Grandstream Networks, Inc.

GVC32XX Series

Video Conference System for Android™

Security Guide

Table of Contents

Table of Figures

OVERVIEW

This document presents a summary of security measures, factors, and configurations that users are recommended to consider when configuring and deploying the GVC32xx.

Note: We recommend using the latest firmware for latest security patches.

The following sections are covered in this document:

- **Web UI/SSH Access**
  Web UI access is protected by username/password and login timeout. Two-level user management is configurable. SSH access is supported for mainly troubleshooting purpose and it's recommended to disable it in normal usage.

- **Device Control Security**
  The GVC32xx has multiple ways to limit the use for network settings, apps, and other settings if not necessary for the end user.

- **Security for SIP Account and Calls**
  The SIP account uses specific port for signaling and media stream transmission. It also offers configurable options to block anonymous calls and unsolicited calls.

- **Network Security**
  The GVC32xx supports VPN, 802.1X, Bluetooth for network access. VPN secures remote connection and 802.1X provides network access control. it's recommended to turn Bluetooth off if not used.

- **Security for GVC32XX Services**
  GVC32xx supports service such as HTTP/HTTPS/TFTP provisioning, TR-069, LDAP, as well as allows ADB and FTP access. For provisioning, we recommend using HTTPS with username/password and using password-protected XML file. For services such as ADB, we recommend disabling them if not used to avoid potential port exposure

- **Deployment Guidelines for GVC32XX**
  This section introduces protocols and ports used on GVC32xx and recommendations for routers/firewall settings.

This document is subject to change without notice.

WEB UI/SSH ACCESS

GVC32xx Web UI Access

The GVC32xx embedded web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a web browser such as Microsoft IE, Mozilla Firefox, Google Chrome and etc. With this, administrators can access and configure all available GVC32xx information and settings. It is critical to understand the security risks involved when placing the GVC32xx phone on public networks and it's recommended not to do so.

Web UI Access Protocols

HTTP and HTTPS are supported to access the GVC32xx web UI and can be configured under web UI → Settings → Security Settings → Web/SSH Access. To secure transactions and prevent unauthorized access, it is highly recommended to:

1. Use HTTPS instead of HTTP.
2. Avoid using well known port numbers such as 80 and 443.

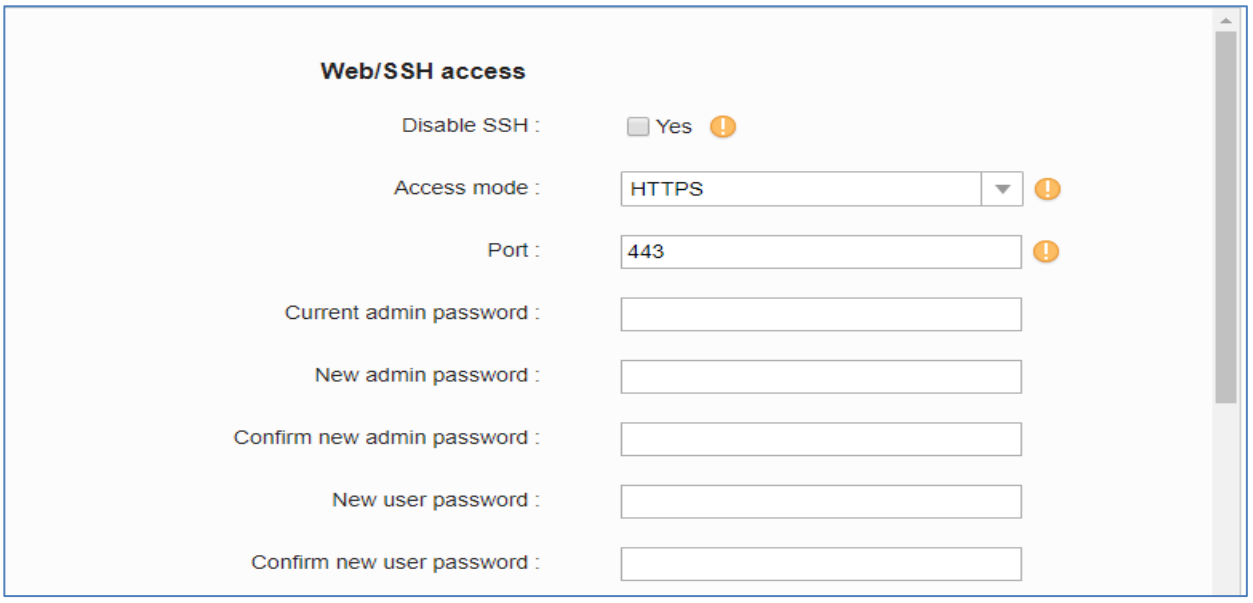

Figure 1: Web UI Access Settings

User Login

Username and password are required to log in the GVC32XX web UI.

Figure 2: GVC32xx Web UI Login

After logging in, the system will detect that the default password is used and requires users to change it.

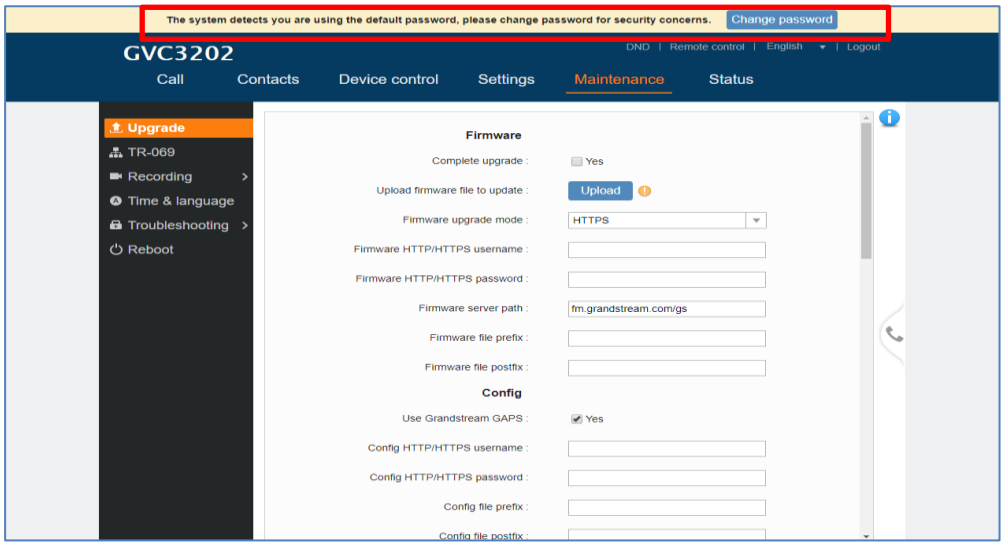

Figure 3: GVC32xx Admin Password Change

Users can press on **Change Password** to change the password for default user "admin", or navigate to Settings → Security Settings-> Web/SSH access and change the Admin/User password. The password length must be between 6 and 32 characters. Strong password with a combination of numbers, uppercase letters, lowercase letters, and special characters is always recommended for security purpose.

User Management Levels

Two user privilege levels are currently supported:

- **Admin**
- **User**

Admin login has access to all of the GVC32xx's web UI pages and can execute all available operations. User login has limited access to the web UI pages. With user login, the user is allowed to access and configure the following settings:

- **Call**
- **Contacts**
- **Device Control**
- **Status**
- **Settings: Network Settings, Peripheral, security settings**
- **Maintenance: Recording, Time & Language, Troubleshooting.**

It is recommended to keep admin login with administrator only. And end user should be provided with user-level login only, if web UI access is needed.

SSH Access

The GVC32xx allows access via SSH for advanced troubleshooting purpose. This is usually not needed unless the administrator or Grandstream support needs it for troubleshooting purpose. SSH access on GVC32XX is enabled by default and uses port number 22. It's recommended to disable it for daily normal usage from web UI → Settings → Security settings → Web/SSH access → Disable SSH, changing this setting will require reboot to take effect.

Figure 4: SSH Access on GVC32xx

DEVICE CONTROL SECURITY

Screen lock

Screen lock setting is under LCD → Settings → System → Security → Screen Security. Set password for screen lock. Enter a 6-digit password for screen lock. When the GVC3200/GVC3202 boots up again, a screen lock code will be required. The users can unlock the screen by entering the code using the GVC remote control.

Permission to install apps from unknown sources

"Unknown Sources" setting is under LCD → Settings → System → Security → Device administration. It is recommended to disable "Unknown source" to prevent installing apps from unknown sources if the device is used at public properties.

GUI Config Tool Settings

This is available for the GVC320x only

The GUI config tool is a tool designed to customize the GUI desktop layout as well as GUI configuration for devices. Here is the link to download the GUI config tool:
http://www.grandstream.com/tools/gui_customization_tool_v3.9.0.zip

From there, the administrator can build a customized file to display/hide certain applications, configure parameters on the phone with specific configuration items, and enable/disable some applications and much more. The tool would generate a file "GVC320xcust" which should be uploaded to a HTTP/TFTP server. Then the user needs to configure the server address as GUI Customization File URL under web UI → Maintenance → Upgrade → Cust file → GUI customization file URL to download the file to GVC320x.

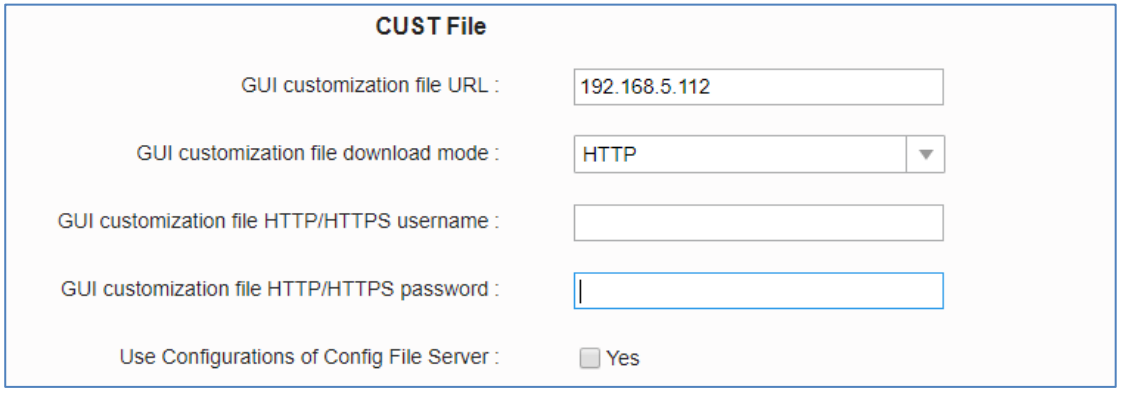

Figure 5: Cust File Provision Page

For more details, please refer to the guide:
http://www.grandstream.com/tools/gvc320x_gui_customization_guide.pdf

SECURITY FOR SIP ACCOUNTS AND CALLS

Protocols and Ports

By default, after factory reset, the SIP account is active. Since the default local SIP port is 5060 for account 1, this allows user to make direct IP call even if the account is not registered to any PBX. If the user is not using any account, it is recommended to uncheck the settings from web UI → Settings → SIP → General → Account Active to deactivate account.

- **SIP transport protocol:**
  The GVC32xx supports SIP transport protocol "UDP" "TCP" and "TLS". By default, it's set to "UDP". It's recommended to use "TLS" so the SIP signaling is encrypted. SIP transport protocol can be configured under web UI → Settings → SIP →SIP→ SIP transport. When "TLS" is used, we recommend using "sips" instead of "sip" for SIP URI scheme to ensure the entire SIP transaction is secured instead of "best-effort".

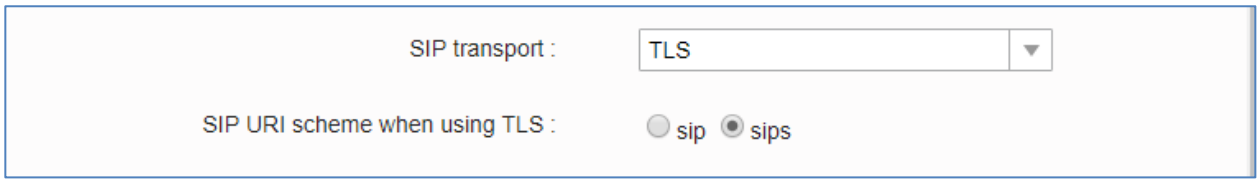

Figure 6: Configure TLS as SIP Transport

SIP TLS certificate, private key and password can be configured under GVC32xx web UI→Settings→Security Settings→SIP.

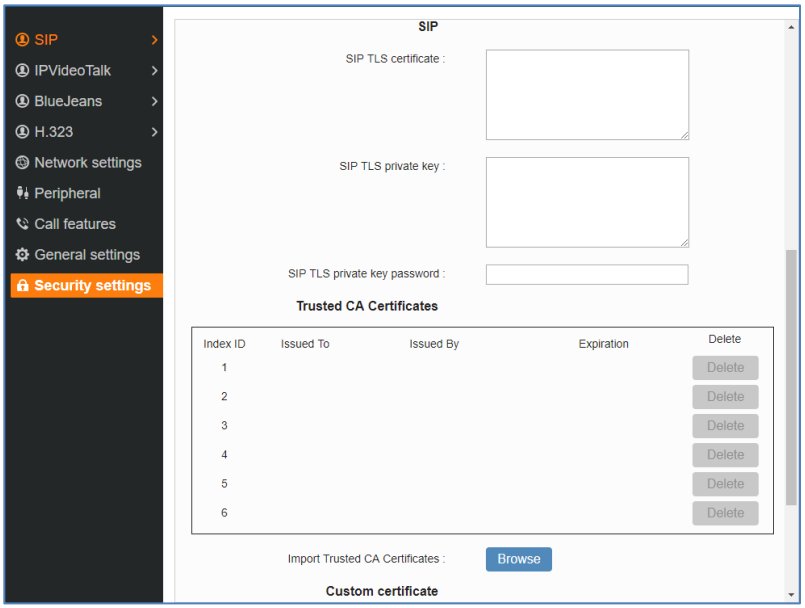

Figure 7: SIP TLS Settings on GVC32xx

When SIP TLS is used, the GVC32XX also offers additional configurations to check domain certificate and validate certificate chain. These settings can be found under web UI → Settings → SIP → SIP.

- **Check Domain Certificate**:
  If enabled, the GVC32xx will check the domain certificate when TLS/TCP is used for SIP transport. The default setting is “No”.

- **Validate Certification Chain**:
  If enabled, the GVC32xx will validate server’s certification chain when TLS/TCP is used for SIP transport. The default setting is “No”.

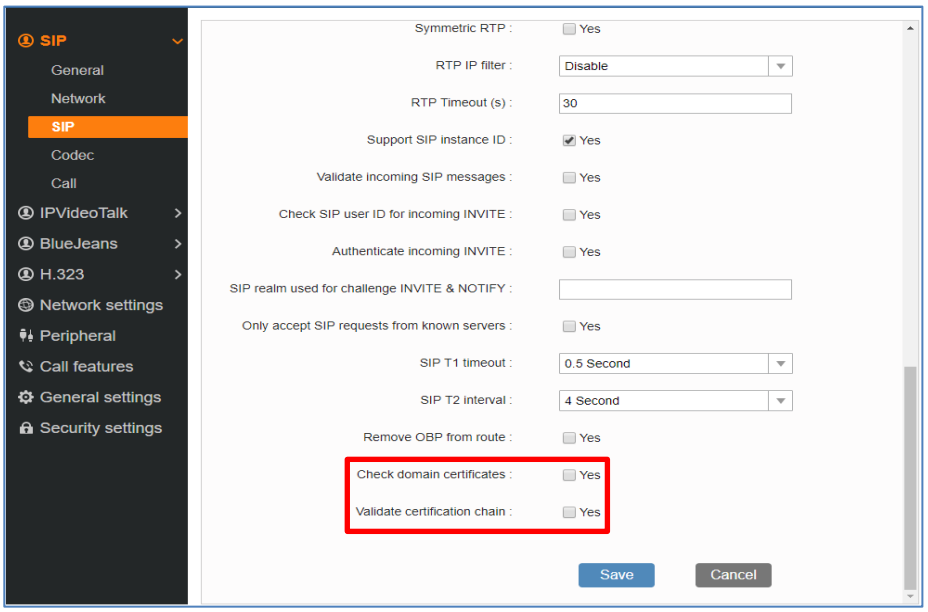

Figure 8: Additional SIP TLS Settings

- **Local SIP port when using UDP/TCP:**
  Default SIP port used is 5060. The local SIP port can be configured under Settings→SIP→SIP→ Local SIP port.

- **Local SIP port when using TLS:**
  The SIP TLS port is the UDP SIP port plus 1. For example, if local SIP port is 5060, its TLS port would be 5061.

- **Local RTP port:**
  The default port value is 5004. This parameter can be configured from web UI → Settings → General Settings → 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.

Anonymous/Unsolicited Calls Protection

If the user would like to have anonymous SIP calls blocked, please go to GVC32xx web UI → Settings → SIP → Call Settings and enable option "Reject anonymous call". This will automatically block the SIP call if the caller ID is anonymous.

Additionally, the GVC32xx has built-in mechanism that detects and stops the spam SIP calls from ringing the devices. Please see below web UI → Settings → SIP → SIP. It is recommended to enable highlighted options to validate incoming SIP requests.

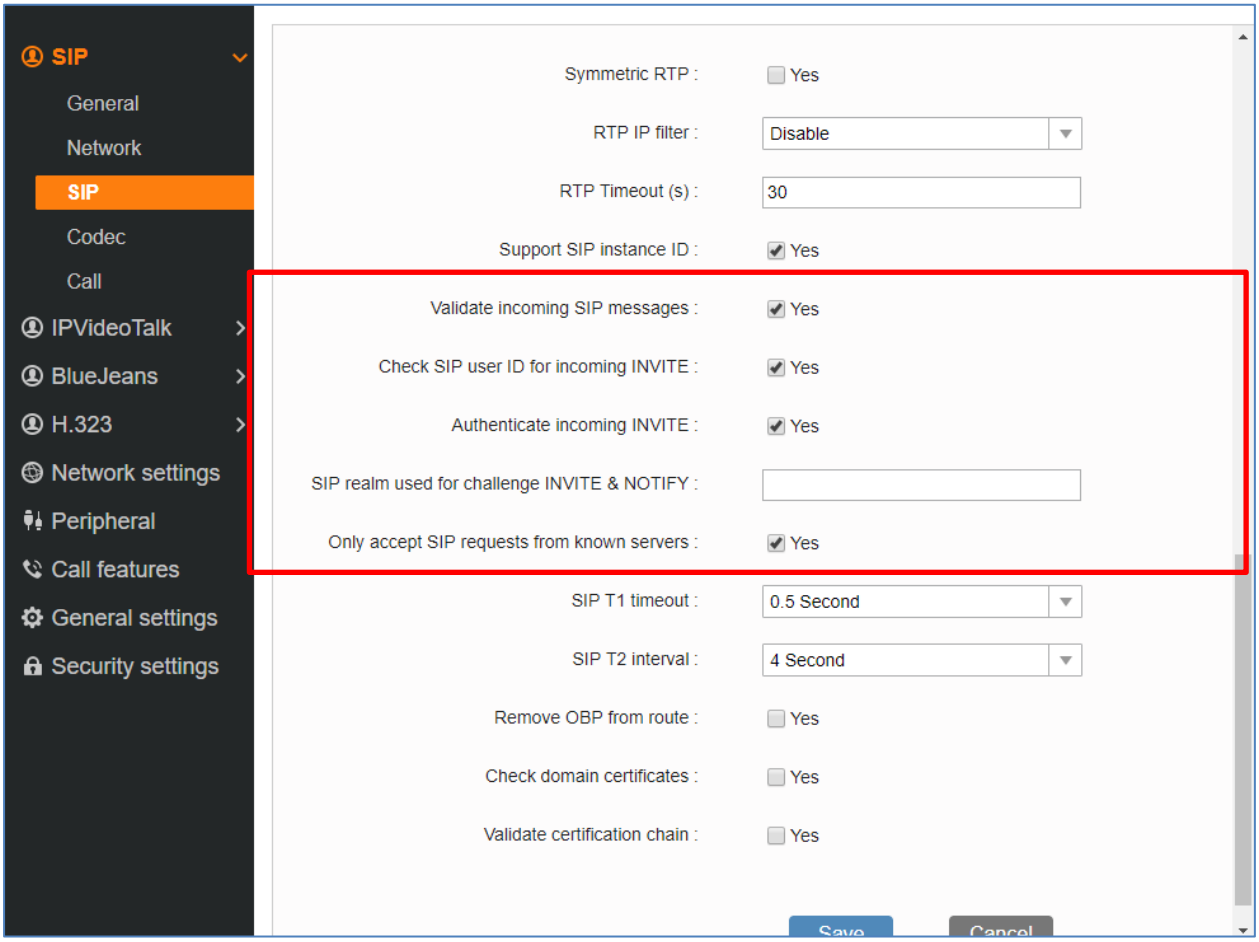

Figure 9: Settings to Block Unwanted Calls

- **Only Accept SIP Requests from Known Servers:**
  When set to "Yes", the GVC32xx will answer the SIP request from saved servers and only the SIP requests from saved servers will be accepted. The SIP requests from the unregistered server will be rejected. The default setting is "No".

- **Check SIP User ID for Incoming INVITE:**
  This configures the GVC32xx to check the SIP User ID in the Request URI of the SIP INVITE message from the remote party. If it doesn't match the phone's SIP User ID, the call will be rejected. The default setting is "No".

- **Validate Incoming INVITE:**
  This configures the GVC32xx to authenticate the SIP INVITE message from the remote party. If set to "Yes", the phone will challenge the incoming INVITE for authentication with SIP 401 Unauthorized response. The default setting is "No".

- **SIP Realm Used for Challenge INVITE & NOTIFY:**
  Configure this item to validate incoming INVITE and NOTIFY. To use this feature, “Validate Incoming INVITE” must be enabled first for it to take effect for INVITE. For NOTIFY, “Disable SIP NOTIFY Authentication” must be unchecked first under web UI → Maintenance → Upgrade → Advanced Settings. The SIP NOTIFY message information for the provision includes check- sync, re-sync and reboot.

SRTP

To protect voice communication from eavesdropping, the GVC32xx phones support SRTP for media traffic using AES 128&256. It is recommended to use SRTP if server supports it. SRTP can be configured in web UI → SIP → Codec.

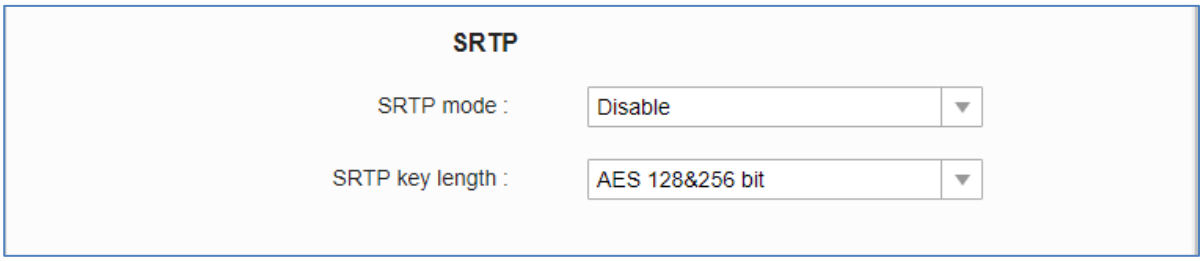

Figure 10: SRTP Settings

NETWORK SECURITY

VPN

Users can add VPN using different protocols (PPTP, L2TP/IPSec PSK, L2TP/IPSec RSA, IPSec Xauth PSK, IPSeXauth RSA and IPSec Hybrid RSA). VPN settings can be configured from GVC32xx LCD menu → Applications → Settings → Network → VPN and Tap on "Add VPN file" to access configuration page as shown below:

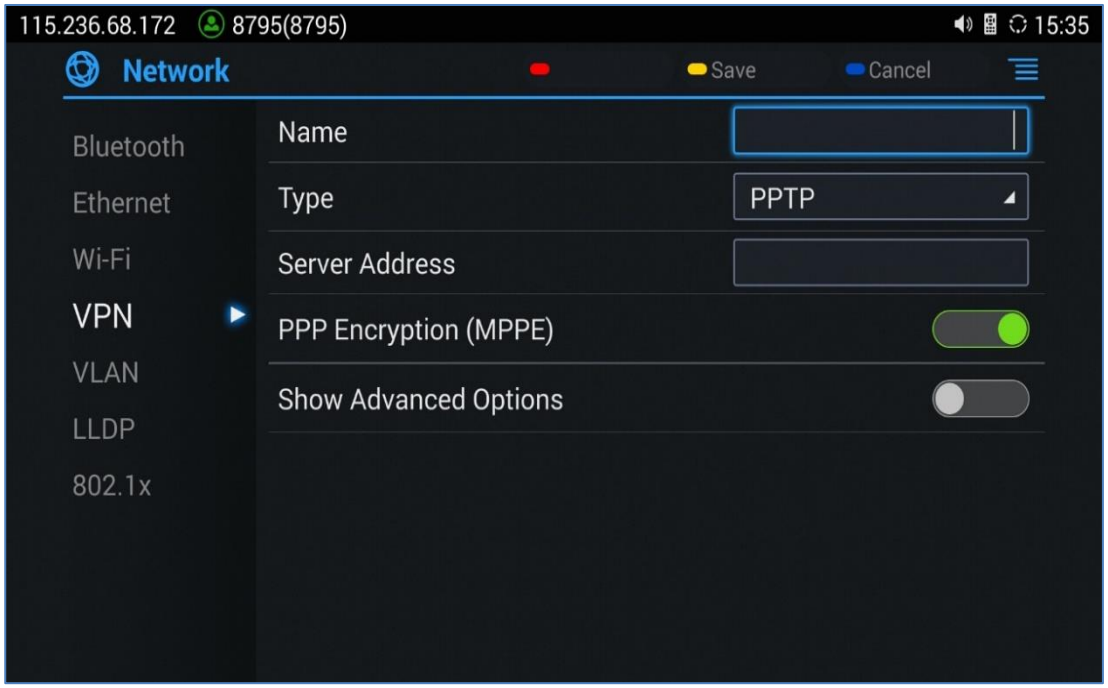

Figure 11: GVC32xx VPN profile configuration

802.1X

GVC32xx supports EAPOL where access to switchports can be controlled with identity/password and certificate. By default, it is disabled. When it is enabled, there are 3 different mode for selection: EAP-MD5, EAP-TLS and EAP-PEAP. Network administrators can set this up accordingly for media access control and network security purpose.

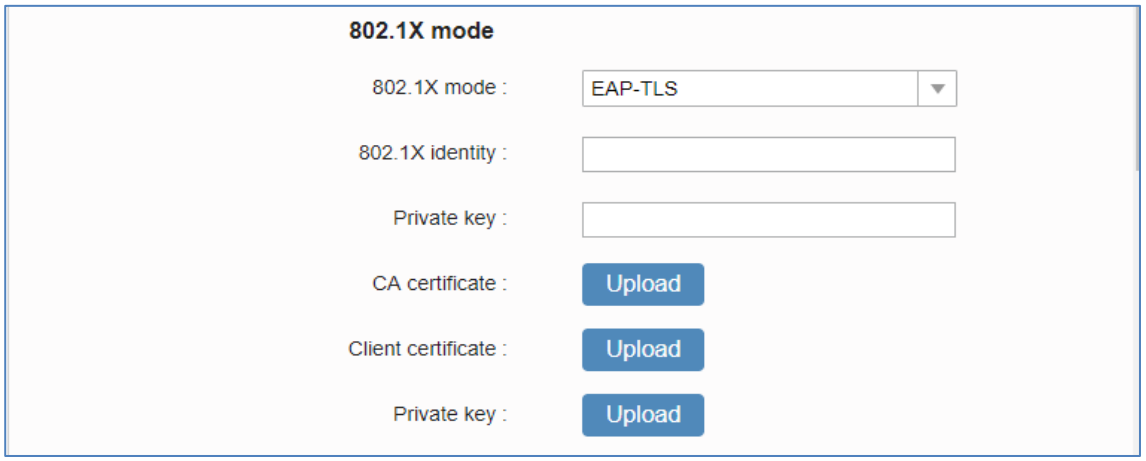

Figure 12: 802.1X Settings

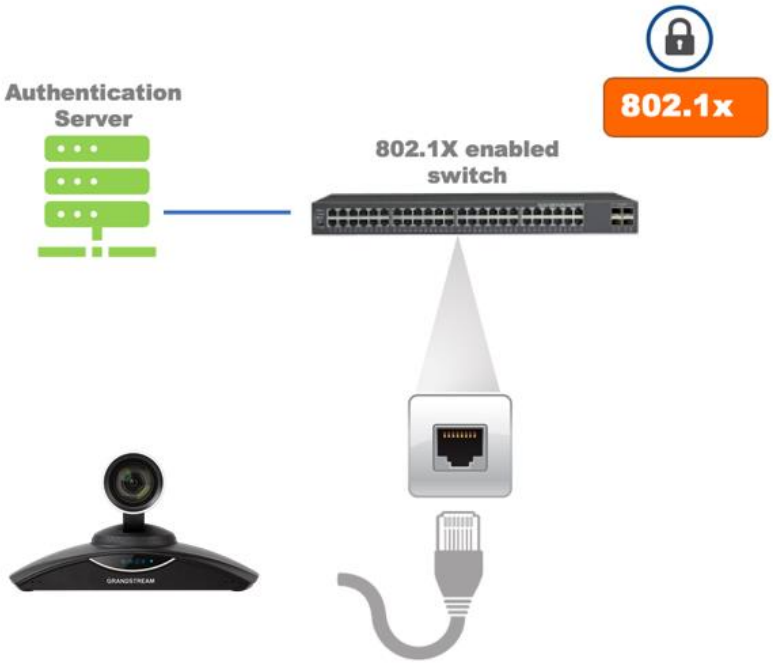

Figure 13: 802.1X for GVC32xx Deployment

Bluetooth

GVC32xx supports Bluetooth for Bluetooth headset connection, file transferring and for connecting external speakers to be used as audio input and output. By default, Bluetooth is disabled and it can be enabled from LCD settings → Network → Bluetooth. If there is no Bluetooth device used with GVC32XX, it's recommended to turn off Bluetooth so it's not discoverable by nearly Bluetooth devices.

Provisioning via Configuration File

GVC32XX supports downloading configuration file via HTTP/HTTPS/TFTP. Below figure shows the options for config file provisioning.

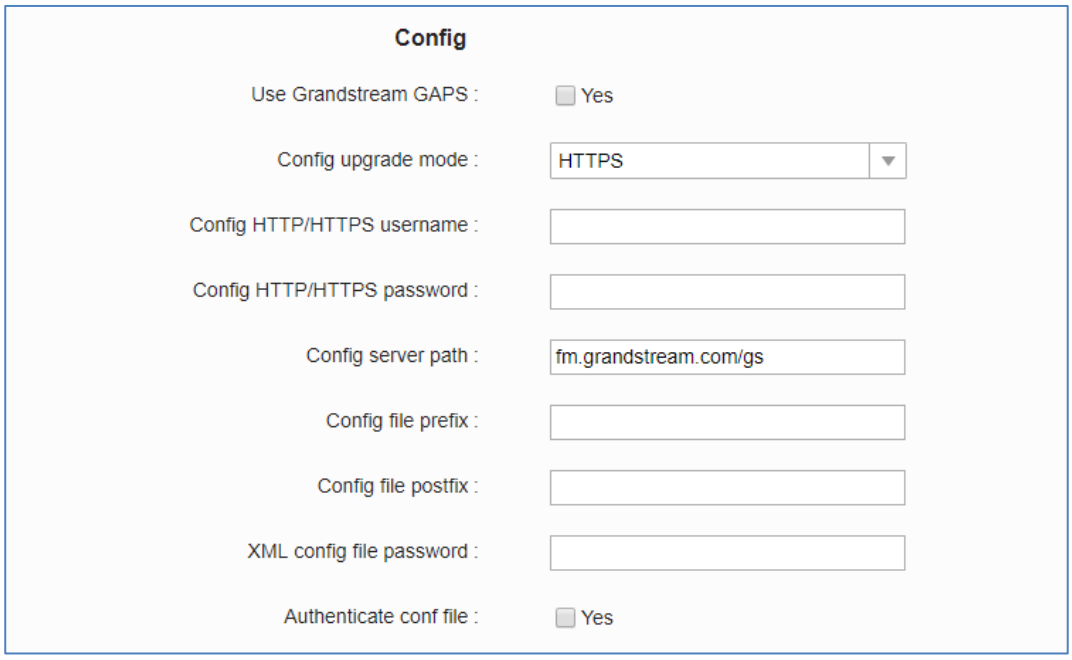

Figure 14: GVC32xx Config File Provisioning

We recommend users to consider the following options for added security when deploying the GVC32xx with provisioning.

- **Config Upgrade Via: HTTPS:**
  By default, HTTPS is selected. This is recommended so the traffic is encrypted while travelling through the network.

- **HTTP/HTTPS User Name and Password:**
  This can be set up as required on the provisioning server when HTTP/HTTPS is used. Only when the GVC32xx has the correct username and password configured, it can be authenticated by the provisioning server and the config file can be downloaded.

- **Authenticate Config file:**
  This sets the GVC32xx to authenticate configuration file before applying it. When set to “Yes”, the configuration file must include P value P2 with GVC32xx’s administration password. If it is missed or does not match the password, the GVC32XX will not apply the config file.

- **XML Config File Password:**
  The GVC32xx XML config file can be encrypted using OpenSSL. When it's encrypted, the GVC32xx must supply the correct password in this field so it can decrypt XML configuration file after downloading it. Then the configuration can be applied to the GVC32xx. Please note this feature is supported on XML config file instead of the binary config file. Therefore, it's recommended to use XML config file format and encrypt it with this feature.

- **Validate Certificate Chain:**
  This configures whether to validate the server certificate when downloading the firmware/config file. If set to "Yes", the phone will download the firmware/config file only from the legitimate server.

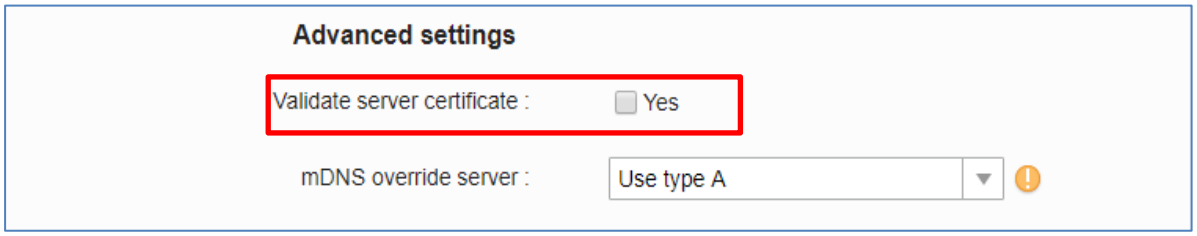

Figure 15: Validate Certification Chain

GVC32xx supports uploading CA certificate to validate the server certificate and this setting is under GVC32xx web UI → Settings → Security Settings.

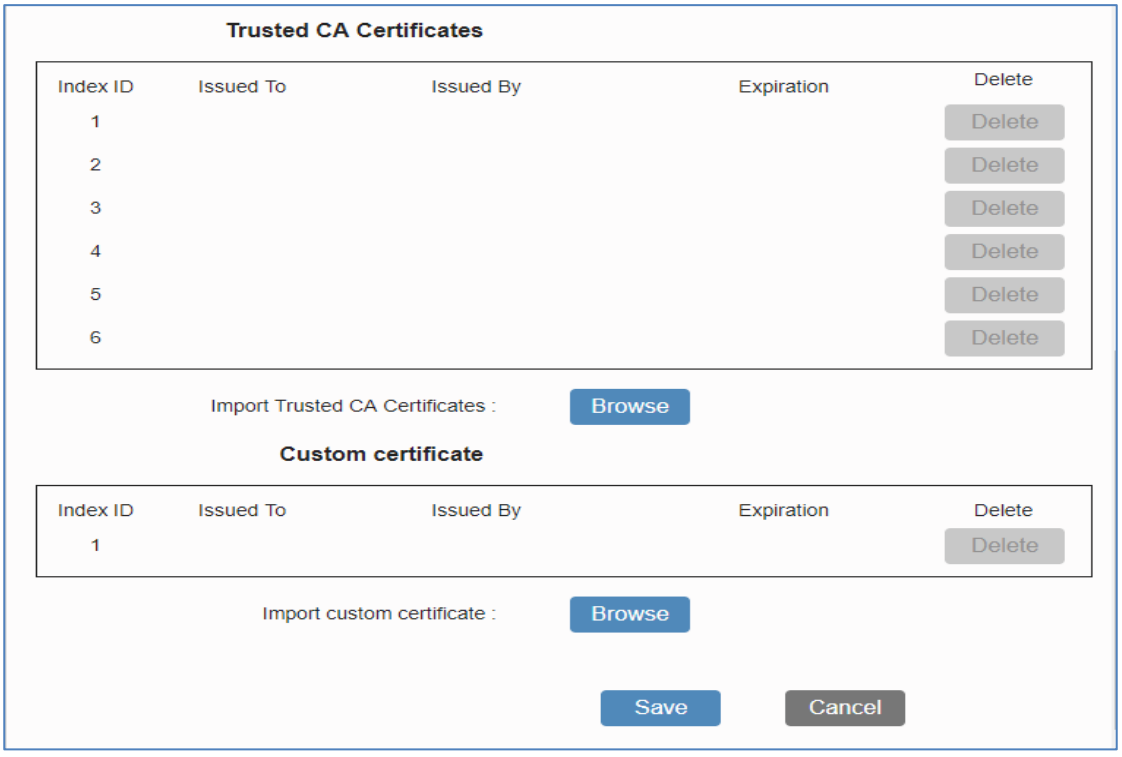

Figure 16: Certificate Management

Firmware Upgrading

Similar to configuration file provisioning, GVC32xx supports downloading firmware file via HTTP/HTTPS/TFTP. The firmware file is encrypted and GVC32xx ensures only authentic, signed and untampered firmware file can run. Here are the recommended settings for firmware downloading.

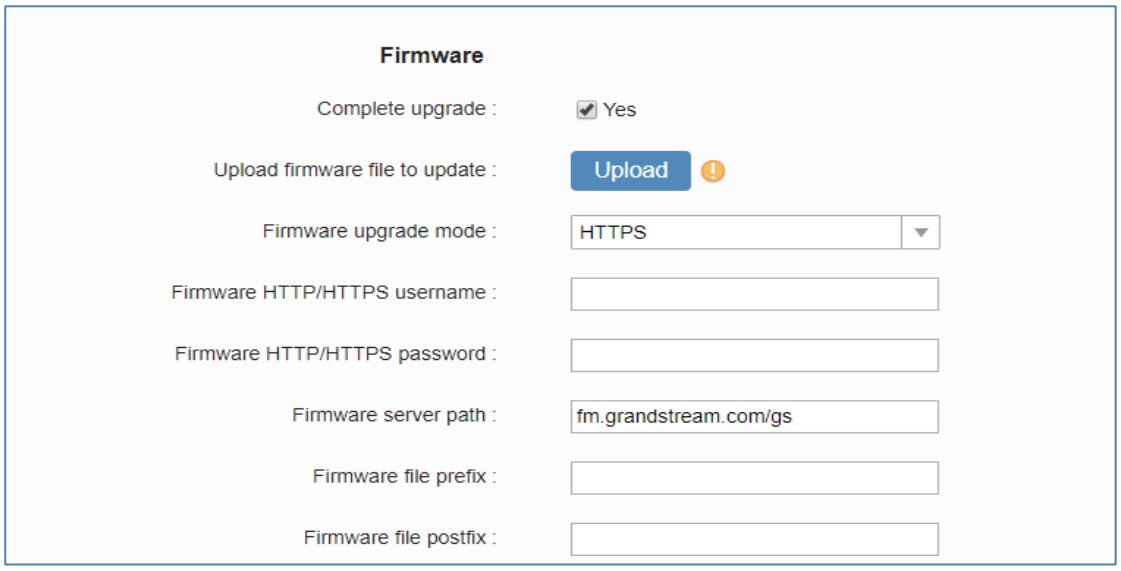

Figure 17: Firmware Upgrade Configuration

- **Firmware Upgrade Mode: HTTPS.**
  HTTPS is recommended so the traffic is encrypted while travelling through the network.

- **HTTP/HTTPS User Name and Password:**
  This can be set up as required on the provisioning server when HTTP/HTTPS is used. Only when the GVc32xx has the correct username and password configured, it can be authenticated by the firmware server and the firmware file will be downloaded.

- **Validate Certificate Chain:**
  This configures whether to validate the server certificate when downloading the firmware/config file. If set to "Yes", the GVC32xx will download the firmware/config file only from the legitimate server.

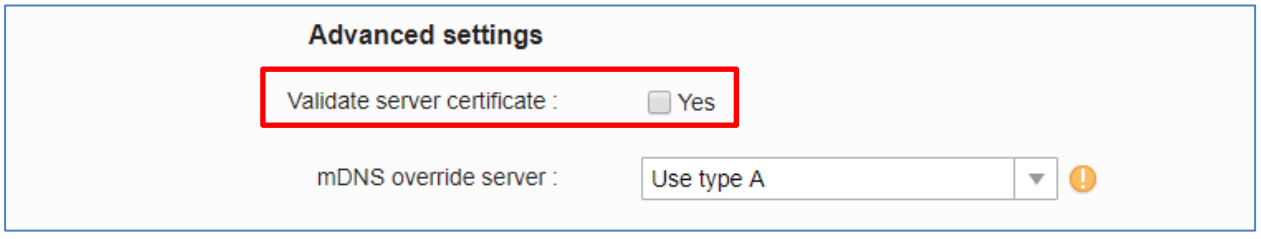

Figure 18: Validate Certification Chain

The GVC32xx supports uploading CA certificate to validate the server certificate and this setting is under GVC32xx web UI → Settings → Security Settings.

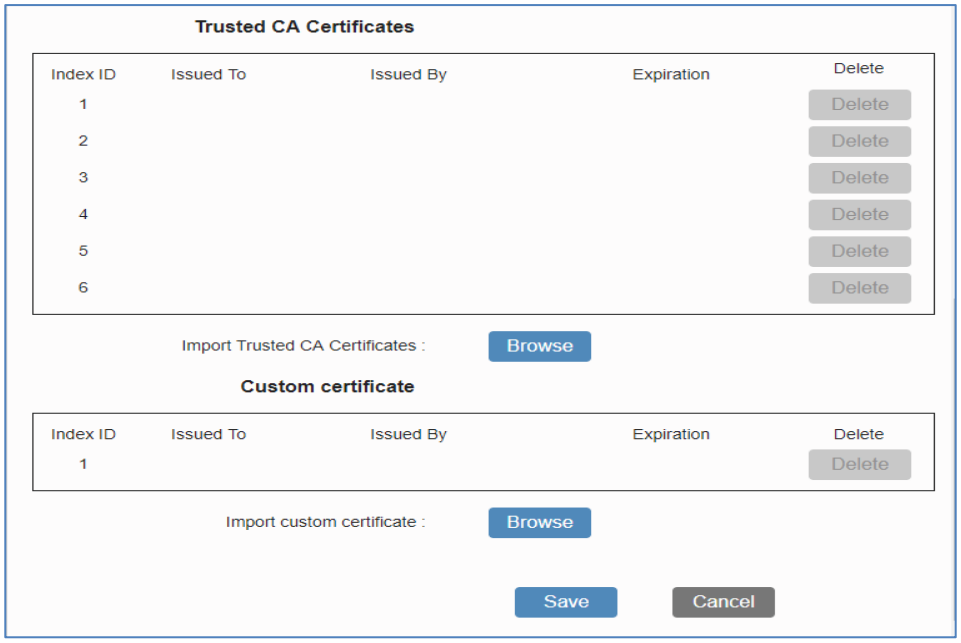

Figure 19: Certification Management

TR-069

TR-069 is enabled by default, which means the connection request port 86400 is open for TR-069 session. If the user does not need TR-069 service, it's recommended to disable it. When TR-069 is enabled and the service is to be used, users can also consider using a different connection request port other than the well-known port 86400 for security purpose.

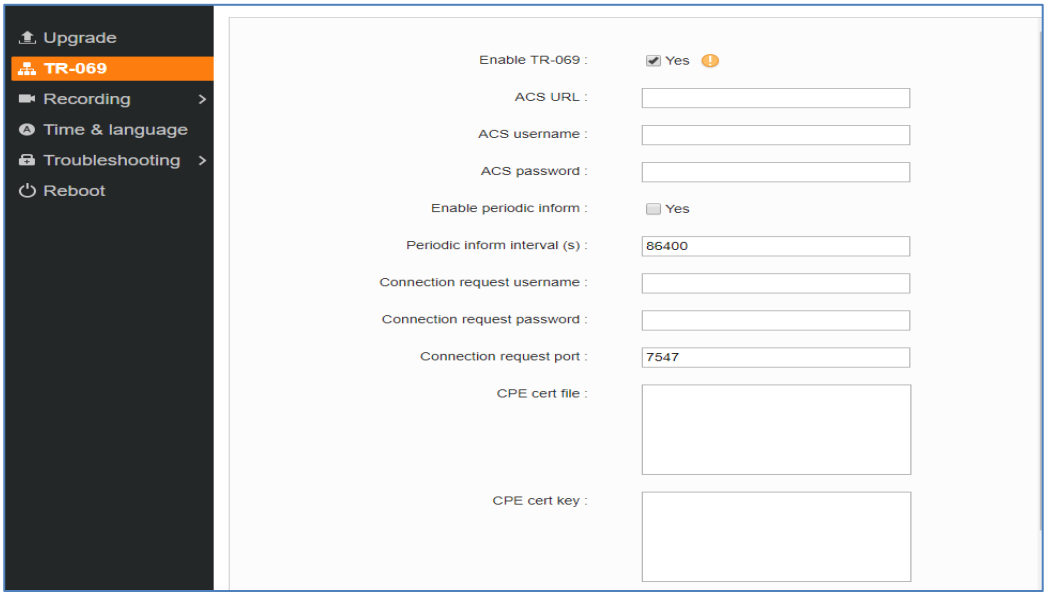

Figure 20: TR-069 Connection Settings Page

ADB Service

Android Debug Bridge (ADB) is a versatile command-line tool that allows users to communicate with GVC32xx for installing apps, debugging apps and running specific commands. To enable ADB connection, users must turn on developer mode from WEB UI → Maintenance → Troubleshooting → Developer Mode. The port number used for ADB connection is 5555. It is not recommended to enable developer mode if ADB connection is not needed.

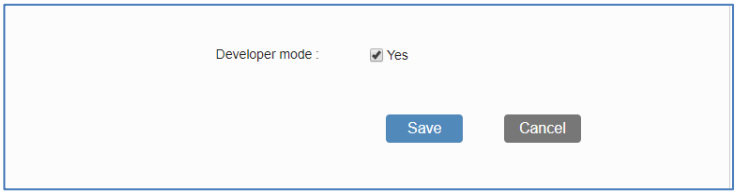

Figure 21: Enabling Developer Mode

LDAP

GVC32xx supports LDAP to obtain enterprise contacts from LDAP server. It's recommended to change the default connection mode "LDAP" to "LDAPS" to protect and encrypt LDAP queries and responses using SSL/TLS.

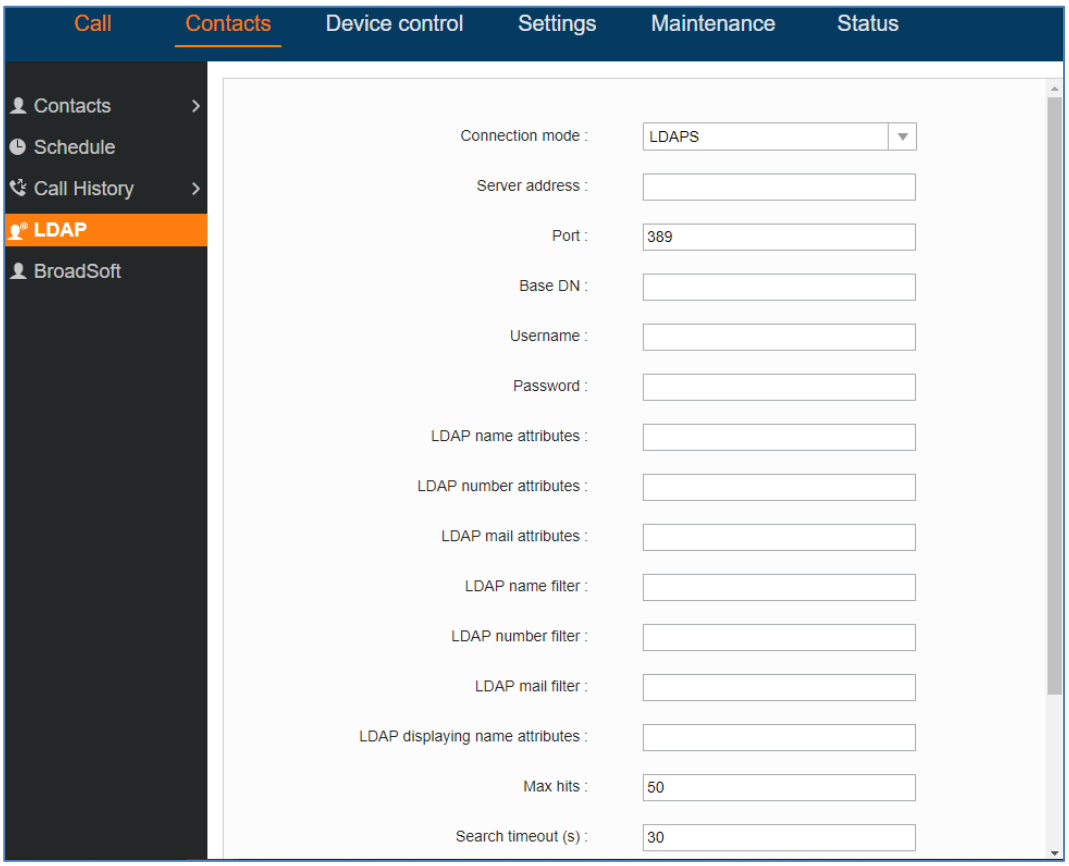

Figure 22: GVC32xx LDAP Settings

Syslog

GVC32xx supports sending Syslog to a remote syslog server. By default, it's sent via UDP and we recommend to change it to "SSL/TLS" so the syslog messages containing device information will be sent securely over TLS connection.

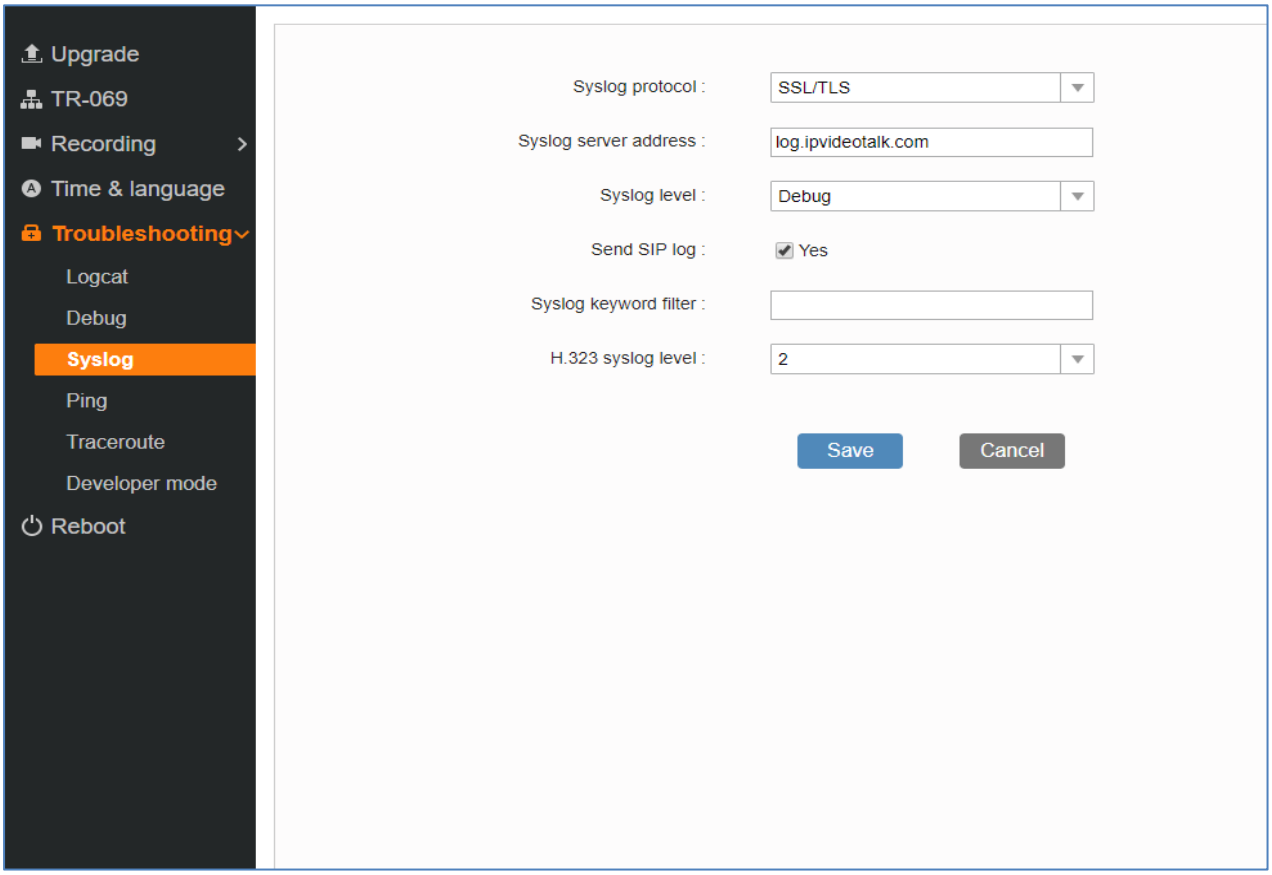

Figure 23: Syslog Protocol

SECURITY GUIDELINES FOR GVC32XX DEPLOYMENT

Often times the GVC32XXs are deployed behind NAT. The network administrator can consider following security guidelines for the GVC32XX to work properly and securely.

- **Turn off SIP ALG on the router**
  On the customer's router, it's recommended to turn off SIP ALG (Application Layer Gateway). SIP ALG is common in many routers intending to prevent some problems caused by router firewalls by inspecting VoIP packets and modifying it if necessary. Even though SIP ALG intends to prevent issues for VoIP devices, it can be implemented imperfectly causing problems, especially in some cases SIP ALG modifies SIP packets improperly which might cause VoIP devices fail to register or establish calls.

- **Use TLS and SRTP for SIP calls**
  On the GVC32XX, it's recommended to use TLS for SIP transport with "sips" in SIP URL scheme for SIP signaling encryption, and use SRTP for media encryption. Below are the SIP ports and RTPs port used on the GVC32XX if the network administrator needs to create firewall rules.
    - Users can configure the local SIP port to be used for sip calls under Settings→SIP→SIP→ Local SIP port. The default SIP port used is 5060.
    - Users can configure the local RTP port under web UI → Settings → General Settings → Local RTP port. The default port value is 5004. 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.

  Note:
  On the customer's firewall, it's recommended to ensure SIP port is opened for the SIP accounts on the GVC32XX. It's not necessary to use the default port 5060 on the firewall. Instead, the network administrator can consider mapping a different port on the firewall for GVC32XX SIP port 5060 for security purpose.

- **Use HTTPS for web UI access**
  GVC32XX Web UI access should be equipped with strong administrator password in additional to using HTTPS. Also, do not expose the GVC32XX web UI access to public network for normal usage.

- **Use HTTPS for firmware downloading and config file downloading**
  Use HTTPS for firmware downloading and provisioning. Besides that, set up username and password for the HTTP/HTTPS server to require authentication. It's also recommended to turn on "Validate Certification Chain" so the GVC32XX will validate server certificate when downloading the firmware or config file.