Grandstream Networks, Inc.

WP820

Enterprise Portable Wi-Fi Phone

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 WP820.

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 WP820 has multiple ways to limit the use for network settings, 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 WP820 supports OpenVPN, 802.1X and Bluetooth. OpenVPN secures remote connection and 802.1X provides network access control. For Bluetooth it's recommended to turn it off if not used.

- **Security for WP820 Services**
  WP820 supports service such as HTTP/HTTPS/TFTP provisioning, TR-069, LDAP. 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 WP820**
  This section introduces protocols and ports used on WP820 and recommendations for routers/firewall settings.

This document is subject to change without notice.

WEB UI/SSH ACCESS

WP820 Web UI Access

The WP820 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 etc. With this, administrators can access and configure all available WP820 information and settings. It is critical to understand the security risks involved when placing the WP820 phone on public networks and it is recommended not to do so.

Web UI Access Protocols

HTTP and HTTPS are supported to access the WP820 web UI and can be configured under **web UI → System 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.

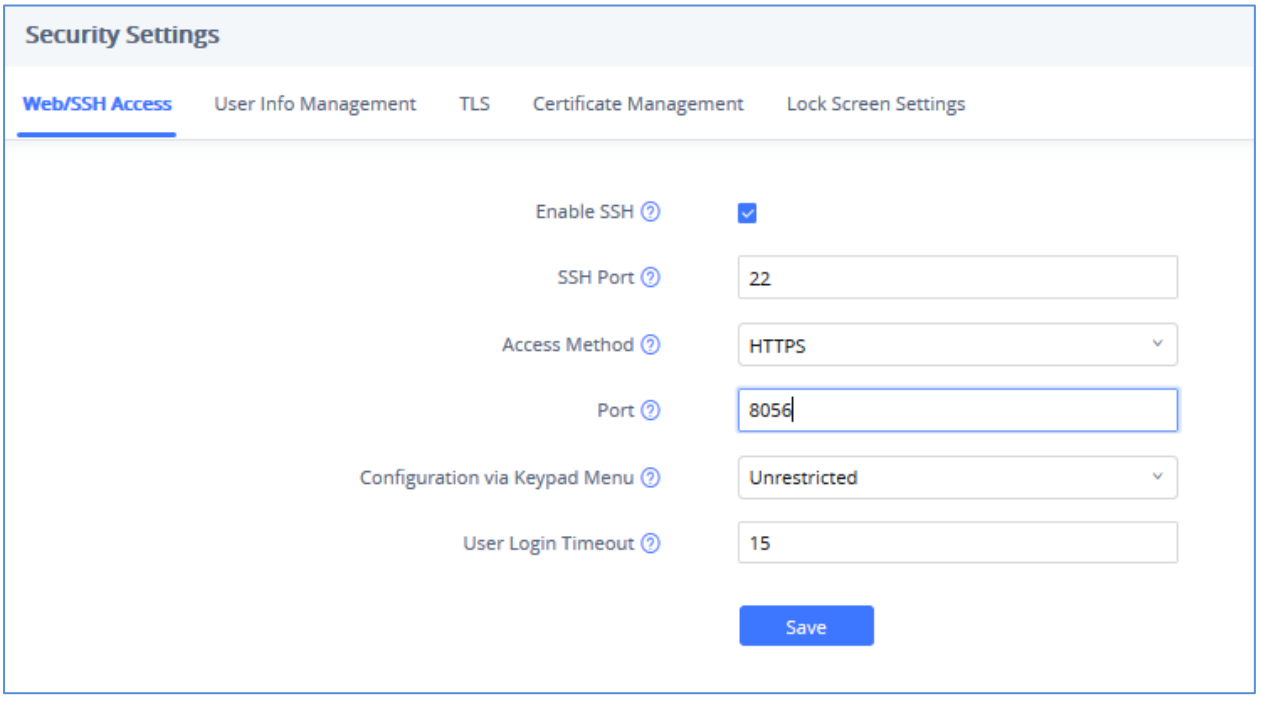

Figure 1: Web UI Access Settings

User Login

Username and password are required to log in the WP820 web UI.

Figure 2: WP820 Web UI Login

The factory default username is “admin” and the default password is “admin”. The WP820 web UI require to change the default password at first time login.

Figure 3: WP820 Admin Password Change

To change the password for default user "admin", navigate to **System Settings → Security Settings → User Info Management**. 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 WP820'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 not allowed to configure the following settings:

- **Account Settings**
- **Phone Settings → General Settings / Ringtone / Video Settings**
- **Network Settings → Advanced Network Settings**
- **System Settings → TR069**
- **Maintenance → Upgrade / Event Notification**
- **Value-added Service**

Even user login can access certain web UI pages, it has less options compared to admin login, such as in **System Settings → Security Settings** page.
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.

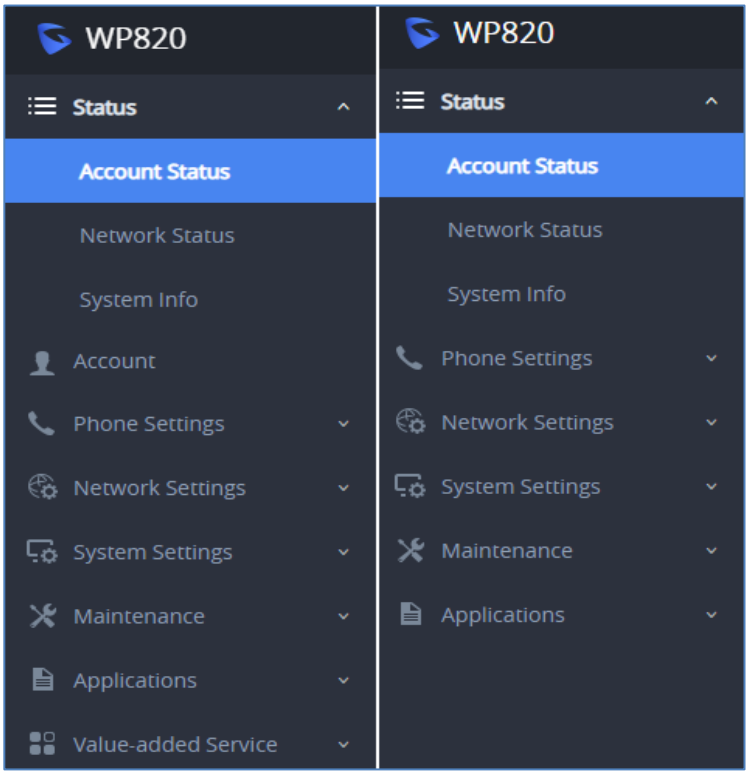

Figure 4: Admin (left) and User (right) Web Access

SSH Access

The WP820 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 WP820 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.

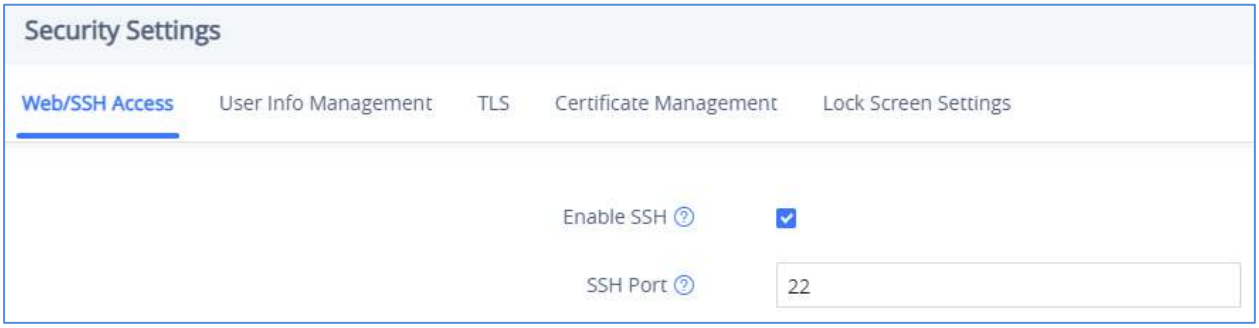

Figure 5: SSH Access on WP820

DEVICE CONTROL SECURITY

From WP820 **web UI → System Settings → Security Settings → Web/SSH Access**, administrator can set whether the user can use specific features or install apps from LCD, shown as below.

Figure 6: Limit Access to Advanced Settings and Apps 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:**
  Account, Advanced Settings, Wireless & Network options will not be displayed in LCD settings menu.
- **Basic Settings & Network Settings:**
  Account and advanced Settings option 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.

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 WP820 SIP accounts. WP820 supports up to 2 SIP accounts.

- **SIP transport protocol:**
-

  The WP820 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".

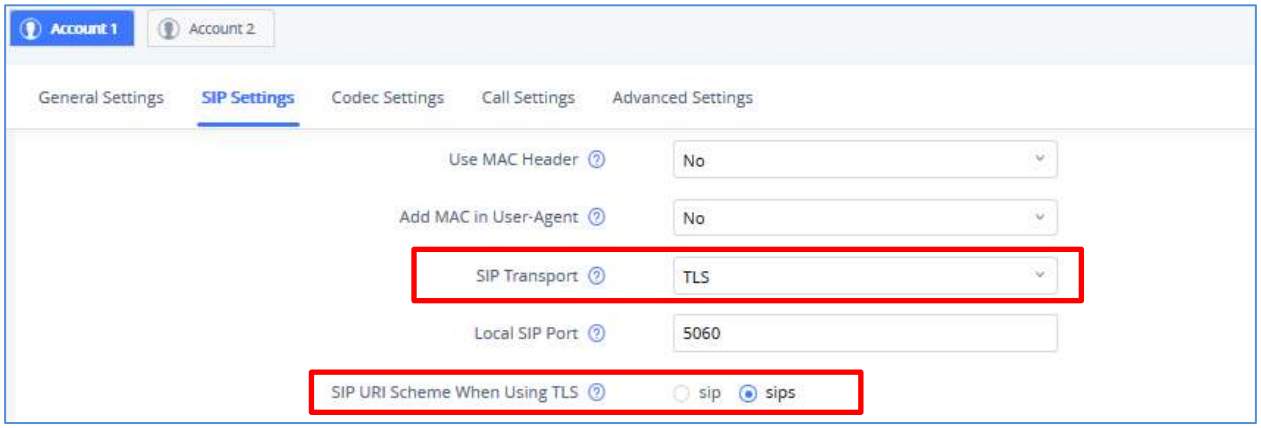

Figure 7: Configure TLS as SIP Transport

SIP TLS certificate, private key and password can be configured under WP820 **web UI→System Settings→Security Settings → TLS →SIP TLS**.

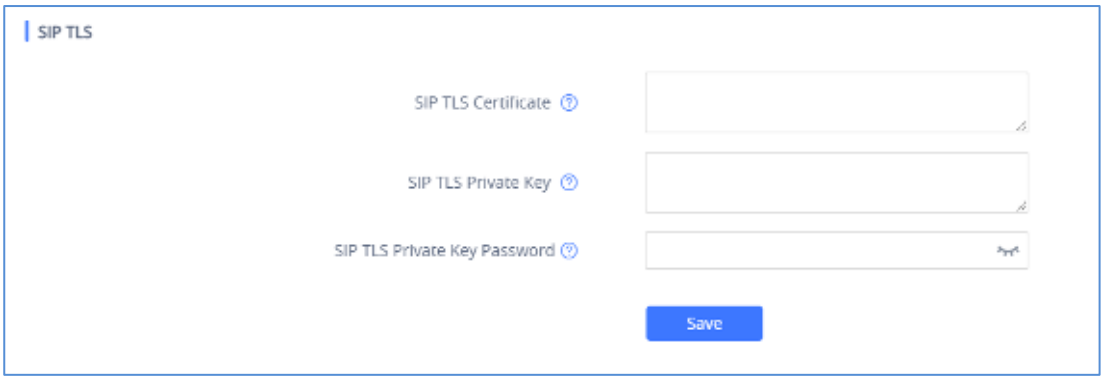

Figure 8: SIP TLS Settings on WP820

When SIP TLS is used, the WP820 also offers additional configurations to check domain certificate and validate certificate chain. These settings can be found under **web UI → Account → Account x → Advanced Settings**.

- **Check Domain Certificate**:
  If enabled, the WP820 will check the domain certificate when TLS/TCP is used for SIP transport. The default setting is "No".

- **Validate Certification Chain**:
  If enabled, the WP820 will validate server's certification chain when TLS/TCP is used for SIP transport.The default setting is "No".

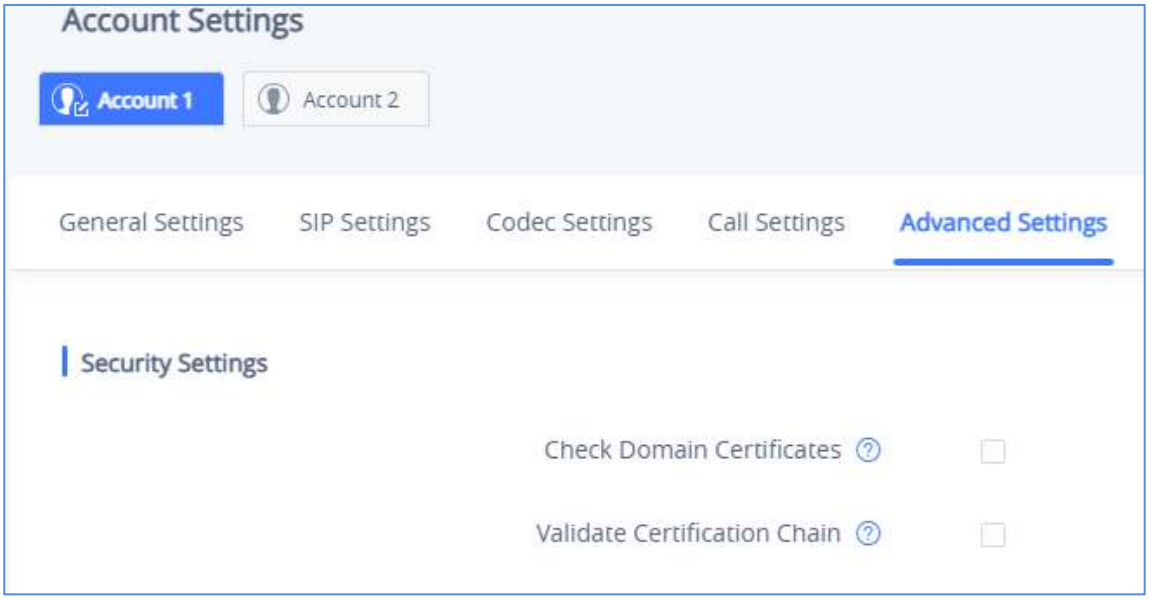

Figure 9: Additional SIP TLS Settings

- **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. 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 50040. Below is the range the WP820 uses for different RTP from **web UI → Phone Settings → General Settings**. (N is from 0 to 1, representing two SIP accounts).

Audio RTP port:	Port_Value+10*N
Audio RTCP port:	Port_Value+10*N+1
FEC RTP port	Port_Value+10*N+4
FEC RTCP port	Port_Value+10*N+5

Anonymous/Unsolicited Calls Protection

If the user would like to have anonymous calls blocked, please go to WP820 **web UI → Account → Account x → Call Settings** and enable option "**Intercept Anonymous Calls**". This will automatically block the SIP calls if the caller ID is anonymous.

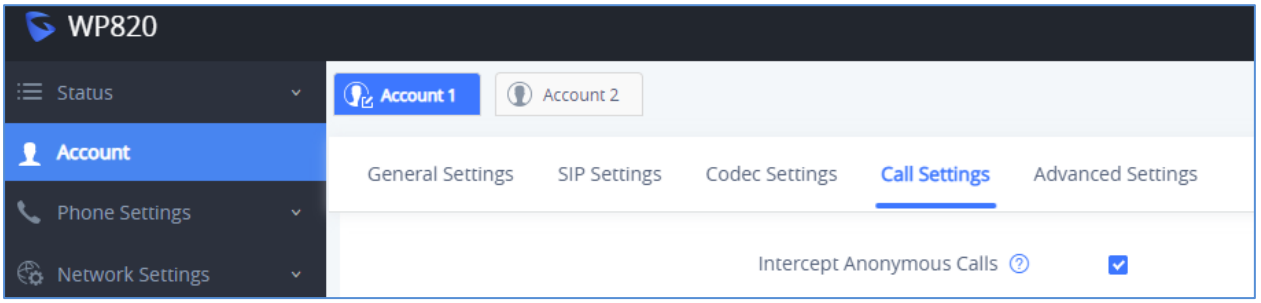

Figure 10: Settings to Block Anonymous Call

Additionally, the WP820 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.

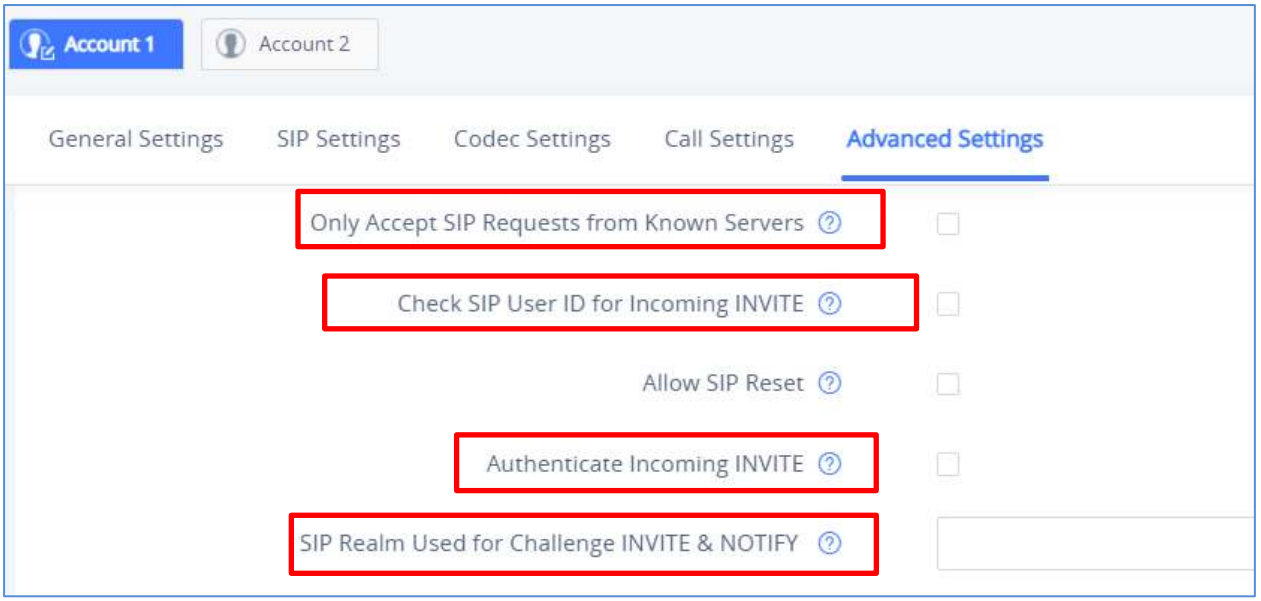

Figure 11: Settings to Block Unwanted Calls

- **Only Accept SIP Requests from Known Servers:**
  When set to "Yes", the WP820 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 WP820 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 WP820 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, "Authenticate Incoming INVITE" must be enabled first for it to take effect for INVITE. For NOTIFY, "SIP NOTIFY Authentication" must be enabled first under **web UI → Maintenance → Upgrade → Advanced Settings**. The SIP NOTIFY message information for the provision includes check- sync, resync and reboot.

Note: The above settings depend also on the server tolerance, if all incoming calls are no longer received after checking the above settings, please make sure that only "**Only Accept SIP Requests from Known Servers**" is the one set to **Yes**.

SRTP

To protect voice communication from eavesdropping, the WP820 phones support SRTP for media traffic using AES 128&256, AES 128 or AES 256. It is recommended to use SRTP if server supports it. SRTP can be configured in **web UI → Account → Codec Settings**.

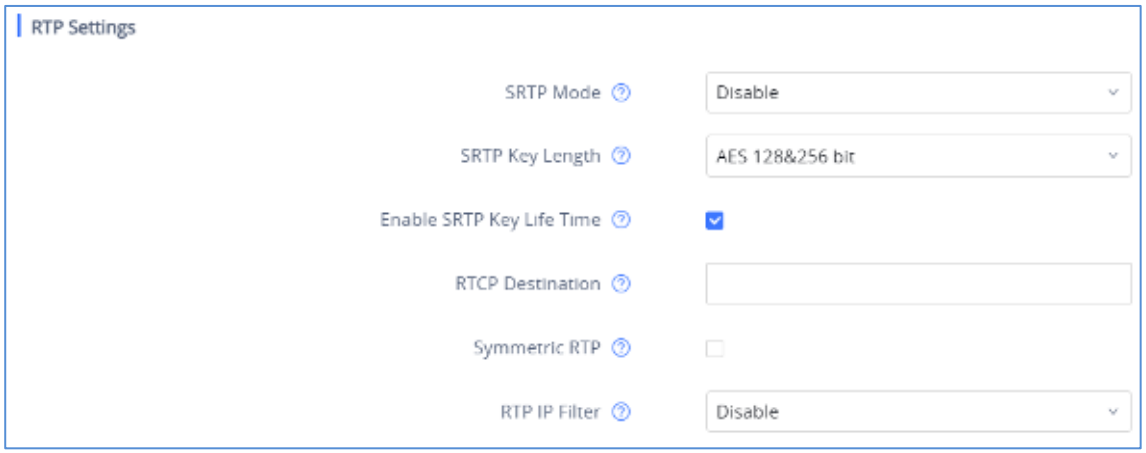

Figure 12: SRTP Settings

NETWORK SECURITY

OpenVPN®

WP820 supports OpenVPN® and by default it is disabled. It can be enabled and used for secure remote connection. If the device is using OpenVPN® to access network, it is recommended to use a different port other than the default well-known port 1194 for added security. Please see OpenVPN® related settings shown as below from **web UI → Network Settings → OpenVPN® Settings**.

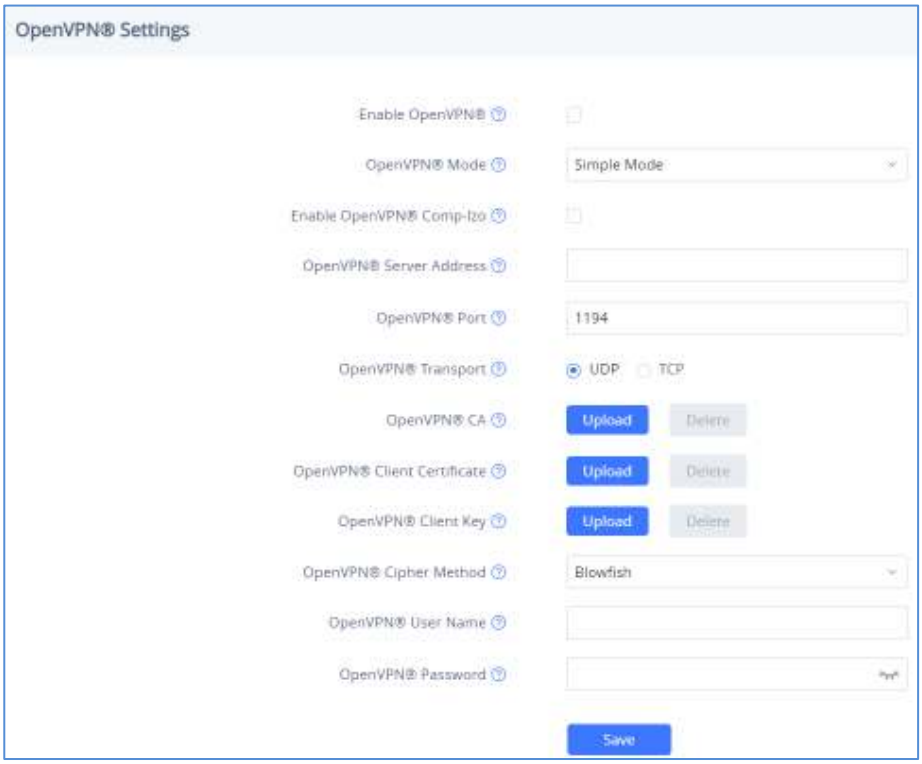

Figure 13: OpenVPN® Settings

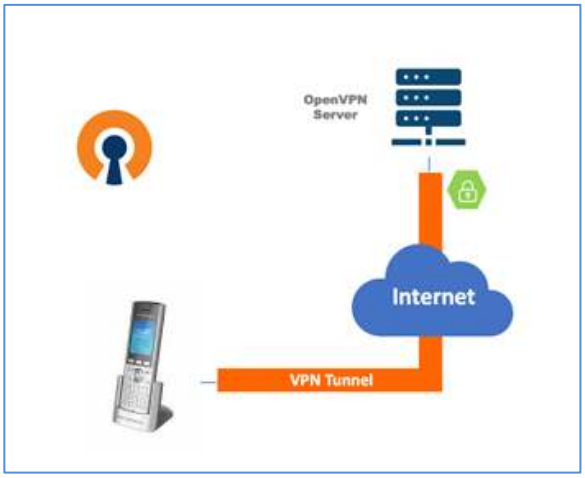

Figure 14: OpenVPN® for Secure Network Access

802.1x

WP820 supports EAPOL where access to switchports can be controlled with identity/password and certificate. When "WPA Enterprise" is selected, there are 4 different mode for selection: PEAP, TLS, TTLS and PWD. Network administrators can set this up accordingly for media access control and network security purpose under **web UI → Network Settings → WIFI Settings→ Add Network**.

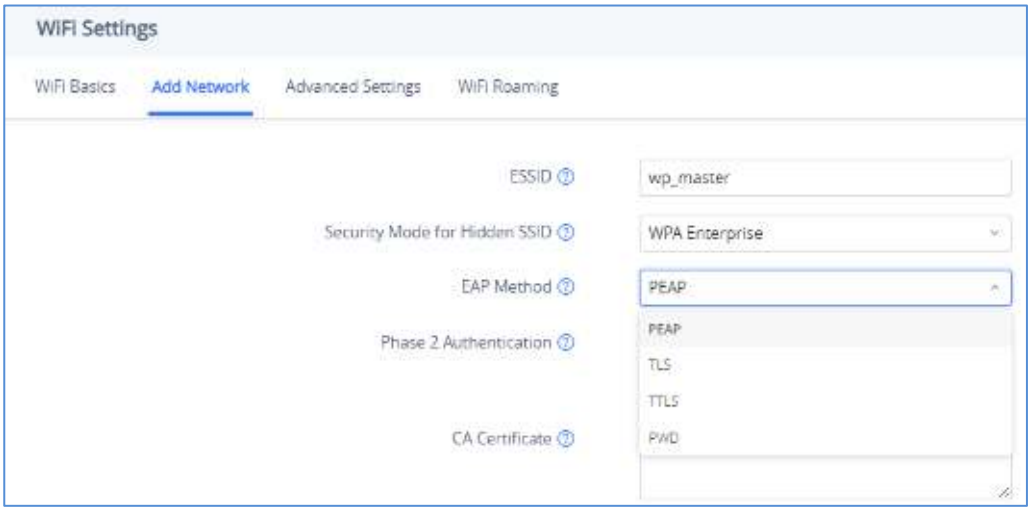

Figure 15: EAP Method Settings

Figure 16: 802.1X for WP820 Deployment

Bluetooth

WP820 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 WP820, it is recommended to turn off Bluetooth so it's not discoverable by nearly Bluetooth devices.

SECURITY FOR WP820 SERVICES

Provisioning via Configuration File

WP820 supports downloading configuration file via HTTP/HTTPS/TFTP under **web UI → Maintenance → Upgrade→ Config File**. Below figure shows the options for config file provisioning.

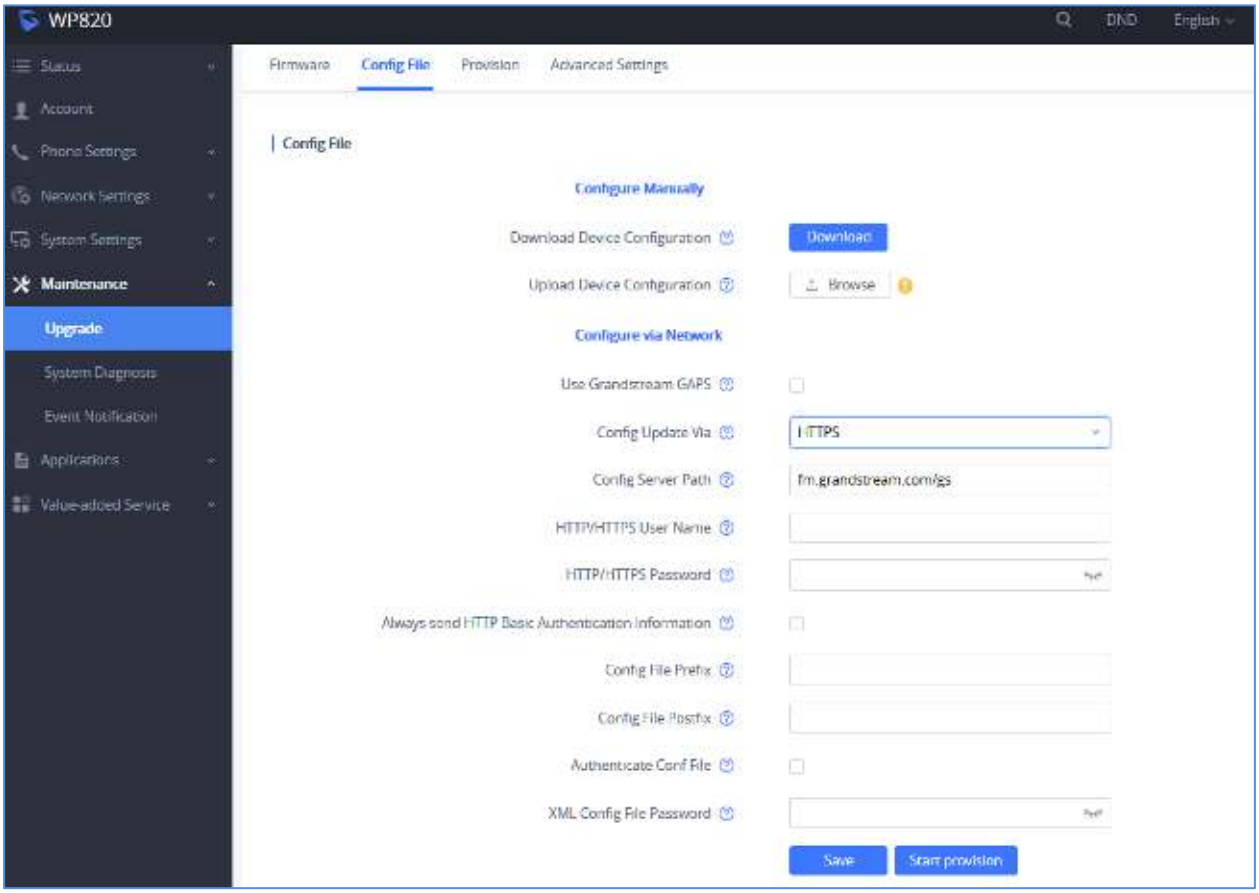

Figure 17: WP820 Config File Provisioning

We recommend users to consider the following options for added security when deploying the WP820 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 WP820 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 WP820 to authenticate configuration file before applying it. When set to “Yes”, the configuration file must include P value P1 with WP820’s administration password. If it is missed or does not match the password, the WP820 will not apply the config file.

- **XML Config File Password:**
  The WP820 XML config file can be encrypted using OpenSSL. When it is encrypted, the WP820 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 WP820. 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. The setting is under **web UI → Maintenance → Upgrade→ Advanced settings.**

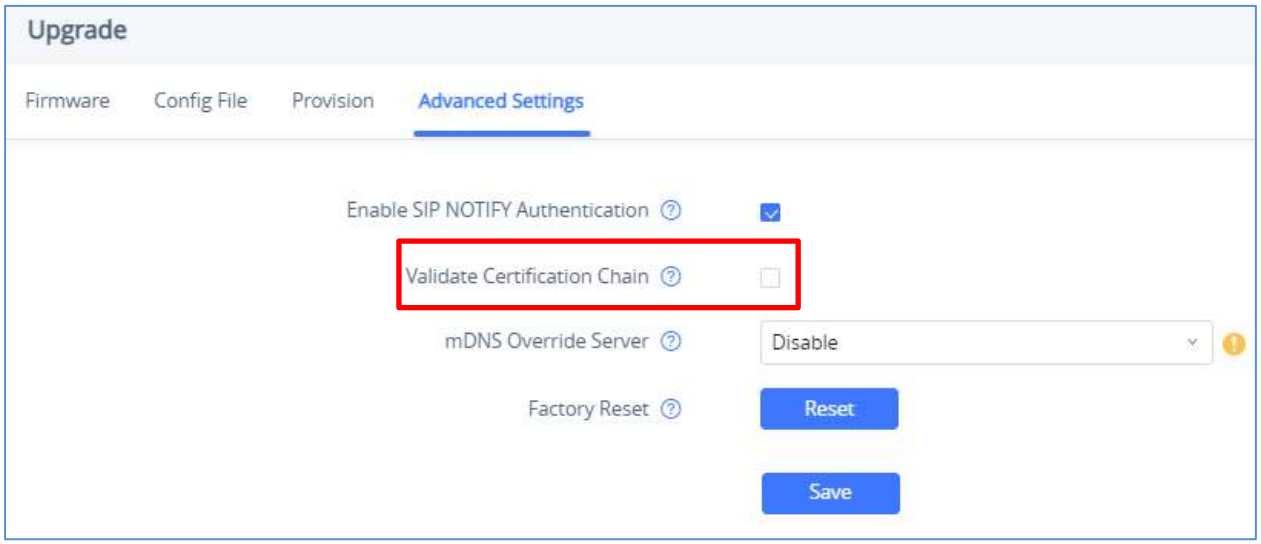

Figure 18: Validate Certification Chain

WP820 supports uploading CA certificate to validate the server certificate and this setting is under **WP820 web UI → System Settings → Security Settings → Certificate Management**.

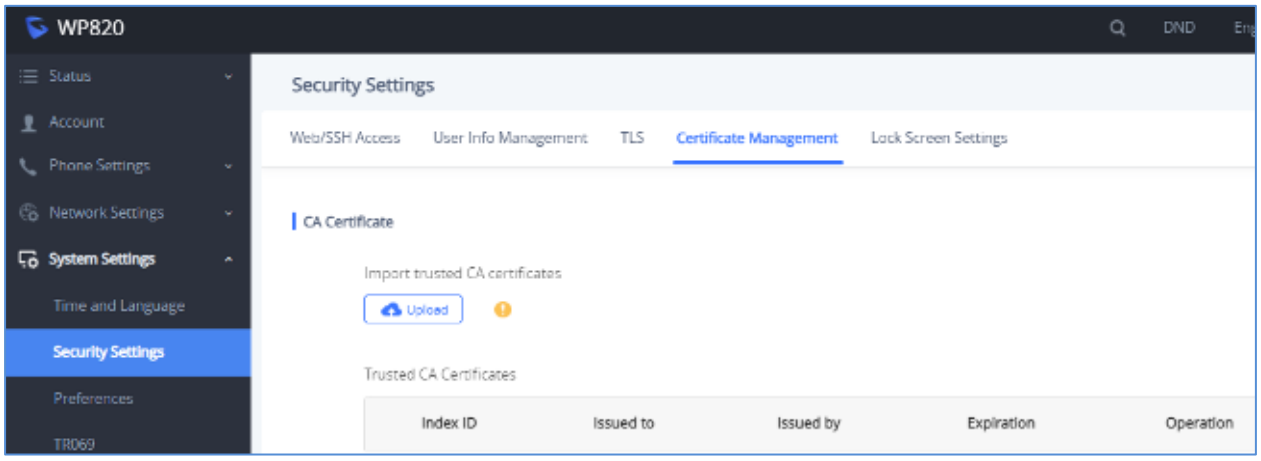

Figure 19: Certificate Management

Firmware Upgrading

Similar to configuration file provisioning, WP820 supports downloading firmware file via HTTP/HTTPS/TFTP. The firmware file is encrypted and WP820 ensures only authentic, signed and untampered firmware file can run. Here are the recommended settings for firmware downloading.

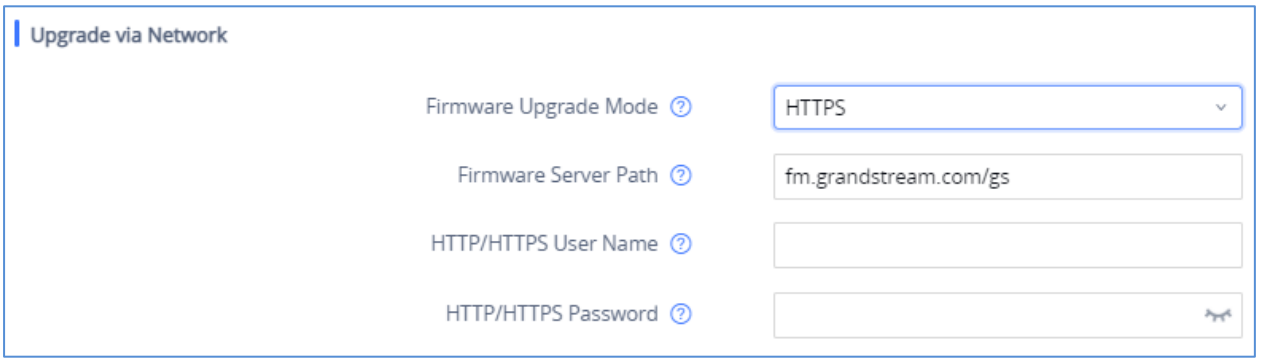

Figure 20: WP820 Firmware Upgrade Configuration

- **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 WP820 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.

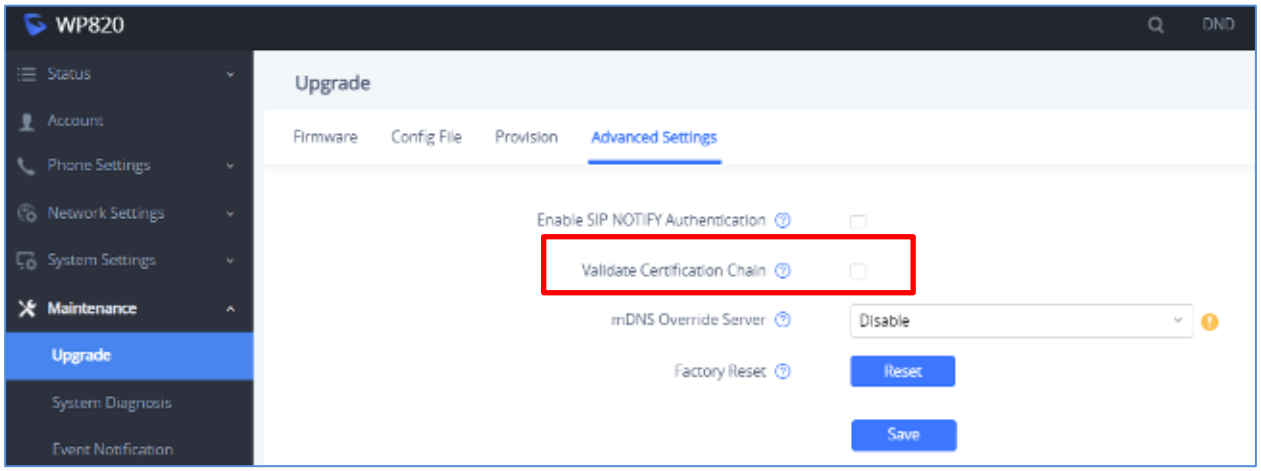

Figure 21: Validate Certification Chain

WP820 supports uploading CA certificate to validate the server certificate and this setting is under WP820 **web UI→System Settings→Security Settings→Certificate Management**.

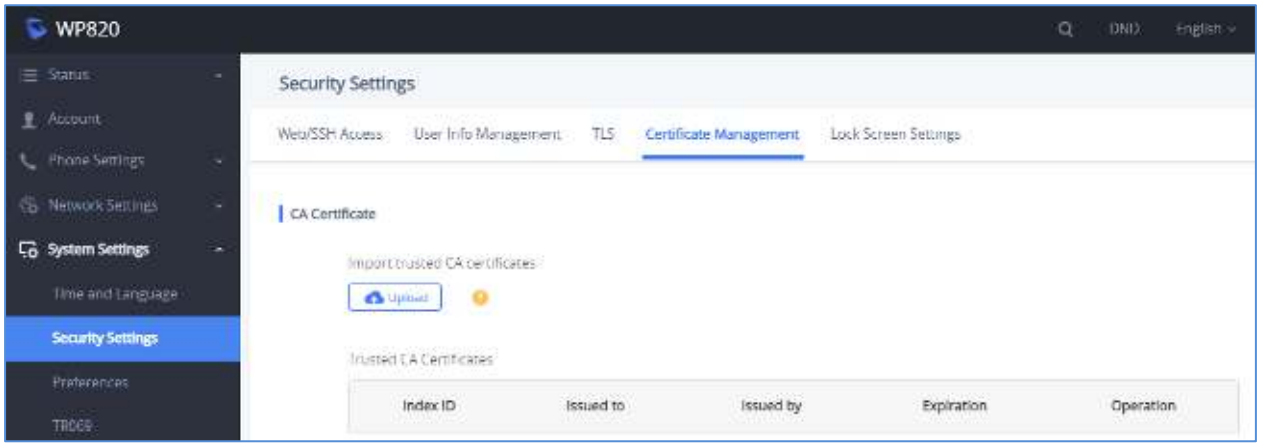

Figure 22: Certification Management

TR-069

TR-069 is enabled by default, which means the connection request port 7547 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 7547 for security purpose. The setting is under **web UI→System Settings→TR069**

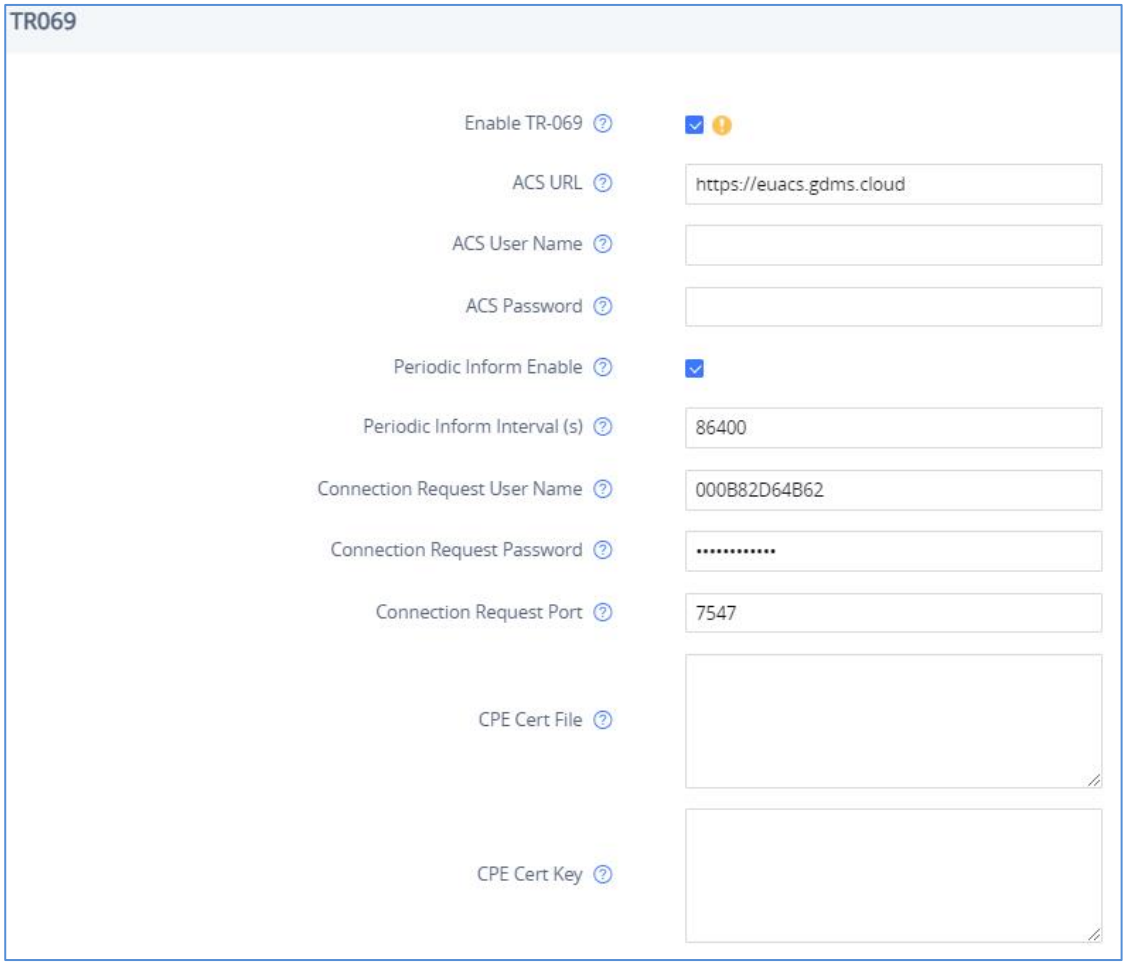

Figure 23: TR-069 Connection Settings Page

LDAP

WP820 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. The setting is under **web UI→Applications→LDAP Phonebook.**

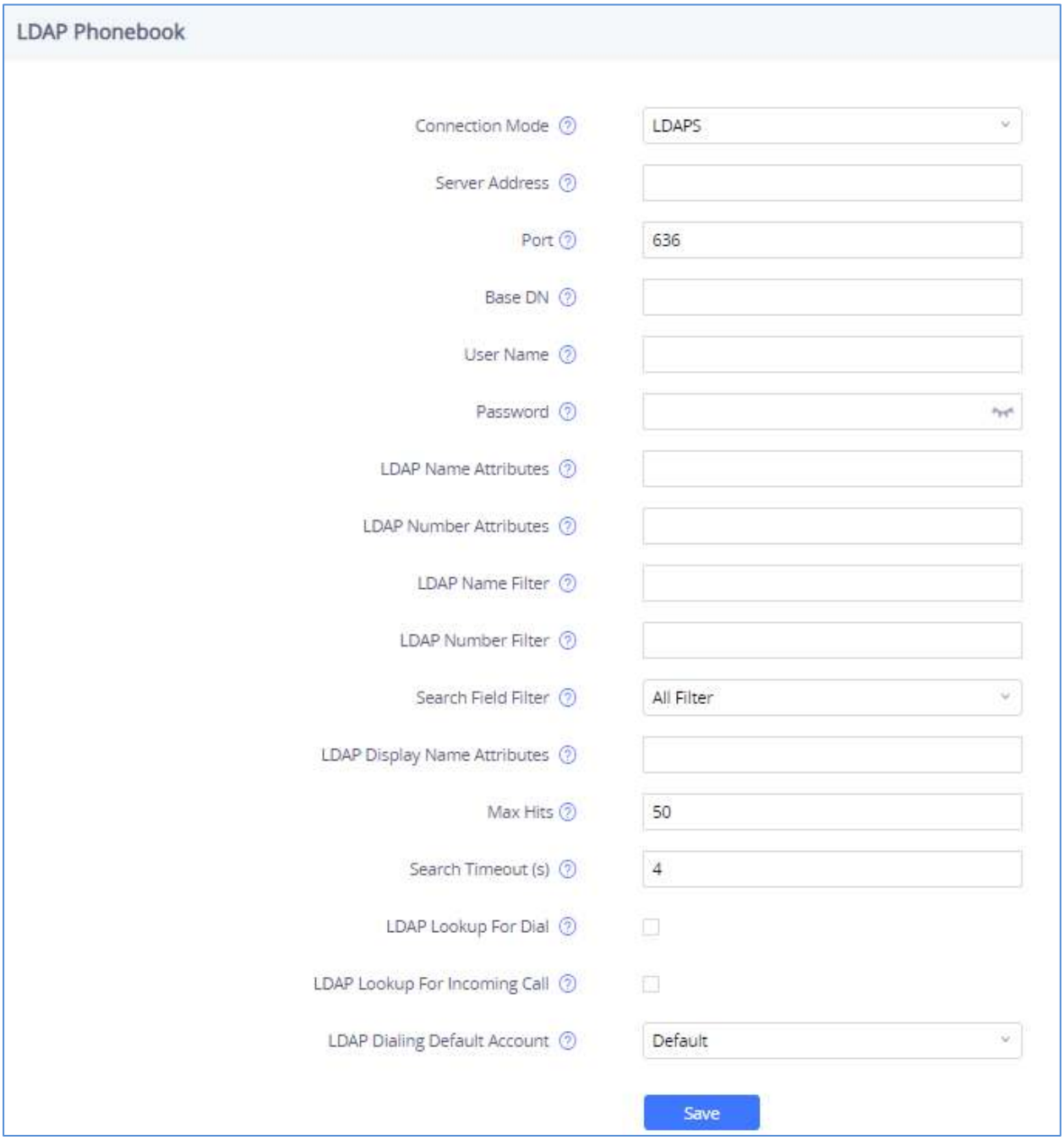

Figure 24: WP820 LDAP Settings

Syslog

WP820 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. The setting is under **web UI→Maintenance→ System Diagnosis→ Syslog.**

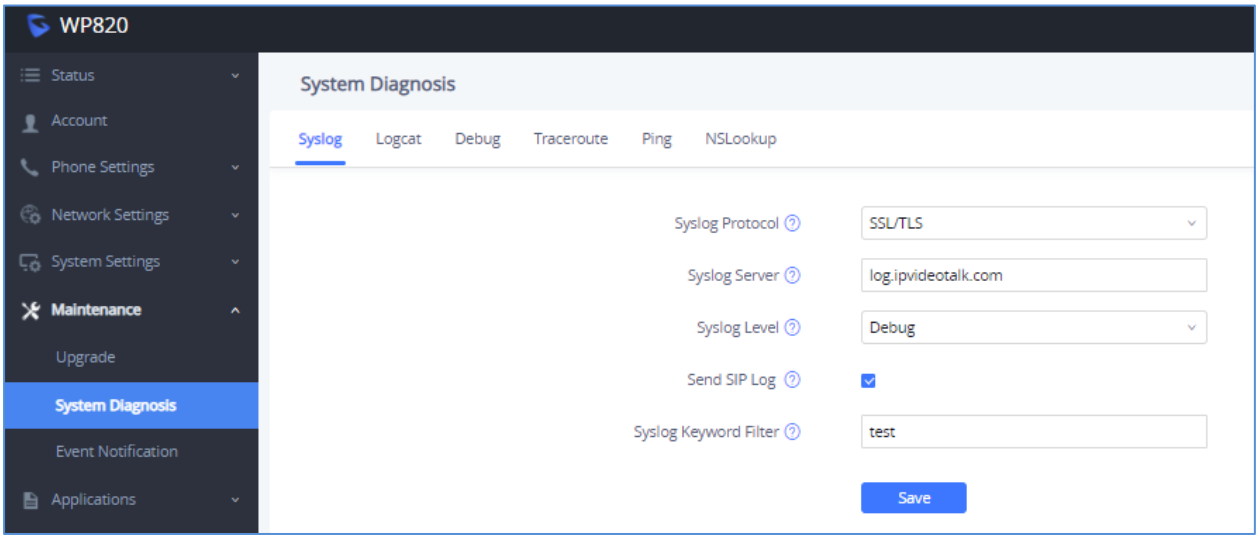

Figure 25: Syslog Protocol

SECURITY GUIDELINES FOR WP820 DEPLOYMENT

Often times the WP820s are deployed behind NAT. The network administrator can consider following security guidelines for the WP820 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 WP820, it is 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 WP820 if the network administrator needs to create firewall rules.

SIP Account x	Default Local SIP Port	Audio RTP/RTCP Port
Account 1	5060 for UDP/TCP 5061 for TLS	RTP: 50040 RTCP: 50041
Account 2	5062 for UDP/TCP 5063 for TLS	RTP: 50050 RTCP: 50051

  Note:
  On the customer's firewall, it is recommended to ensure SIP port is opened for the SIP accounts on the WP820. 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 WP820 SIP port 5060 for security purpose.

- **Use HTTPS for web UI access**
  WP820 Web UI access should be equipped with strong administrator password in additional to using HTTPS. Also, do not expose the WP820 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 is also recommended to turn on "Validate Certification Chain" so the WP820 will validate server certificate when downloading the firmware or config file.