Grandstream Networks, Inc.

GAC2500

Audio Conference Phone 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 GAC2500.

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 GAC2500 has multiple ways to limit the use for network settings, apps, and other settings if not necessary for the end user.

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

- **Network Security**
  The GAC2500 supports VPN, 802.1X, Bluetooth. VPN secures remote connection and 802.1X provides network access control. it's recommended to turn off Bluetooth if not used.

- **Security for GAC2500 Services**
  GAC2500 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 and FTP, we recommend disabling them if not used to avoid potential port exposure.

- **Deployment Guidelines for GAC2500**
  This section introduces protocols and ports used on GAC2500 and recommendations for routers/firewall settings.

This document is subject to change without notice.

WEB UI/SSH ACCESS

GAC2500 Web UI Access

The GAC2500 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 GAC2500 information and settings. It is critical to understand the security risks involved when placing the GAC2500 phone on public networks and it's recommended not to do so.

Web UI Access Protocols

HTTP and HTTPS are supported to access the GAC2500 web UI and can be configured under web UI → Maintenance → Security Settings. 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.

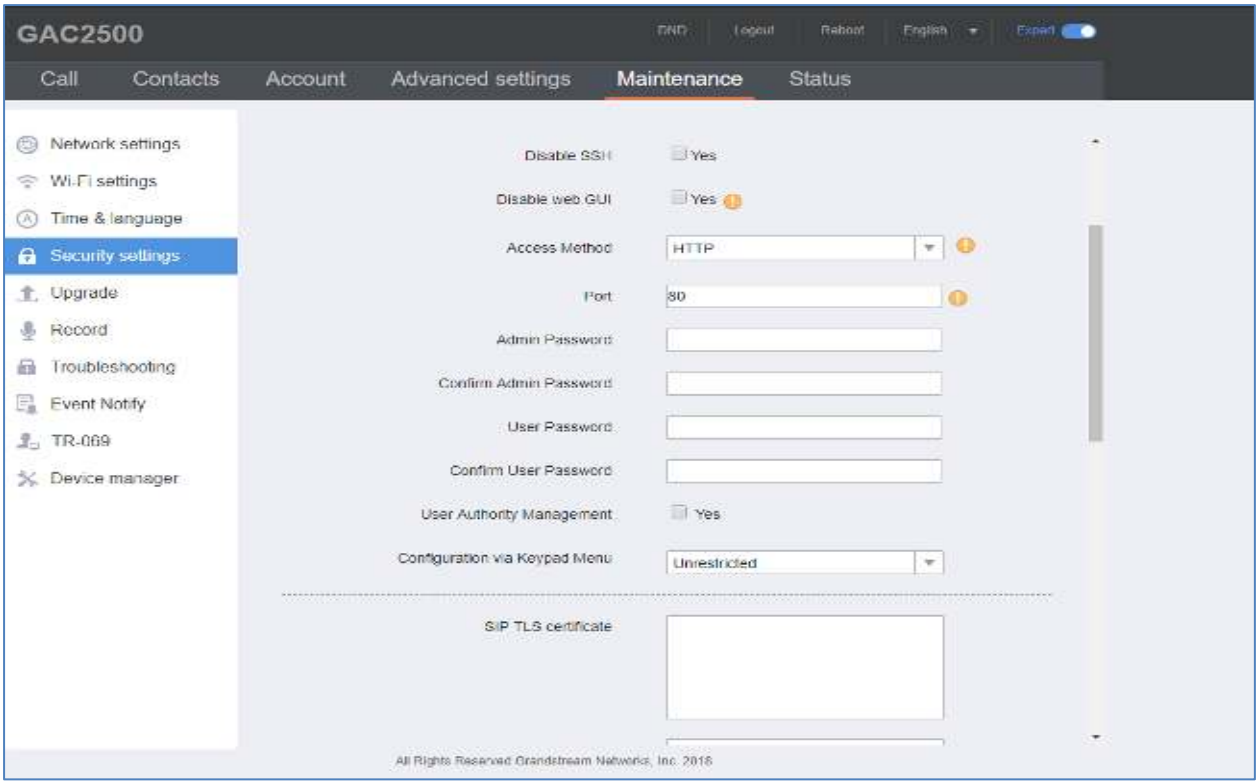

Figure 1: Web UI Access Settings

User Login

Username and password are required to log in the GAC2500 web UI.

Figure 2: GAC2500 Web UI Login

The factory default username is “admin” and the default password is “admin”. The GAC2500 web UI require to change the default password at first time login.

Figure 3: GAC2500 Admin Password Change

To change the password for default user "admin", Press on **Change Password** in the highlighted upper corner or navigate to Maintenance → Security Settings. The password length must 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 GAC2500'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 configure the following settings:

- **Call**
- **Contacts**
- **Account: Call Settings**
- **Advanced: MPK General Settings, MPK LCD Settings**
- **Maintenance: Network Settings, Time & Language, Security Settings, Device Manager**
- **Status: Account Status, Network Status, System Info**

Even if user login can access certain web UI pages, it has less options compared to admin login.
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 GAC2500 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 GAC2500 is enabled by default with port 22 used. It's recommended to disable it for daily normal usage. If SSH access needs to be enabled, changing the port to a different port other than the well-known port 22 is a good practice.

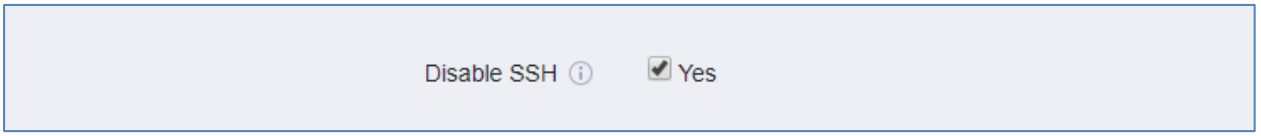

Figure 4: Disable SSH Access on GAC2500

DEVICE CONTROL SECURITY

From GAC2500 web UI → Maintenance → Security Settings. administrator can set whether the user can use specific features:

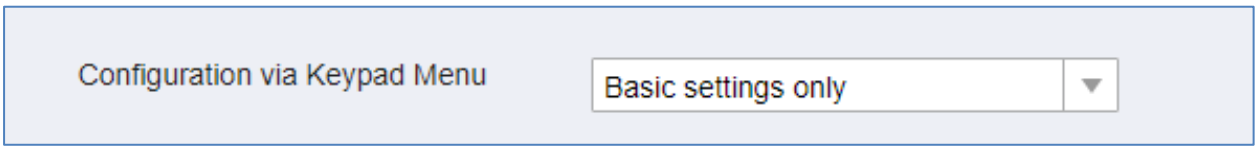

Figure 5: Limit Access to Advanced Settings on LCD

Configuration via Keypad Menu

This option configures access for keypad Menu settings on the Settings interface of the phone. It is recommended to use "Constraint Mode" for end users.

- **Unrestricted:**
  Configure all settings on the LCD settings interface.
- **Basic Settings Only:**
  Advanced Settings, Wireless & Network options will not be displayed in LCD settings menu.
- **Constraint Mode:**
  The user is required to enter the correct admin password to access Wireless & Network options and Advanced Settings.

Permission to Install/Uninstall Apps

This option configures the permission for users to install/uninstall 3rd party applications. "Unknown Sources" setting is under LCD → Advanced Settings → General Settings. It is recommended to use "Not allow" if the device is used at public properties.

- **Allow:**
  The user can install/uninstall any 3rd party apps as needed.
- **Require admin password:**
  The user needs to enter the correct admin password before he/she can install/uninstall 3rd party apps.
- **Require admin password if the app source is unknown:**
  The user needs to enter the correct admin password only when installing apps from unknown source. Admin password is also required when the user uninstalls the 3rd party apps.
- **Not allow:**
  The user cannot install/uninstall third-party apps. Unknown sources setting is not available under this mode.

GUI Config Tool Settings

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 remove access for certain apps and task bar features. The tool would generate a file "GAC2500cust" 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 Config Server Path to download the file to GAC2500.

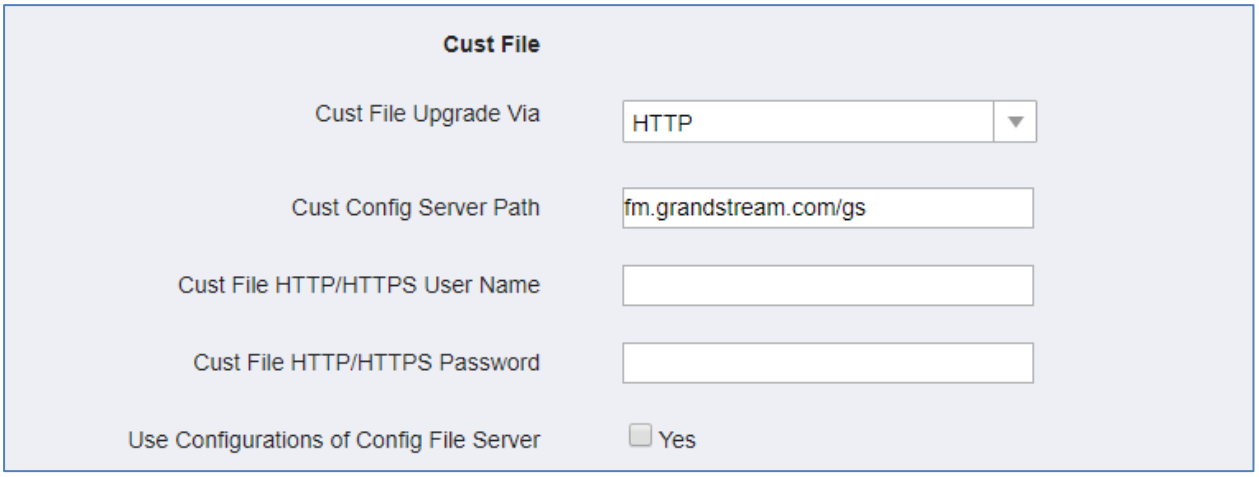

Figure 6: Cust File Provision Page

For more details, please refer to the guide:
http://www.grandstream.com/tools/gac2500_gui_customization_guide.pdf

SECURITY FOR SIP ACCOUNTS AND CALLS

Protocols and Ports

By default, after factory reset, the SIP account 1 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 → Account → General Settings → Account Active to deactivate account 1.

Below are the ports/protocols used on GAC2500 SIP accounts. GAC2500 supports up to 6 SIP accounts.

- **SIP transport protocol:**
  The GAC2500 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 per SIP account under web UI → Account → Account x → SIP Settings. 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".

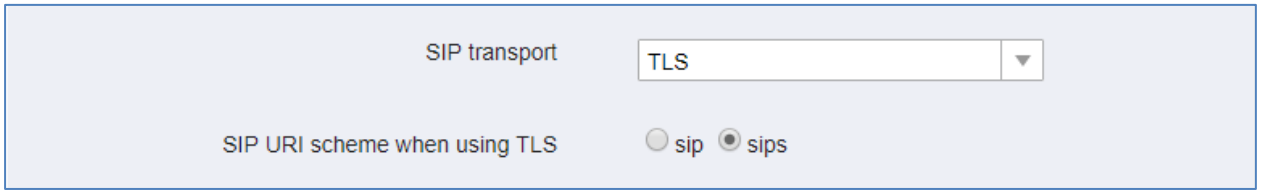

Figure 7: Configure TLS as SIP Transport

SIP TLS certificate, private key and password can be configured under GAC2500 web UI→Maintenance → Security Settings → SIP TLS.

Figure 8: SIP TLS Settings on GAC2500

When SIP TLS is used, the GAC2500 also offers additional configurations to check domain certificate and validate certificate chain. These settings can be found under web UI → Account → Account x → SIP Settings.

- **Check Domain Certificate**:
  If enabled, the GAC2500 will check the domain certificate when TLS/TCP is used for SIP transport. The default setting is "No".

- **Validate Certification Chain**:
  If enabled, the GAC2500 will validate server's certification chain when TLS/TCP is used for SIP transport. The default setting is "No".

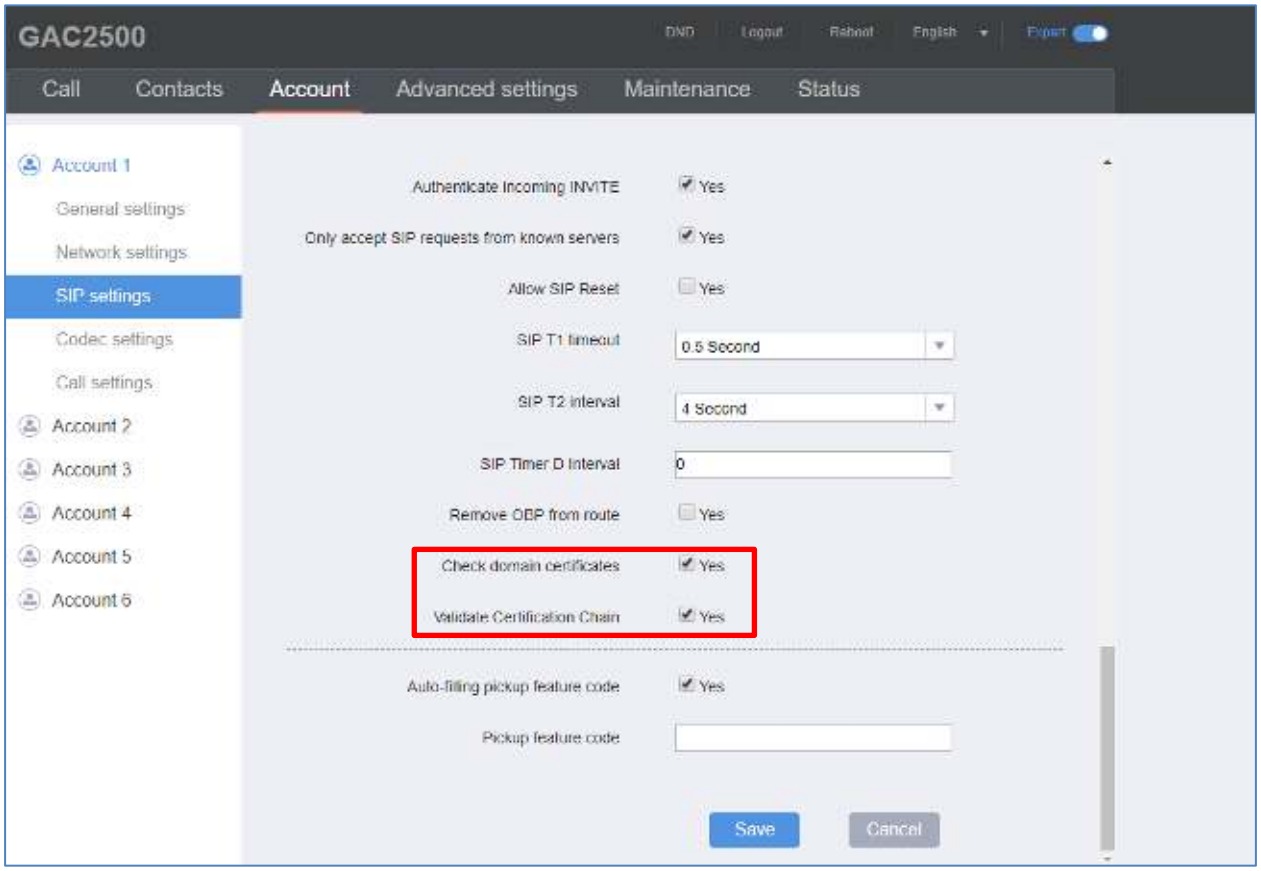

Figure 9: Additional SIP TLS Settings

- **Local SIP port when using UDP/TCP:**
  Starting from 5060 for account 1, the port numbers increase by 2 for account x. For example, 5062 is the default local SIP port for account 2, 5064 for account 3, etc. The local SIP port can be configured under Account→SIP Settings for each SIP account.

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

- **Local RTP port:**
  The default port value is 5004. The Local RTP port can be configured from web UI → Advanced Settings → General Settings. This parameter defines the local RTP-RTCP port pair used to listen and transmit. If it is configured with X, in channel 0 the port X will be used for audio RTP message, the port X+1 for audio RTCP message, the port X+2 for video RTP message and the port X+3 for video RTCP. In Channel 1, each port number will be incremented by 4 for each message. This increment rule will apply to other channels and other port numbers. By default, the Account 1 will use Channel 0, Account 2 Channel 1, Account 3 Channel 2, Account 4 Channel 3, and Account 5 Channel 4 and Account 6 Channel 5. If an account needs to establish multiple session simultaneously, the system will use the ports in the next available channels. The valid range is from 1024 to 65400.

Anonymous/Unsolicited Calls Protection

If the user would like to have anonymous calls blocked, please go to GAC2500 web UI → Account → Account x → Call Settings and enable option "Reject Anonymous call". This will automatically block the SIP call if the caller ID is anonymous.

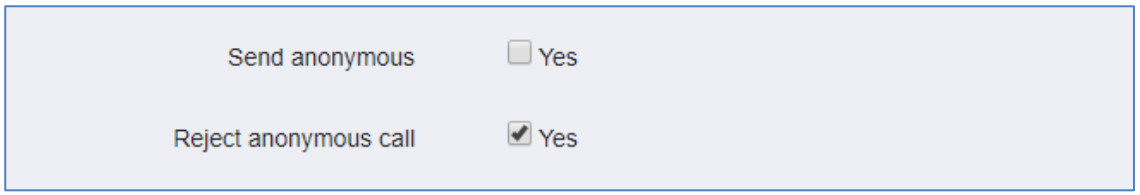

Figure 10: Settings to Block Anonymous Call

Additionally, the GAC2500 has built-in mechanism that detects and stops the spam SIP calls from ringing the phones. Please see below web UI → Account → Account x → Advanced Settings. It is recommended to enable highlighted options to validate incoming SIP requests.

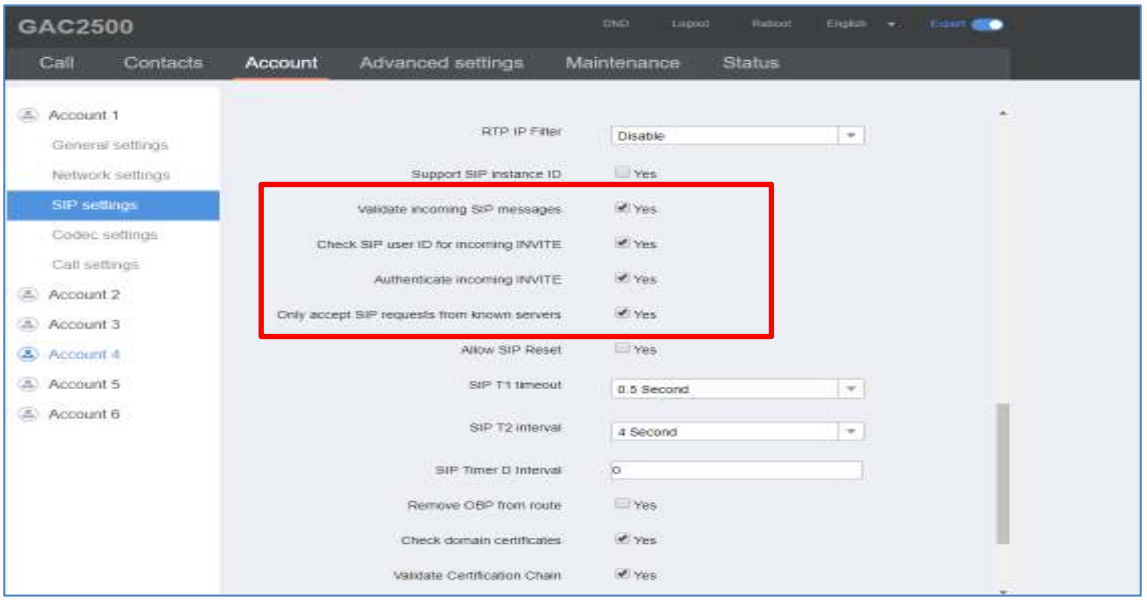

Figure 11: Settings to Block Unwanted Calls

- **Only Accept SIP Requests from Known Servers:**
  When set to “Yes”, the GAC2500 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 GAC2500 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”.

- **Authenticate Incoming INVITE:**
  This configures the GAC2500 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".

- **Validate incoming SIP messages:**
  Specifies if the phone system will check the incoming SIP messages caller ID and CSeq headers. If the message does not include the headers, it will be rejected.

SRTP

To protect voice communication from eavesdropping, the GAC2500 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 → Account → Codec Settings.

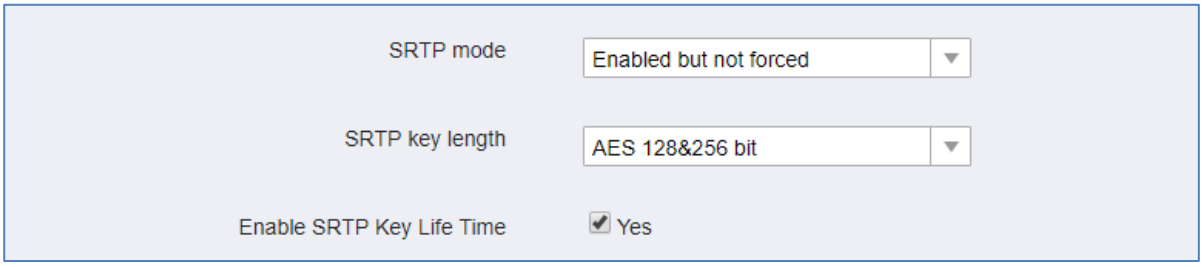

Figure 12: SRTP Settings

When **SRTP Key Life Time** parameter is enabled, during the SRTP call, the SRTP key will be valid within 231 SIP packets, and phone will renew the SRTP key after this limitation.

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 GAC2500 LCD Settings → Advanced settings → Wireless & network → VPN and Tap on "Add VPN file" to access configuration page as shown below:

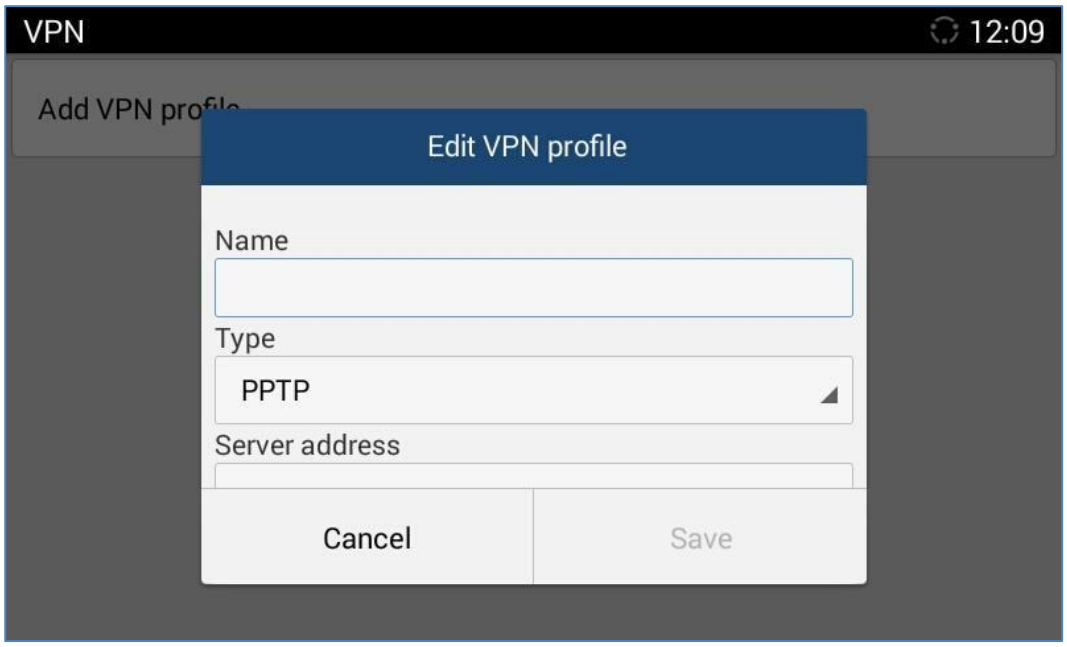

Figure 13: VPN Settings

802.1X

GAC2500 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.

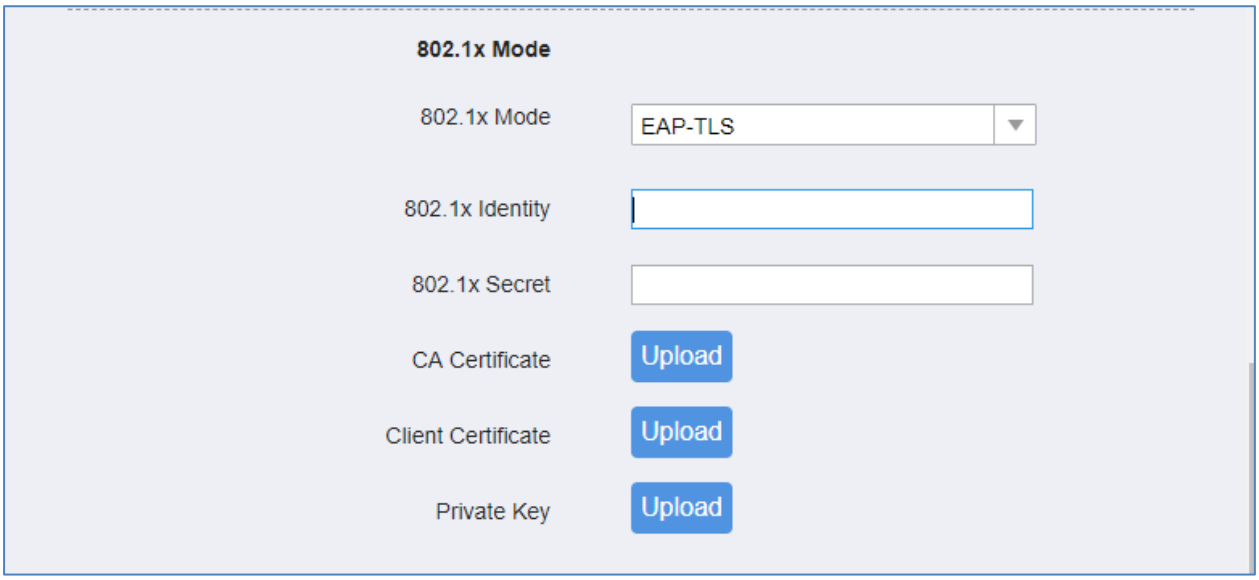

Figure 14: 802.1X Settings

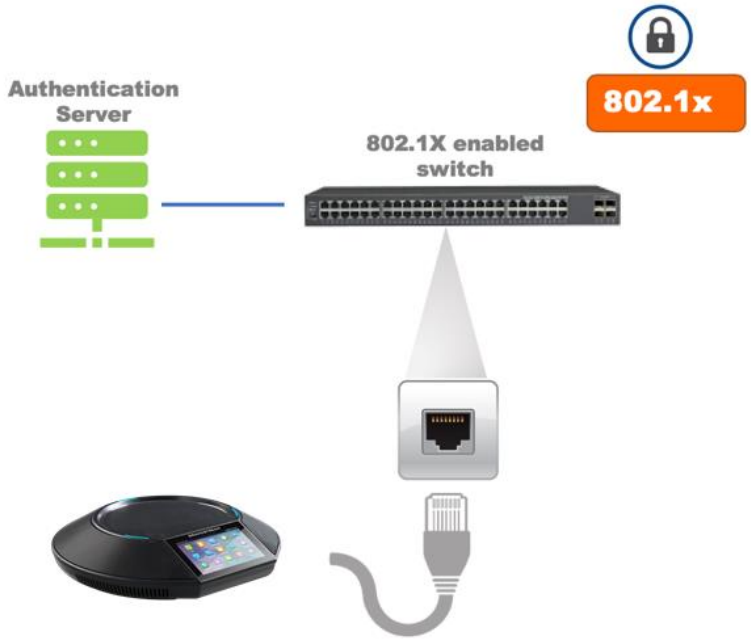

Figure 15: 802.1X for GAC2500 Deployment

Bluetooth

GAC2500 supports Bluetooth for Bluetooth headset connection, file transferring and handsfree mode for cell phones. By default, Bluetooth is disabled and it can be enabled from LCD. If there is no Bluetooth device used with GAC2500, it's recommended to turn off Bluetooth so it's not discoverable by nearly Bluetooth devices.

SECURITY FOR GAC2500 SERVICES

Provisioning via Configuration File

GAC2500 supports downloading configuration file via HTTP/HTTPS/TFTP. Below figure shows the options for config file provisioning.

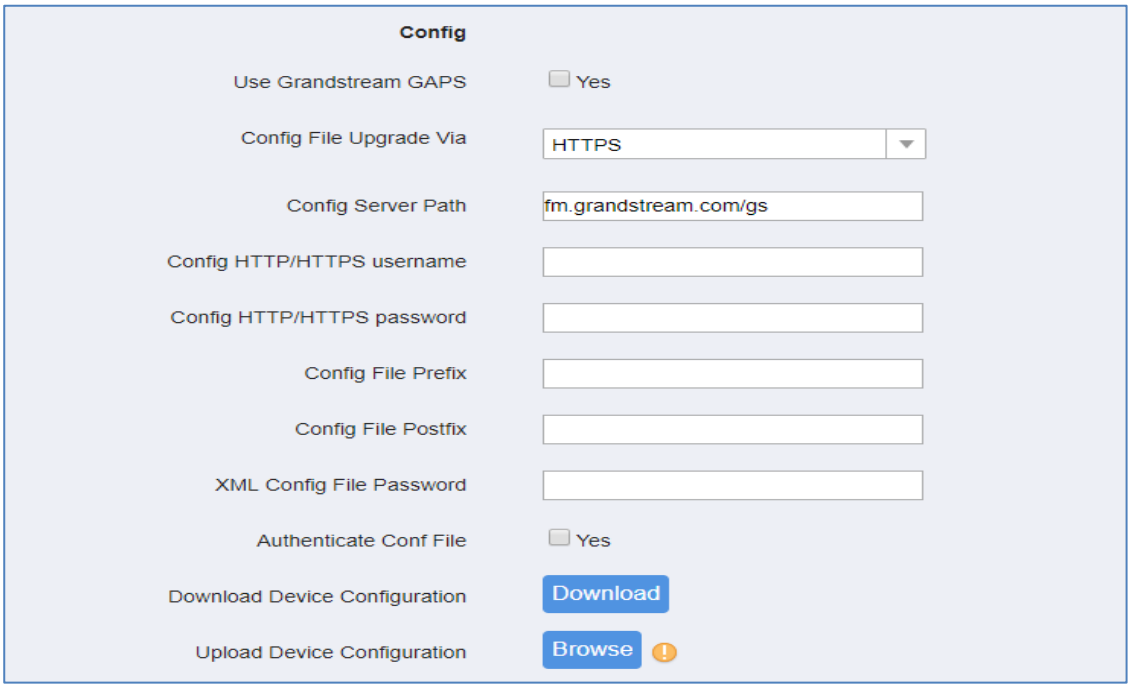

Figure 16: GAC2500 Config File Provisioning

We recommend users to consider the following options for added security when deploying the GAC2500 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 GAC2500 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 GAC2500 to authenticate configuration file before applying it. When set to "Yes", the configuration file must include P value P1 with GAC2500's administration password. If it is missed or does not match the password, the GAC2500 will not apply the config file.

- **XML Config File Password:**
  The GAC2500 XML config file can be encrypted using OpenSSL. When it's encrypted, the GAC2500 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 GAC2500. 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.

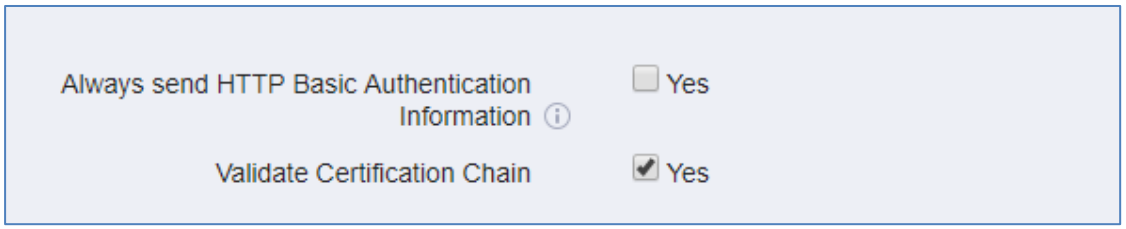

Figure 17: Validate Certification Chain

GAC2500 supports uploading CA certificate to validate the server certificate and this setting is under GAC2500 web UI → System Settings → Security Settings.

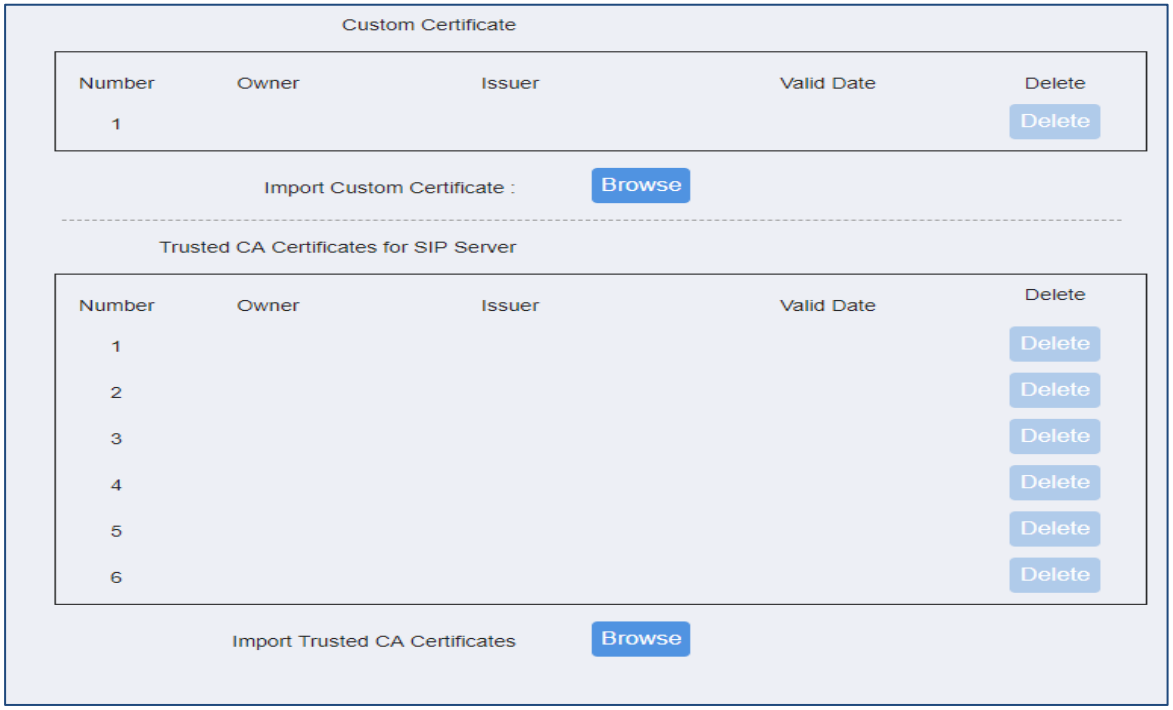

Figure 18: Certificate Management

Firmware Upgrading

Similar to configuration file provisioning, GAC2500 supports downloading firmware file via HTTP/HTTPS/TFTP. The firmware file is encrypted and GAC2500 ensures only authentic, signed and untampered firmware file can run. Here are the recommended settings for firmware downloading.

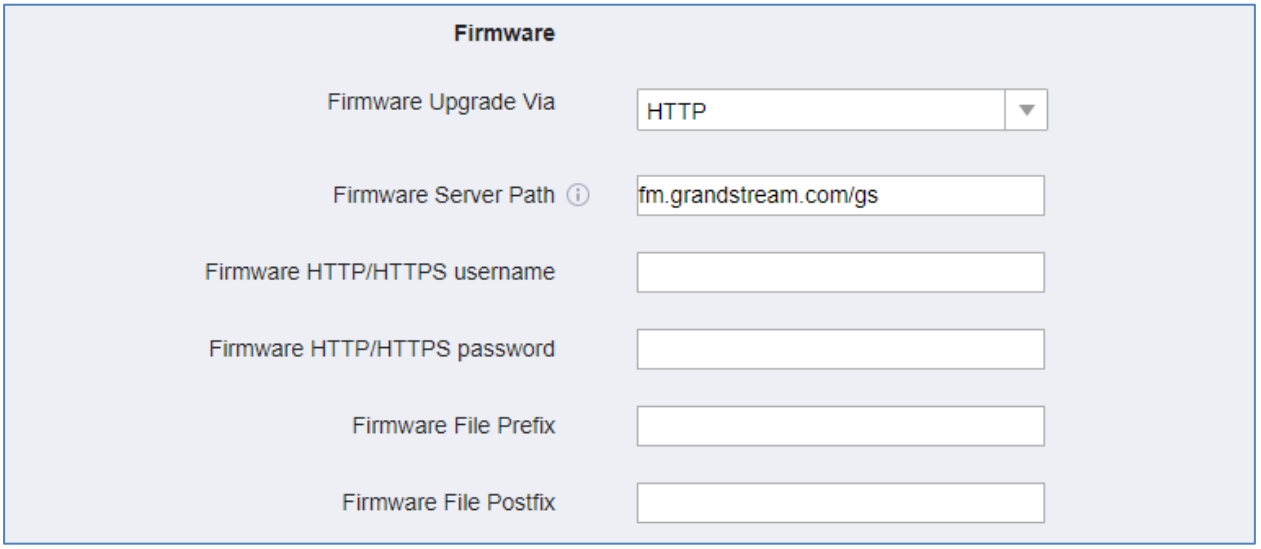

Figure 19: GAC2500 Firmware Upgrade Configuration

- **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 GAC2500 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 phone will download the firmware/config file only from the legitimate server.

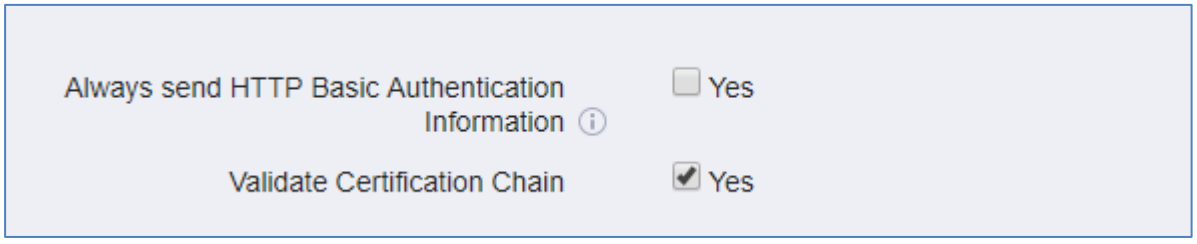

Figure 20: Validate Certification Chain

GAC2500 supports uploading CA certificate to validate the server certificate and this setting is under GAC2500 web UI→System Settings→Security Settings.

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.

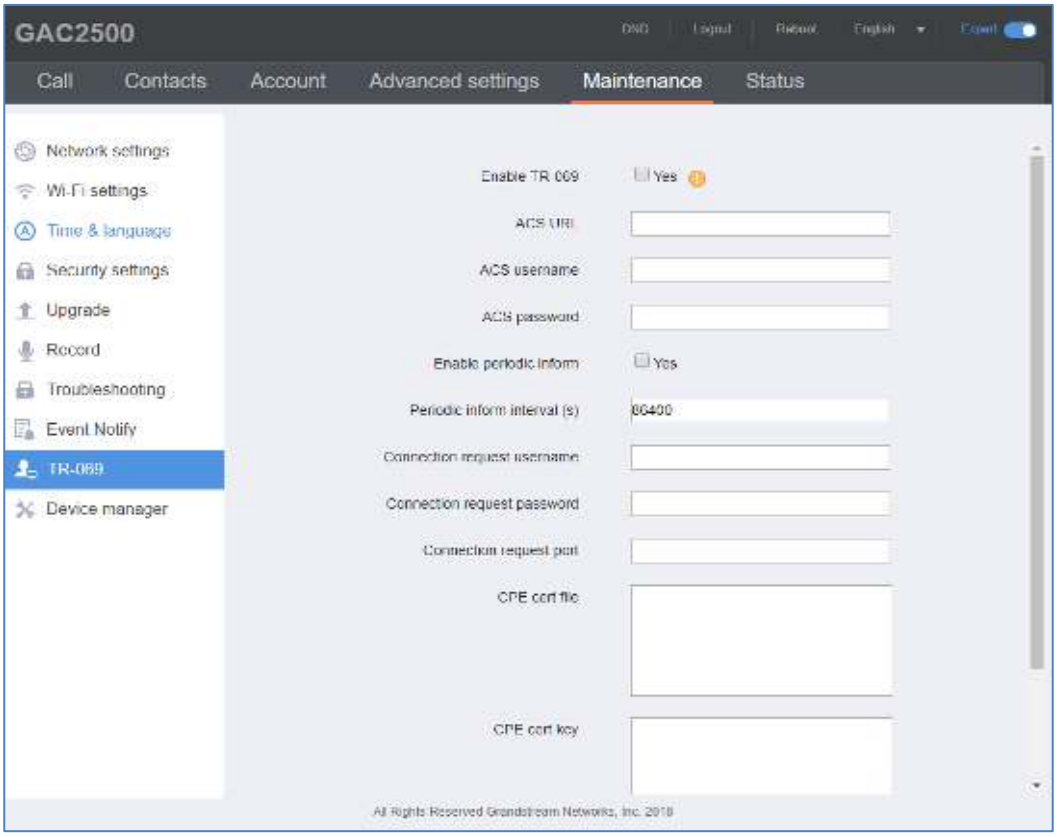

Figure 21: TR-069 Connection Settings Page

FTP Server

FTP server is disabled by default on GAC2500. It can be enabled from LCD menu→ app. FTP service on GAC2500 uses port 2121. After the user enables FTP server on GAC2500 and connects to it, users can browse the GAC2500 files such as screenshots from a remote PC. It is recommended to disable the FTP server during normal usage, and only turn it on for specific purpose. After the file is retrieved, please disable the FTP server.

Figure 22: FTP Service On

ADB Service

Android Debug Bridge (ADB) is a versatile command-line tool that allows users to communicate with GAC2500 for installing apps, debugging apps and running specific commands. To enable ADB connection, users must turn on developer mode under LCD system security menu first and accept the RSA key from remote device to allow access. The port number used for ADB connection is 5555. It is not recommended to enable developer mode if ADB connection is not needed.

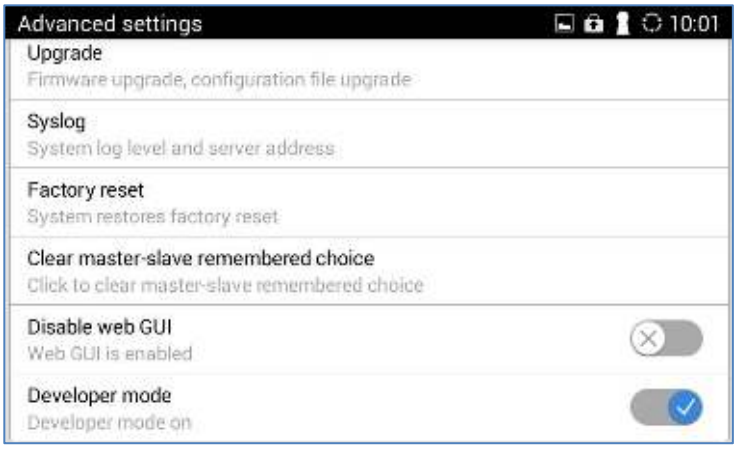

Figure 23: Developer Mode Enabled

LDAP

GAC2500 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.

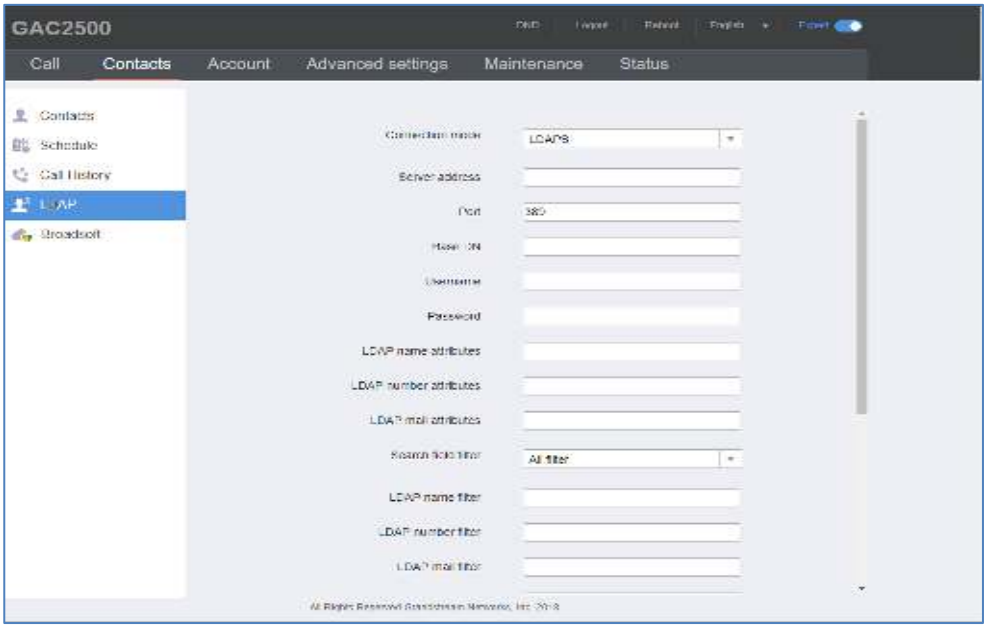

Figure 24: GAC2500 LDAP Settings

Syslog

GAC2500 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.

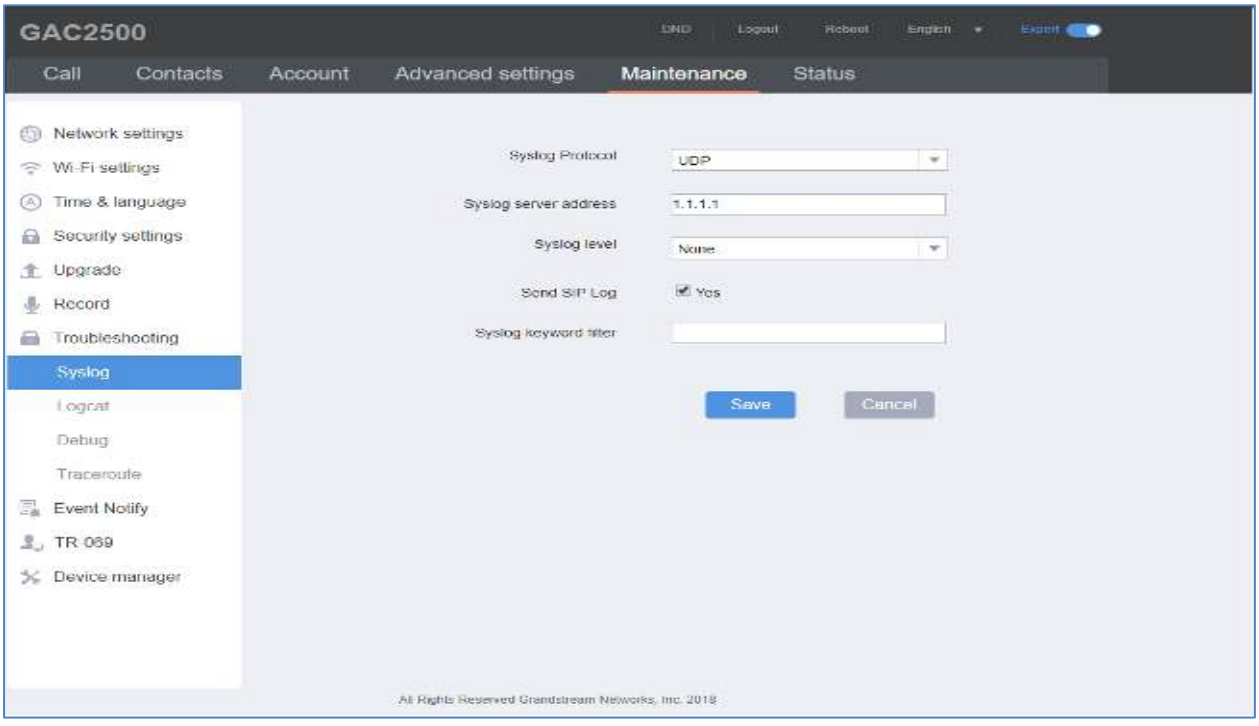

Figure 25: Syslog Protocol

SECURITY GUIDELINES FOR GAC2500 DEPLOYMENT

Often times the GAC2500s are deployed behind NAT. The network administrator can consider following security guidelines for the GAC2500 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 GAC2500, 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 GAC2500 if the network administrator needs to create firewall rules.
    - Starting from 5060 for account 1, the port numbers increase by 2 for account x. For example, 5062 is the default local SIP port for account 2, 5064 for account 3, etc. The local SIP port can be configured under Account→SIP Settings for each SIP account.
    - The Local RTP port can be configured from web UI → Advanced Settings → General Settings. This parameter defines the local RTP-RTCP port pair used to listen and transmit. If it is configured with X, in channel 0 the port X will be used for audio RTP message, the port X+1 for audio RTCP message, the port X+2 for video RTP message and the port X+3 for video RTCP. In Channel 1, each port number will be incremented by 4 for each message. This increment rule will apply to other channels and other port numbers. By default, the Account 1 will use Channel 0, Account 2 Channel 1, Account 3 Channel 2, Account 4 Channel 3, and Account 5 Channel 4 and Account 6 Channel 5. Default setting is 5004.The valid range is from 1024 to 65400

  Note: On the customer's firewall, it's recommended to ensure SIP port is opened for the SIP accounts on the GAC2500. It's not necessary to use the default port 5060/5062/… on the firewall. Instead, the network administrator can consider mapping a different port on the firewall for GAC2500 SIP port 5060 for security purpose.

- **Use HTTPS for web UI access**
  GAC2500 Web UI access should be equipped with strong administrator password in additional to using HTTPS. Also, do not expose the GAC2500 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 GAC2500 will validate server certificate when downloading the firmware or config file.