Grandstream Networks, Inc.

GRP26XX Series

Security Manual

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 our GRP series of IP Phones.

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. Three-level user management is configurable. SSH access is supported for mainly troubleshooting purpose and it is recommended to disable it in normal usage.

- **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.

- **Security for GRP Services**
  GRP supports service such as HTTP/HTTPS/TFTP/FTP/FTPS and TR-069 for provisioning. For better security, we recommend using HTTPS/FTPS with username/password and using password-protected XML file. We recommend disabling TR-069 (disabled by default) if not used to avoid potential port exposure.

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

This document is subject to change without notice.

WEB UI/SSH ACCESS

Web UI Access

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

Web UI Access Protocols

HTTP and HTTPS are supported to access the GRP's web UI and can be configured under **web UI → Maintenance → Security settings → Security**.

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.

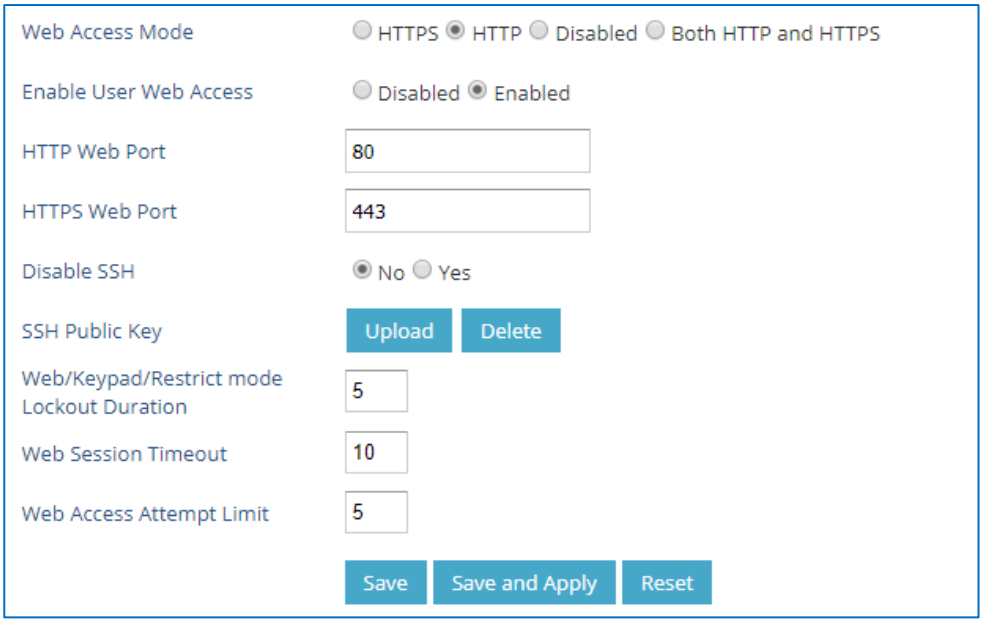

Figure 1 : Web UI Access Settings

3. The GRP allow 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 the device 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.

Admin Login

Username and password are required to log in the GRP's web UI.

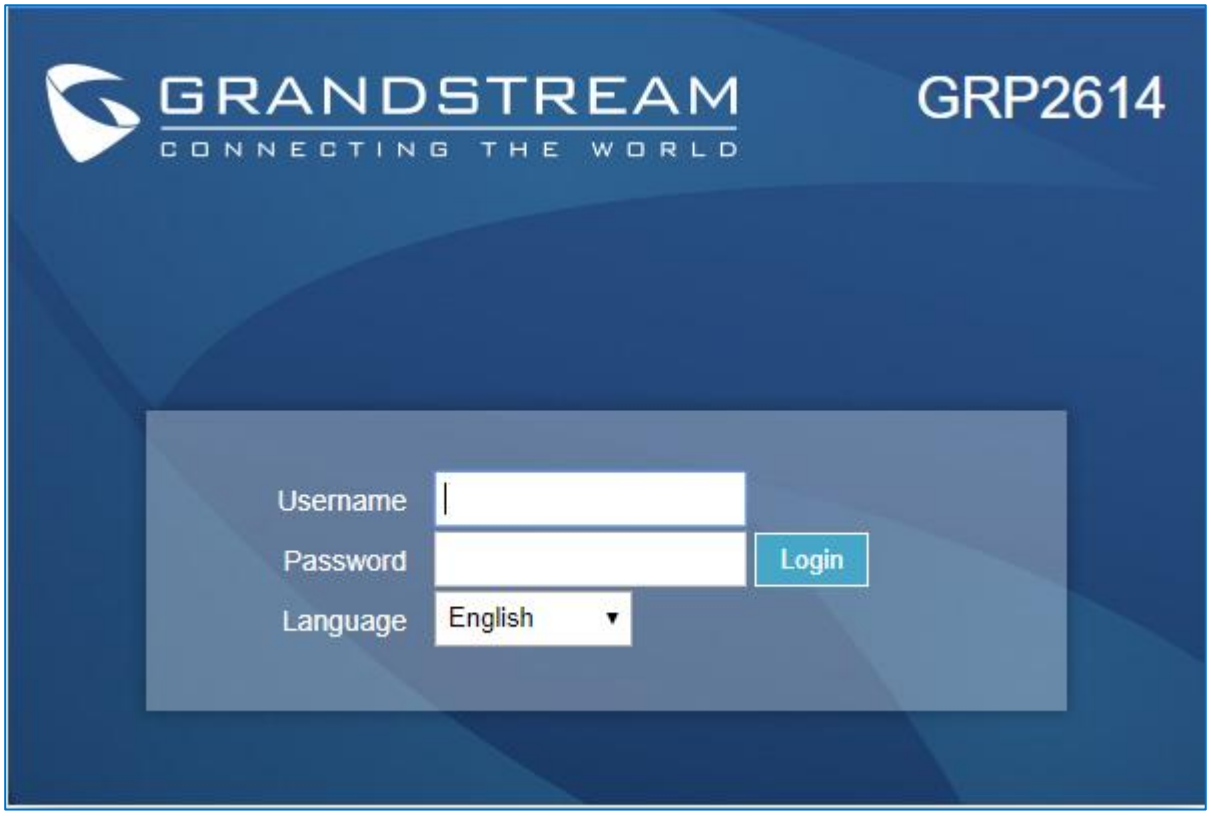

Figure 2 : Web UI Login

The factory default username for administrator level is "admin" and the default password is a random password available on the sticker at the back of the unit. Changing the default password at first time login is highly recommended.

When accessing the GRP phones for the first time or after factory reset, users will be asked to change the default administrator password before accessing GRP Web interface.

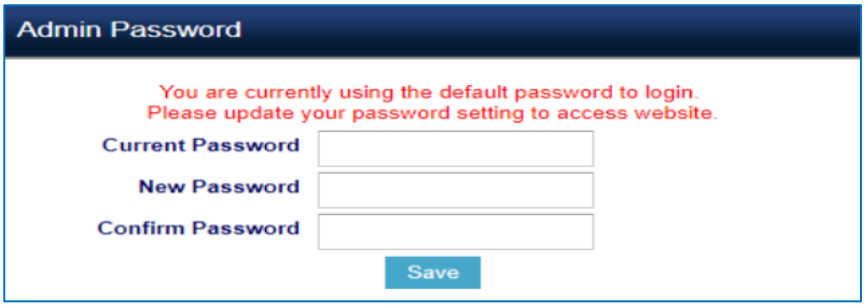

Figure 3 : Change Password on First Boot

To change the password for default user "admin", navigate to **Web GUI → Maintenance →Web Access**

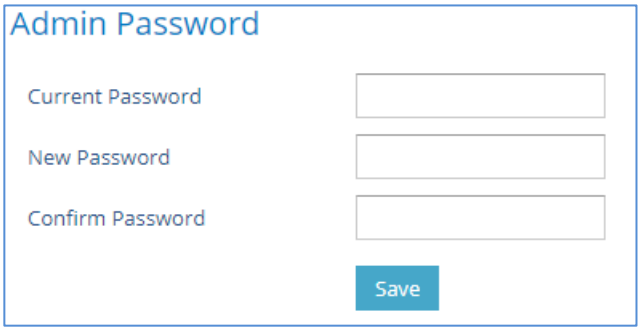

Figure 4: Change Admin Level Password

The password length must be between 6 and 25 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**

User Level	Username	Password	Web Pages Allowed
User Level	user	123	Only Status and Basic Settings
Administrator Level	admin	Random password available on the sticker at the back of the unit.	All pages

NOTES:

- It is recommended to keep admin login for administrator only. And user should be provided with user level login only, if web UI access is needed.
- Change User Level Password upon the first login by following the below steps:
  1. Access your GRP web UI by entering its IP address in your favorite browser.
  2. Enter your admin password.
  3. Go to **Basic Settings** → **New User Password** and Enter the new password.
  4. Confirm the new password.
  5. Press “Save” at the bottom of the page to save your new settings.

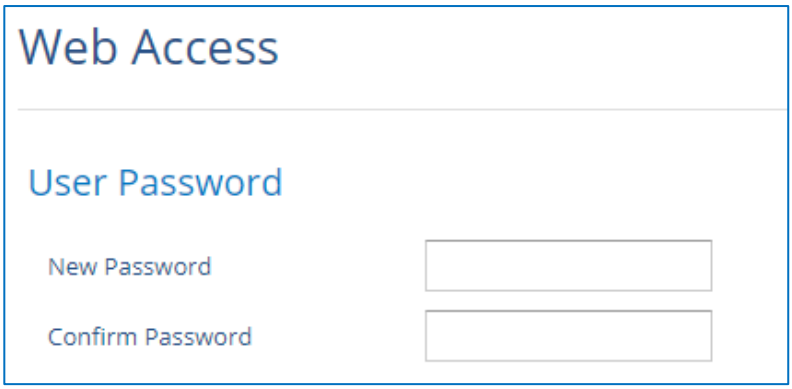

Figure 5 : Change User Level password

SECURITY FOR SIP ACCOUNTS AND CALLS

Protocols and Ports

By default, after a factory reset, all the accounts are active. Knowing the default local SIP port (Account1: 5060; Account2 : 5062 …) users can make direct IP call even if the accounts are not registered to any PBX. Therefore, it is recommended to disable the unused ports. Under **Web GUI → Accounts → Account X → General Settings → Account Active: "No"**

- Users can also disable Direct IP calls on all ports under **Settings → Call Features:** Set "**Disable Direct IP Call:"** to "Yes"

- **SIP transport protocol:**
  The GRP 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 Account under **web UI → Accounts → Account X → SIP Settings → Basic 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".

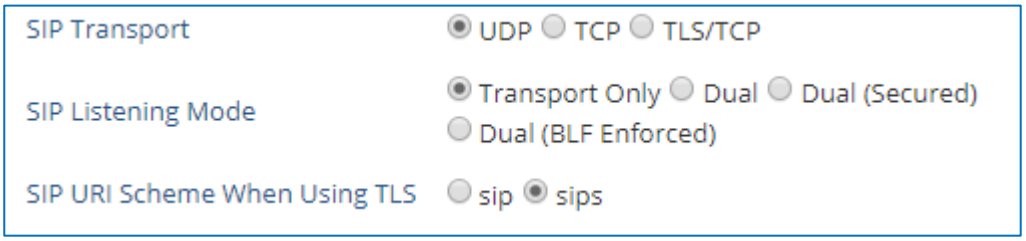

Figure 6 : Configure TLS as SIP Transport

SIP TLS certificate, private key and password can be configured under **Maintenance → Security Settings → Security** page:

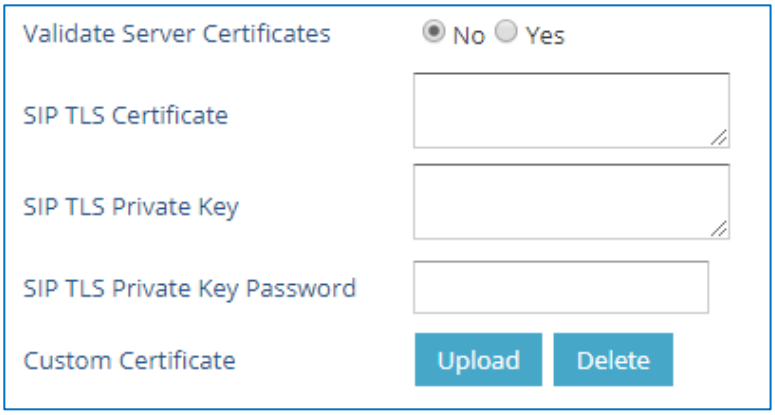

Figure 7 : SIP TLS Settings

When SIP TLS is used, the GRP also offer additional configurations:

- **Validate Server Certificates**:

This feature allows users to validate server certificates with our trusted list of TLS connections

- **Trusted CA Certificates**: Uses the certificate for Authentication

Figure 8 : Additional SIP TLS Settings

- **Local SIP port when using UDP/TCP:**
  Starting from 5060 for Account 1, the port numbers increase by 2 for each account. For example, 5062 is the default local SIP port for Account 2.

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

Anonymous/Unsolicited Calls Protection

If the user would like to have anonymous calls blocked, please go to GRP's **Web GUI → Account X → Call Settings** and set "**Anonymous Call Rejection** "to "**Yes**" : The GRP will then reject all incoming calls with anonymous caller ID by sending a "486 Busy here" message.

Figure 9 : Anonymous Call Rejection

- **Additional SIP security settings:**

under **Web GUI → Account X → SIP Settings → Security Settings**:

- **Accept Incoming SIP from Proxy Only**:

Set "**Yes**" to force the GRP to Check SIP address of the Request URI in the incoming SIP message; if it doesn't match the SIP server address of the account, the call will be rejected.

Additionally, the GRP has built-in mechanism that detects and stops the spam SIP calls from ringing the phones. Please see below the settings.

- **Validate Incoming SIP Messages:**

Set "**Yes**" to Validate incoming messages by checking caller ID and CSeq headers. If the message does not include the headers, it will be rejected.

- **Check SIP User ID for Incoming INVITE:**

Set "**Yes**" to enable checking the SIP User ID in the Request URI of incoming INVITE; if it doesn't match the GRP SIP User ID, the call will be rejected. Direct IP calling will also be disabled if checked.

- **Authenticate Incoming INVITE:**

Set "**Yes**" to Challenge the incoming INVITE for authentication with "SIP/401 Unauthorized" message

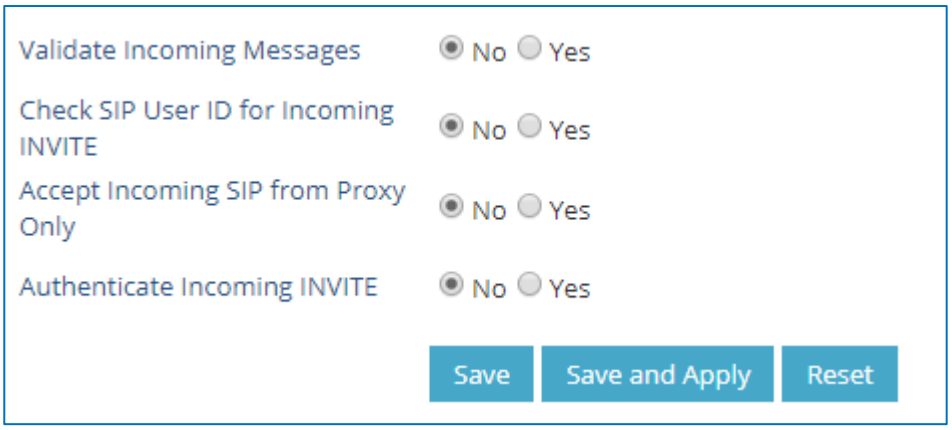

Figure 10 : Settings to Block Anonymous Call

SRTP

To protect voice communication from eavesdropping, the GRP support SRTP for media traffic using AES 128&256. It is recommended to use SRTP if it's supported by the SIP server (Or the service provider). SRTP can be configured under **Web GUI → Account X → Audio Settings.**

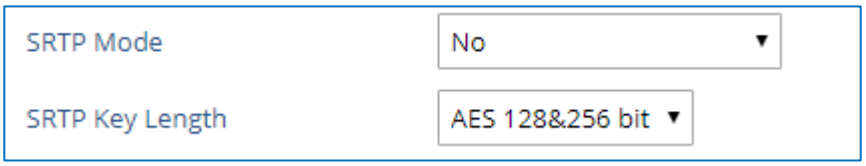

Figure 11 : SRTP Settings

Selects SRTP mode to choose ("No", "Enabled but not forced", "Enabled and forced", or "Optional"). Default is No. It uses SDP Security Description to exchange key.

SNMP

SNMP protocol is used for Network management. We recommend disabling it if it is not in use. Users can do that from the GRP's Web GUI, under **Network → SNMP Settings** page:

- Set "**Enable SNMP**:" to "No"

Figure 12 : SNMP Setting

SECURITY FOR GRP SERVICES

Firmware Upgrade and Provisioning

The GRP IP Phones support downloading configuration file via TFTP, HTTP/HTTPS, FTP/FTPS. Below figure shows the related options under **Web GUI → Maintenance → Upgrade and Provisioning**

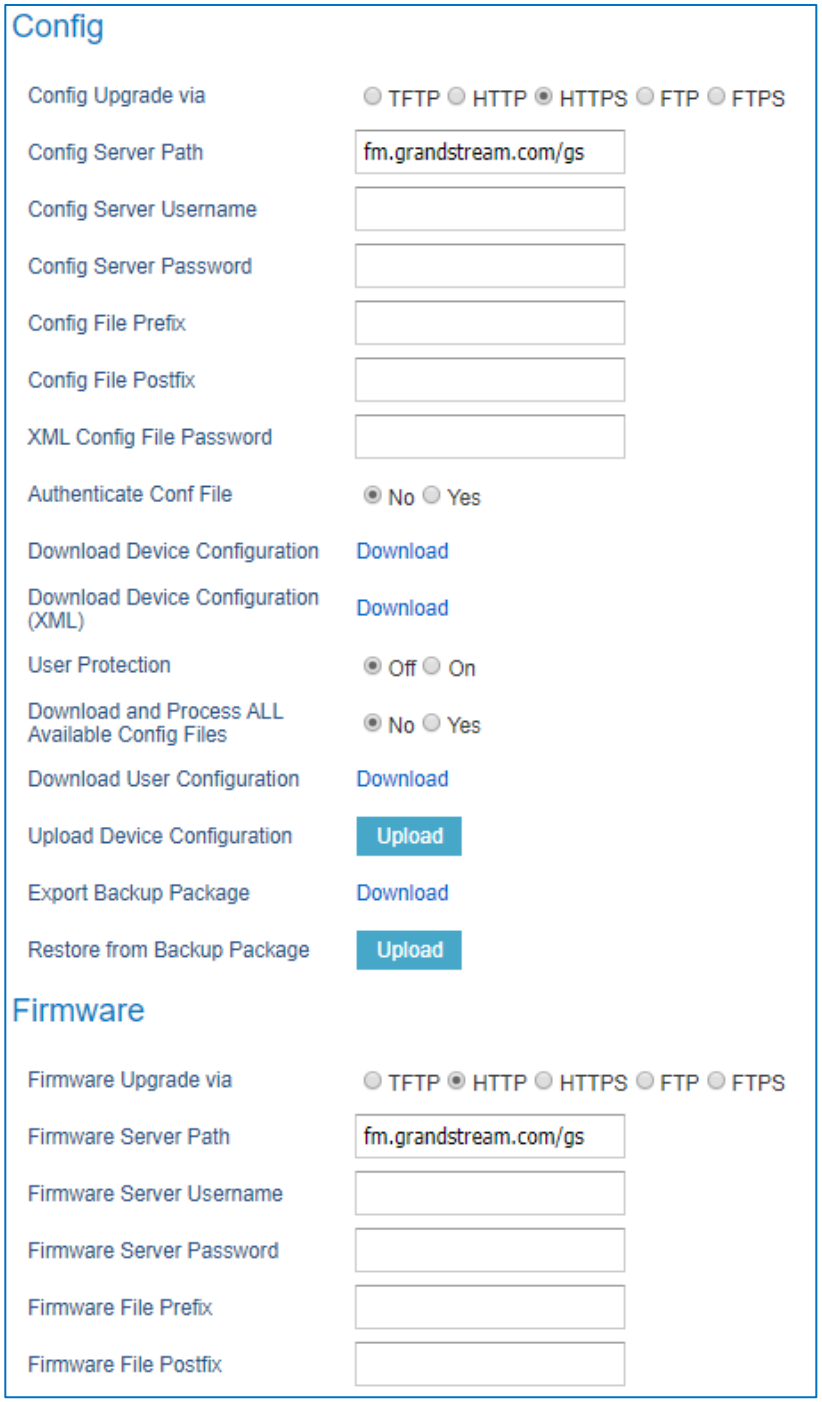

Figure 13 : Upgrade and Provisioning

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

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

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

- **Authenticate Config file:**
  This sets the GRP to authenticate the configuration file before applying it. When set to "Yes", the configuration file must include P value P1 with GRP system's administration password. If it is missed or does not match the password, the GRP will not apply the config file.

- **XML Config File Password:**
  The GRP XML config file can be encrypted using OpenSSL. When it's encrypted, the GRP must supply the correct password in this field so it can decrypt XML configuration file after downloading it. Then the configuration can be applied. 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 Server Certificates: (**under **Maintenance → Security settings → Security)**
  This configures whether to validate the server certificate when downloading the firmware/config file. If set to "Yes", the GRP will download the firmware/config file only from the legitimate server.

TR-069

TR-069 is disabled by default, it's recommended to disable it if not used.

When TR-069 is enabled under **Maintenance → TR-069,** and the service is to be used, users can set up the following:

- **ACS URL**: Specifies URL of TR-069 Auto Configuration Servers.
- **ACS Username/Password**: Enters username/Password to authenticate to ACS.
- **Periodic Inform Enable**: Sends periodic inform packets to ACS.
- **Periodic Inform Interval**: Sets frequency that the inform packets will be sent out to ACS.
- **Connection Request Username/Password**: Enters username/Password for ACS to connect to the GRP.

- **CPE SSL Certificate**: Configures the Cert File for the ATA to connect to the ACS via SSL.
- **CPE SSL Private Key**: Specifies the Cert Key for the ATA to connect to the ACS via SSL

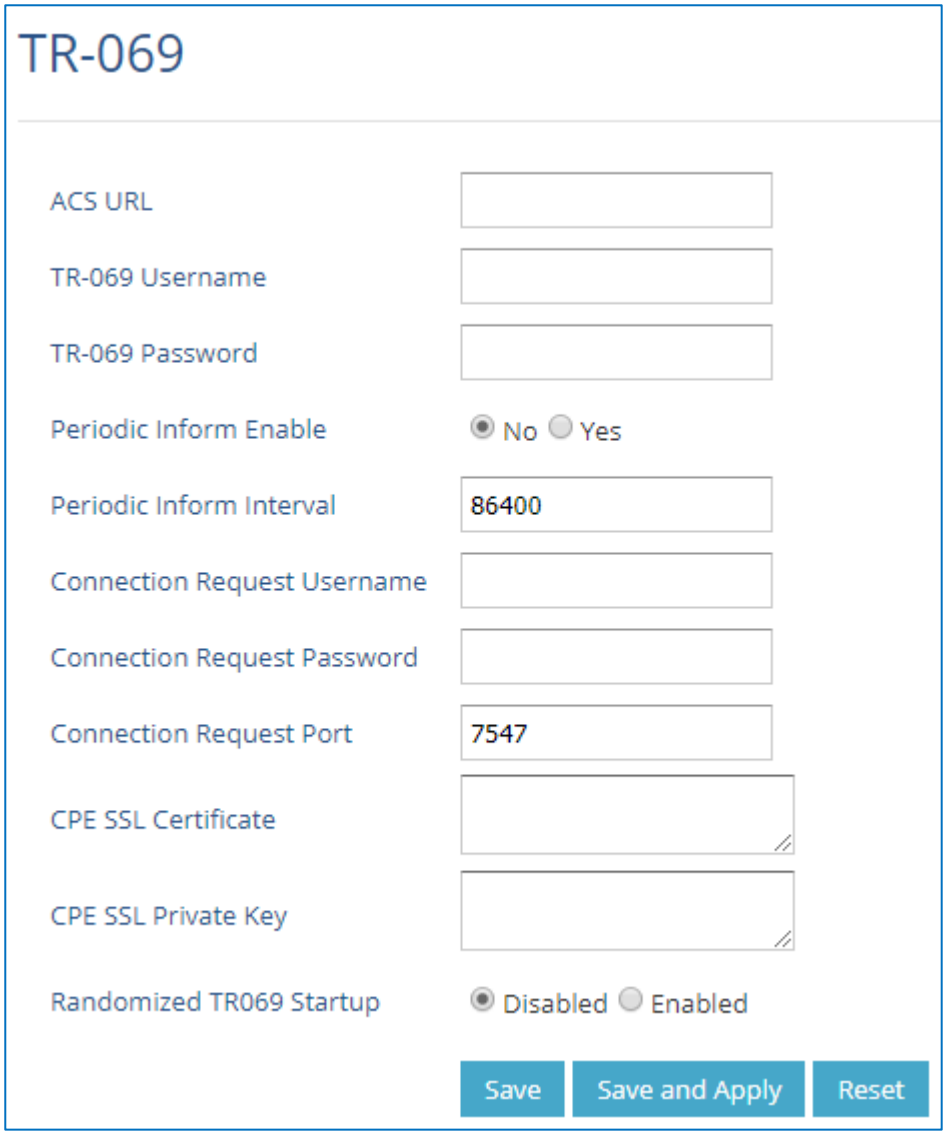

Figure 14 : TR-069 Connection Settings

Syslog

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

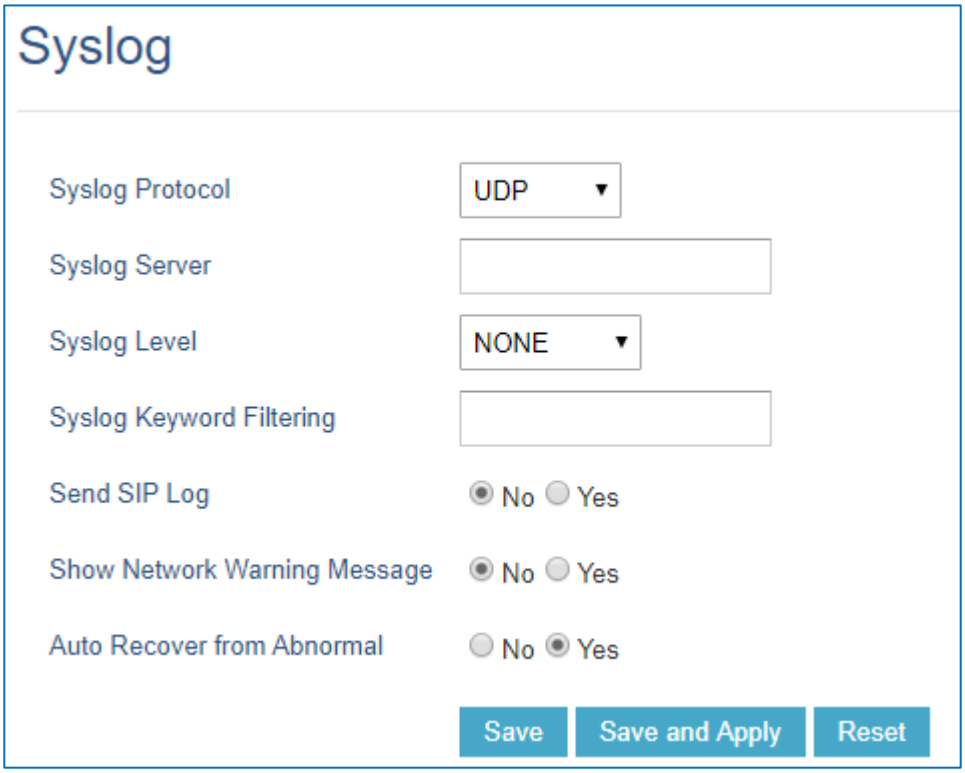

Figure 15 : Syslog Protocol

SECURITY GUIDELINES FOR GRP DEPLOYMENT

Often the GRP are deployed behind NAT. The network administrator can consider following security guidelines for the GRP 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 GRP, 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 the SIP ports and RTPs port used on the GRP if the network administrator needs to create firewall rules.

  - Under web UI → **Account x → SIP Settings → Basic Settings,** the feature "Local SIP Port" defines the local SIP port used to listen and transmit. The default value when using SIP transport protocol UDP/TCP is 5060 for Account 1, 5062 for Account 2, 5064 for Account 3, 5066 for Account 4… When using TLS as SIP transport protocol the default value is 5061 for Account 1, 5063 for Account 2, 5065 for Account 3, … The valid range is from 1 to 65535.

  - Under web UI → **Settings → General Settings**, the feature "Local RTP Port" defines the local RTP port used to listen and transmit. Local RTP port ranges from 1024 to 65400 and must be even. It is the base RTP port for channel 0. When configured channel 0 will use this port_value for RTP, and port_value+1 for RTCP. Channel 1 will use port_value+2 for RTP and so on, until reaching the limit and then it will be reset to first port_value. The default value is 5004 for RTP and 5005 for RTCP.

  For the GRP26XX phones, it is possible to select a range for the Local RTP port from 48 to 10000. Default setting is 200.

  Note: On the customer's firewall, it's recommended to ensure SIP port is opened for the SIP accounts on the GRP. 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 GRP SIP port 5060 for security purpose.

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