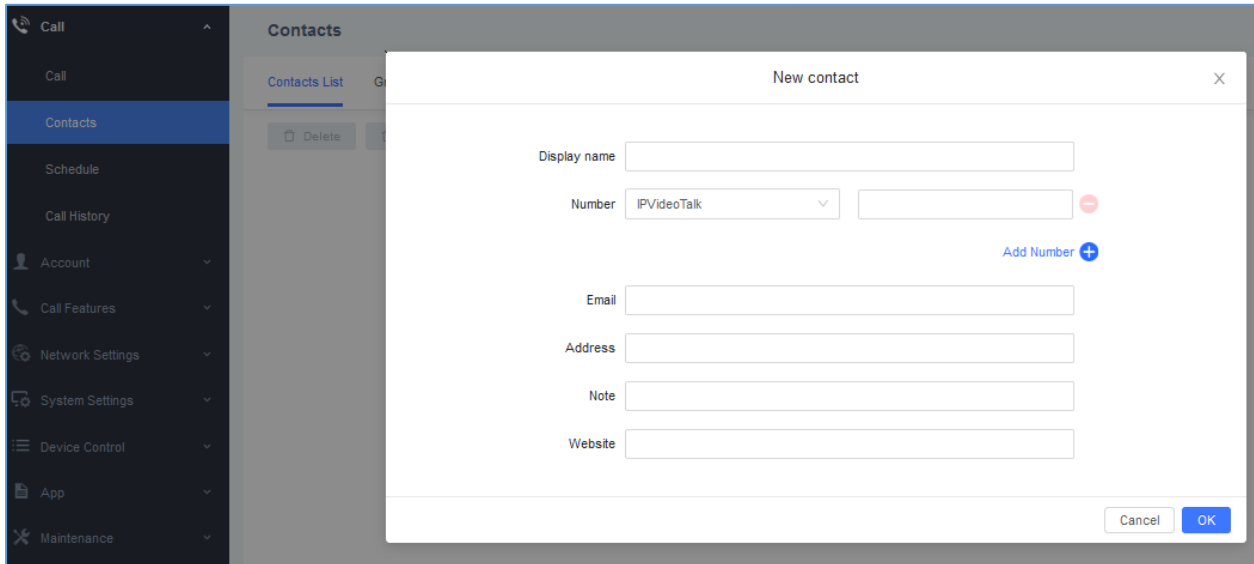
Figure 7: Add New Contact

Table 3: Contacts Parameters

Parameters	Descriptions	
Display Name	Specify the name of the contact entry.	
Number	**Account**	Specify which account will be associated with the contact entry. It is the account used when dialing this contact. Available options are: SIP, IPVideoTalk, H.323.
	Phone number	Enter the phone number of the contact.
Email	Specify the Email of the contact.	
Address	Specify the Address of the contact.	
Note	You can enter a note for this contact.	
Website	Specify the website of this contact.	

Call/Schedule

Users could use schedule meetings from GVC3220 Web UI→**Call**→**Schedule**.

Click on "New Meeting" to schedule a new conference.
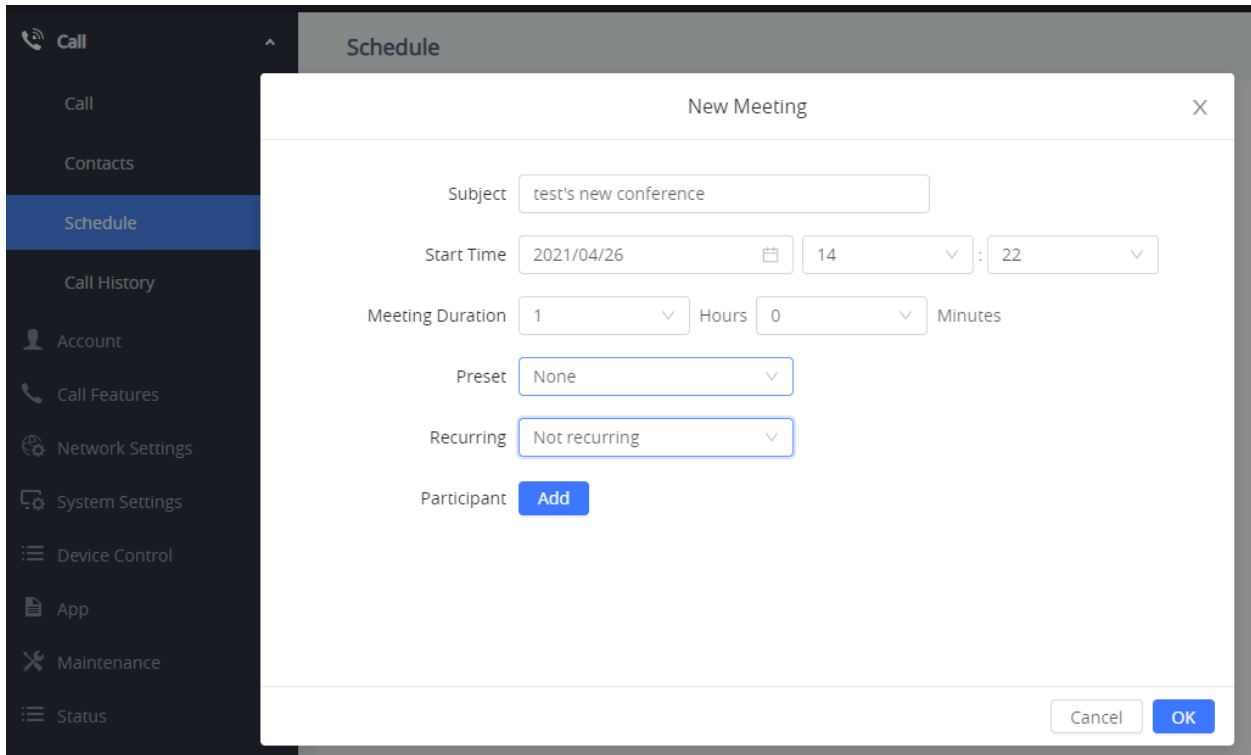
Figure 8: Schedule

Table 4: Schedule

Parameters	Descriptions
Subject	It is used to set the conference name to identify this conference.
Start Time	It is used to configure the start time of the conference.
Meeting Duration	Set the duration of the conference.
Preset	It is used to select a camera preset when the scheduled conference starts, the GVC3220's camera will be automatically placed to the preset position. Default is "None"
Recurring	Users could repeat the scheduled conference, to repeat the conference depending on the chosen option: • Not recurring • Every Weekday (Mon-Fri) • Every weekly (day) • Monthly (by day) • Custom
Participant	Click on Change member to select and add participants to the conference.

Call/Call History

Users could view Call History GVC3220 Web UI→**Call**→**Call History**.

shows all calls (outgoing, received, missed).

GVC3220 Administration Guide
Version 1.0.1.35
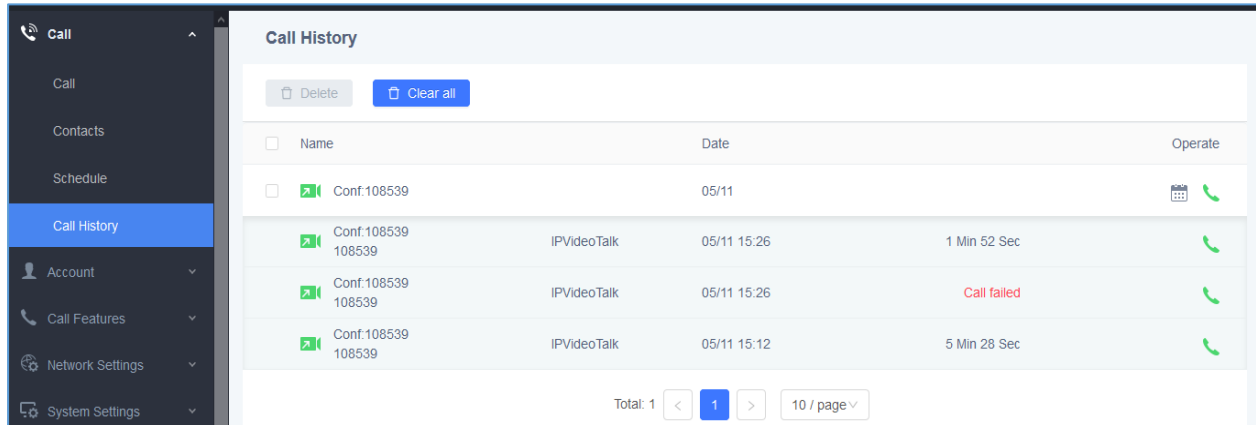
Figure 9: Call History

Account

The Settings page lists Account Settings for SIP, IPVideoTalk, H323, and Video Conf Service Platform. The GVC3220 supports up to 4 accounts:

- One SIP account that the user can register to any SIP platform
- One H.323 account that the user can register to any H.323 platform.
- IPVideoTalk account that is supported by Grandstream's IPVideoTalk service.
- Zoom Account
- BlueJeans account.

The following table shows all the settings that SIP and H.323 accounts has. Please note the IPVideoTalk account and BlueJeans account have a subset of the settings that the SIP account has.

Account/SIP/General Settings

Parameters	Descriptions
Account Active	This field indicates whether the account is active. If disabled, the device will not send registration information to SIP server. The default setting is enabled.
Account Name	It is used to configure the name associated with each account to be displayed on the upper left corner of LCD.
SIP Server	It is used to configure the URL or IP address, and port of the SIP server. This should be provided by VoIP service providers (ITSP).
Secondary SIP Server	It is used to configure the URL or IP address, and port of the secondary SIP server. When the connection request sent to SIP server fails, the device will try to use the secondary SIP server.
Tertiary SIP Server	It is used to configure the URL or IP address, and port of the tertiary SIP server. When the connection request sent to SIP server and secondary SIP server fails, the device will try to use the tertiary SIP server.

SIP User ID	It is used to configure the user account information, provided by your VoIP service provider (ITSP). It is usually in the form of digits similar to phone number or actually a phone number.
SIP Authentication ID	It is used to configure the SIP service subscriber's Authenticate ID used for authentication. It can be identical to or different from the SIP User ID.
SIP Authentication Password	It is used to configure the account password required for the device to authenticate with the ITSP (SIP) server before the account can be registered. After saving, it will appear as hidden for security purpose.
Display Name	It is used to configure the SIP server subscriber's name (optional) that will be used for Caller ID display. The configured content will be included in the From, Contact and P-Preferred-Identity headers of SIP INVITE message.
Voice Mail Access Number	This parameter allows you to access voice messages by entering voice mail or dialing access number. On the device, the users can select **Settings→Advanced→Voice Mail** and click on the account to dial out to voicemail portal.
Tel URI	If the device 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 "Disable".

Account/SIP/Network Settings

Parameters	Descriptions
Outbound Proxy	It is used to configure the IP address or the Domain name of the Primary Outbound Proxy, Media Gateway, or Session Border Controller. It is used by the device for Firewall or NAT penetration in different network environments. If a symmetric NAT is detected, STUN will not work and ONLY an Outbound Proxy can provide a solution.
Secondary Outbound Proxy	It is used to configure the IP address or the Domain name of the Secondary Outbound Proxy, Media Gateway, or Session Border Controller. The device will try to connect the Secondary outbound proxy only if the primary outbound proxy fails.
DNS Mode	It is used to set which DNS service will be used to look up IP address for SIP server's hostname. It can be selected from the dropdown list: • A Record (Default) ; SRV; NATPTR/SRV. If the device needs DNS SRV resource, in which case the DNS server responds with more than one result, it should be set to "SRV" or "NATPTR/SRV".
NAT Traversal	It is used to configure the NAT traversal mechanism used on the device. It can be selected from the dropdown list: • NAT NO • STUN

| | • Keep-alive
• uPnP
• Auto
• OpenVPN
• TURN

If the outbound proxy is configured and used, it can be set to "NAT NO".

If set to "STUN" and STUN server is configured, the device will periodically send STUN message to the SUTN server to get the public IP address of its NAT environment and keep the NAT port open. STUN will not work if the NAT is symmetric type.
If set to "Keep-alive", the device will send the STUN packets to maintain the connection that is first established during registration of the device. The "Keep-alive" packets will fool the NAT device into keeping the connection open and this allows the host server to send SIP requests directly to the registered device.
If the device needs to use OpenVPN to connect to host server, please set it to "VPN".

If the firewall and the SIP device behind the firewall are both able to use UPnP, it can be set to "UPnP". Both parties will negotiate the port used to allow SIP packets to go through.

If it is set to "TURN", the protocol is designed to be used as part of the ICE (Interactive Connectivity Establishment) approach to NAT Traversal.

The default setting is "Keep-alive". |
| **Proxy-Require** | It is used to add the Proxy-Required header in the SIP message. It is used to indicate proxy-sensitive features that must be supported by the proxy. Do not configure this parameter unless this feature is supported on the SIP server. |

Account/SIP/SIP Settings

Parameters	Descriptions
SIP Registration	It is used to set if allowing the device to send SIP Register messages to the proxy/server. The default setting is "Yes".
Unregister Before New Registration	If it is set to "All", the SIP user's registration information will be cleaned when the device starts pre-registration after rebooting. The SIP Contact header will contain "*" to notify the server to unbind the connection. If set to "Instance", the device only cleans the current SIP user's info. The default setting is "Instance".
Register Expiration (m)	It is used to configure the time period (in minutes) in which the device refreshes its registration with the specified registrar. The default setting is 60. The maximum value is 64800 (about 45 days) and the minimum value is 1 minute.
Subscribe Expiration (m)	Specifies the frequency (in minutes) in which the device refreshes its subscription with the specified register server. The maximum value is 64800(about 45 days).
Registration Retry Wait Time (s)	It is used to configure the time period (in seconds) in which the device will retry the registration process in the event that is failed. The default setting is 20. The maximum value is 3600 (1 hour).
Local SIP Port	It is used to configure the local SIP port used to listen and transmit. The default setting is 5060. The valid range is from 5 to 65535.
SUBSCRIBE for MWI	It is used to set if the device will subscribe voice message service. If it is set to "Yes", the device will periodically send SIP SUBSCRIBE message for Message Waiting Indication service. GVC3220 supports both synchronized and non-synchronized MWI. The default setting is "No".
Enable Session Timer	It is used to set if the device will use the session timer. If it is set to "Yes", it will be added in the SIP INVITE message to notify the server. The default setting is "Yes".
Session Expiration (s)	It is used to configure the device's SIP session timer. It enables SIP sessions to be periodically "refreshed" via a SIP request (UPDATE, or re-INVITE). If there is no refresh via an UPDATE or re-INVITE message, the session will be terminated once the session interval expires. Session Expiration is the time (in seconds) where the session is considered timed out, provided no successful session refresh transaction occurs beforehand. The default setting is 180 with a valid range from 90 to 64800.
Min-SE (s)	It is used to configure the minimum session expiration timer (in seconds) if the device acts as a timer refresher. The default setting is 90. The valid range is from 90 to 64800.
UAC Specify Refresher	It is used to set the party which will refresh the active session if the device makes outbound calls. If it is set to "UAC" and the remote party does not support Refresher feature, the device will refresh the active session. If it is set to "UAS", the remote party will refresh it. If it is set to "Omit", the header will be omitted so that it can be selected by the negotiation mechanism. The default setting is "Omit".

UAS Specify Refresher	It is used to set the party which will refresh the active session if the device receives inbound calls. If it is set to "UAC", the remote party will refresh the active session. If it is set to "UAS" and the remote party does not support refresh feature, the device will refresh it. The default setting is "UAC".
Force INVITE	It is used to set the SIP message type to refresh the session. If it is set to "Yes", the Session Timer will be refreshed by using the SIP INVITE message. Otherwise, the device will use the SIP UPDATE or SIP OPTION message. The default setting is "No".
Caller Request Timer	This is used to set the caller party to act as refresher. If set to "Yes" and both parties support session timers, the device will enable the session timer feature when it makes outbound calls. The SIP INVITE will include the content "refresher=uac". The default setting is "No".
Callee Request Timer	This is used to set the callee party to act as refresher. If set to "Yes" and both parties support session timers, the device will enable the session timer feature when it receives inbound calls. The SIP 200 OK will include the content "refresher=uas". The default setting is "No".
Force Timer	It is used to activate the session timer feature on the device. If it is set to "Yes", the device will use the session timer even if the remote party does not support this feature. If it is set to "No", the device will enable the session timer only when the remote party supports this feature. To turn off the session timer, select "No". Default setting is "No".
Enable 100rel	It is used to activate the PRACK (Provisional Acknowledgment) method. This option is very important to support PSTN internetworking. PRACK improves the network reliability by adding an acknowledgement system to the provisional Responses (1xx). If set to "Yes", the device will respond to the 1xx response from the remote party. The default setting is "No".
Caller ID Display	It is used to set the header tag from the SIP INVITE message for the Caller ID display. If it is set to Auto, the device will use one of the available headers in the priority hierarchy of P-Asserted Identify Header, Remote-Party-ID Header and From Header. If it is set to "From Header", it will use the From Header information for the Caller ID. If it is set to "Disabled", all the incoming calls Caller ID will be displayed with "Unavailable". The default setting is "Auto".
Use Privacy Header	Controls whether the Privacy header will present in the SIP INVITE message or not, whether the header contains the caller info. When set to "default", the Privacy Header will show in INVITE only when "Huawei IMS" special feature is on. If set to "Yes", the Privacy Header will always show in INVITE. If set to "No", the Privacy Header will not show in INVITE. The default setting is "Default".
Use P-Preferred-Identity Header	It is used to set if the P-Preferred-Identity Header will be presented in the SIP INVITE message. If set to "default", the P-Preferred-Identity Header will be omitted in SIP INVITE message when "Huawei IMS" special feature is active. If set to "Yes", the P-Preferred-Identity Header will always be presented. If set to "No", it will be omitted. The default setting is "Default".

Use Mac Header	Configures whether to use MAC header. If set to "No", all SIP messages will not contain MAC header; If set to "Only for REGISTER", MAC header will only be included in SIP REGISTER and UNREGISTER messages; If set to "Yes to All SIP", all outgoing SIP REGISTER messages will contain MAC header.
Add MAC In User-Agent	Configures whether to add MAC address in User-Agent header. If set to "No", all outgoing SIP messages will not attach MAC address to the User-Agent header; If set to "Yes except REGISTER", all outgoing SIP messages except REGISTER message will attach the MAC address to the User-Agent header; If set to "Yes to All SIP", all outgoing SIP messages including REGISTER message will attach MAC address to the User-Agent header.
SIP Transport	It is used to set the protocol used to transport the SIP message. It can be selected from TCP/UDP/TLS. The default setting is "UDP".
RTP IP Filter	It is used to configure whether to filter received RTP packets. The options are "Close", "IP Only" and "IP and Port". The default setting is "Disable". This setting can be used with "Symmetric RTP". Please see below: • **Symmetric RTP = No, RTP IP Filter = Close** The device sends RTP packets to the IP:Port included in SDP and accepts RTP packets from any address. • **Symmetric RTP = Yes, RTP IP Filter = Close** The device sends RTP packets to the IP:Port where the RTP packets come from and accepts RTP packets from any address. • **Symmetric RTP = No, RTP IP Filter = IP Only** The device sends RTP packets to the IP:Port included in SDP and only accepts RTP packets from the IP in the SDP. • **Symmetric RTP = Yes, RTP IP Filter = IP Only** The device sends RTP packets to the IP:Port where the RTP packets come from and only accepts RTP packets from the IP in the SDP. • **Symmetric RTP = Yes, RTP IP Filter = IP and Port** The device only sends RTP packets to the IP:Port included in SDP and only accepts RTP packets from the IP:Port in the SDP.
RTP Timeout (s)	Configures the RTP timeout of the phone. If the phone does not receive the RTP packet within the specified RTP time, the call will be automatically disconnected. The default range is 0-600. If set to 0, the phone will not hang up the call automatically.
SIP URI Scheme When Using TLS	It is used to set SIP header – "SIP" or "SIPs", which will be used if TLS is selected for SIP Transport. The default setting is "SIP".

Use Actual Ephemeral Port in Contact with TCP/TLS	It is used to set the port information in the Via header and Contact header of SIP message when the device uses TCP or TLS. If set to "No", these port numbers will use the permanent listening port on the device. Otherwise, they will use the ephemeral port for the particular connection. The default setting is "No".
RFC2543 Hold	If yes, c=0.0.0.0 will be used in INVITE SDP for hold.
Symmetric RTP	It is used to enable the symmetric RTP mechanism. If set to "Yes", the device will use the same socket/port for sending and receiving the RTP messages. Default is "No".
Support SIP Instance ID	It is used to set if the device will send SIP Instance ID. The SIP instance ID is used to uniquely identify the device. If set to "Yes", the SIP Register message Contact header will include +SIP instance tag. The default setting is "Yes".
Validate Incoming SIP Messages	It is used to set if the device will check the incoming SIP messages caller ID and Cseq headers. If the message does not include the headers, it will be rejected. The default setting is "No".
Check SIP User ID for Incoming INVITE	It is used to set if the device will check the SIP User ID in the Request URI of the SIP INVITE message from the remote party. If it does not match the SIP User ID. configured on the device, the call will be rejected. If set to "Yes", this feature will be active. The default setting is "No".
Authenticate Incoming INVITE	It is used to set if the device will authenticate the SIP INVITE message from the remote party. If set to "Yes", the device will challenge the incoming INVITE for authentication with SIP 401 Unauthorized response. The default setting is "No".
SIP Realm Used for Challenge INVITE & NOTIFY	This is used to verify incoming INVITE and NOTIFY (including check-sync, re-sync, and reboot). It is only effective when SIP authentication is enabled.
Only Accept SIP Requests from Known Servers	It is used to set if the device will answer the SIP request from saved servers. If set to "Yes", only the SIP requests from saved servers will be accepted and the SIP requests from the unregistered server will be rejected. The default setting is "No".
SIP T1 Timeout	It is used to define an estimate of the round-trip time of transactions between a client and server. If no response is received in T1, the figure will increase to 2*T1 and then 4*T1. The request re-transmit retries would continue until a maximum amount of time define by T2. The default setting is 0.5 second.
SIP T2 Timeout	It is used to define the maximum retransmit time of any SIP request messages (excluding the SIP INVITE message). The re-transmitting and doubling of T1 continues until it reaches the T2 value. The default setting is 4 second.

Parameters	Descriptions
Remove OBP from Route	It is used to set if the device will remove outbound proxy URI from the Route header. This is used for the SIP Extension to notify the SIP server that the device is behind a NAT/Firewall. If it is set to "Yes", it will remove the Route header from SIP requests. The default setting is "No".
Check Domain Certificates	It is used to set if the device will check the domain certificates if TLS/TCP is used for SIP Transport.
Validate Certification Chain	When the SIP transport protocol is "TLS" and this option is enabled, the certificates in device system and the trusted CA certificates uploaded by the user will be validated.

Account/SIP/Codec Settings

Parameters	Descriptions
Audio	
DTMF	It is used to set the parameter to specify the mechanism to transmit DTMF (Dual Tone Multi-Frequency) signals. There are 3 supported modes: • **In audio** DTMF is combined in the audio signal (not very reliable with low-bit-rate codecs). • **RFC2833** Specify DTMF with RTP packet. Users could know the packet is DTMF in the RTP header as well as the type of DTMF. • **SIP INFO** Use SIP INFO to carry DTMF. The disadvantage of this mode is that it is easy to cause desynchronized of DTMF and media packet if the SIP and RTP messages are required to transmitted, respectively. The default setting is "RFC2833".
DTMF Payload Type	It is used to configure the RTP payload type that indicates the transmitted packet contains DTMF digits. The valid range is from 96 to 127. The default setting is "101".
Preferred Audio Codec	It lists the available and enabled audio codecs for this account. Users can enable the specific audio codecs by moving them to the Selected box and set them with a priority order from top to bottom. This configuration will be included with the same preference order in the SIP SDP message. The codec option includes "PCMU", "PCMA", "Opus", "G.722", "G.722.1", "G.722.1c", iLBC, G.729A/B.
Codec Negotiation Priority	It is used to configure the codec negotiation sequence when the GVC3220 is acted as a callee. If set to "Caller", the device will negotiate codec by SDP codec sequence from the received SIP INVITE message. If set to "Callee", the device will negotiate codec according to the codec priority configuration on the device itself. The default setting is "Callee".

Silence Suppression	It is used to set the silence suppression/VAD feature. If it is set to "Yes", when silence is detected, a small quantity of VAD packets (instead of audio packets) will be sent during the period of no talking. If set to "No", this feature is disabled. The default setting is "No".
Voice Frames Per TX	It should be noted that the "ptime" value for the SDP will change with different configurations here. This value is related to the codec used and the actual frames transmitted in payload during the call. e.g.: if set to 2 and the first codec is G.729 or G.711, the "ptime" value is 20ms for the SDP. If the TX exceeds the maximum allowable value, the device will use and save the maximum allowed value according to what the first codec is. For end users, it is recommended to use the default setting, as incorrect settings may influence the audio quality. The default setting is "2".
G.722.1 Rate	It is used to select encoding rate for G.722.1 codec. It supports 24kbps or 32kbps. The default setting is "24kbps encoding rate".
G.722.1 Payload Type	It is used to configure payload type for G.722.1 codec. The valid range is 100-126. The default setting is "104".
G.722.1C Rate	Selects encoding rate for G.722.1C codec
G.722.1C Payload Type	Enter G.722.1C codec payload type. The valid range is from 96 to 126. The default value is 103.
Opus Payload Type	It is used to configure payload type for Opus codec. The valid range is 96-126. The default setting is "123".
iLBC Frame Size	Selects iLBC packet frame size. Default is 30ms
Use First Matching Codec in 200OK SDP	If set to "Yes", the device will use the first matching vocoder in the sent 200OK SDP as the codec. The default setting is "No".
Enable Audio RED With FEC	If set to "Yes", FEC will be enabled for audio call. The default setting is "No".
Audio FEC Payload Type	Configures audio FEC payload type. The valid range is from 96 to 126. The default value is 121.
Audio RED Payload Type	Configures audio RED payload type. The valid range is from 96 to 126. The default value is 124
Video	
Enable RFC5168 Support	If set to "Yes", the RFC5168 mechanism will be enabled for video call. RFC5168 allows SIP party to request the sender to refresh its video frame in H.264 or refresh the full picture in VP8. The default setting is "Yes".
Packet Retransmission	When the function is enabled, signaling will carry RTX information, if the final negotiation is succeeded, the related media RTX function will realize packet loss retransmission purpose. When this function is disabled. then packet loss retransmission cannot be used.

Enable Video FEC	If enabled, the video sender will temporarily allocate part of the bandwidth to one data channel to send FEC data to system, thus, to improve the video quality the receiver gets. Enabling this function will take up part of bandwidth and reduce call rate. The default setting is "Yes".
FEC Payload Type	It is used to configure FEC payload type. The range is 96-127. The default setting is 120.
Enable FECC	If set to "Yes", You can control the camera of the opposite side for video call, but the opposite site must support FECC, and allow remote control on its local camera. The default setting is "Yes".
FECC H.224 Payload Type	It is used to configure FECC H.224 payload type. The valid range is from 96 to 127. The default value is 125.
SDP Bandwidth Attribute	Select the SDP bandwidth attribute from "Standard", "Media Level" or "None". The default setting is "Media Level". • Standard: Use AS at the session level and TIAS at the media level. • Media Level: Use AS at the media level. • None: Do not change the format. **Note:** Please do not change the format as it may cause decode failure if the user is unclear about what format the server supports.
Video Jitter Buffer Maximum (ms)	Configures the video buffer size according to the network environment. The valid range is 0-1000, the default setting is 50.
Enable Video Gradual Decoder Refresh Function	GDR (Gradual decoder refresh) by P frame including the method of applying I block group to achieve asymptotic refresh. If set to "Yes", GDR will bring better network adaptability. The default setting is "No
Preferred Video Codec	This parameter lets you select your preferred video codec from the "available" list. The H.264 codec is recommended.
Image Size	Selects the image size. The default setting is "1080p".
Video Bit Rate	Configures the bite rate of the video. The video bit rate can be adjusted based on the network environment. Increasing the video bit rate may improve video quality if the bandwidth is permitted. If the bandwidth is not permitted, the video quality will decrease due to packet loss. The default setting depends on H.264 Image Size: • H.264 Image Size = 4k, Video Bit Rate can be set to integer value from 1Mbps to 8Mbps. • H.264 Image Size = 1080p, Video Bit Rate can be set to integer value from 1Mbps to 4Mbps. • H.264 Image Size = 720p, Video Bit Rate can be set to integer value from 512kbps to 2Mbps. • H.264 Image Size = 4SIF/4CIF/VGA, Video Bit Rate can be set to integer value from 384kbps to 1Mbps.

Video Frame Rate	Configures the frame rate for SIP video call. The default is 30 fps. Increase frame rate will take up bandwidth; the video quality will be reduced if not allocated enough bandwidth.
H.264 Payload Type	Enter H.264 codec payload type. The valid range is from 96 to 126. The default value is 99.
Packetization-mode	The packetization mode can be set to 0, 1 or Auto. When it's set to 0 or 1, the INVITE will include packetization mode value as 0 or 1. If it's set to Auto, the INVITE will include both 0 and 1, and the packetization mode value is a result of negotiation between the endpoint and the server. Default setting is 1.
H.264 Profile Type	It is used to set the H.264 profile type. It can be selected from the dropdown list. • Baseline Profile • Main Profile • High Profile • BP&MP&HP The default setting is "BP&MP&HP". Lower profile is easier to decode while higher profile provides higher compression ratio. For device with low CPU, select "Baseline Profile". Also, "Baseline Profile" is likely to be used in a video conference that has high demanding for the video quality.
Use H.264 Constrained Profiles	Configures whether to use H.264 CBP to establish video call with WebRTC. The function takes effect when H.264 profile setting includes BP type. It is recommended to set to "Yes" when establish video call with WebRTC. The default setting is "No".
Presentation settings	
Enable Presentation	If set to "Yes", the device will be able to receive the presentation stream in video calls and video meetings. The default setting is "Yes".
Initial INVITE with media info	If it is enabled, the initial INVITE packet sent from GVC to server will carry BFCP media information. If not, the related media info will be included in re-INVITE packet and the BFCP negotiation with some specific servers might be failed.
Presentation H.264 Image Size	It is used to select the H.264 image size from "720P" or "1080P". The default setting is "1080P".
Presentation H.264 Profile Type	Select the H.264 profile type from "Baseline Profile", "Main Profile", "High Profile" or "BP&MP&HP". The default setting is "BP&MP&HP". Lower profile type is easier to decode, while higher level has higher compression ratio. For device with low CPU, select "Baseline Profile". Also, "Baseline Profile" is likely to be used in a video conference that has high demand for the video quality.

Presentation Video Bit Rate	Configures the bit rate of the video. The video bit rate can be adjusted based on the network environment. Increasing the video bit rate may improve video quality if the bandwidth is permitted. If the bandwidth is not permitted, the video quality will decrease due to packet loss. The default setting depends on presentation H.264 image size. • Presentation H.264 Image Size = 1080p, Video Bit Rate can be set to an integer value from 1024kbps to 4096kbps • Presentation H.264 Image Size = 720p, Video Bit Rate can be set to an integer value from 512kbps to 2048kbps
Presentation Video Frame Rate	Configures the video frame rate for presentation. The options are 5fps, 10fps and 15fps. The default setting is 15fps.
BFCP Transport Protocol	Defines the transport protocol used for BFCP. Users can choose from Auto/UDP/TCP. The default setting is "UDP". If "Auto" is configured, the device will automatically switch between "UDP" and "TCP".
RTP Settings	
SRTP Mode	It is used to set if the device will enable the SRTP (Secured RTP) mode. It can be selected from dropdown list: • Disable • Enabled but not forced • Enabled and forced SRTP uses encryption and authentication to minimize the risk of denial of service. (DoS). If the server allows to use both RTP and SRTP, it should be configured as "Enabled but not forced". The default setting is "Enabled But Not Force".
SRTP Key Length	It is to configure all the AES (Advanced Encryption Standard) key size within SRTP. It can be selected from dropdown list: • AES 128&256 bit • AES 128 bit • AES 256 bit If it is set to "AES 128&256 bit", the device will provide both AES 128 and 256 cipher suite for SRTP. If set to "AES 128 bit", it only provides 128-bit cipher suite; if set to "AES 256 bit", it only provides 256-bit cipher suite. The default setting is "AES 128&256 bit".

Account/SIP/Call Settings

Parameters	Descriptions
Remote Video	It is used to set the preference to handle video request from the remote party during

Request	an audio call. It can be selected from the dropdown list. • "**Prompt**": A message will be prompted if a video request is received. Users can select "Yes" to establish video or "No" to reject the request. • "**Accept**": Video request will be accepted automatically, and video will be established. • "**Deny**": Video request will be rejected automatically. The default setting is "prompt".
Dial Plan Prefix	It is used to configure the prefix to be added to each dialed number. All numbers use this account will automatically add the prefix. e.g.: The prefix is 5, the phone number is 337, and then the dial number is 5337.
Disable Dial plan	Defines whether to disable dial plan when dialing from dial Page, Contact, Call History and Click2Dial. If set to "Yes", dial plan will be disabled for the above cases.
Dial Plan	1. Valid Value: 1,2,3,4,5,6,7,8,9,0,*,#,T； 2. Dial Plan Rules: a) • xx - any 2-digit numbers from 0-9 b) • xx+ - at least 2-digit numbers from 0-9 c) • xx. - at least 1-digit number from 0-9 d) • xx? - 1 or 2 digit numbers from 0-9 e) • ^ - exclude f) • T - dialing delay when matched g) • [3-5] – any digit of 3, 4, or 5 h) [147] - any digit of 1, 4, or 7 i) <2=011> - replace digit 2 with 011 when dialing j) \{x+\} - allow dialing all digit numbers 3. Examples: Example 1: \{[369]11 | 1617xxxxxxx\} Allow 311, 611, and 911 or any 10 digit numbers with leading digits 1617; Example 2: \{^1900x+ | <=1617>xxxxxxx\} Block any number of leading digits 1900 or add prefix 1617 for any dialed 7 digit numbers;
Refer-To Use Target Contact	It is used to set if the device will use the target's Contact header tag to the Refer-To header in the SIP REFER message during an attended transfer. Default setting is "No".
Auto-Answer	It is set to allow answering an incoming call. If it is set to "Yes", the device will automatically enable the speaker phone to answer all the incoming calls after a short reminding beep. If set to "Enable Intercom/Paging", it will automatically answer the incoming calls

	whose SIP INVITE includes auto-answer tag in the info header. The default setting is "No".
Send Anonymous	It is used to set if the device will make an anonymous outgoing call. If it is set to "Yes", the "From" header in the SIP INVITE messages will be set to anonymous, essentially blocking the Caller ID to be displayed. The default setting is "No".
Reject Anonymous Call	If it is set to "Yes", the device will reject the calls whose SIP INVITE message includes Anonymous information in the From header. The default setting is "No".
Call Log	It is used to categorize the call logs saved for this account. If it is set to "Log All", all the call logs of this account will be saved. If set to Log Incoming/Outgoing Calls (Missed Calls Not Record), the whole call history will be saved other than missed call. If it set to Disable Call All, none of the call history will be saved. The default setting is "Log All".
Special Feature	It is to configure device's setting to meet different vendors server requirements. Users can choose from Standard, BroadSoft, CBCOM, RNK, China Mobile, ZTE IMS, Mobotix, ZTE NGN, or Huawei IMS depending on the server type. The default setting is "Standard".
Feature Key Synchronization	It is used for the BroadSoft standard call feature synchronization. If it is enabled, the device will send SIP SUBSCRIBE message to the server and receive SIP NOTIFY message from the server to synchronize the DND, Call Forwarding and Call Center features. The default setting is "Disable".
Enable Call Features	If set to "Yes", call features (including call forwarding, DND and etc.) will be supported locally instead of using the feature code supported on SIP server/proxy. For example, if *72+number is dialed, the incoming calls will be forward to this number unconditionally. The default setting is "No". Refer to the chapter **_Call Features_** for more details in the GVC3220 User Guide.
Ring Timeout (s)	It is used to define the expiration timer (in seconds) for the rings with no answer. The default setting is 60.
Use # as Dial Key	It is used to set the device whether to use the "#" key as the "Send" key. If set to "Yes", if the end user taps the "#" key on the remote control, the device will send out the typed digits. If set to "No", the "#" key is included as part of the dialing string and please make sure the dial plan is properly configured to allow dialing # out. The default setting is "Yes".
Upload Local MOH Audio File	It is used to load the MOH (Music on Hold) file to the device. Click on "Browse" button to upload the music file from local PC. The MOH audio file has to be in .wav or .mp3 format. **Note:** Please be patient while the audio file is being uploaded. It could take more than 3

	minutes to finish the uploading especially the file size is large. The button will show as "Processing" during the uploading. Once done, it will show as "Browse" again. Click on "Save" on the bottom of the web page and "Apply" on the top of the web page to save the change.
Enable Local MOH	If set to "Yes", the local MOH will be enabled. Users need to upload local MOH audio file. Once enabled, users could play the file when holding the call. Default setting is No.
Account Ring Tone	It is used to configure the ringtone for the account. Users can set ringtones from the dropdown list. User can also import customized ringtone from LCD Setting menu. The customized ringtone file name will also be showed up in the dropdown list that allows user to select.
Call forwarding	
Call Forwarding	It is used to set the Call Forwarding feature for this account. • **None**: Setting the feature to NONE will disable Call Forward • **Unconditional**: If set to UNCONDITIONAL, it will forward all calls to a particular number • **Time based**: With TIME BASED forward, set a time range for the calls to be forwarded: - *Schedule***:** Configures the period of time to forward the call when "Time based" Call Forward type is used. The time is 24-hours format HH:mm, 10:00 for example. - *In schedule forward to:* When "Time based" Call Forward Type is used, specifies the number to be forwarded to within the configured Time Period above. - *Out schedule forward to:* When "Time based" Call Forward Type is used, specifies the number to be forwarded to when it is not within the configured Time Period. • **Others**: When set to OTHERS, the call forwarding rules can be customized based on following options: - *Enable busy forward:* If set to "Yes", when the device is busy, call will be forwarded to the number specified below on "Busy to". - *Forward Busy To:* Specifies the number to be forwarded to for Call Forward Busy. - *Enable no answer forward:* If set to "Yes", when there is no answer from the device, call will be forwarded

to the number specified below on "No answer to".

Another field "No answer timeout (s)" is added below to specify the timeout (in seconds) before the call is forwarded on no answer. The default value is 20 seconds.

- *Forward No Answer To:*

Specifies the number to be forwarded to for Call Forward No Answer. When the device is not answering, the new call will be forwarded to this number.

- *No Answer Timeout (s):*

Configures the timeout (in seconds) before the call is forwarded when an incoming call is not answered on the phone. The default value is 20 seconds

- *Enable DND forward:*

If set to "Yes", call will be forwarded to the number specified below on "DND to", when the phone is activating DND.

- *Forward DND To:*

Specifies the number to be forwarded to when DND is on.

Ringtone

| **Match Incoming Caller ID** | It is used to specify the rules for the incoming calls. If the incoming caller ID or Alert Info matches the number, pattern or Alert Info text rules, the device will play the selected distinctive ringtone.
The rule policy:
• Specific caller ID number. For example, 8321123
• A defined pattern with certain length using **x** and **+** to specify, where **x** could be any digit from 0 to 9.
Samples:
xx+: at least 2-digit number
xx: only 2-digit number
[**345**]**xx**: 3-digit number with the leading digit of 3, 4 or 5
[**6-9**]**xx**: 3-digit number with the leading digit from 6 to 9
• Alert Info text
 Users could configure the matching rule as certain text (e.g., priority) and select the custom ring tone mapped to it.
The custom ring tone will be used if the device receives SIP INVITE with Alert-Info header in the following format:
Alert-Info: <http://127.0.0.1>; info=priority |
| **Distinctive Ring** | It is used to select the distinctive ring tone if the incoming caller ID matched the |

Tone	specified Matching Incoming Caller ID rule. If so, the device will play the selected ringtone.

Account/IPVideoTalk/General Settings

Parameters	Descriptions
Enable IPVideoTalk	Enable IPVideoTalk service, if set to "YES", the system will support IPVideoTalk related functions. The default value is "YES", which will take effect after restart. Need reboot to take effect.
Account Active	This field indicates whether the account is active. The default value for account H.323 is "No" and the default value for the other accounts is "Yes."
Display Name	The SIP server subscriber's name (optional) that will be used for Caller ID display.
SIP Transport	Determines the network protocol used for the SIP transport. For IPVideoTalk and Zoom, users can choose from TCP/TLS. For other accounts, users can choose from TCP/UDP/TLS.

Account/IPVideoTalk/Codec Settings

Parameters	Descriptions
Preferred Video Codec	This parameter lets you select your preferred video codec from the "available" list. The H.264 codec is recommended
Image Size	Selects the image size. The default setting is "1080p".
Video Bit Rate	Configures the bite rate of video calls. The video bit rate can be adjusted based on the network environment. Increasing the video bit rate may improve video quality if there is available bandwidth. If the bandwidth is exceeded than the video quality will decrease due to packet loss. The default setting depends on Image Size: **Image Size = 1080p**, Video Bit Rate can be set to integer value from 1Mbps to 4Mbps. **Image Size = 720p**, Video Bit Rate can be set to integer value from 512kbps to 2Mbps. **Image Size = 4SIF/4CIF/VGA**, Video Bit Rate can be set to integer value from 384kbps to 1Mbps.

Account/IPVideoTalk/Call Settings

Parameters	Descriptions
Auto Answer When Idle	If set to "Yes", the device will automatically turn on the speaker to answer incoming calls after a short reminder beep. The default setting is "No".

Account/H.323/General Settings

Parameters	Descriptions
Account Active	This field indicates whether the H.323 account is active. The default setting is "No".
Enable GK	This defines whether to enable GK. If enabled, the device will register to GK automatically. The default setting is "No".
Enable H.460	It is used to define whether to enable H.460.18/19 to support H.323 account, in order to make the IP calls through public Internet without intermediate nodes. To use this feature, set "Use NAT IP" to the public IP for GVC3220 under GVC3220 web UI→**Settings**→**General Settings**.
GK Discover Mode	This configures GK discover mode to be "Auto" or "Manual". • If set to "Auto", the device will discover GK automatically and register to GK. • If set to "Manual", please configure "GK Address" and "Site Number". The device will discover GK via GK address and register to GK. The default setting is "Auto".
Site Number	It used to configure H.323 conference ID of the GVC3220. The GVC3220 can be reached by calling the site number. The site number is numeral only.
GK Authentication Username	Enter the username for GK authentication.
GK Authentication Password	Enter the password for GK authentication.
Voice Mail Access Number	This ID is usually the VM portal access number. For example, in Asterisk server, 8500 could be used.
Register Expiration (m)	This specifies the frequency (in minutes) in which the device refreshes its registration with the specified registrar. The default value is 60 minutes (1 hour). The maximum value is 1,440 minutes (1 day). The minimum value is 1 minute.
H.323 Local Port	This defines the local H.323 port used to listen. Default value is 1720.

	It is used to enable the symmetric RTP mechanism. If set to "Yes", the GVC3220 will use the same socket/port for sending and receiving the RTP messages. The default
Symmetric RTP	setting is "No".

Account/H.323/Codec Settings

Parameters	Descriptions
DTMF	This parameter specifies the mechanism to transmit DTMF digits. There are 3 supported mode: • In audio • RFC2833 • H245 signal.
Preferred Audio Codec	PCMA, PCMU, G.722, G.722.1 and G.722.1C are supported on the device for the H.323 account. Users can select the audio codec from the "Available" list to "Selected" list and configure the audio codec priority by adjusting the order in the "Selected" list. The "Selected" vocoders will be included in the SDP message with the same order.
Image Size	It is used to set the H.264 image size. It can be selected from the dropdown list. • 1080P • 720P • 4CIF • 4SIF • VGA The default setting is 1080P.
Video bit rate	It is used to configure the bit rate of the video device. The default setting is 2048kpbs. It is recommended to increase bit rate if bandwidth allows. If the bandwidth is not enough, the video quality will be reduced. • H.264 Image Size = 1080p, the Video Bit Rate can be set to a value from 2048kbps to 4096kbps. • H.264 Image Size = 720p, the Video Bit Rate can be set to a value from 1024kbps to 2048kbps. H.264 Image Size = 4SIF/4CIF/VGA, the Video Bit Rate can be set to a value from 384 to 1024 Kbps.
Video frame rate	It is used to configure the video frame rate. The supported video frame rates are 5 fps, 15fps, 25 fps, 30 fps and VFR. The default setting is "30 fps".
H.264 payload type	It is used to configure the H.264 codec message payload type format. The default setting is 99. The valid range is from 96 to 127.
Packetization Mode	The packetization mode (0, 1 or Auto) for the video packets. The default setting is 0

Account/H.323/Call Settings

Parameters	Descriptions
Auto-Answer	If set to "Yes", the device will automatically turn on the speaker to answer incoming calls after a short reminder beep. The default setting is "No".
Enable H225 Keep-alive	If enabled, the device will only send H255 keep-alive as callee and the interval is 19 seconds. The default setting is "No".
Enable H245 Keep-alive	If enabled, the device will send H245 keep-alive packet as caller or callee, and the interval is 19 seconds. The default setting is "No".
Enable RTDR	If enabled, the device will send RTDP (Round Trip Delay Request) packet as H245 keep-alive packet every 10 seconds. The timeout interval is 30 seconds and will hang up the call once timed out. The default setting is "No". **Note:** If enabled, it may cause incompatibility issue with certain devices.

Account/ Video Conf Service Platform/Bluejeans/General Settings

Parameters	Descriptions
Account Active	It is used to indicate whether if the BlueJeans account is active. The default setting is "Yes".
Display Name	It is used to define the displayed name shown on the callee side once the GVC3220 makes a BlueJeans call.

Account/ Video Conf Service Platform/Bluejeans/Codec Settings

BlueJeans account Codec section is the same as on SIP account. Please refer to the Account/SIP/Codec Settings section for more details.

Account/ Video Conf Service Platform/Bluejeans/Call Settings

Parameters	Descriptions
Call Log	Configures Call Log settings on the device. The default setting is "Log All".
Use # as Dial Key	Allows users to configure the "#" key as the "Send" key. If enabled, the "#" key will immediately dial out the entered digits. In this case, this key is essentially equivalent to the "Send" key. If set to "No", the "#" key is treated as part of the dialed string.
Upload Local MOH Audio File	Click Browse to upload audio file from PC. The MOH audio file should be ".wav" or ".mp3" format. It may take a long time uploading and processing the file, please be patient.
Enable Local MOH	If set to "Yes", the local MOH will be enabled. A local MOH audio file needs to be uploaded for this feature to work. Once enabled, the phone will play the file while

| | holding a call. The default setting is "No". |

Account/ Video Conf Service Platform/Zoom/General Settings

Parameters	Descriptions
Account Active	It is used to indicate whether if the Zoom account is active. The default setting is "Yes".
Zoom Server	The URL or IP address, and port of the Zoom server. This is provided by your VoIP service provider (ITSP).
Display Name	The SIP server subscriber's name (optional) that will be used for Caller ID display.

Account/ Video Conf Service Platform/Zoom/SIP Settings

Zoom SIP Settings section is the same as on SIP account. Please refer to the Account/SIP/SIP Settings section for more details.

Account/ Video Conf Service Platform/Zoom/Codec Settings

Zoom account Codec section is the same as on SIP account. Please refer to the Account/SIP/Codec Settings section for more details.

Account/ Video Conf Service Platform/Zoom/Call Settings

Parameters	Descriptions
Call Log	Configures Call Log settings on the device. The default setting is "Log All".
Use # as Dial Key	Allows users to configure the "#" key as the "Send" key. If enabled, the "#" key will immediately dial out the entered digits. In this case, this key is essentially equivalent to the "Send" key. If set to "No", the "#" key is treated as part of the dialed string.
Upload Local MOH Audio File	Click Browse to upload audio file from PC. The MOH audio file should be ".wav" or ".mp3" format. It may take a long time uploading and processing the file, please be patient.
Enable Local MOH	If set to "Yes", the local MOH will be enabled. A local MOH audio file needs to be uploaded for this feature to work. Once enabled, the phone will play the file while holding a call. The default setting is "No".

Call Features

Call Features/General Settings

Parameters	Descriptions

Local RTP Port	This parameter defines the local RTP-RTCP port pair used to listen and transmit. It is the base RTP port for channel 0. When configured, for audio, channel 0 will use this port_value for RTP and the port_value+1 for its RTCP; channel 1 will use port_value+6 for RTP and port_value+7 for its RTCP. For video, channel 0 will use port_value+2 for RTP and port_value+3 for its RTCP; channel 1 will use port_value+8 for RTP and port_value+9 for RTCP. The default value is 5004.
Use Random Port	When set to "Yes", this parameter will force random generation of both the local SIP and RTP ports. This is usually necessary when multiple devices are behind the same full cone NAT. The default setting is "No". **Note:** This parameter must be set to "No" for Direct IP Calling to work.
Keep-alive Interval (s)	It is used to specify how often the device will send a Binding Request packet to the SIP server in order to keep the "ping hole" on the NAT router to open. The default setting is 20 seconds. The valid range is from 10 to 160.
STUN/TURN Server	It is used to configure the URI of STUN (Simple Traversal of UDP for NAT) / TURN (Traversal Using Relays around NAT) server. The device will send STUN Binding Request packet to the STUN server to learn the public IP address of its network. Only non-symmetric NAT routers work with STUN. The default setting is "stun.ipvideotalk.com".
TURN Server Username	It is used to configure the username for TURN server.
TURN Server Password	It is used to configure the password for TURN server.
Use NAT IP	It is used to configure the IP address for the Contact header and Connection Information in the SIP/SDP message. It should ONLY be used if it is required by your ITSP. The default setting is keep the box blank.

Call Features/Call Settings

Parameters	Descriptions
Audio	
Enable Call-waiting Tone	If set to "No", the call waiting tone will be disabled. In this case, only the LED indicator will blink to remind call waiting status. The default setting is "Yes".
Enable DND Reminder Ring	If set to "No", when DND feature is on, the ring splash reminder for incoming calls will be muted. The default setting is "Yes".
Auto Mute On Entry	Configures whether to mute the call on entry automatically. If set to "Disable", then do not use auto mute function; If set to "Auto Mute on Outgoing Call", then mute

	automatically when the other party answers the outgoing call; If set to "Auto Mute on Incoming Call", then mute automatically when answers the incoming call; If set to "Mute on Incoming & Outgoing Call", then mute automatically when the call gets through. **Note:** this function only take effect when the phone is from the idle status to call status. Users could click the Mute button on call interface to cancel the current mute status. The default setting is "Disable".
Rules	
Escape "#" as "%23" in SIP URI	Replaces "#" by "%23" for some special situations. The default setting is "Yes".
Enable In-call DTMF Display	When it is set to "No", the DTMF digits entered during the call will not display. The default setting is "Yes".
Filter Characters	Set the characters to filter when dialing out numbers. Users could set up multiple characters. For example, if set to "[()-]", when dialing (0571)-8800-8888, the character "()-" will be automatically filtered and the device will dial 057188008888 directly instead. Note: this function does not work on the local call page of the device.
Enable Call-waiting	Enables the call waiting feature. The default setting is "Yes".
Enable Direct IP Call	Enables Direct IP Call. The default setting is "Yes".

Call Features/Site Name

Parameters	Descriptions
Site Name	Specifies the site name to be imposed on the video of local video. When joining a multipoint conference, this site name is displayed in other participants' video. The default value is null.
Background Transparency	Set the display background transparency to be Opaque, 5%, 10%,15% and 20%. The default setting is "Opaque".
Display Position	It is used to configure the site name's position to be at Upper Left Corner, Upper Right Corner, Lower Left Corner or Lower Right Corner on the video. The default setting is "Upper Left Corner".
Display Duration	It is used to configure the duration to display the site name. The options are "Do Not Display", "1 Minute", "5 Minutes", "10 Minutes" or "Always Display". The default setting is "Always Display".
Font Color	It is used to specify the color in which the site name is displayed. Click on the field and color selection will be available for the user to choose. The default color is white.
Font Size	It is used to specify the font size for the site name display. The user could select from

	the smallest to the largest. The default value is Medium.
Bold	It is used to specify whether the site name is displayed in bold. The default value is No.
Horizontal Offset	Fine-tunes the site name's position left or right on the local video. Value range: 0%-100%. The default value is 0%.
Vertical Offset	Fine-tunes the site name's position up or down on the local video. Value range: 0%-100%. The default value is 0%.

Call Features/Audio Control

Parameters	Descriptions
GMD Pickup Distance	Set the range of GMD pickup distance during AEC calibration. After saving, please conduct AEC calibration at the terminal and check the audio effect. Select "Auto" and the GMD pickup distance will be automatically configured during AEC calibration. The default value is "Auto".
Echo Delay	Configures the device's HDMI audio delay to match the audio latency of different TV sets.
Ringtone Volume	Users can slide left or right to adjust ringtone volume.
Media Volume	Users can slide left or right to adjust media volume.
Device Ringtone	Select device ringtone from the dropdown list.
Notification Ringtone	Select device notification ringtone from the dropdown list.
Audio Device	Set the audio input/output device for call or media voice.
Ring Back Tone	Configures tone frequencies based on parameters from the local telecom provider. By default, they are set to the North American standard. Frequencies should be configured with known values to avoid uncomfortable high pitch sounds. Syntax: f1=val,f2=val [,c=on1/off1[-on2/off2[-on3/off3]]];(Frequencies are in Hz and cadence on and off are in 10ms)ON is the period of ringing ("On time" in 'ms') while OFF is the period of silence. In order to set a continuous ring, OFF should be zero. Otherwise it will ring ON ms and a pause of OFF ms and then repeat the pattern. Up to three cadences are supported.
Busy Tone	Configures tone frequencies based on parameters from the local telecom provider. By default, they are set to the North American standard. Frequencies should be configured with known values to avoid uncomfortable high pitch sounds. Syntax: f1=val,f2=val [,c=on1/off1[-on2/off2[-on3/off3]]];(Frequencies are in Hz and cadence on and off are in 10ms)ON is the period of ringing ("On time" in 'ms') while OFF is the period of silence. In order to set a continuous ring, OFF should be zero. Otherwise it will ring ON ms and a pause of OFF ms and then repeat the pattern. Up to three cadences are supported.

Reorder Tone	Configures tone frequencies based on parameters from the local telecom provider. By default, they are set to the North American standard. Frequencies should be configured with known values to avoid uncomfortable high pitch sounds. Syntax: f1=val,f2=val [,c=on1/off1[-on2/off2[-on3/off3]]];(Frequencies are in Hz and cadence on and off are in 10ms)ON is the period of ringing ("On time" in 'ms') while OFF is the period of silence. In order to set a continuous ring, OFF should be zero. Otherwise it will ring ON ms and a pause of OFF ms and then repeat the pattern. Up to three cadences are supported.
Confirmation Tone	Configures tone frequencies based on parameters from the local telecom provider. By default, they are set to the North American standard. Frequencies should be configured with known values to avoid uncomfortable high pitch sounds. Syntax: f1=val,f2=val [,c=on1/off1[-on2/off2[-on3/off3]]];(Frequencies are in Hz and cadence on and off are in 10ms)ON is the period of ringing ("On time" in 'ms') while OFF is the period of silence. In order to set a continuous ring, OFF should be zero. Otherwise it will ring ON ms and a pause of OFF ms and then repeat the pattern. Up to three cadences are supported.
Default Ring Cadence	Configure the default ring cadence for the ring back tone. The default setting is c=2000/4000;

Call Features/Video Settings

Parameters	Descriptions
Start Video Automatically	It is used to set if the device will enable the video feature automatically when it makes an outbound call. If set to "Yes", the video codec attributes will be included in the SIP INVITE message. Or the attributes will not be included. The default setting is "Yes".
Video Display Mode	Set the video display mode to "Original proportion" or "Proportional add black edge". If set to "Original proportion", the device displays video in its original proportion that received from remote party, if the remote video display proportion is different from the device, the device will stretch or compress video to display it; If set to "Proportional add black edge", the device will display video in its original proportion, if still exists spare space, the device will add black edge on it. The default setting is "Original proportion".
Enable Frame Skipping in Video Decoder	It is used to reduce video distortion. If set to "Yes", the GVC3220 will skip the P frame in lost video packet to decode I frame in the next video packet. The default setting is "No".
Share Screen	
Presentation Image Size	Selects the presentation image size. Default is 1080P.

Parameters	Descriptions
Presentation Video Bit Rate	Configures the bit rate of the video. The video bit rate can be adjusted based on the network environment. Increasing the video bit rate may improve video quality if the bandwidth is permitted. If the bandwidth is not permitted, the video quality will decrease due to packet loss.
Presentation Video Frame Rate	Configure the video frame rate for presentation. Default is 15fps.

Network Settings

Network Settings lists Basic Settings, Wi-Fi, OpenVPN®, and Advanced Settings.

Network Settings/Ethernet Settings

Parameters	Descriptions
Preferred Internet protocol	Allows user to select the preferred Internet Protocol whether IPv4 or IPv6.
IPv4	
Address Type	Allows users to configure the appropriate network settings on the device. Users could select "DHCP", "Static IP" or "PPPoE". By default, it is set to "DHCP". • **DHCP**: Obtain the IP address via one DHCP server in the LAN. ALL domain values about static IP/PPPoE are unavailable (although some domain values have been saved in the flash.) • **PPPoE**: Configures PPPoE account/password. Obtain the IP address from the PPPoE server via dialing. • **Static IP**: Manually configures IP Address, Subnet Mask, Default Router's IP Address, DNS Server 1, and DNS Server 2.
DHCP VLAN override	DHCP Option 132 defines VLAN ID and DHCP Option 133 defines priority tag ID. GVC3220 supports DHCP VLAN override via DHCP Option 132 and DHCP Option 133, or encapsulated DHCP Option 132 and DHCP Option 133 in DHCP Option 43. Users could select "Disable", "DHCP Option 132 and DHCP Option 133", or "Encapsulated in DHCP Option 43". By default, it is set to "Encapsulated in DHCP Option 43": • When set to "DHCP Option 132 and DHCP Option 133", the GVC3220 will get DHCP Option 132 as VLAN ID and get DHCP Option 133 as VLAN priority, from the DHCP server directly. • When set to "Encapsulated in DHCP Option 43", the GVC3220 will get VLAN ID and VLAN priority value from the DHCP Option 43 which has DHCP Option 132 and DHCP Option 133 encapsulated. In this case, please make sure the option "Allow DHCP Option 43 and Option 66 to Override Server" is enabled.

Host name (Option 12)	It is used to configure the name of the client in the DHCP request. It is optional but may be required by some Internet Service Providers.
Vendor Class ID (Option 60)	It is used to configure the vendor class ID header in the DHCP request. The default setting is "Grandstream GVC3220".
Layer 2 QoS 802.1Q/VLAN Tag (Ethernet)	It is used to define the VLAN Identifier of the Layer 2 frames. The default value 0 which means the frame does not belong to any VLAN. **Note:** Please do not change the setting before understanding the VLAN's settings. Otherwise the device cannot get the correct IP address.
Layer 2 QoS 802.1p Priority Value (Ethernet)	It is used to define the Priority Code Point within a Layer 2 frame header. The valid range from 0 to 7. The Default value is 0 which is equivalent to the Routine class for the Class of Service. Need reboot to take effect.
IP Address	It is used to configure the device's static IP address if the static IP is used.
Subnet Mask	It is used to configure the network's subnet mask if the static IP is used.
Gateway	It is used to configure the network's gateway address if the static IP is used.
DNS Server 1	It is used to configure the primary DNS IP address if the static IP is used.
DNS Server 2	It is used to configure the secondary DNS IP address if the static IP is used.
PPPoE Account ID	It is used to configure the PPPoE account ID if the PPPoE is used.
PPPoE Password	It is used to configure the PPPoE password if the PPPoE is used.
IPv6	
IPv6 Address	Allows users to choose whether to get automatically the IPv6 address from DHCP server (Auto-configured) or configure a static IPv6 address (Statically configured). Default is Auto configured.
Static IPv6 Address	It is used to configure a static IPv6 address if Statically configured is used.
IPv6 Prefix Length	It is used to set the IPv6 prefix length if Statically configured is used. Default is 64.
DNS Server 1	It is used to configure the primary DNS IP address if Statically configured is used.
DNS Server 2	It is used to configure the secondary DNS IP address if Statically configured is used.
Preferred DNS Server	It is used to configure the preferred DNS server.
802.1x Mode	
802.1x Mode	It is used to enable and select the 802.1x mode for the device. The supported 802.1x modes are: • EAP-MD5 • EAP-TLS • EAP-PEAP The default setting is "Disable".

802.1x Identity	It is used to fill in the identity information for the selected 802.1x mode. This setting will be displayed only if 802.1x mode is enabled.
802.1x Secret	It is used to enter the secret for the 802.1x mode. This setting will be displayed only if the 802.1x mode is enabled.
Private Key	It is used to enter the private key password for the 802.1x mode. This setting will be displayed only if the 802.1x mode is enabled.
CA Certificate	It is used to upload the CA Certificate file to the device. This setting will be displayed only if the 802.1x mode is enabled.
Client Certificate	It is used to load the Client Certificate file to the device. This setting will be displayed only if the 802.1x TLS mode is enabled.

Network Settings/Wi-Fi Settings

Parameters	Descriptions
Wi-Fi Function	This parameter enables/disables the Wi-Fi function. The default setting is set to "No"
ESSID	This parameter sets the ESSID for the Wireless network. Press "Scan" to scan for the available wireless network. The number in brackets represents the signal intensity.
Add Network	
ESSID	Enter the ESSID name.
Security Mode For Hidden SSID	This parameter defines the security mode used for the wireless network when the SSID is hidden.
Advanced Settings	
Country Code	Configures the Wi-Fi country code. The default value is "US". Need reboot to take effect.

Network Settings/OpenVPN® Settings

Parameters	Descriptions
Enable OpenVPN®	Enables/disables OpenVPN® functionality and requires the user to have access to an OpenVPN® server. Note: To use OpenVPN® functionalities, users must enable OpenVPN® and configure all of the settings related to OpenVPN®, including server address, port, OpenVPN® CA, certificate, and key. Additionally, the user must also set the SIP account to use "VPN" for the "NAT Traversal" (under Account → Network Settings).
OpenVPN® Mode	Simple mode only supports some basic or common parameters configuration; Professional mode supports configuration file upload in zipped format, which is totally customized by need, please refer to https://openvpn.net for more information.

Enable OpenVPN® Comp-Izo	Enables/disables the LZO compression. When LZO compression is enabled on the OpenVPN server, this option needs to be checked otherwise there will be a network connection failure. The P-value for this functionality is P8508 with two possible values 0 and 1; 0 – OFF/1 - ON. Default setting is NO.
OpenVPN® Server Address	Defines the URL/IP address for the OpenVPN® server.
OpenVPN® Port	Defines the network port for the OpenVPN® server. The default setting is 1194.
OpenVPN® Transport	Determines network protocol used for OpenVPN® (UDP or TCP). The default setting is TCP.
OpenVPN® CA	OpenVPN® CA file (ca.crt) required by the OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device.
OpenVPN® Client Certificate	OpenVPN® CA file (ca.crt) required by the OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device.
OpenVPN® Client Key	OpenVPN® Client key (*.key) required by OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device.
OpenVPN® Cipher Method	The cipher method of OpenVPN®, must be the same cipher method used by the OpenVPN® server. Supported methods are: Blowfish, AES-128, AES-256 and Triple-DES.
OpenVPN® Username	Configures the OpenVPN® authentication username (optional).
OpenVPN® Password	Configures the OpenVPN® authentication password (optional).

Network Settings/Advanced Network Settings

Advanced Network Settings	
Preferred DNS 1	Configures the preferred DNS 1 address.
Preferred DNS 2	Configures the preferred DNS 2 address.
Enable LLDP	It is used to enable the LLDP (Link Layer Discovery Protocol) feature on the device. If it is set to "Yes", the device will broadcast LLDP PDU to advertise its identity and capabilities and receive same from a physical adjacent layer 2 peer. The default setting is "Yes".
LLDP TX Interval(s)	Configures the interval the phone sends LLDP-MED packets. Default is 30. Need reboot to take effect
Enable CDP	Configures whether to enable CDP to receive and/or transmit information from/to CDP-enabled devices. Default is Enabled. Need reboot to take effect
Layer 3 QoS for SIP	This field defines the Layer 3 QoS parameter for IP Precedence, Diff-Serv or MPLS. The default setting is 26.
Layer 3 QoS for	Defines the Layer 3 QoS parameter for audio packets. This value is used for IP

Audio	Precedence, Diff-Serv or MPLS. The default setting is 46.
Layer 3 QoS for Video	Defines the Layer 3 QoS parameter for video packets. This value is used for IP Precedence, Diff-Serv or MPLS. The default setting is 34.
HTTP/HTTPS User-agent	This sets the user-agent for HTTP/HTTPS request. Need reboot to take effect
SIP User-agent	This sets the user-agent for SIP. If the value includes word "$version", will replace it with the real system version. Default is "Grandstream GVC3220 $version".
Proxy	
HTTP/HTTPS Proxy Hostname	It is used to configure the HTTP/HTTPS proxy URI of the network. Some of networks require going through a proxy to access to the Internet. The default setting is keeping this field blank.
HTTP/HTTPS Proxy Port	It is used to configure the HTTP/HTTPS proxy port number of the network. Some of networks require going through a proxy to access to the Internet. The default setting is keeping this field blank.
Bypass Proxy For	It is used to define the specific URI that the device can directly access to without HTTP/HTTPS proxy. If it is filled, the device will bypass the proxy to send the packets to the specific URI. The default setting is keeping this filed blank.

System Settings

System Settings lists Power Manager, Time & Date, TR069, Security Settings, and Peripheral.

System Settings/Power Manager

Parameters	Descriptions
Timeout Options	Set the timeout options, optional for into sleep mode and shut down, the default value is "Enter sleep mode".
Timeout Setup	According timeout option to set the timeout, if the time is set to "Never", the terminal will not be automatically entered into sleep mode or turn it off. The default value is "After 30 mins".
Screensaver Timeout	Set the screensaver timeout for the GVC to enter screensaver mode. The default value is 5 minutes.
Shutdown	Set disable or enable the device shutdown. If "disable" is selected, the shutdown function of remote control, software interface or Web UI will be disabled. The default is "enable".
Reboot	Set the device to restart.
Sleep	Set the device to sleep mode.

System Settings/Time & Language

Parameters	Descriptions
Assign NTP Server Address 1	It is used to define the URL or IP address of the NTP server 1. The device may obtain the current date and time information from the server. The default setting is "us.pool.ntp.org".
Assign NTP Server Address 2	It is used to define the URL or IP address of the NTP server 2. The default setting is empty.
Set Date	Manually set the current date for device.
Set Time	Manually se the current time for device.
Time zone	It is used to set the local time zone for the device. It covers the global time zones and user can selected the specific one from the drop-down list.
DHCP Option 42 Override NTP Server	It is used to set if the device will allow the DHCP offer overrides the NTP server address setting. If it set to "Yes", the DHCP offer with Option 42 will override the device's NTP server address setting. The default setting is "Yes".
DHCP Option 2 to Override Time Zone Setting	It is used to set if the device will allow the DHCP offer overrides the Time Zone setting. If it set to "Yes", the DHCP offer with Option 2 will override the device's time zone setting. The default setting is "No".
Use 24-hour Format	Check/uncheck to display the time using 24-hour time format or not. For example, in 24-hour format, 13:00 will be displayed instead of 1:00 pm. The default setting is "Yes".
Date Display Format	It is used to set the format used to display the date. It can be selected from the drop-down list. The default setting is MM/DD/YYYY. • Normal (M/DD/YYYY): 6/30/2020 • YYYY/MM/DD: 2020/06/30 • MM/DD/YYYY: 06/30/2020 • DD/MM/YYYY: 30/06/2020
Language	
Language Selection	Select the language from the drop-down menu.
Select Language File	Press "Browse" to bring up a file selection menu to select the local .txt file to upload to the device.

System Settings/ TR-069

Parameters	Descriptions
Enable TR-069	Enables TR-069. If enabled, the device will send a session request to the ACS server. The default setting is enabled.

Parameters	Descriptions
ACS URL	URL for TR-069 Auto Configuration Servers (ACS). The default setting is: https://acs.gdms.cloud/
ACS Username	ACS username for TR-069.
ACS Password	ACS password for TR-069.
Enable Periodic Inform	Enables periodic inform. If enabled, the device will send inform requests to the ACS periodically. The default setting is disabled.
Periodic Inform Interval (s)	Configures the periodic inform interval to send inform packets to the ACS.
Connection Request Username	The username for the ACS to connect to the device. It should match the configuration in the ACS.
Connection Request Password	The password for the ACS to connect to the device. It should match the configuration in the ACS.
Connection Request Port	The port used by the device for ACS requests. It should not be occupied by other protocol used on the device. For example, it cannot be 5060 or 5004 which are already used for SIP protocol.
CPE Cert File	The CPE Cert File for the device to connect to the ACS via SSL.
CPE Cert Key	The CPE Cert Key for the device to connect to the ACS via SSL.

System Settings/Security Settings

Parameters	Descriptions
Web/SSH Access	
Enable SSH	If set to "No", the device will not allow any SSH access to the device. The default setting is "Yes".
Access Method	It is used to set which protocol will be used to access the device's Web GUI. It can be selected from HTTP and HTTPS. The default setting is HTTP.
Port	It is used to set which port will be used to access the device's Web GUI. By default, if HTTP is selected, the port number will be 80; if HTTPS is selected, the port number will be 443.
User Info Management	
Current Admin Password	Enters current logged-in user's password. This field is case sensitive.
New Admin Password	Allows the user to change the admin password. The password field is purposely blank after clicking the "Save" button for security purpose. This field is case sensitive with a maximum length of 32 characters.

Confirm New Admin Password	Enters the new Admin password again to confirm.
New User Password	Allows the administrator to set the password for user-level web GUI access. This field is case sensitive with a maximum length of 32 characters.
Confirm New User Password	Enter the new User password again to confirm.
Screen Lock Password	
Delete screen lock password	Allows the administrator to clear the screen lock password without submitting the old one if it was configured.
Screen lock password	Allows the administrator to set a password for screen lock. The field supports 6-digit number.
Confirm screen lock password	It is used to enter the new screen lock password again to confirm.
SIP TLS	
Minimum TLS version	Defines the minimum accepted TLS version by the GVC. Options are: 1.0, 1.1 and 1.2.
Maximum TLS version	Defines the maximum accepted TLS version by the GVC. Options are: 1.0, 1.1 and 1.2, and "No limit"
SIP TLS Certificate	Defines the SSL certificate used for SIP over TLS to access particular websites. The device supports SIP over TLS encryption, realizing it via the built-in private key and SSL certificate. The SSL certificate the user specifies for TLS encryption should be X.509 format.
SIP TLS Private Key	Defines the SSL private key used for SIP over TLS. The SSL private key the user specified for TLS encryption should be X.509 format.
SIP TLS Private Key Password	Defines the SSL private key password used for SIP over TLS.
Certificate Management	
Import Trusted CA certificates	Click the "Upload" to upload certificate file from PC. The certificate file should be ".pem", ".crt" , ".cer" or ".der" format. Need reboot to take effect
Add user certificates	Click "Upload" to upload user certificate file from PC. The certificate file should be ".crt", ".cer", ".pem", ".p12", or ".pfx" format.
Import Custom Certificate	Uploads certificate file from PC using Browse button. The certificate file should be ".pem", ".crt", and ".cer" or ".der" format. The Browse button will turn to "Processing" and back to "Browse" once the uploading is finished. **Note:** Users can also delete uploaded custom certificate by clicking on "Delete".

Parameters	Descriptions
HDMI	
Primary HDMI out resolution	Configures the output image resolution of HDMI 1. Greater resolution value means higher image definition. Please select the same resolution as the output display device. The device will automatically read the resolution supported by the output display device and compare it with the resolution supported by itself. Only the resolution supported by both will be used. The device will automatically obtain the optimal resolution when it boots up for the first time.
Secondary HDMI out resolution	Configures the output image resolution of HDMI 2. Greater resolution value means higher image definition. Please select the same resolution as the output display device. The device will automatically read the resolution supported by the output display device and compare it with the resolution supported by itself. Only the resolution supported by both will be used. The device will automatically obtain the optimal resolution when it boots up for the first time.
Enable Automatically When The Presentation Source Is Accessed	If enabled, then the device will display presentation automatically when HDMI is plugged in; If desibled, a pop-up box will prompt the users to select "Ok" or "Cancel". If the users click neither "Ok" nor "Cancel", then the device will display presentation automatically after 30s timeout. The default setting is "No".
HDMI Sound Output Control	Set HDMI sound output. When only HDMI 1 is connected, combined with "Audio Device" configuration, device supports sound output from HDMI 1. Note: HDMI sound output control takes effect only when sound output set in Audio Device is HDMI.
Camera	
Move speed	Specifies the moving speed and zoom speed for the camera. "1" is slowest and "16" is fastest. The default setting is "8".
Initial position	Specifies the initial position of the camera when the device is powered up. • **System default position**: The camera moves to its default position after bootup. • **Position when power off**: After bootup, the camera moves to the latest position before reboot. The default setting is System default position.
Camera Mirroring	When the mirror image is opened, the local camera image becomes the mirror image. The default is not open.

Device Control

Users could add preset and manipulate the camera via PTZ control and Enable/Disable Remote Control.

Device Control/Preset Settings

- Click one preset to apply the preset.
- Click the un-configured preset and adjust via the PTZ control panel, then save the configurations.
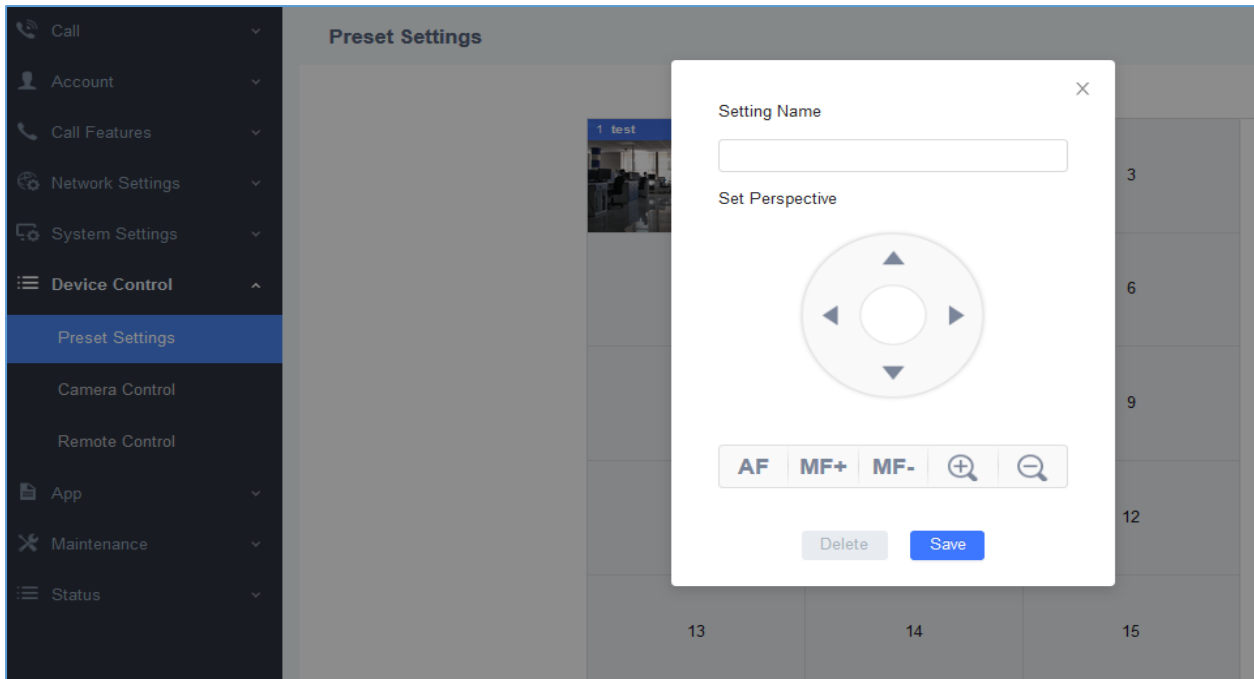
Figure 10: GVC3220 Web UI - Preset Settings

Device Control/Camera Control

This page allows users to manipulate the camera via PTZ control.

GVC3220 Administration Guide
Version 1.0.1.35
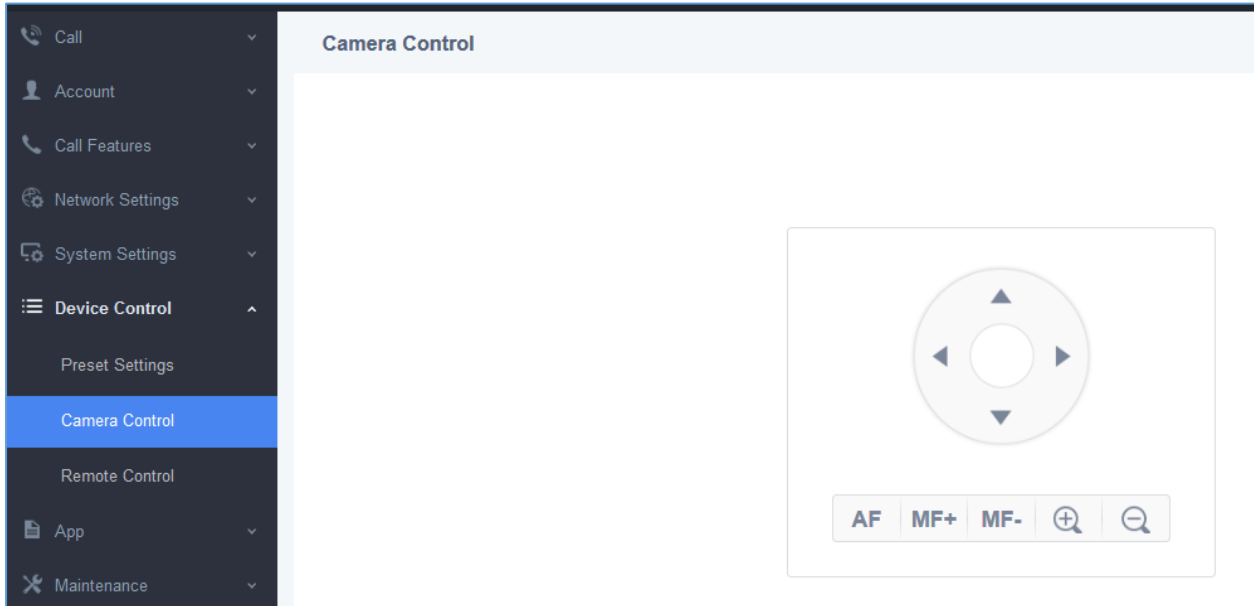
Figure 11: GVC3220 Web UI - Camera Control

Device Control/Remote Control

Parameters	Descriptions
Disable Remote Control App Connect	If set to "Yes", the Remote control App can be paired to the device via Bluetooth, but it cannot connect to the device to perform any operations. The default setting is "No".

App

The App setting page lists, LDAP Contacts, BroadSoft Directories, Recording Management, And 3rth Party Application.

App/LDAP Contacts

Parameters	Descriptions
Connection Mode	It is used to select which protocol will be used for LDAP searching, LDAP or LDAPS.
Server Address	It is used to configure the URI of the LDAP (Lightweight Directory Access Protocol) server.
Port Number	It is used to configure the LDAP server port. The default LDAP port number is 389.
Base DN	It is used to configure the LDAP search base. This is the location in the directory where the search is requested to begin. Example: dc=grandstream, dc=com

	ou=Boston, dc=grandstream, dc=com
Username (Binding DN)	It is used to configure the bind "Username" for querying LDAP servers. Some LDAP servers allow anonymous binds in which case the setting can be left blank.
Password	It is used to configure the bind "Password" for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.
LDAP Name Attributes	It is used to configure the "name" attributes of each record which are returned in the LDAP search result. This field allows the users to configure multiple space separated name attributes. Example: gn cn sn description
LDAP Number Attributes	It is used to configure the "number" attributes of each record which are returned in the LDAP search result. This field allows the users to configure multiple space separated number attributes. Example: telephoneNumber telephoneNumber Mobile
LDAP Mail Attributes	It is used to configure the "mail" attributes of each record which are returned in the LDAP search result. Example: Mail
LDAP Name Filter	It is used to configure the filter used for name lookups. Examples: (|(cn=%)(sn=%)) returns all records which has the "cn" or "sn" field starting with the entered prefix; (!(sn=%)) returns all the records which do not have the "sn" field starting with the entered prefix; (&(cn=%) (telephoneNumber=*)) returns all the records with the "cn" field starting with the entered prefix and "telephoneNumber" field set.
LDAP Number Filter	It is used to configure the filter used for number lookups. Examples: (|(telephoneNumber=%)(Mobile=%) returns all records which has the "telephoneNumber" or "Mobile" field starting with the entered prefix; (&(telephoneNumber=%) (cn=*)) returns all the records with the "telephoneNumber" field starting with the entered prefix and "cn" field set.
LDAP Mail Filter	It is used to configure the filter used for mail lookups. Example: (mail=%)
Search Field Filter	Configures filters used upon LDAP search. The default settings is "All Filter". The P-value for this functionality is P27806 with 4 possible values, 0 – All Filter, 1 – Name Filter, 2 – Number Filter, 3 – Mail Filter. Default value is 0 – All Filter.

Parameters	Descriptions
LDAP Displaying Name Attributes	It is used to configure the entry information to be shown on phone's LCD. Up to 3 fields can be displayed. Example: %cn %sn %telephoneNumber
Max Hits	It is used to configure the maximum number of results to be returned by the LDAP server. If set to 0, server will return all search results. The default setting is 50.
Search Timeout (s)	Configures the search timeout value. If exceeds the value and the server does not response, then stop searching. The default setting is 30.
LDAP Lookup When Dialing	It is used to set if allow the phone system to do the LDAP number searching when making outgoing calls. The default setting is "No".
Search LDAP For Incoming Call	It is used to set if allow the phone system to do LDAP number searching for incoming calls. The default setting is "No".

App/BroadSoft Directories

Parameters	Descriptions
XSI Service Settings	
Authentication Type	Defines the authentication type in way of login or use SIP. If set to "Login Credentials", please fill in Username and Password in the following options; if set to "SIP Credentials", please fill in Username, User ID, and Password. The default setting is "SIP Credentials".
Server	Configures the BroadSoft XSI server URI. If the server uses HTTPS, please add the header "HTTPS" ahead of the Server URI. For instance, "https://SERVER_URI".
Port	Configures the BroadSoft XSI server port. The default port is 80. If the server uses HTTPS, set to 443.
Action path	Customizes domain name for XSI request. If blank, XSI requests will be sent to configured XSI server URL (for instance: https://SERVER_URI). If specified, configured action path will be added to configured XSI server. (for instance: https://SERVER_URI/ACTION_PATH".
BroadSoft User ID	Determines the User ID for BroadSoft XSI server.
SIP Authentication ID	Determines username for BroadSoft XSI server when Authentication Type is set to "SIP Credentials".
SIP Authentication Password	Determines password for BroadSoft XSI server when Authentication Type is set to "SIP Credentials".
BroadSoft	Specifies how often the phone system sends HTTP/HTTPS query to the BroadSoft

Directory & Call Logs Update Interval (s)	XSP server to update the BroadSoft Call History. The default setting is 1800 seconds.
BroadSoft Directory Hits	Determines how many entry results will be showed in each query. If it is configured, the phone system will add the header to the HTTP query. The valid range is from 1 to 1000. The default setting is blank, which means to use the server's default value.
Associated BroadSoft Account	Configures the associated BroadSoft account when dialing BroadSoft contacts.
BroadSoft Directory Order	Configures the BS contact order on the LCD. The order of contact categories on the Web GUI from top to bottom is same as the order from left to right on the BS contact app. Select one item and click the Up/Down arrow to adjust the order.
Network Directories	
Group Directory	Enables/disables the BroadSoft XSI Group Directory features on the phone. The name filed is used to name the directory. If it keeps blank, the phone system will use the default name "Group" for it.
Enterprise Directory	Enables/disables the BroadSoft XSI Enterprise Directory features on the phone. The name filed is used to name the directory. If it keeps blank, the phone system will use the default name "Enterprise" for it.
Group Common	Enables/disables the BroadSoft XSI Group Common features on the phone. The name filed is used to name the directory. If it keeps blank, the phone system will use the default name "Group Common" for it.
Enterprise Common	Enables/disables the BroadSoft XSI Enterprise Common features on the phone. The name filed is used to name the directory. If it keeps blank, the phone system will use the default name "Enterprise Common" for it.
Personal Directory	Enables/disables the BroadSoft XSI Personal Directory features on the phone. The name filed is used to name the directory. If it keeps blank, the phone system will use the default name "Personal Directory" for it.
Missed Call Log	Enables/disables the BroadSoft XSI Missed Call Log features on the phone. The name filed is used to name the directory. If it keeps blank, the phone system will use the default name "Missed" for it.
Placed Call Log	Enables/disables the BroadSoft XSI Placed Call Log features on the phone. The name filed used to name the directory. If it keeps blank, the phone system will use the default name "Outgoing" for it.
Received Call Log	Enables/disables the BroadSoft XSI Received Call Log features on the phone. The name filed used to name the directory. If it keeps blank, the phone system will use the default name "Incoming" for it.

App/Recording Management

Users could find video/audio recording files on this web page, download the file to PC to listen to or delete the files. The recording files can be stored using internal storage or in external SD card/ USB drive, FTP Server or NAS Extended Storage.
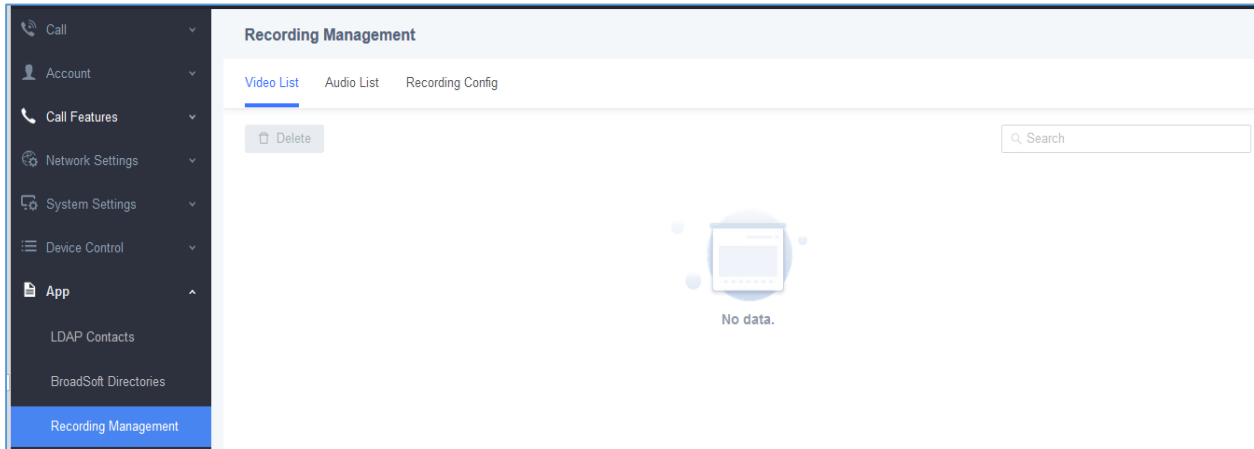
Figure 12: GVC3220 Web UI – Video/Audio list Recording

App/Recording Management/Recording Config

Under GVC3220 web UI→**App**→**Recording Management**→**Recording Config**, an option "Save path" is available for users to select the path to save the recording file. The user can select external SD card or USB storage device when they are plugged in.

Figure 13: GVC3220 Web UI - Recording Config

App/Third Party Application

Parameters	Descriptions
Auto Launch	Configures whether to automatically launch a third party application at boot up. If there

GVC3220 Administration Guide
Version 1.0.1.35

| Application On Start Up | are multiple third party applications installed on device, select one of them to launch automatically at boot up. The default setting is "Forbidden". |

Maintenance

Maintenance section lists Upgrade, Troubleshooting.

Maintenance/Upgrade

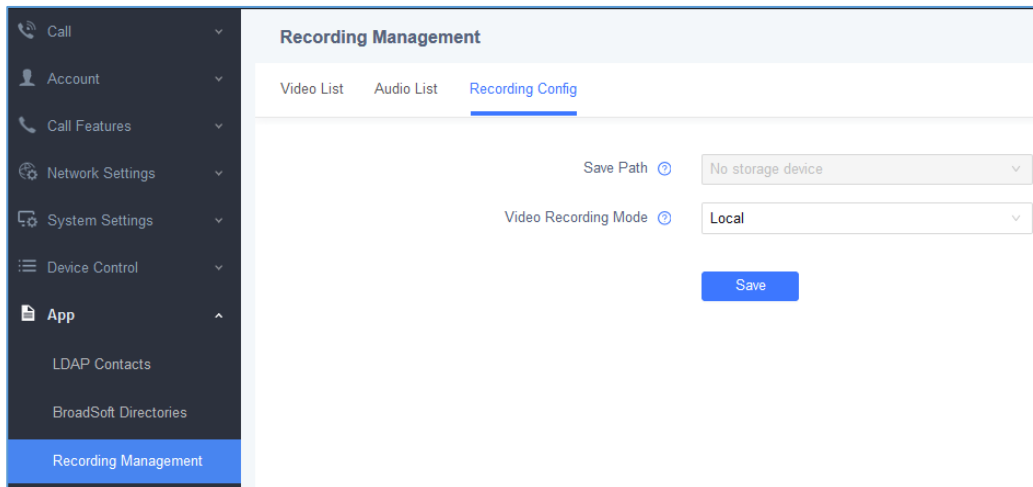| Parameters	Descriptions
Firmware	
Complete Upgrade	• When set to "Yes", the device will keep the user data and replace all other files. • When set to "No", the device will compare the firmware file and only replace the part that has update. The default setting is "No". For example: if the device cannot fully boot-up but the user still login web UI, please enable this feature to recover the system.
Upload Firmware File to Update	Manually upload firmware file from PC to the device system directly.
Firmware Upgrade Mode	It is used to set the upgrading protocol for the device to retrieve firmware file. It can be selected from TFTP, HTTP and HTTPS. The default setting is HTTPS.
Firmware Server Path	It is used to define the server path for upgrading the firmware. It can be different from the Config Server Path. Default setting is "fm.grandstream.com/gs".
Firmware HTTP/HTTPS Username	It is used to type the username for the HTTP/HTTPS server authentication for firmware server.
Firmware HTTP/HTTPS Password	It is used to type the password for the HTTP/HTTPS server authentication for firmware server.
Firmware File Prefix	It is used to set the prefix characters for the firmware files. If it is configured, only the firmware with the matching encrypted prefix will be downloaded and flashed into the device system. It allows the ITSP to lock firmware updates.
Firmware File Postfix	It is used to set the post characters for the firmware files. If it is configured, only the firmware with the matching encrypted postfix will be downloaded and flashed into the device system. It allows the ITSP to lock firmware updates.
Config File	
Use Grandstream GAPS	It is used to configure the download path and update mode for the configuration file server. If set to "Yes", the GVC3220 will set the download path of the configuration file to fm.grandstream.com/gs by default, and use HTTPS protocol to connect to the server. If set to "No", users can manually configure the path and update mode to retrieve the configuration file.

Config Upgrade Mode	When "Use Grandstream GAPS" is set to "No", users can use this option to set the provisioning protocol for the device to retrieve the config file. It can be selected from TFTP, HTTP and HTTPS. The default setting is HTTPS.
Config Server Path	When "Use Grandstream GAPS" is set to "No", users can use this field to define the server path for provisioning the configuration file. It can be different from the Firmware Server Path. Default setting is "fm.grandstream.com/gs".
Config HTTP/HTTPS Username	It is used to type the username for the HTTP/HTTPS server authentication for config server.
Config HTTP/HTTPS Password	It is used to type the password for the HTTP/HTTPS server authentication for config server.
Always send HTTP Basic Authentication Information	It is used to set if the device includes the credential information in the HTTP/HTTPS request messages to download the cfg.xml file. If it is set to "Yes ", the credential information will always be included in the HTTP/HTTPS messages regardless the server's challenge. The default setting is "No".
Config File Prefix	It is used to set the prefix characters for the configuration files. If it is configured, only the firmware with the matching encrypted prefix will be downloaded and flashed into the device system.
Config File Postfix	It is used to set the prefix characters for the configuration files. If it is configured, only the firmware with the matching encrypted postfix will be downloaded and flashed into the device system.
Authenticate Conf File	It is used to set if the device authenticates the configuration file before applying it. If it set to "Yes", the configuration file must include value P1 with device's administration password. If it is missed or does not match the password, the device will not apply the configuration in the config file. The default setting is "No".
XML Config File Password	The password for encrypting the XML configuration file using OpenSSL. The password is to decrypt the XML configuration file if it is encrypted via OpenSSL.
Download Device Configuration	It is used to download the device configuration file in text format. The config file includes all the P value parameters for device's current settings except password for security purpose.
Upload Device Configuration	It is used to upload the configuration file to the device.
CUST File	
GUI customization file download mode	Select the GUI customization file download mode: "HTTP", "HTTPS" or "TFTP".
GUI customization file URL	This setting defines the server path for the GUI customization file where the GVC3220 will download it from. Default value is fm.grandstream.com/gs.
GUI customization file HTTP/HTTPS username	Enter the username to access the HTTP/HTTPS server to download cust file, if required by the server.

GUI customization file HTTP/HTTPS password	Enter the password to access the HTTP/HTTPS server to download cust file, if required by the server.
Use Configurations of Config File Server	If selected, the GVC3220 will download the cust file in the same way as retrieving configuration file, i.e., same server and downloading mode, etc.
Provision/Automatic Upgrade	
Automatic Upgrade	Enables automatic upgrade and provisioning. The default setting is "Check Every Day". If set to "Check Every Day", "Check Every Week" or "Check at a Period Time", fill in time interval below for upgrade. The shortest time interval is 60 minutes. If set to "No", only upgrade when reboot the device.
Enable Randomized Automatic Upgrade	Setting whether to upgrade automatically at random. It means whether the device will upgrade automatically at random time point in the setting period. This option is mainly used for multiple devices upgrade at the same time.
Automatic Upgrade Hour (0-23)	Defines the hour of the day (0-23) to check the HTTP/TFTP server for firmware upgrades or configuration files changes. This option is available when "Automatic Upgrade" is set to "Check Every Day ". The default setting is "1".
Firmware Upgrade and Configuration File Detection	It is used to define the rules for automatic upgrade on the device. It can be selected from the following: • Always Check at bootup • When F/W pre/suffix changes, • Skip the Firmware Check.
Upgrade With Prompt	If set to "No", the device will automatically start upgrading after downloading the firmware files. Otherwise, users would need to confirm in the prompted message before upgrading process is started. The default value is "Yes".
Provision	
Automatic Upgrade	Enable automatic HTTP upgrade and provisioning. The default setting is "No".
Firmware Upgrade And Configuration File Detection	Defines the rules for automatic upgrade and configuration file: Always Check at bootup, when prefix/suffix changes, Skip the Firmware Check. Need reboot to take effect.
Upgrade With Prompt	If set to "No", the device will automatically start upgrading after downloading the firmware files. Otherwise, users would need to confirm in the prompted message before upgrading process is started. The default value is "Yes".
Config Provision	Device will download the configuration files and provision by the order you set.
Advanced Settings	
Disable SIP NOTIFY Authentication	If set to "Yes", the device will not challenge NOTIFY with 401 authentication. The default setting is "No".
Validate Server Certificate	It is used to configure whether to validate the server certificate when download the firmware/config file. If set to "Yes", the device will download the firmware/config file

	only from the legitimate server. The default setting is "No".
mDNS Override Server	It is used to set if the device will broadcast the Multicast DNS (mDNS) message during booting up to allow itself to be discovered and be configured by the SIP platform. If it is set to "User Type A', the device will broadcast the MDNS message "A_grandstream-cfg.local"; if it is set to "Use Type SRV", the MDNS message will be "SRV_grandstream-cfg.local". The default setting is "Use Type A". Need reboot to take effect
Allow DHCP option 43 and option 66 to override server	If DHCP option 43 or DHCP option 66 is turned ON in the LAN, the TFTP server setting can be overridden. The default setting is "Yes". Need reboot to take effect
DHCP Option 120 Override SIP Server	Enables DHCP Option 120 from local server to override the SIP Server on the device. The default setting is "Yes" Need reboot to take effect
3CX Auto Provision	It is used to set if the device will broadcast the SIP SUBSCRIBE message during booting up to allow itself to be discovered and be configured by the SIP platform. The default setting is "Yes". Need reboot to take effect
Factory Reset	It is used to reset the device to the default factory setting mode. If the "Clear the SD card" is checked, the SD card storage mounted to the device will be format as well.

Maintenance/Troubleshooting

Syslog	
Syslog Protocol	Select the transport protocol over which log messages will be carried. **UDP:** Syslog messages will be sent over UDP. **SSL/TLS:** Syslog messages will be sent securely over TLS connection. To upload server CA certificate, follow below steps: ✓ Copy CA file in SD card and plug it to the phone. ✓ Go to LCD menu **Settings→Security Settings→Install from SD card** to install the CA file.
Syslog Server Address	Configures the URI which the phone system will send the syslog messages to. The default setting is "log.ipvideotalk.com".

GVC3220 Administration Guide
Version 1.0.1.35

Syslog Level	Selects the level of logging for syslog. The default setting is "None". There are 4 levels from the dropdown list: DEBUG, INFO, WARNING and ERROR. The following information will be included in the syslog packet: • **DEBUG** (Sent or received SIP messages). • **INFO** (Product model/version on boot up, NAT related info, SIP message summary, Inbound and outbound calls, Registration status change, negotiated codec, Ethernet link up). • **WARNING** (SLIC chip exception). • **ERROR** (SLIC chip exception, Memory exception). **Note**: Changing syslog level does not require a reboot to take effect.
Send SIP Log	Configures whether the SIP log will be included in the syslog messages.
Syslog Keyword Filter	Only send the syslog with keyword, multiple keywords are separated by comma. Example: set the filter keyword to "SIP" to filter SIP log.
H.323 Syslog Level	Select H.323 Syslog level in the drop-down menu, the default setting is "Off", which means no H323 syslog info in syslog. You can also select from level 1 to 10, 10 is the highest level.
Logcat	
Clear Log	Clears the log files saved in the phone system.
Log Tag	Configures the filter to display the specified process log file.
Log Priority	Selects the log priority to display. It can be selected from list below: • Verbose (Default Setting) • Debug • Info • Warning • Error • Fatal • Silent (suppress all output)
Debug	
One-click Debugging	
One-click Debugging	Capture the checked info in the debugging list, click "Start" to debug if including "Capture trace" item and click "Stop" to end, Click "Capture" in another situation. All retrieved files will be generated to a package, and the last package will be overwritten, while the trace file will stay remain.
Debug Info Menu	Display a list of info items that can be debugged, currently supports system logs, info log, capture package, tombstones and ANR log. The captured data can be

	viewed in "Debug information list". The default is all selected.
Debug Info List	You can select the existing debugging info package or grab package. Click the "Delete" button on the right to delete the file.
View Debug Info	You can select the existing debugging info package or grab package. Click the "Delete" button on the right to delete the file.
Core Dump	
Enable Core Dump Generation	Configures whether to generate and save the core dump file when the program crashes. The default setting is "No".
Core Dump List	Selects the existing core dump file in the drop-down box. Users could delete the file by pressing on "Delete" button.
View Core Dump	Press "List" button to view all existing core dump files. The files are listed in chronological order, users could click the file name to download the file to the local computer.
Record	
Record	Click to start capturing audio data, click the "Stop" button to end. To capture the audio data of the device can help to locate audio issues. The default is not enabled. You can record up to 1-minute audio data.
Recording List	Choose the existing audio file. Click the "Delete" button on the right to delete this file.
View Recording	Click on the "List" button to view. The captured audio data will be sorted by time. Click to download the data to the computer for analysis. Note: The audio data file will be saved under FileManager → Internal Storage → Recfiles folder. Users can also delete files under this folder.
Traceroute	
Target Host	The IP address or URL for the Target Host of the Traceroute. Press **Start** to send traceroute request to configured target host. Press **Stop** to end traceroute running process.
Developer Mode	
Developer Mode	If turned on, ADB (Android Debug Bridge) function will be enabled on the device. The default setting is "Disabled".
Ping	
Target Host	The IP address or URL for the Target Host of the ping. Press **Start** to send ping request to configured target host. Press **Stop** to end ping running process.
NSLookup	

Hostname	Enter a host name and find out the corresponding IP address. It will also do reverse name lookup and find the host name for an IP address you specify
Remote Diagnosis	
Remote Diagnosis	Set whether to allow remote diagnostics, only for the Grandstream background server to remote diagnose the device and access Web UI, please turn it on carefully. 2 days (48h) timeout mechanism will be automatically closed after opening. The default value is "off".

Status

The Status page lists Account Status, Interface Status, Network Status, System Info and Remote control status, and License.

Status/Account Status

Parameters	Descriptions
Account	It lists the accounts available on device.
Number	It displays the SIP User ID of the account (if applicable).
SIP Server	It displays the SIP server address for the account (applicable to SIP account only).
Status	It shows the registration status of the account: Registered or Unregistered.

Status/Interface Status

Connection status for each interface is displayed with different icons here. The icon in green indicates "Connected" and the icon in grey means "Not Connected".

Figure 14: GVC3220 Web UI - Interface Status

Status/Network Status

Parameters	Descriptions
MAC Address	This is the global unique ID of device.
NAT Type	The type of NAT connection used by the device.
IPV4	

IPV4 Address Type	Displays how the device obtains IP address. It could be DHCP, Static IP or PPPoE.
IPv4 Address	IP Address obtained or configured on the device.
Subnet Mask	Subnet mask obtained or configured on the device.
Gateway	The gateway address obtained or configured on the device.
DNS Server 1	DNS Server 1 obtained or configured on the device.
DNS Server 2	DNS Server 2 obtained or configured on the device.
IPV6	
IPv6 Address Type	The configured address type: DHCP, Static IP.
IPv6 Address	IP Address obtained or configured on the device.
IPv6 DNS Server 1	DNS Server 1 obtained or configured on the device.
IPv6 DNS Server 2	DNS Server 2 obtained or configured on the device.

Status/System Info

Parameters	Descriptions
Product Model	Device model: GVC3220
Hardware Version	Device hardware version.
Part Number	Device Part Number (PN).
System Version	Device system version. This is the firmware version on the device. When upgrading firmware, this is the version number to refer to.
Boot Version	Device boot version.
Kernel Version	Device kernel version.
Android™ Version	Device Android™ version 9.
System Up Time	Device system up time since the last reboot.

Status/Remote Control Status

Parameters	Descriptions
Hardware Version	The remote control hardware version.
Software Version	The remote control software version.
Patch Version	The remote control patch version.

Remote Control Battery	The remote control battery status.

Note: The remote-control status is displayed only when the remote control is paired and connected to the GVC3220. Otherwise, it will be shows as "Unknown".

FIRMWARE UPGRADE

GVC3220 supports software upgrade via the following methods:

- Manually upload firmware file to upgrade (for applicable firmware versions only).
- Upgrade via TFTP firmware server
- Upgrade via HTTP/HTTPS firmware server

⚠ **Note:**

1. Please do not power cycle the device during firmware upgrading process. This might corrupt firmware image and cause the unit to malfunction.
2. Please make sure the firmware file in the firmware server is unzipped and the firmware file name is correct. Firmware file name other than the provided default file name might cause firmware upgrading failure.
3. By default, firmware server path is set to "fm.grandstream.com/gs" using HTTPS protocol.
4. Please go to Grandstream website www.grandstream.com/support/firmware for the release note and latest firmware information.

No Local TFTP/HTTP Servers

Service providers should maintain their own firmware upgrade servers. For users who do not have a TFTP/HTTP/HTTPS server, some free Windows version TFTP servers are 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.

Upgrade GVC3220 via TFTP Server

Here is the instruction to upgrade GVC3220 via TFTP server:

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 GVC3220 device 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. (This step may be different depending on the TFTP server software you are using).
4. Start the TFTP server.
5. On the GVC3220 web UI→**Maintenance**→**Upgrade** page, configure TFTP as the "Firmware upgrade mode" and enter the IP address of the PC in "Firmware server path" field.

GVC3220 Administration Guide
Version 1.0.1.35
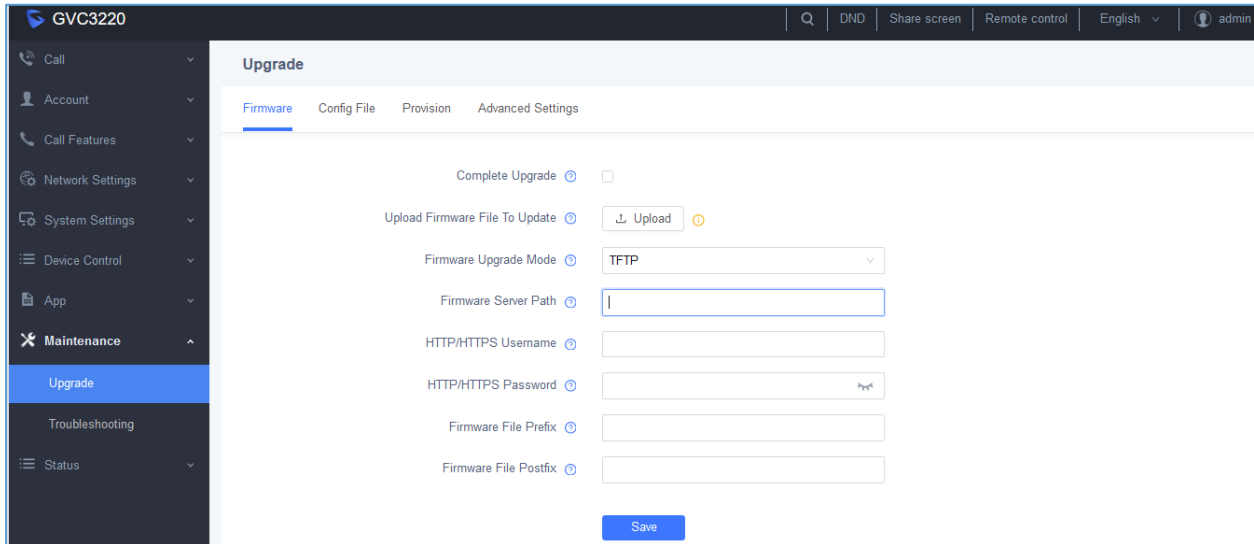
Figure 15: Configure Firmware Server Path

6. Save and apply the change. Then reboot the device.

Please note end users can also choose to download a free HTTP server from http://httpd.apache.org/ or use Microsoft IIS web server.

Provisioning and Configuration File Download

Grandstream SIP Devices can be configured via the Web Interface as well as via a Configuration File (binary or XML) through TFTP or HTTP/HTTPS. The "Config Server Path" is the TFTP, HTTP or HTTPS server path for the configuration file. It needs to be set to a valid URL, either in FQDN or IP address format. The "Config Server Path" can be the same or different from the "Firmware Server Path". A configuration parameter is associated with each particular field on the web configuration page. A parameter consists of a Capital letter P and 2 to 4-digit numeric numbers. i.e., P2 is associated with the "Admin Password" in the Web **GUI→Security Settings → User Info Management** page. For a detailed parameter list, please refer to the corresponding firmware release configuration template in the following link: http://www.grandstream.com/support/tools

When the GVC3220 boots up, it will issue TFTP or HTTP request to download a configuration XML file named "cfgxxxxxxxxxxxx" followed by "cfgxxxxxxxxxxxx.xml", where "xxxxxxxxxxxx" is the MAC address of the device, i.e., "cfg000b820102ab" or "cfg000b820102ab.xml". If downloading "cfgxxxxxxxxxxxx.xml" file is not successful, the provision program will download a generic cfg.xml file. The configuration file name should be in lower case letters.

For more details on XML provisioning, please refer to the following document: http://www.grandstream.com/sites/default/files/Resources/gs_provisioning_guide.pdf

Users could find XML configuration file generator tool and user guide in the following web page. Please use the XML configuration file generator to generate the XML configuration file for your devices' provisioning.
http://www.grandstream.com/support/tools

Remote Control Upgrade

The GVC3220 remote control firmware is embedded with GVC3220 firmware.

Users could check remote control firmware update manually in LCD menu→**Settings**→**Status**→**Remote Control** and click "Check updates".

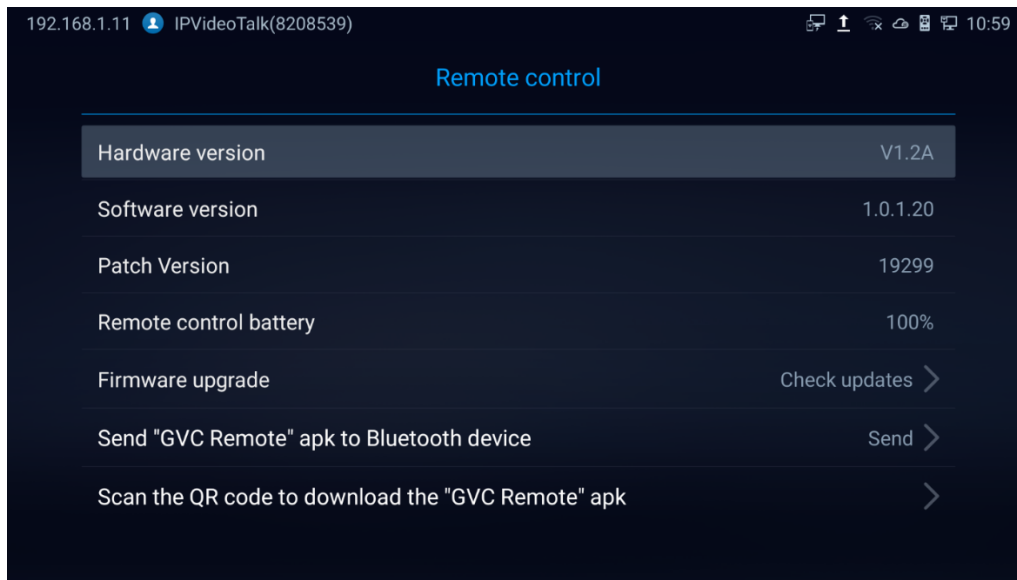**Figure 16: LCD Menu - Remote Control Status**

If there is a new firmware version detected, a confirmation window will pop-up. Click on "**OK**" to proceed to firmware download as shown in below screenshot.
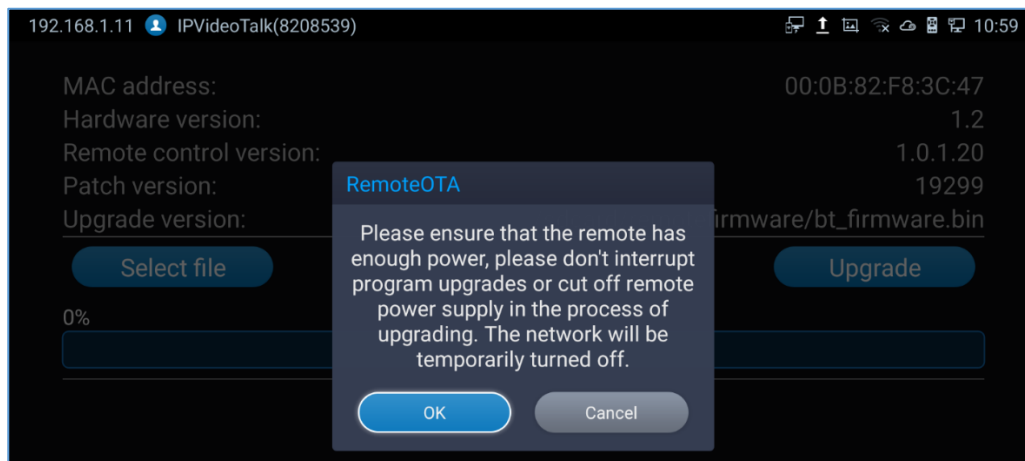
Figure 17: LCD Screen - Remote Control Upgrade Confirmation

GVC3220 Administration Guide
Version 1.0.1.35

Once confirmed, the Remote control firmware download will start.
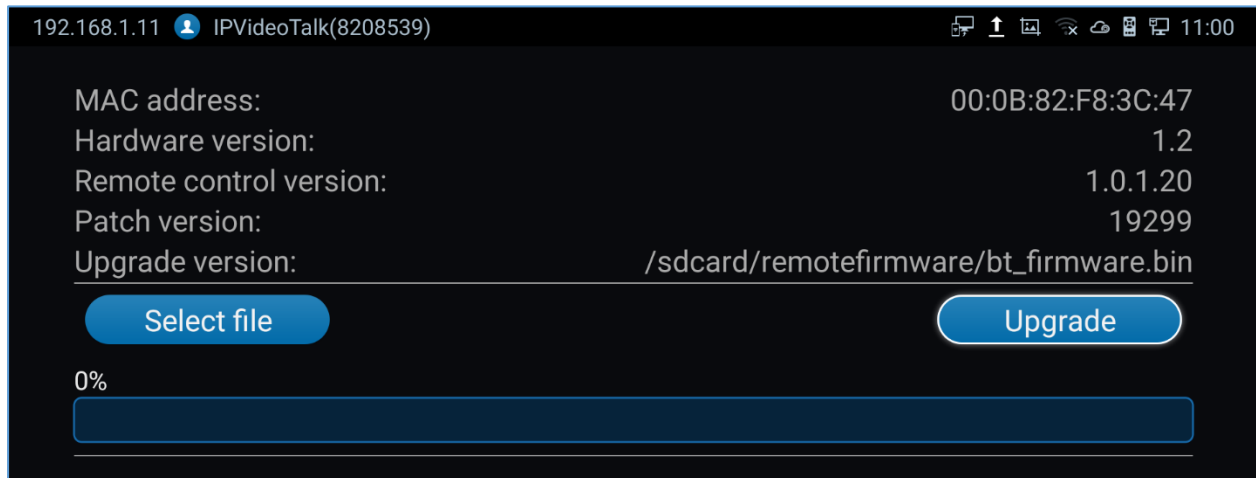
Figure 18: Remote Control Firmware Upgrade

⚠ **Note:**

Please do not unplug GVC3220 power supply or remove remote control battery during remote control upgrading process. Otherwise, the upgrading process will be interrupted and upgrading will fail.

FACTORY RESET

Users could reset GVC3220 to factory settings via the following ways:

- Reset via LCD menu
- Reset via GVC3220 web UI
- Reset via the reset pin hole on the back panel of GVC3220.

Factory reset will delete configuration information and syslog information.

⚠️ **Warning:** Factory reset will erase all GVC3220 configuration information. Please back up all settings or print useful information before making the following operations. If users lose all parameters or records, Grandstream will not take responsibility for the damage or loss.

Reset via LCD Menu

Go to GVC3220 LCD idle screen ➔ **Settings** ➔ **Factory Reset**, click on the "Reset" button to bring up the prompt box as shown below. Click "OK" to reboot the device and restore factory settings.
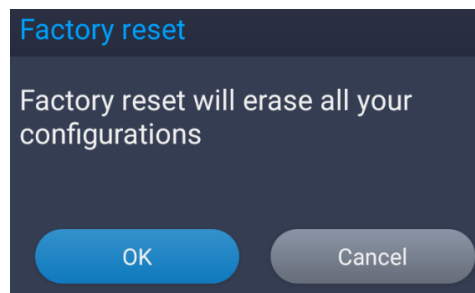

Figure 19: Factory Reset via LCD

Reset via Web UI

1. Log in GVC3220 Web UI ➔ **Advanced Settings** ➔ **Upgrade**, the "Factory Reset" option is on the bottom of the page.
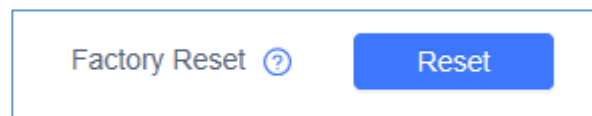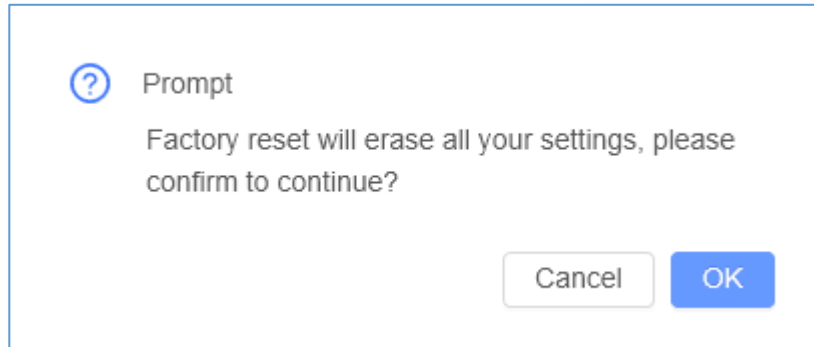

Figure 20: GVC3220 Web UI - Factory Reset

2. Click the "Reset" button to bring up the prompt box as shown below. Click "OK" to reboot the device and restore factory settings.

Figure 21: GVC3220 Web UI - Factory Reset Confirmation

Reset via Reset Pin Hole

There is a Reset pin hole on the back panel of GVC3220. To reset the device, use a small pin to hold against the Reset pin hole for more than 10 seconds to restore to factory settings.

GVC3220 Administration Guide
Version 1.0.1.35

EXPERIENCING THE GVC3220

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 of your questions. Contact a technical support member or submit a trouble ticket online to receive in-depth support.

Thank you again for purchasing Grandstream Video Conferencing System, it will be sure to bring convenience and color to both your business and personal life.

----

* Android is a trademark of Google Inc.

HDMI, the HDMI Logo, and High-Definition Multimedia Interface are trademarks or registered

trademarks of HDMI Licensing LLC in the United States and other countries.