Grandstream Networks, Inc.

HT8XX

Analog Telephone Adaptors

Security Guide

Table of Contents

OVERVIEW 3

WEB UI/SSH ACCESS 4

Web UI Access 4

Web UI Access Protocols 4

User Login 5

User Management Levels 5

SECURITY FOR SIP ACCOUNTS AND CALLS 7

Protocols and Ports 7

Anonymous/Unsolicited Calls Protection 9

SRTP 10

SNMP / RADIUS 10

SECURITY FOR HT8XX SERVICES 11

Firmware Upgrade and Provisioning 11

TR-069 12

Syslog 13

SECURITY GUIDELINES FOR HT8XX DEPLOYMENT 14

Table of Figures

Figure 1 : Web UI Access Settings 4
Figure 2 : Web UI Login 5
Figure 3 : Changing Admin Level password 5
Figure 4 : Changing End-User/Viewer Level password 6
Figure 5 : Configure TLS as SIP Transport 7
Figure 6 : SIP TLS Settings 8
Figure 7 : Additional SIP TLS Settings 8
Figure 8 : Anonymous Call Rejection 9
Figure 9 : Settings to Block Anonymous Call 9
Figure 10 : Settings to Block Unwanted Calls 9
Figure 11 : SRTP Settings 10
Figure 12 : Firmware upgrade and Provisioning 11
Figure 13 : TR-069 Connection Settings 13
Figure 14 : Syslog Protocol 13

OVERVIEW

This document presents a summary of security measures, factors, and configurations that users are recommended to consider when configuring and deploying our HT8XX series of Analog Telephone Adapters.

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 HT8XX Services**
  HT8XX 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 HT8XX**
  This section introduces protocols and ports used on the HT8XX and recommendations for routers/firewall settings.

WEB UI/SSH ACCESS

Web UI Access

The HT8XX 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 HT8XX information and settings. It is critical to understand the security risks involved when placing the Analog Telephone Adapters on public networks and it's recommended not to do so.

Web UI Access Protocols

HTTP and HTTPS are supported to access the HT8XX's web UI and can be configured under **web UI →BASIC 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.
3. Block or restrict WAN Side access (when set to "Yes") by specifying a Blacklist for blocked addresses and a Whitelist for allowed addresses.

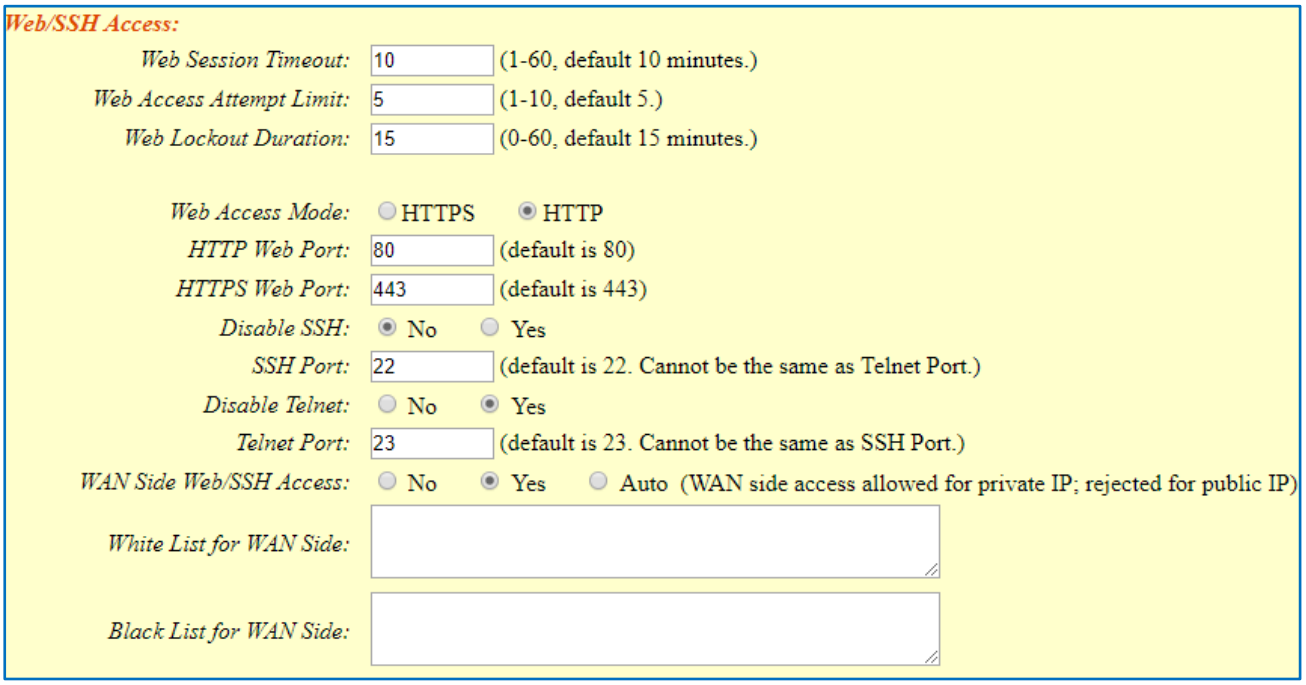

Figure 1 : Web UI Access Settings

4. The HT8XX 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.

User Login

Username and password are required to log in the HT8XX's web UI.

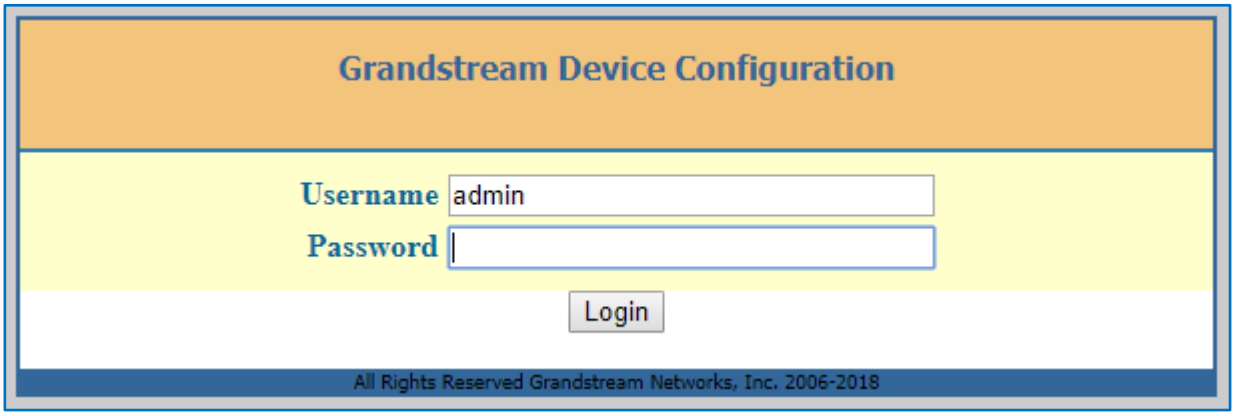

Figure 2 : Web UI Login

The factory default username is "admin" and the default password is "admin". Changing the default password at first time login is highly recommended.

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

Figure 3 : Changing Admin Level password

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

Three user privilege levels are currently supported:

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

User Level	Username	Password	Web Pages Allowed
End User Level	user	123	Only Status and Basic Settings
Administrator Level	admin	admin	All pages
Viewer Level	viewer	viewer	View all pages. Changes not allowed.

NOTES:

- It is recommended to keep admin login for administrator only. And end user should be provided with user/viewer level login only, if web UI access is needed.
- Change User/Viewer Level Password upon the first login by following the below steps:

  1. Access your HT8XX web UI by entering its IP address in your favorite browser.
  2. Enter your admin password (default: admin).
  3. Go to **Basic Settings** → **New End User/Viewer Password** and Enter the new password.
  4. Confirm the new password.
  5. Press "Apply" at the bottom of the page to save your new settings.

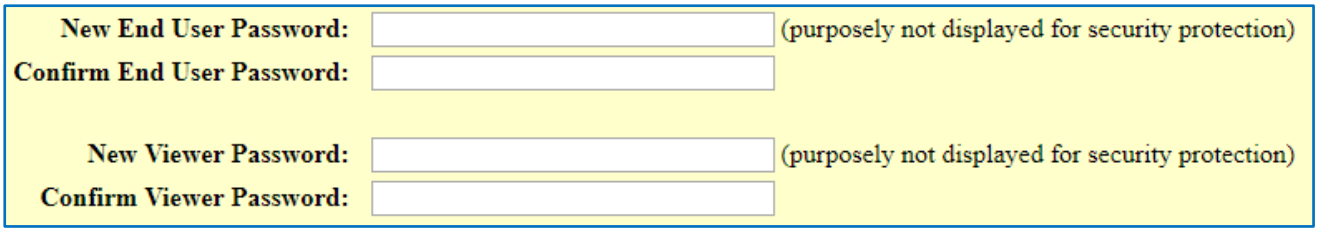

Figure 4 : Changing End-User/Viewer Level password

- For advanced authentication and more security, use "RADIUS Web Access Control" feature to authenticate user for web access. RADIUS server is required for this setup.

SECURITY FOR SIP ACCOUNTS AND CALLS

Protocols and Ports

By default, after factory reset, all accounts are active. Knowing the default local SIP port is (Profile1: 5060 ; Profile2: 6060) users can make direct IP call even if the accounts are not registered to any PBX. Therefore, it is recommended to disable the Ports if they are not is use.

- FXS x → Account Active: "No"
- FXS PORTS → Enable Port: "No"

Users can also disable Direct IP calls on all port under **ADVANCED SETTINGS**: Set "**Disable Direct IP Call:"** to "Yes"

- **SIP transport protocol:**
  The HT8XX 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 FXS PORT under **web UI → FXS x**. Or, per Profile under **web UI → PROFILE x**. 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".

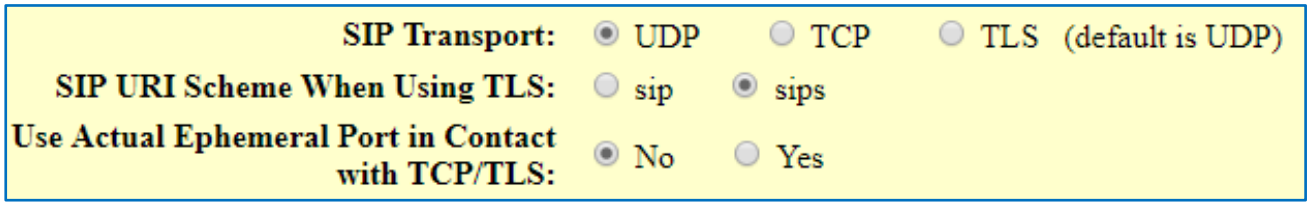

Figure 5 : Configure TLS as SIP Transport

SIP TLS certificate, private key and password can be configured under **ADVANCED SETTINGS** page:

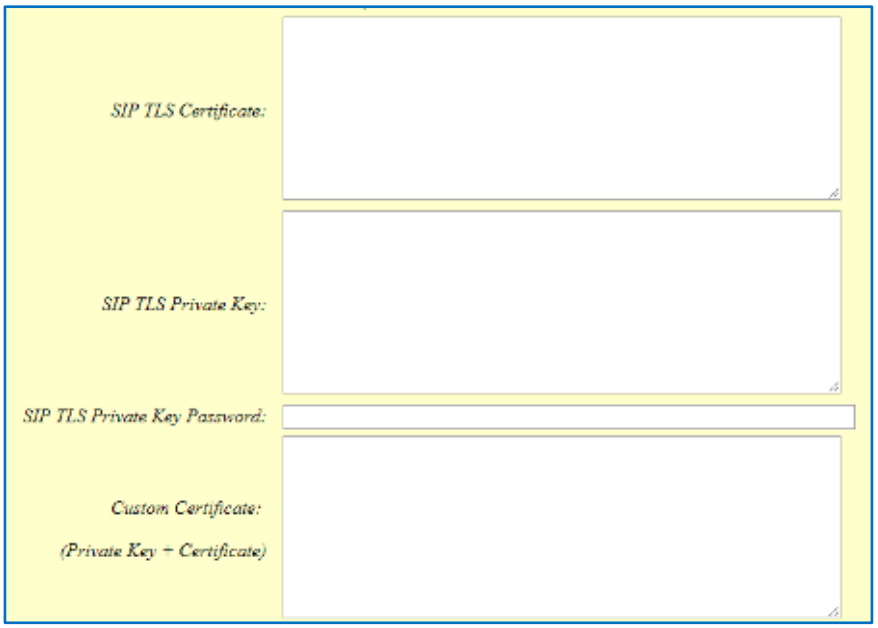

Figure 6 : SIP TLS Settings

When SIP TLS is used, the HT8XX also offer additional configurations

- **Validate Server Certificates**:

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

- **Authenticate server certificate domain/chain**:

Configures whether to validate the domain certificate when download the firmware/config file. If it is set to "Yes", the phone will download the firmware/config file only from the legitimate server.

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

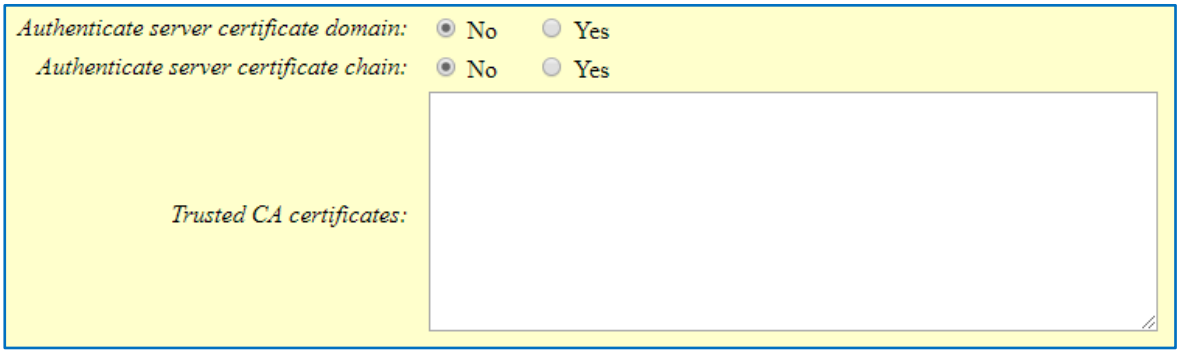

Figure 7 : Additional SIP TLS Settings

- **Local SIP port when using UDP/TCP:**

Starting from 5060 for FXS1, the port numbers increase by 2 for FXS x. For example, 5062 is the default local SIP port for FXS 2.

  - When using Profiles: Profile 1 starting port for the first FXS is 5060 (+2 incrementation for the following FXS x). Profile 2 starting port for the first FXS is 6060 (+2 incrementation for the following FXS x).

- **Local SIP port when using TLS:**
  The SIP TLS port is the UDP SIP port plus 1. For example, if FXS 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 HT8XX's FXS/Profile page and set up the following recommended configuration:

- Set "**Anonymous Call Rejection**" to "**Yes**" will reject incoming calls with anonymous caller ID with "486 Busy here" message.

Figure 8 : Anonymous Call Rejection

- Setting "**Allow Incoming SIP Messages from SIP Proxy Only**" to "**Yes**" will force the HT8XX 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.

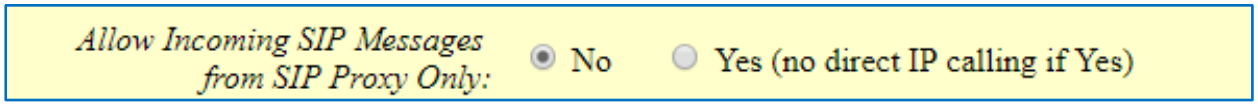

Figure 9 : Settings to Block Anonymous Call

Additionally, the HT8XX has built-in mechanism that detects and stops the spam SIP calls from ringing the phones. Please see below FXS/Profile page.

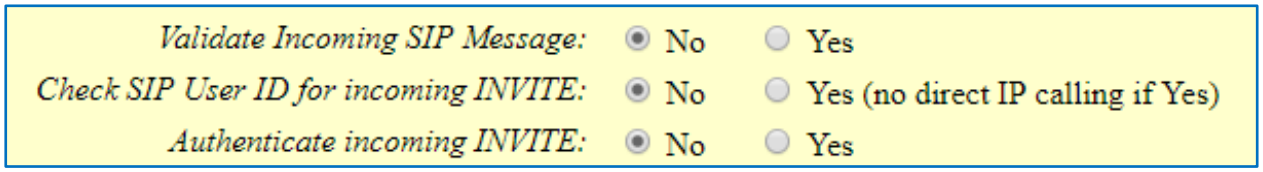

Figure 10 : Settings to Block Unwanted Calls

- **Validate Incoming SIP Message:** Validates 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:** Checks SIP User ID in the Request URI of incoming INVITE; if it doesn't match the HT8XX SIP User ID, the call will be rejected. Direct IP calling will also be disabled if checked.
- **Authenticate Incoming INVITE:** Challenges the incoming INVITE for authentication with "SIP/401 Unauthorized" message

SRTP

To protect voice communication from eavesdropping, the HT8XX support SRTP for media traffic using AES 128&256. It is recommended to use SRTP if server supports it. SRTP can be configured FXS/Profile page.

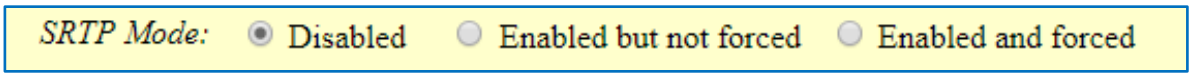

Figure 11 : SRTP Settings

Selects SRTP mode to use ("Disabled", "Enabled but not forced", or "Enabled and forced"). Default is Disabled. It uses SDP Security Description to exchange key.

SNMP / RADIUS

Both SNMP and RADIUS protocols are used for Network management. We recommend disabling them if they are not in use. Users can do that from the HT's Web GUI, under **ADVANCED SETTINGS** page:

- Set "**Enable SNMP**:" to "No"
- Set "**Enable RADIUS Web Access Control:**" to "No"

SECURITY FOR HT8XX SERVICES

Firmware Upgrade and Provisioning

The Analog Telephone Adapters support downloading configuration file via TFTP, HTTP/HTTPS, FTP/FTPS. Below figure shows the options for config file provisioning.

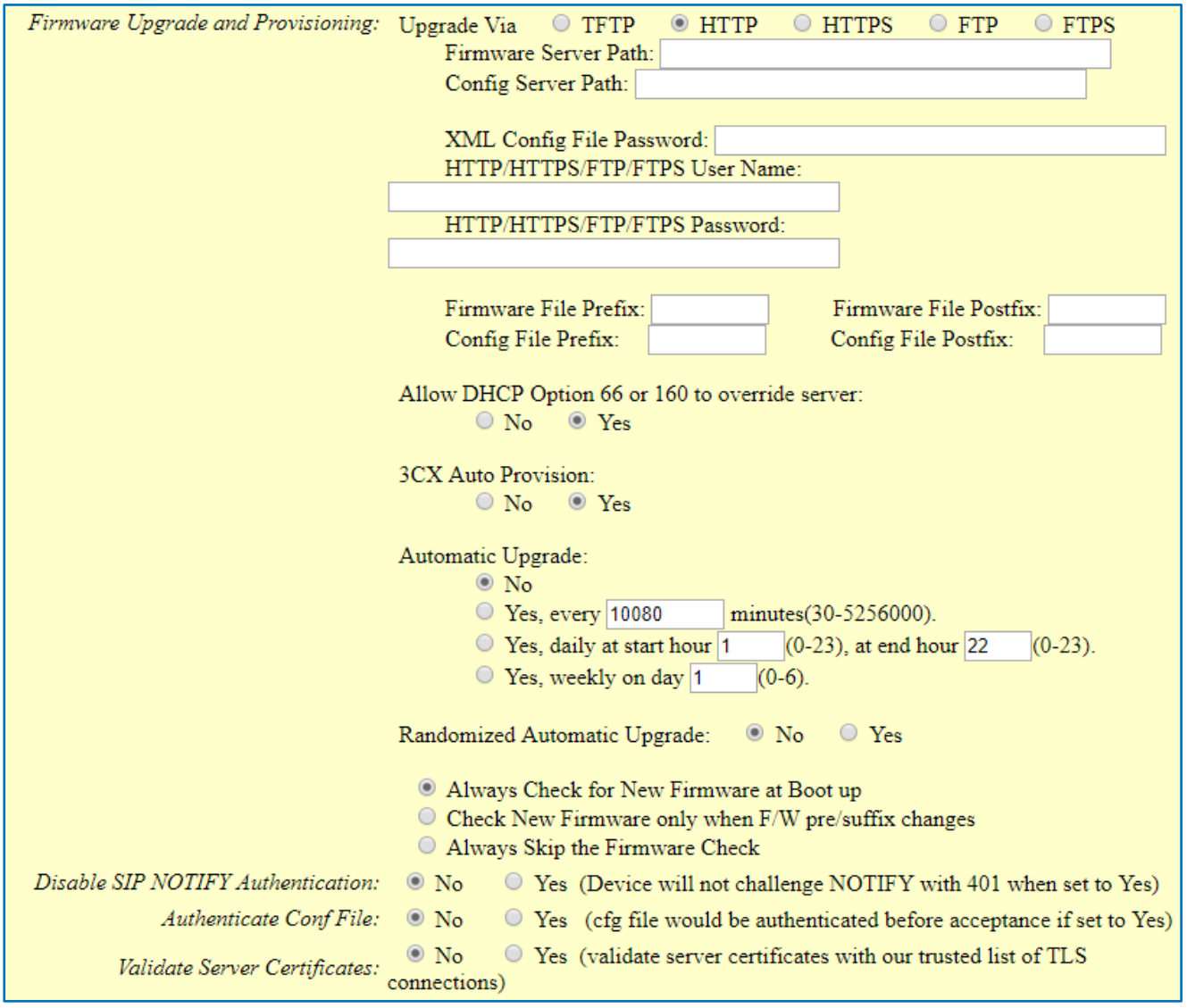

Figure 12 : Firmware upgrade and Provisioning

We recommend users to consider the following options for added security when deploying the HT8XX 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 HT8XX 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 HT8XX to authenticate the configuration file before applying it. When set to “Yes”, the configuration file must include P value P1 with HT8XX administration password. If it is missed or does not match the password, the HT8XX will not apply the config file.

- **XML Config File Password:**
  The HT8XX XML config file can be encrypted using OpenSSL. When it’s encrypted, the HT8XX 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:**
  This configures whether to validate the server certificate when downloading the firmware/config file. If set to "Yes", the HT8XX will download the firmware/config file only from the legitimate server.

TR-069

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

When TR-069 is enabled 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 HT8XX.
- **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

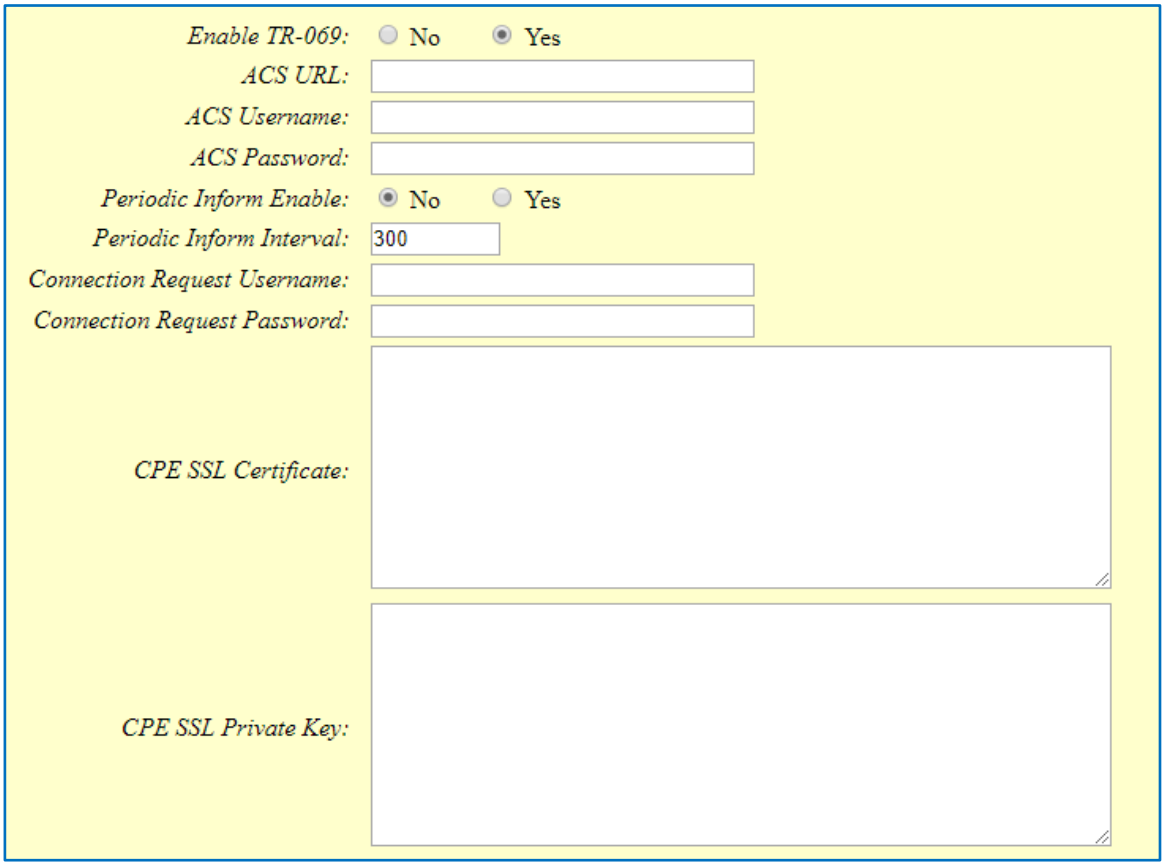

Figure 13 : TR-069 Connection Settings

Syslog

The HT8XX 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.

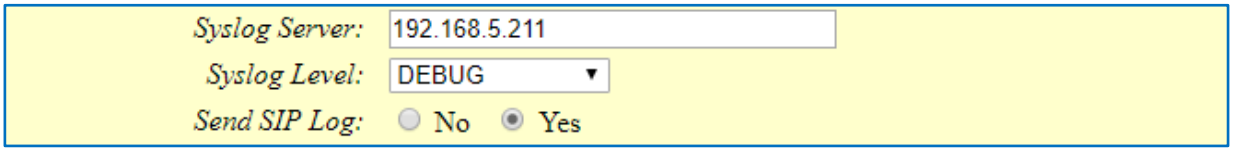

Figure 14 : Syslog Protocol

SECURITY GUIDELINES FOR HT8XX DEPLOYMENT

Often times the HT8XX are deployed behind NAT. The network administrator can consider following security guidelines for the HT8XX 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 HT, 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 table lists all the SIP ports and RTPs port used on the HT8XX if the network administrator needs to create firewall rules.

For **Profile 1**:

SIP FXS x	Default Local SIP Port	Audio RTP/RTCP Port
1	5060 for UDP/TCP 5061 for TLS	RTP: 5004 RTCP: 5005
2	5062 for UDP/TCP 5063 for TLS	RTP: 5008 RTCP: 5009
3	5064 for UDP/TCP 5065 for TLS	RTP: 5012 RTCP: 5013
4	5066 for UDP/TCP 5067 for TLS	RTP: 5016 RTCP: 5017
5	5068 for UDP/TCP 5069 for TLS	RTP: 5020 RTCP: 5021
6	5070 for UDP/TCP 5071 for TLS	RTP: 5024 RTCP: 5025
7	5072 for UDP/TCP 5073 for TLS	RTP: 5028 RTCP: 5029
8	5074 for UDP/TCP 5075 for TLS	RTP: 5032 RTCP: 5033

For **Profile 2**:

SIP FXS x	Default Local SIP Port	Audio RTP/RTCP Port
1	6060 for UDP/TCP 6061 for TLS	RTP: 6004 RTCP: 6005
2	6062 for UDP/TCP 6063 for TLS	RTP: 6008 RTCP: 6009
3	6064 for UDP/TCP 6065 for TLS	RTP: 6012 RTCP: 6013
4	6066 for UDP/TCP 6067 for TLS	RTP: 6016 RTCP: 6017
5	6068 for UDP/TCP 6069 for TLS	RTP: 6020 RTCP: 6021
6	6070 for UDP/TCP 6071 for TLS	RTP: 6024 RTCP: 6025
7	6072 for UDP/TCP 6073 for TLS	RTP: 6028 RTCP: 6029
8	6074 for UDP/TCP 6075 for TLS	RTP: 6032 RTCP: 6033

Note:
On the customer's firewall, it's recommended to ensure SIP port is opened for the SIP accounts on the HT8XX. 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 HT8XX SIP port 5060 for security purpose.

- **Use HTTPS for web UI access**
  HT8XX Web UI access should be equipped with strong administrator password in additional to using HTTPS. Also, do not expose the HT8XX 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 HT8XX will validate server certificate when downloading the firmware or config file.