SIP Phone Configuration Guide

HD100 , HD101

HD130, HD150, HD151

HM201

HD300, HD350W, HD351W

snom

Table of Contents

1 Overview

The purpose of this configuration guide is to provide a basic overview of the SIP phones, allowing IT & Telco technical experienced installers to proceed with provisioning of the phone and register to an IP PBX. The intended audience for this document is Customer Service and Technical Installation Personnel involved in the installation and maintenance of SIP phones. For bulk provisioning, please refer to the Administration Guide for Hotel SIP Phone Admin Tool.

All SIP phones require proper configuration before use. Each SIP phone is equipped with a web portal user interface for easy configuration and administration.

Inter-Op Partners

These SIP phones have successfully passed certification with PBX manufactures such as Alcatel, Avaya, Broadcloud, Broadworks, Mitel, NEC, PhonesSuite and Siemens. For specific details of the system, please contact your PBX service provider.

2 Before Configuration

All SIP phones must be setup & wired correctly before configuration. Please read the model specific quick setup guide for setup & wiring instructions shipped with the phones.

3 Configure via Web Portal

Configure all SIP phones via web portal menus.

3.1 Configuration Process

3.1.1 Step 1: Obtain IP Address

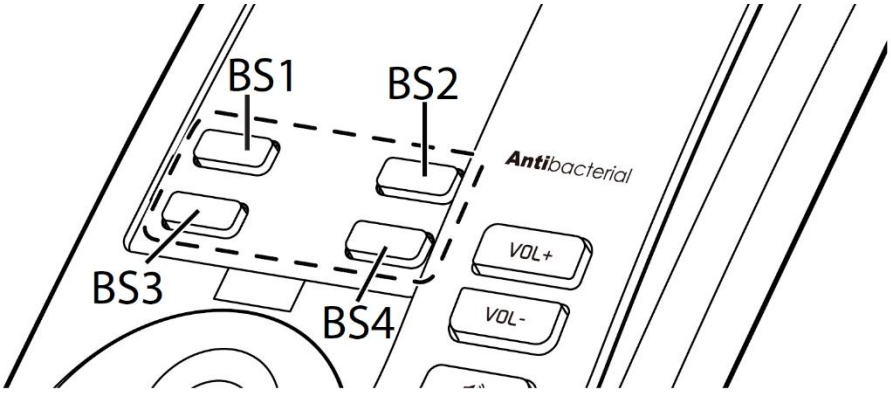
To obtain auto IP address

By default, the phones automatically obtain IP address through DHCP server. You may use a DHCP lease viewer to find out the IP address assigned by matching the MAC address on the back of the phone with the search results displayed.

To discover IP address using the phone IP address read back

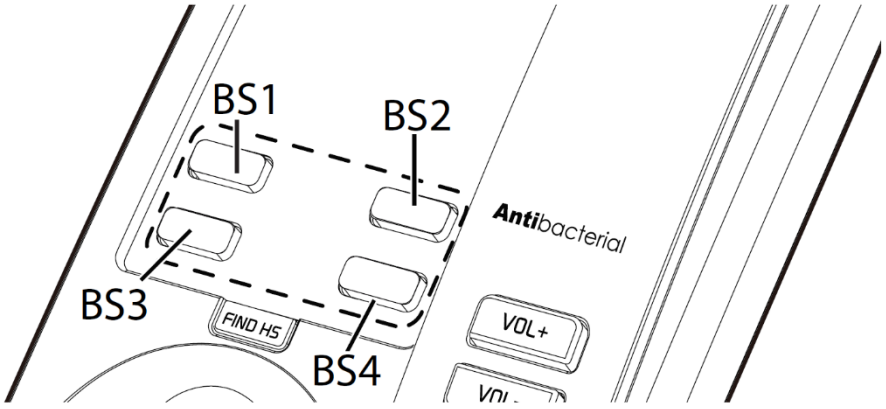
HD100

- Use the keypad to press and hold [VOL+] for more than 5 seconds, and then press [VOL-] [VOL+] [VOL-] [VOL+] [VOL-] [BS1] [BS2] [BS3] in sequence.



HD101

- Press on its handset's keypad [TALK] [*] [*] [*] [*] [1] [2] in sequence.



HD350W & HD351W

- Press on its keypad [*] [4] [7] [1] [2] [3] [3] [#] in sequence.

3.1.2 Step 2: Access Web Portal

The SIP phone embedded web server responds to HTTPS request. Embedded HTML pages allow user to configure the SIP phone via a web browser such as Microsoft's IE (version 6.0 or later) or Mozilla Firefox (version 4.0.1 or later).

Note: If you attempt to access the phones web interface and only end up with an empty / blank page, you most probably tried to use HTTP instead of HTTPS. Please try again with http**s**://

To access the web portal menu via Ethernet:

1. Connect the computer to the same network as the phone.
   - The web enabled computer has to be connected to the same sub-network as the SIP phone. This can easily be done by connecting the computer to the same hub/ switch that the SIP phone is connected to.
2. Make sure the SIP phone is properly installed.
3. Open a web browser on your computer.
4. Enter http**s**:// followed by the IP address of the SIP phone in the address bar of the browser.
   - When the SIP phone is properly connected to a DHCP server, you can use the distributed IP address of the SIP phone. The address is in the format: XXX.XXX.XXX.XXX, where XXX represents a number from 0-255. You need this number to access the web portal menu.
   - Please note most web browsers will report the website / the phone web user interface as unsecure / not private or not trustworthy. This is due the nature of the phone built-in device certificate which comes from a (for your browser) unknown / untrusted source (the Snom Technology Root Authority). Beside that the CN, common name of the device certificate cannot be identical to the IP address used to access the web interface. Due to the production procedure the device certificate CN will correspond the specific LAN MAC address of the phone. So, from the browsers perspective it will remain looking suspicious / invalid, even you manage to import the Snom Technology Root Authority as a trusted source into your browser / PC. This is common per design for embedded devices, like SIP phones and you need to use an exception, confirming to your browser that you like to connect despite the warning. If this exception is not offered in your browser, your browser is most likely managed this way by your corporate IT / security team, and you need to request this option from them.
5. When the login page appears, enter the administrator's username and password to access the web portal menu.
   - The default username is **admin** and the default password is **admin**.

On the Web Portal, there is a navigation bar at the top and the respective submenus on the left.

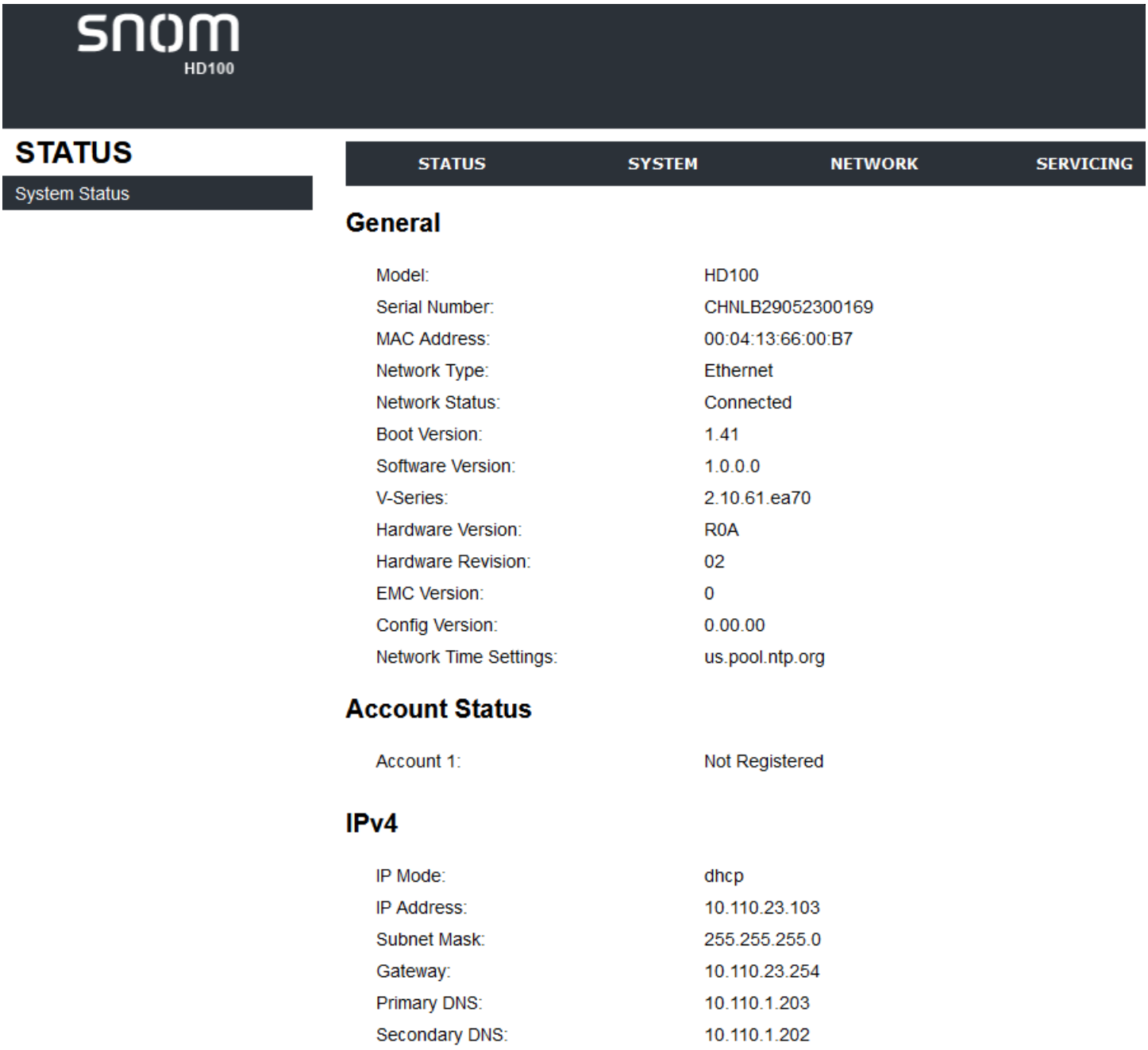
Navigation bar topics:

- STATUS
- SYSTEM
- NETWORK
- SERVICING

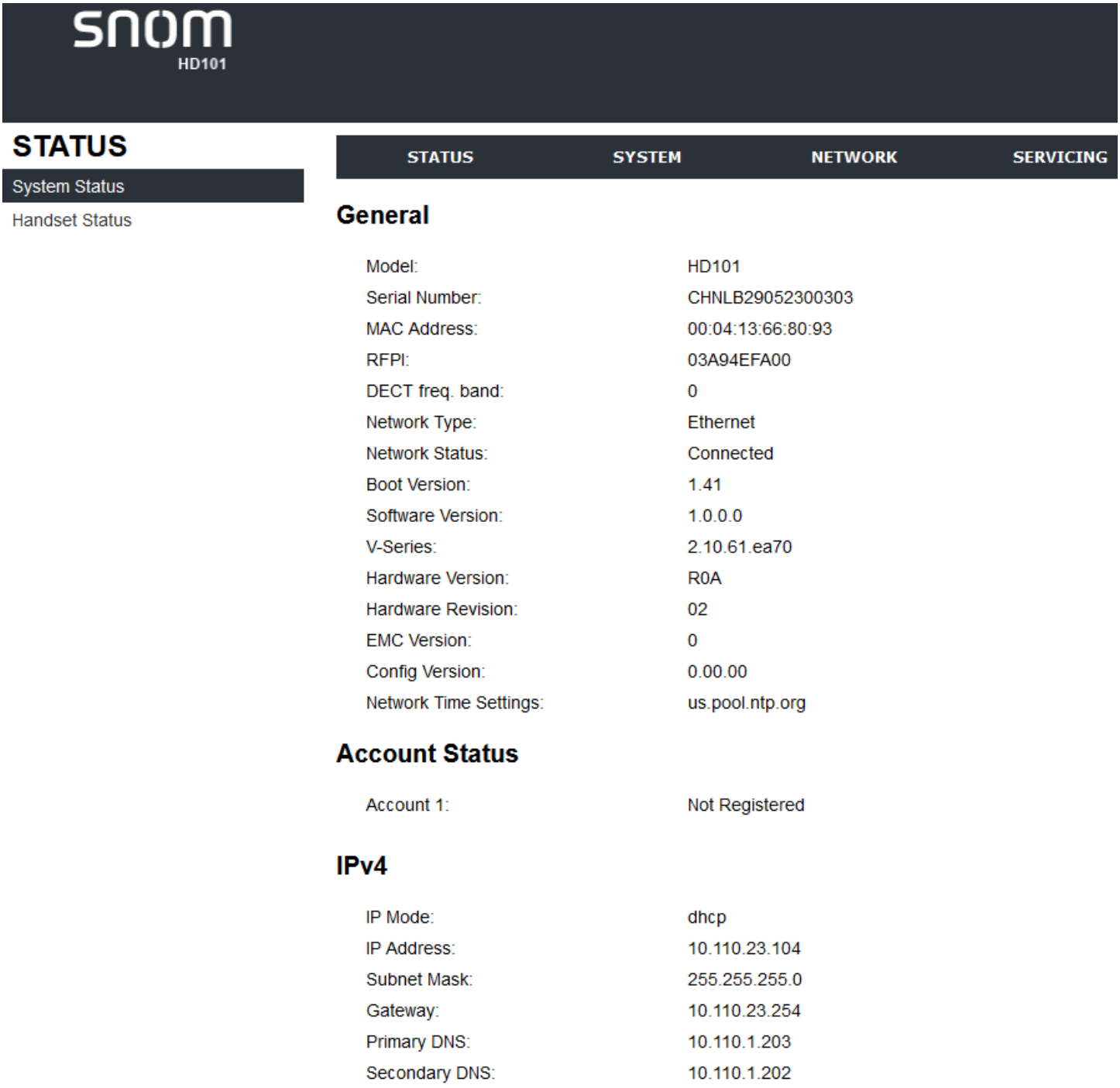
3.1.3 Step 3: Check System Information

At the top navigation menu, select **STATUS**. You will able to review **System Status** and **Handset Status** (i.e. general information about the phone and handsets).

System Status - HD100



System Status - HD101



- **General:** display information about your device, including model, MAC address, and firmware version.
- **Account Status:** display your SIP account registration.
- **IPv4 | IPv6:** display network information regarding your device's network address and network connection.

System status - HM201

Software version: 2.22.6.0 or later

- image pending till product is available

Handset status - HD101, HD351W, HM201 only

- image pending till product is available

The handset status page shows the name and the registration status of all the registered cordless handsets. The page lists the maximum of four handsets, even if fewer handsets are registered. If you have not given the handsets unique names, their default names of HANDSET will appear.

3.1.4 Step 4: Configure Web Portal Pages

3.1.5 Step 5: Reboot Phone System

A phone system reboot, after changing configuration of the following settings, is required in order to apply the new settings:

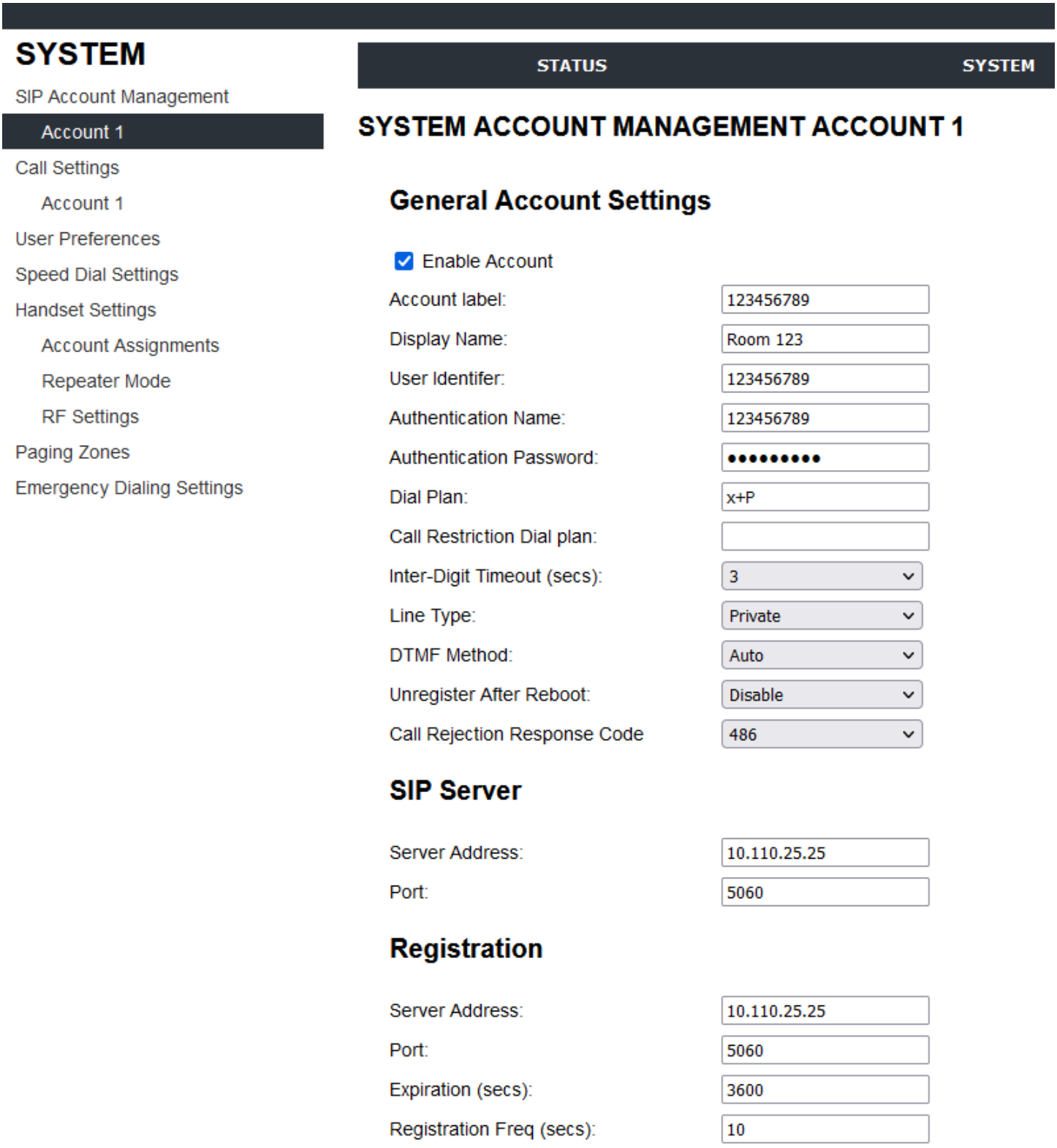
- Network Configuration
- Network Security
- Static IP Mapping
- DECT
- Inter-Op Configuration

After saving the settings, click Reboot to perform phone system reboot.

3.2 Configure System Pages

3.2.1 SIP Account Management

On the SIP Account Management page, you can configure each account you have ordered from your service provider or configured in your SIP-PBX. The SIP Account settings are also available as parameters in the configuration file. See Section 6.6.1 SIP Account Settings ("sip_account" Module).


SYSTEM
SIP Account Management
Account 1
Call Settings
Account 1
User Preferences
Speed Dial Settings
Handset Settings
Account Assignments
Repeater Mode
RF Settings
Paging Zones
Emergency Dialing Settings
STATUS
SYSTEM
SYSTEM ACCOUNT MANAGEMENT ACCOUNT 1
General Account Settings
Enable Account
Account label: 123456789
Display Name: Room 123
User Identifer: 123456789
Authentication Name: 123456789
Authentication Password: ••••••••
Dial Plan: x+P
Call Restriction Dial plan:
Inter-Digit Timeout (secs): 3
Line Type: Private
DTMF Method: Auto
Unregister After Reboot: Disable
Call Rejection Response Code 486
SIP Server
Server Address: 10.110.25.25
Port: 5060
Registration
Server Address: 10.110.25.25
Port: 5060
Expiration (secs): 3600
Registration Freq (secs): 10

3.2.1.1 General Account Settings

Click the links on the web portal for each setting to see the matching configuration file parameter in Section 6.6 Configuration File Parameter Guide. Default values and ranges are listed there.

Setting	Description
Enable Account	Enable or disable the SIP account. Select to enable.
Account label	Enter the name that will appear on the HD10X cordless handset display when account 1 is selected. The Account Label identifies the SIP account throughout the Web Portal and on the handset Line menu.
Display Name	Enter the Display Name. The Display Name is the text portion of the caller ID that is displayed for outgoing calls using account 1.
User Identifier	Enter the User identifier supplied by your service provider. The User ID, also known as the Account ID, is a SIP URI field used for SIP registration. Note: • Do not enter the host name (e.g. "@sipservice.com"). The Web Portal automatically adds the default host name.
Authentication Name	If authentication is enabled on the server, enter the authentication name (or authentication ID) for authentication with the server.
Authentication Password	If authentication is enabled on the server, enter the authentication password for authentication with the server.
Dial Plan	Enter the dial plan, with dialing strings separated by a symbol. See Section 3.2.1.2 Dial Plan.
Call Restriction Dial plan	To restrict users from dialing out numbers through dial plan matching on a per-account basis.
Inter Digit Timeout (sec)	Set how long the HD10X waits after any "P" (pause) in the dial string or in the dial plan.
Line Type	Select the line type to Private or Shared. A private line will be accessible only at the HD10X you are configuring. Shared lines can be assigned to more than one HD10X. For more information about using shared lines, see HD10X User Guide.
DTMF method	Select the default DTMF transmission method. You may need to adjust this if call quality problems are triggering unwanted DTMF tones or you have problems sending DTMF tones in general.
Unregister after reboot	Enable the phone to unregister the account(s) after rebooting - before the account(s) register again as the phone starts up. If other phones that share the same account(s) unregister unexpectedly in tandem with the rebooting HD10X, disable this setting.

3.2.1.2 Dial Plan

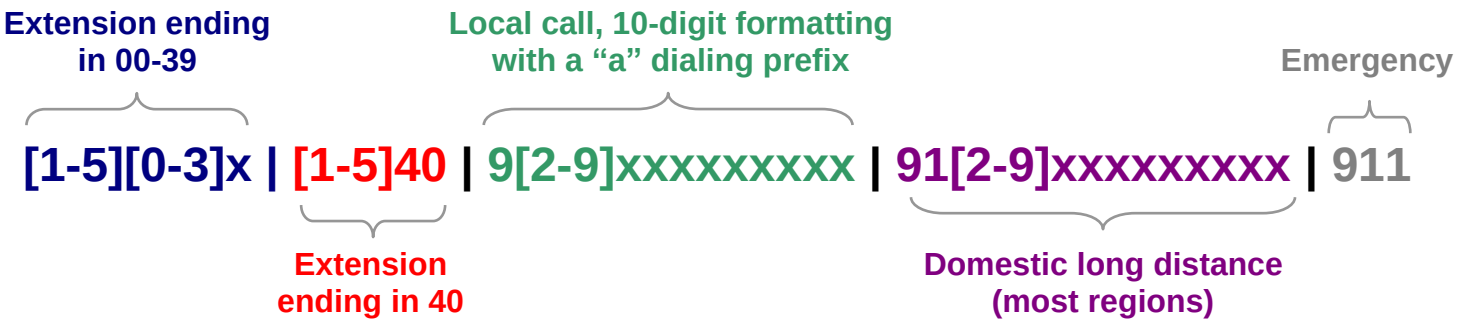
The dial plan consists of a series of dialing rules, or strings, that determine whether what the user has dialed is valid and when the HD10X should dial the number.

Dialing rules must consist of the elements defined in the table below.

Element	Description

x	Any dial pad key from 0 to 9, including # and *.
[0-9]	Any two numbers separated by a hyphen, where the second number is greater than the first. All numbers within the range or valid, excluding # and *.
x+	An unlimited series of digits.
,	This represents the playing of a secondary dial tone after the user enters the digit(s) specified or dials an external call prefix before the comma. For instance, "9,xxxxxxx" means the secondary dial tone is played after the user dials 9 until any new digit is entered. "9,3xxxxxx" means only when the digit 3 is hit would the secondary dial tone stop playing.
PX	This represents a pause of a defined time; X is the pause duration in seconds. For instance, "P3" would represent pause duration of 3 seconds. When "P" only is used, the pause time is the same as the Inter Digit Timeout (see Section 3.2.1 SIP Account Management).
(0:9)	This is a substitution rule where the first number is replaced by the second. For example, "(4:723)xxxx" would replace "46789" with "723-6789". If the substituted number (the first number) is empty, the second number is added to the number dialed. For example, in "(:1)xxxxxxxxxx", the digit 1 is appended to any 10-digit number dialed.
|	This separator is used to indicate the start of a new pattern. Can be used to add multiple dialing rules to one pattern edit box.

A sample dial plan appears below.



3.2.1.3 SIP Server Settings

SIP Server

Server Address: 10.244.185.71
Port: 5060

Setting	Description
Server address	Enter the IP address or domain name for the SIP server.
Port	Enter the port number that the SIP server will use.

3.2.1.4 Registration Settings

Registration

Server Address: 10.244.185.71
Port: 5060
Expiration (secs): 3600
Registration Freq (secs): 10

Setting	Description
Server address	Enter the IP address or domain name for the registrar server.
Port	Enter the port number that the registrar server will use.
Expiration (secs)	Enter the desired registration expiry time in seconds
Registration Freq (secs)	Enter the desired registration retry frequency in seconds. If registration using the Primary Outbound Proxy fails, the Registration Freq setting determines the number of seconds before a registration attempt is made using the Backup Outbound Proxy

3.2.1.5 Outbound Proxy Settings

Outbound Proxy

Server Address: 10.244.185.71
Port: 5060

Setting	Description
Server Address	Enter the IP address or domain name for the proxy server.
Port	Enter the port number that the proxy server will use.

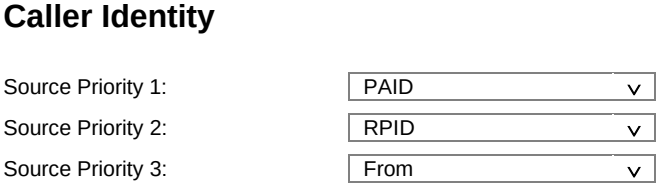
3.2.1.6 Backup Outbound Proxy Settings

Backup Outbound Proxy

Server Address:
Port: 5060

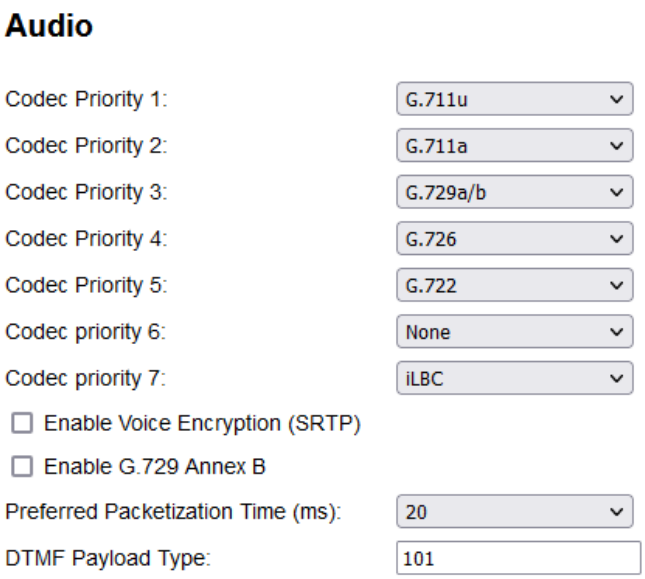
Setting	Description
Server Address	Enter the IP address or domain name for the backup proxy server.
Port	Enter the port number that the backup proxy server will use.

3.2.1.7 Caller Identity Settings



Setting	Description
Source Priority 1	Select the desired caller ID source to display on the incoming call screen: "From" field, RPID (Remote-Party ID) or PAI (P-Asserted Identity) header.
Source Priority 2	Select the lower-priority caller ID source.
Source Priority 3	Select the lowest-priority caller ID source.

3.2.1.8 Audio Settings



Setting	Description
Codec priority 1	Select the codec to use first during a call.
Codec priority 2	Select the codec to use second during a call if the previous codec fails.
Codec priority 3	Select the codec to use third during a call if the previous codec fails.
Codec priority 4	Select the codec to use fourth during a call if the previous codec fails.
Codec priority 5	Select the codec to use fifth during a call if the previous codec fails.
Codec priority 6	Select the codec to use sixth during a call if the previous codec fails.
Codec priority 7	Select the codec to use seventh during a call if the previous codec fails.
Enable voice encryption (RTP)	Select to enable secure RTP for voice packets.
Enable G.729 Annex B	When G.729a/b is enable, select to enable G.729 Annex B, with voice activity detection (VAD) and bandwidth-conserving silence suppression.
Preferred Packetization Time (ms)	Select the packetization interval time.
DTMF Payload Type	Set the DTMF payload type for in-call DTMF from 96-127.

3.2.1.9 Quality of Service

Quality of Service

DSCP (voice): 46

DSCP (signaling): 26

Setting	Description
DSCP (voice)	Enter the Differentiated Services Code Point (DSCP) value from the Quality of Service setting on your router or switch.
DSCP (signaling)	Enter the Differentiated Services Code Point (DSCP) value from the Quality of Service setting on your router or switch.

3.2.1.10 Signaling Settings

Signaling Settings

Local SIP Port: 5060

Transport: UDP

Setting	Description
Local SIP port	Enter the local SIP port.
Transport	Select the SIP transport protocol: • TCP (Transmission Control Protocol) is the most reliable protocol and includes error checking and delivery validation. • UDP (User Datagram Protocol) is generally less prone to latency, but SIP data may be subject to network congestion. • TLS (Transport Layer Security) - the HD10X supports secured SIP signalling via TLS. Optional server authentication is supported via user-uploaded certificates. TLS certificates are uploaded using the configuration file.

3.2.1.11 Voice Settings

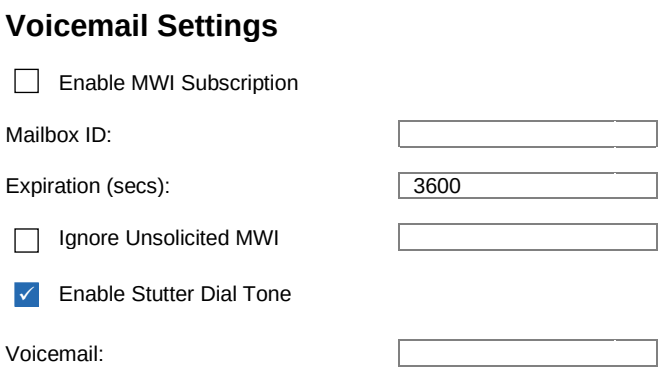
Voice

Min Local RTP Port: 18000

Max Local RTP Port: 19000

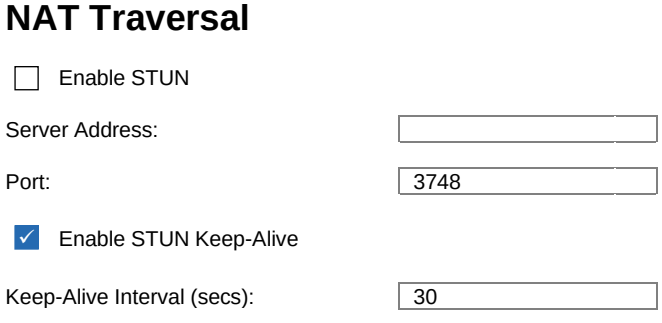
Setting	Description
Min Local RTP Port	Enter the lower limit of the Real-time Transport Protocol (RTP) port range. RTP ports specify the minimum and maximum port values that the phone will use for RTP packets.
Max Local RTP Port	Enter the upper limit of the RTP port range.

3.2.1.12 Voicemail Settings



Setting	Description
Enable MWI Subscription	When enabled, the account subscribes to the "message summary" event package. The account may use the User ID or the service provider's "Mailbox ID".
Mailbox ID	Enter the URI for the mailbox ID. The phone uses this URI for the MWI subscription. If left blank, the User ID is used for the MWI subscription.
Expiration (secs)	Enter the MWI subscription expiry time (in seconds) for account 1.
Ignore unsolicited MWI	When selected, unsolicited MWI notifications - notifications in addition to, or instead of SUBSCRIBE and NOTIFY methods - are ignored for account 1. If the HD10X receives unsolicited MWI notifications, the Message Waiting LED will not light to indicate new messages. Disable this setting if: • MWI service does not involve a subscription to a voicemail server. That is, the server supports unsolicited MWI notifications. • You want the Message Waiting LED to indicate new messages when the HD10X receives unsolicited MWI notifications.
Enable Stutter Dial Tone	Enables or disables the stutter dial tone for that account (indicating message(s) waiting) when the phone goes off hook.
Voicemail	Enter the voicemail retrieval feature access code.

3.2.1.13 NAT Traversal

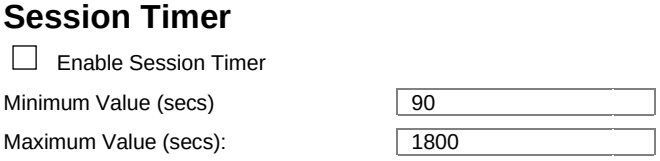


Setting	Description
Enable STUN	Enables or disables STUN (Simple Traversal of UDP through NATs) for account 1. The Enable STUN setting allows the HD10X to identify its publicly addressable information behind a NAT via communicating with a STUN server.
Server Address	Enter the STUN server IP address or domain name.
Port	Enter the STUN server port.
Enable STUN Keep-Alive	Enable or disables UDP keep-alive. Keep-alive packets are used to maintain connections established through NAT.
Keep-Alive Interval(sec)	Enter the interval (in seconds) for sending UDP keep-alive.

3.2.1.14 Music on Hold Settings

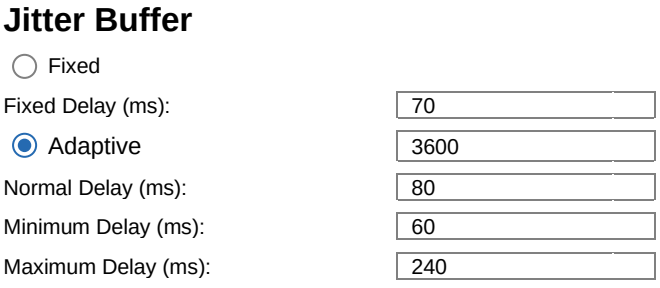
Setting	Description
Enable Local MoH	Enables or disables a hold-reminder tone that the user hears when a far-end caller puts the call on hold.

3.2.1.15 Session Timer



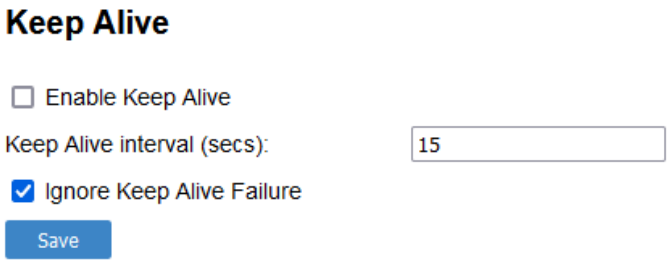
Setting	Description
Enable Session Timer	Enter the lower limit of the Real-time Transport Protocol (RTP) port range. RTP ports specify the minimum and maximum port values that the phone will use for RTP packets.
Minimum Value (sec)	Set the session timer minimum value (in seconds) for account 1.
Maximum Value (sec)	Set the session timer maximum value (in seconds) for account 1.

3.2.1.16 Jitter Buffer



Setting	Description
Fixed	Enable fixed jitter buffer mode.
Fixed Delay (ms)	If Fixed is selected, enter the fixed jitter delay.
Adaptive	Enable adaptive jitter buffer mode.
Normal Delay (ms)	If Adaptive is selected, enter the normal or “target” delay.
Minimum Delay (ms)	Enter the minimum delay.
Maximum Delay(ms)	Enter the maximum delay. This time, in milliseconds, must be at least twice the minimum delay.

3.2.1.17 Keep Alive

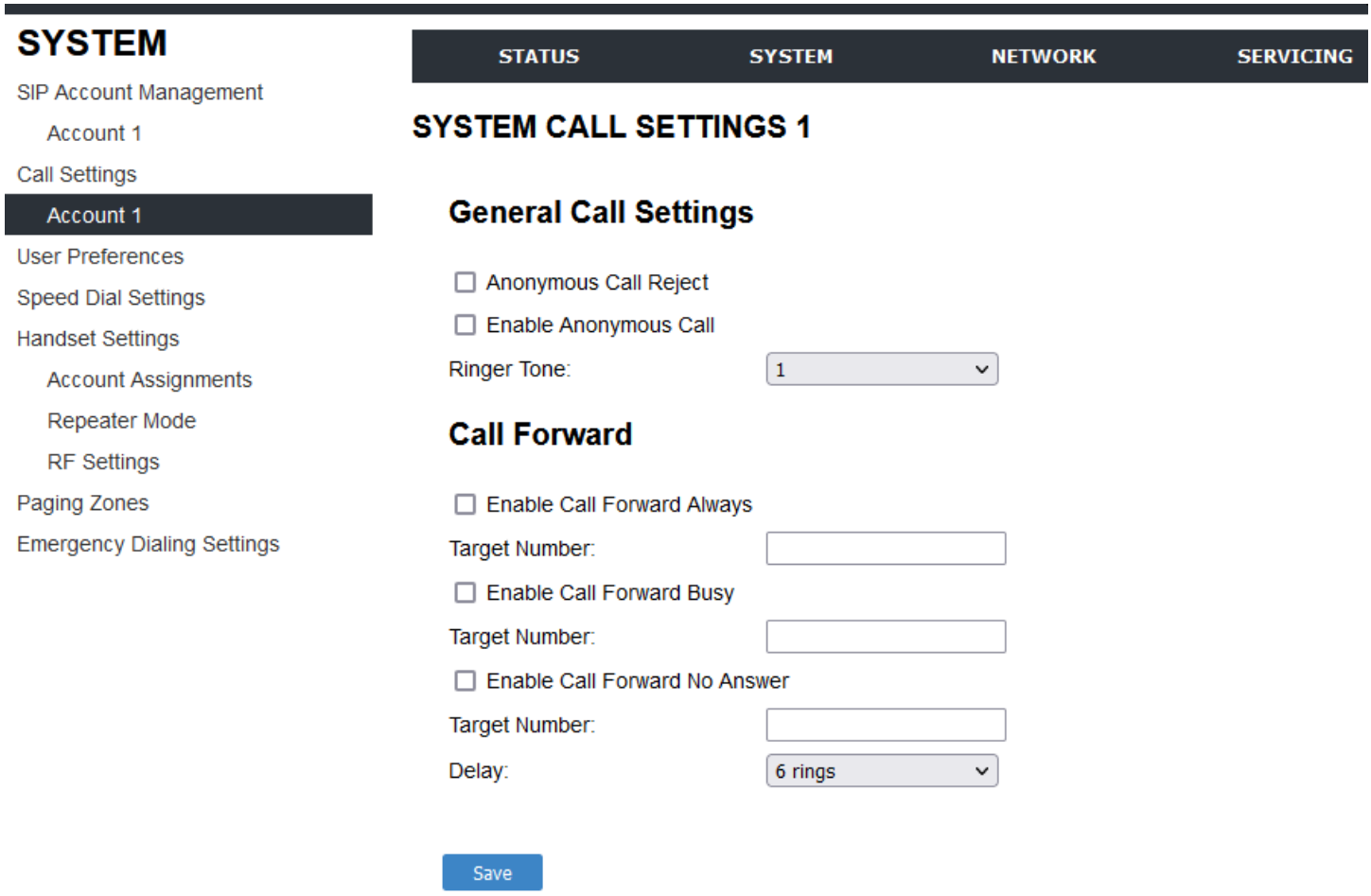


Setting	Description
Enable Keep Alive	Enable SIP keep alive in service of NAT traversal and as a heartbeat mechanism to audit the SIP server health status. Once enabled, OPTIONS traffic should be sent whenever the account is registered. OPTIONS traffic will occur periodically according to the keep-alive interval.
Keep Alive interval (sec)	Set the interval at which the OPTIONS for the keep-alive mechanism are sent.
Ignore Keep Alive Failure	Enable the phone to ignore keep-alive failure, if the failure can trigger account re-registration and re-subscription (and active calls are dropped).

3.2.2 Call Settings

You can configure call settings for each account. Call Settings include Call Forward settings.

The call settings are also available as parameters in the configuration file. See Section 6.6.11 Call Settings ("call_settings" Module).



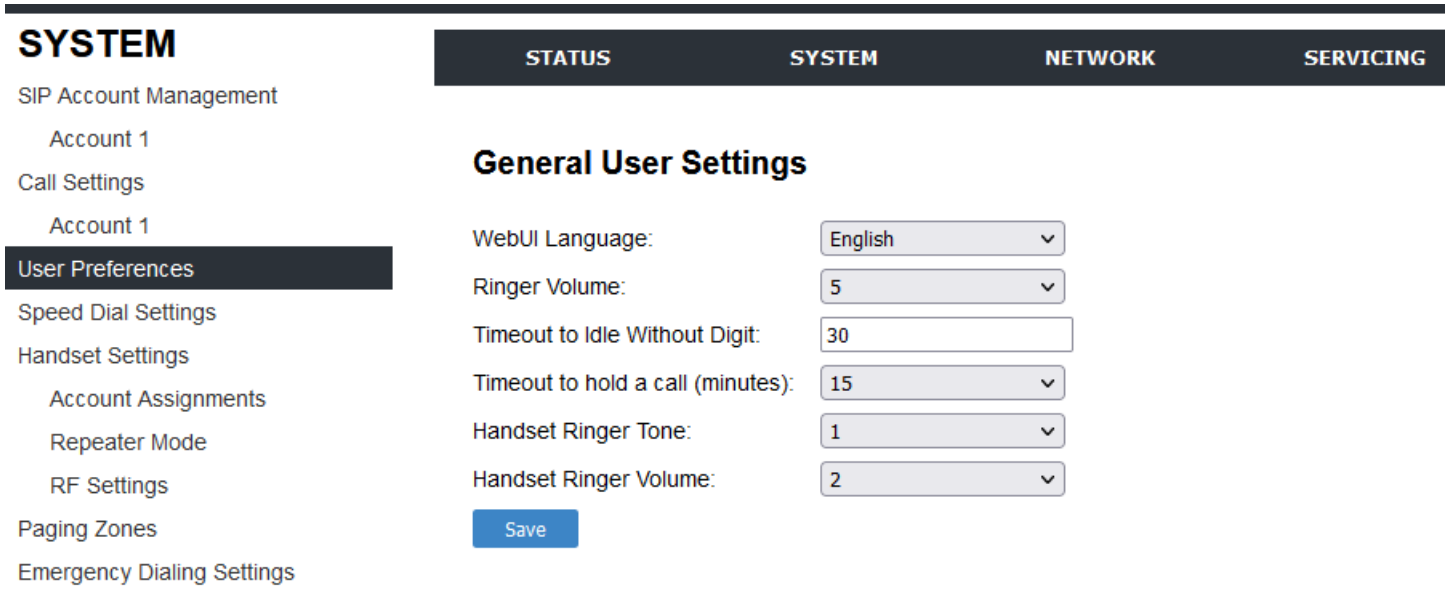
3.2.2.1 General Call Settings

Setting	Description
Anonymous Call Reject	Enables or disables rejecting calls indicated as "Anonymous".
Enable Anonymous Call	Enables or disables outgoing anonymous calls. When enabled, the caller name and number are indicated as "Anonymous".
Ringer Tone	Set the ringer tone for incoming calls on the account.

3.2.3 User Preferences

On the User Preferences page, you can configure some basic settings for the phone and set the language that appears on the Web Portal. The User Preferences page is also available to phone users when they log on to the Web Portal.

The user preference settings are also available as parameters in the configuration file. See Section 6.6.10 User Preference Settings ("user_pref" Module) .



3.2.3.1 General User Settings

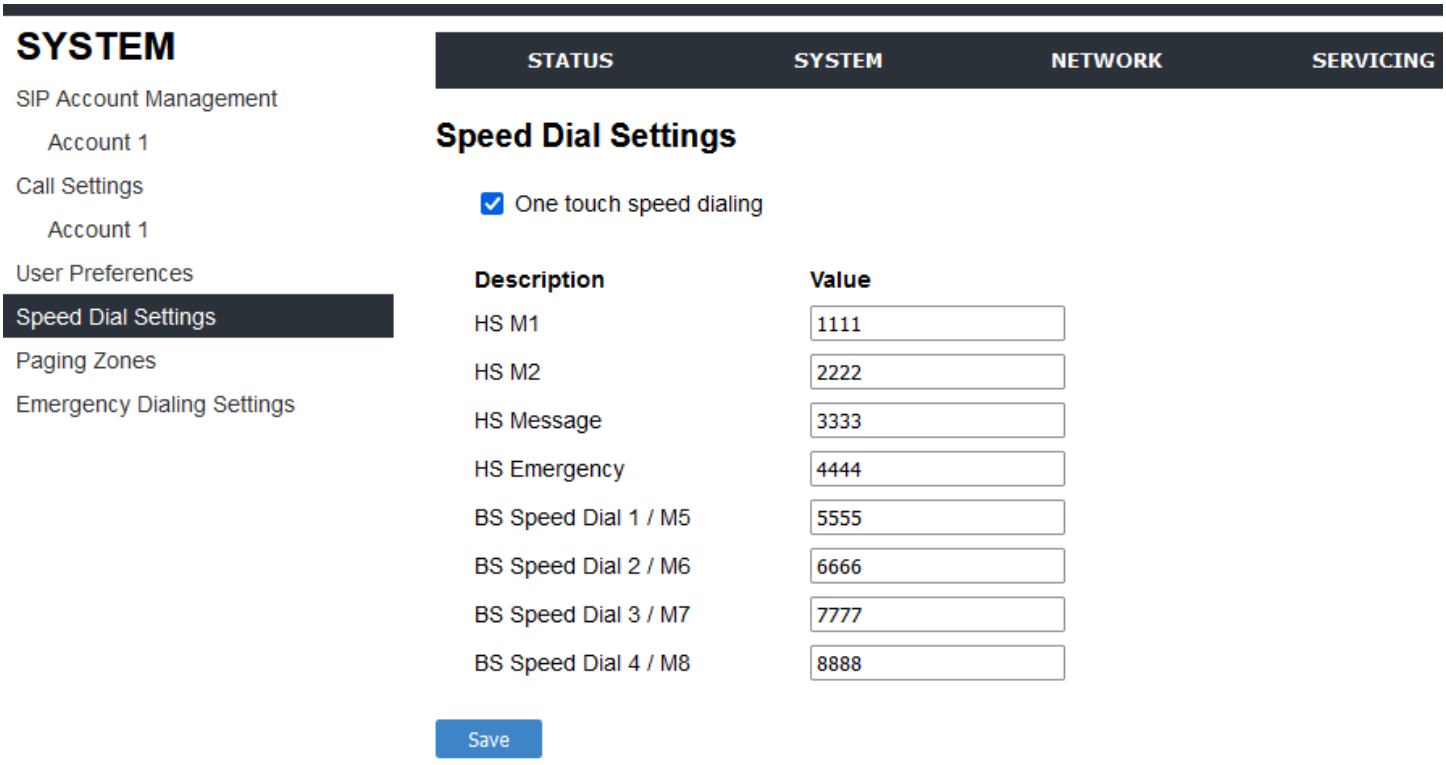
Click the link for each setting to see the matching configuration file parameter in Section 6.6. Configuration File Parameter Guide. Default values and ranges are listed there.

Setting	Description
Web Portal Language	Set the language that appears on the Web Portal.
Ringer Volume	Set the ringer volume for incoming calls. You can also use the VOLUME ▼ or▲ keys on the HD10X.
Timeout to Idle Without Digit	Set the timeout (in seconds) after the phone goes off hook and no digits are input. After the timeout, the phone returns to idle mode.

3.2.4 Speed Dial Settings (all the models except HM201)

On the Speed Dial Settings page, you can enter up to 10 speed dial numbers for the telephone base and 2 speed dial numbers for the cordless handset.

To dial a speed dial number, press the desired speed dial key on the telephone base or the cordless handset.



The speed dial key settings are also available as parameters in the configuration file. See Section 6.6.12 Programmable Feature Key Settings ("pfk" Module).

After entering information on this page, click **SAVE**. To enter speed dial numbers:

1. In the Value column, enter a phone number for the desired speed dial key.
2. Click **SAVE**.

3.2.4.1 Speed Dial Keys

Click the link for each setting to see the matching configuration file parameter in Section 6.6.12 Programmable Feature Key Settings ("pfk" Module).

Setting	Description
Speed Dial	BS: Speed dial keys on telephone base (Key 1-10). HS: Speed dial keys on cordless handset (HS SER. & HS EMER.) See the images below.
Value	The phone number that the speed dial key dials when pressed and held.

3.2.5 Handset Settings

The Handset Settings allow you to configure account assignments and names for the cordless handset that are registered to the base station. For more information on registering cordless handsets, see HD10X specific setup guide.

The network settings are also available as parameters in the configuration file. See Section 6.6.2 Handset Settings ("hs_ settings" Module).

3.2.5.1 Account Assignments

The Account Assignments table lists the maximum of four handsets, even if there are fewer handset registered. The registration status of currently registered handset does not affect what is listed on this table.

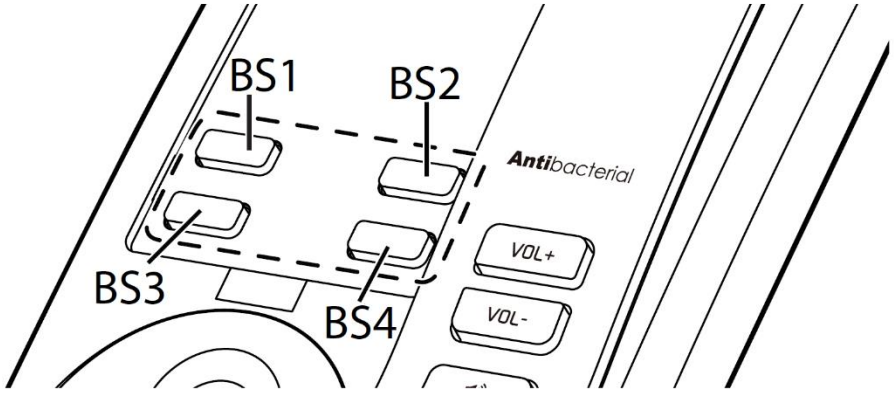
For the HD10X phone, the table always displays the maximum one account.

If you have not entered any unique handset names yet, then the default name of "HANDSET" appears.

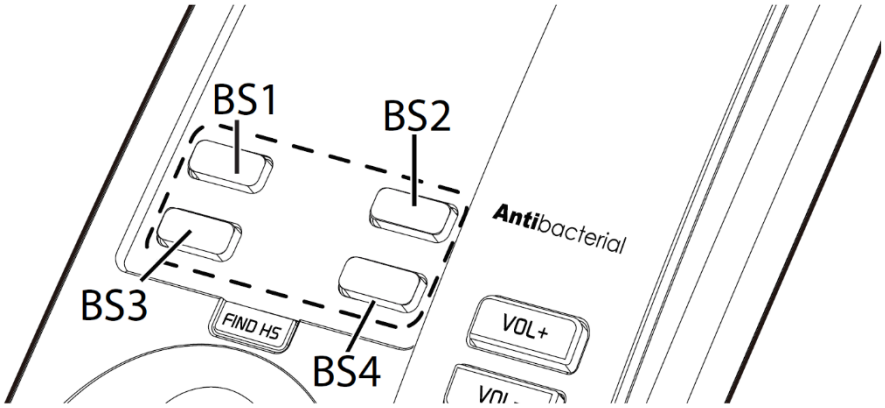
On the Account Assignments table, you can select which accounts will be available for both incoming and outgoing calls on each handset.

The handset will first attempt to use the account you select under Default when going off-hook.

Speed Dial - BS: Telephone Base: HD100

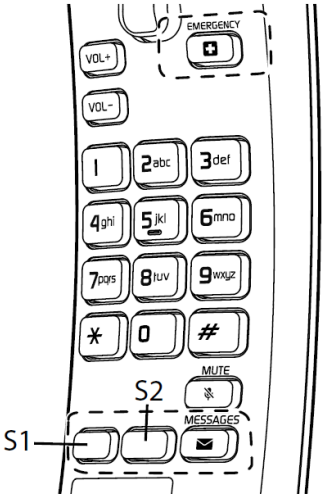


HD101



Speed Dial - HS: Cordless Handset:

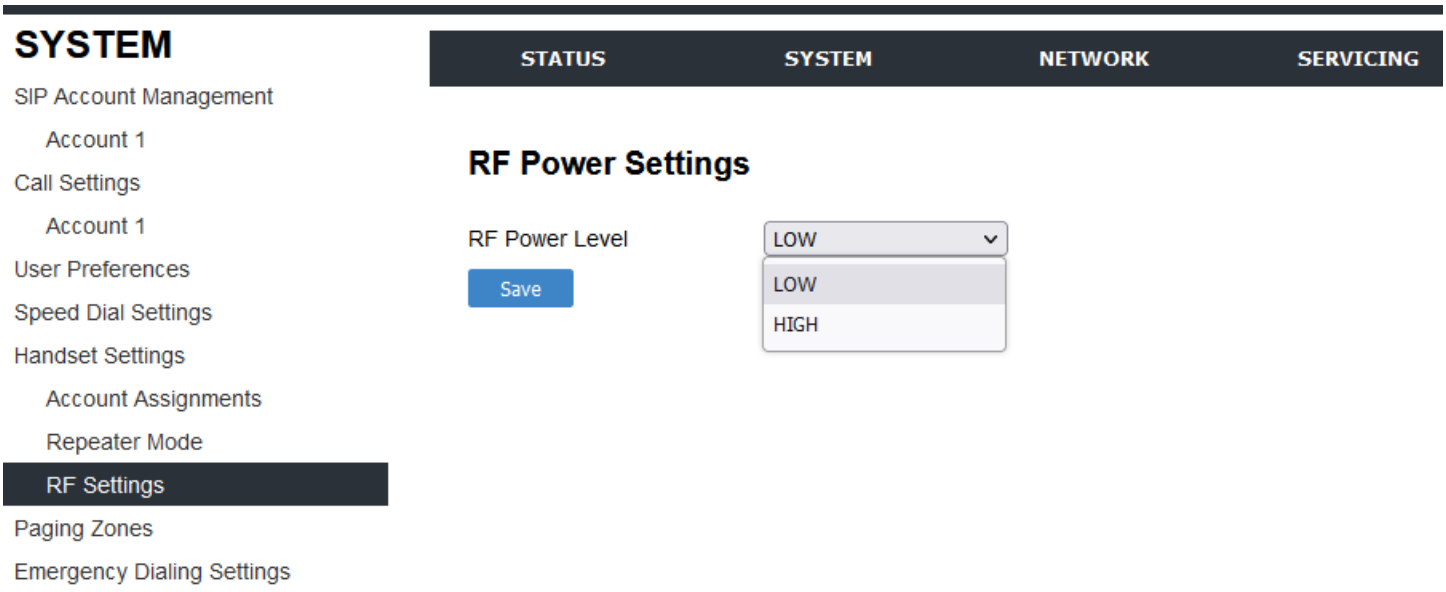
HD100



HD101

3.2.5.2 RF Power Settings

On the RF Power Settings page, you can select the RF power level of the telephone.



Setting	Description
RF Power Level	Set the DECT RF power level. Choose either High or Low, depending on the hotel environment. If there are interferences caused by phones among hotel rooms, choose **Low**. If there are interferences caused by other electronic devices from the environment, choose **High**.

3.2.6 Emergency Dialing Settings

On the Emergency Dialing Settings page, you can enable/disable and configure the Emergency Dialing feature.

If enabled, and the telephone goes off hook for a period of time specified by the Delay timer, the pre-defined Phone Number will automatically be dialed.

Setting	Description
Enable Emergency Dialing	Enable or disable Emergency Dialing. Select to enable.
Phone Number	Set the phone number to be dialed by the Emergency Dialing feature.
Delay (sec)	Set the delay (in seconds) between the phone going off hook and the phone number being dialed.

3.3 Configure Network Pages

You can set up the HD10X for your network configuration on the Network pages. Your service provider may require you to configure your network to be compatible with its service, and the HD10X settings must match the network settings.

The network settings are grouped into Basic and Advanced Settings. IPv4 and IPv6 protocols are supported.

When both IPv4 and IPv6 are enabled and available, the following guidelines apply when determining which stack to use:

- For outgoing traffic, the IP address (or resolved IP) in the server field - either IPv4 or IPv6 - will determine which stack to be used.
- In general, most operations can be associated with one of the servers listed on the Basic Network Settings page. However, for operations triggered by/dependent upon network status, the phone must determine which server to use. For example, a special case like the "Network down" can be ambiguous for server association. Because its primary purpose is to aid in troubleshooting SIP registration issues, this case will be associated with the SIP registration server.
- DNS entries with both IPv4 and IPv6 settings can be used to resolve FQDN entries. There are no preferences with the order of the DNS queries.
- Pcap should include traffic for both stacks.
- Dual stack operations should be transparent to PC port traffic.

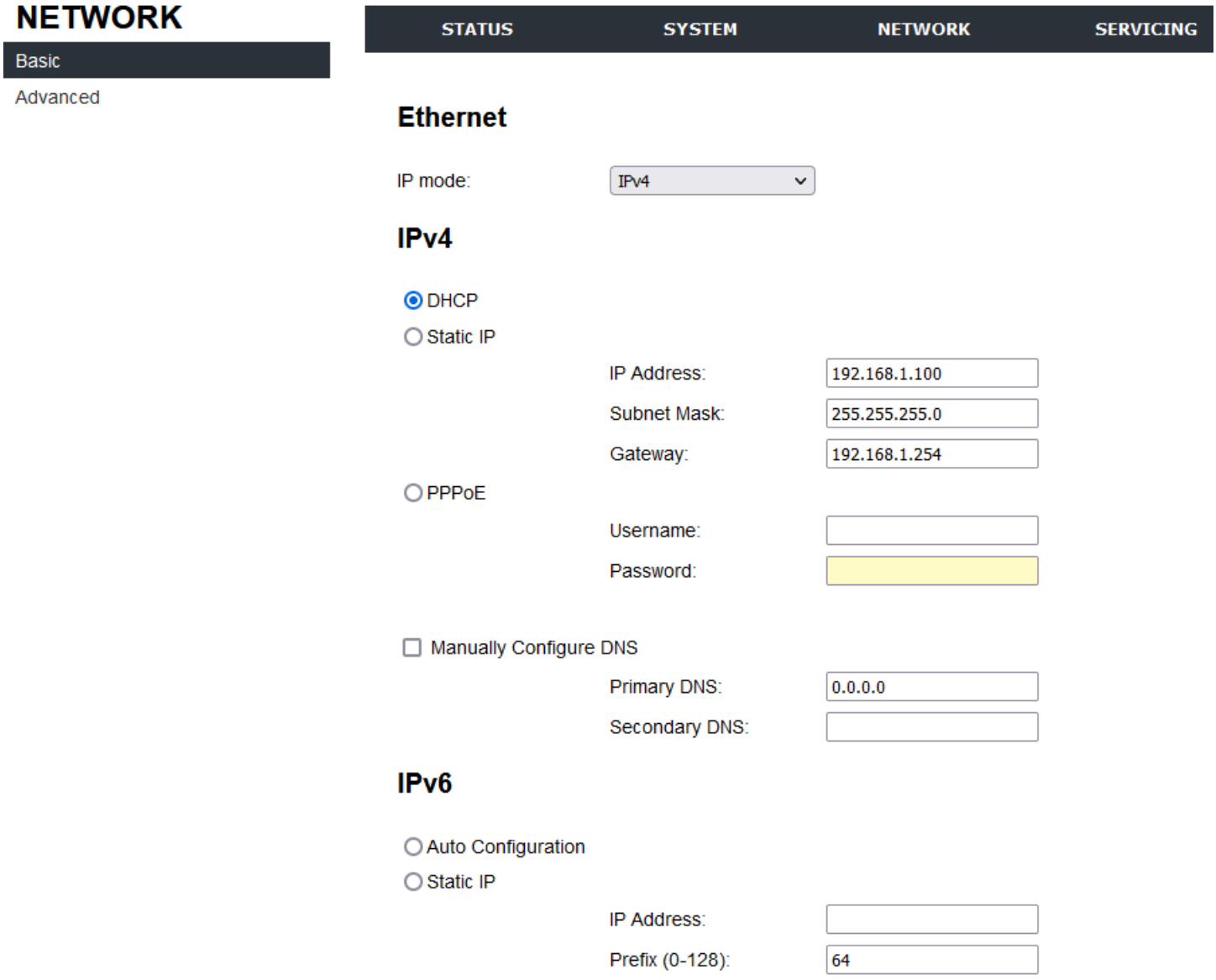
Note

- PnP is not supported on IPv6.
- VPN is not supported in IPv6 or PPPoE.

The network settings are also available as parameters in the configuration file. See Section 6.6.3 Network Settings ("network" Module).

After entering information on this page, click **SAVE** to save it.

3.3.1 Basic Network Settings



Note

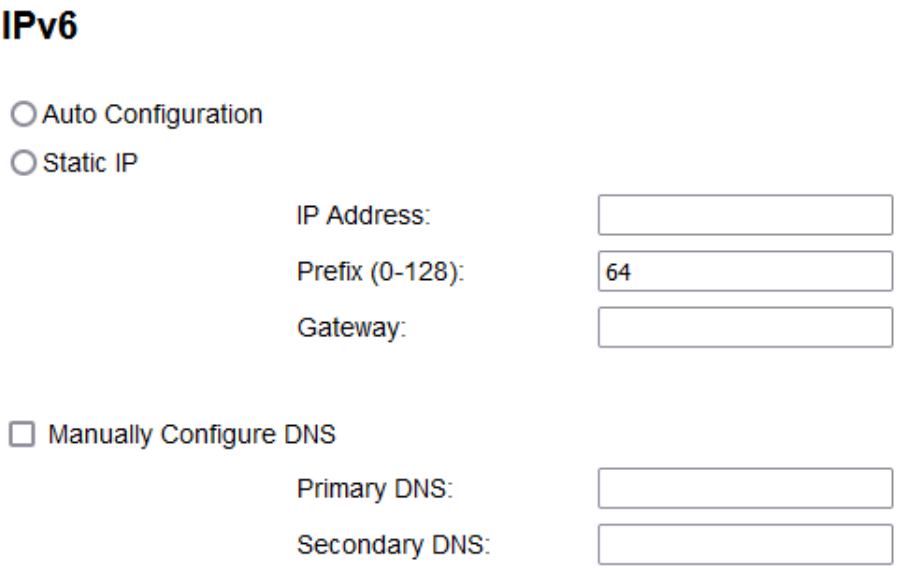
- Only qualified IT engineers who know TCP/IP principles and protocols are allowed to configure static IP settings.

Click the link for each setting to see the matching configuration file parameter in Section 6.6.3 Network Settings ("network" Module). Default values and ranges are listed there.

3.3.1.1 IPv4

Setting	Description
Disable	Disables all related IPv4 settings.
DHCP	DHCP is selected (enabled) by default, which means the HD10X will get its IP address, Subnet Mask, Gateway, and DNS Server(s) from the network. When DHCP is disabled, you must enter a static IP address for the HD10X, as well as addresses for the Subnet Mask, Gateway, and DNS Server(s).

Static IP	When Static IP is selected, you must enter a static IP address for the HD10X, as well as addresses for the Subnet Mask, Gateway, and DNS Server(s).
IP Address	If DHCP is disabled, enter a static IP address for the HD10X.
Subnet Mask	Enter the subnet mask.
Gateway	Enter the address of the default gateway (in this case, your router).
PPPoE	Select to enable PPPoE (Point-to-Point Protocol over Ethernet) mode.
Username	Enter your PPPoE account username.
Password	Enter your PPPoE account password.
Manually Configure DNS	Select to enable manual DNS configuration.
Primary DNS	If DHCP is disabled, enter addresses for the primary and secondary DNS servers.
Secondary DNS	



3.3.1.2 IPv6

Setting	Description
Disable	Disables all the related IPv6 settings
Auto Configuration	Auto configuration is selected (enabled) by default, which means the HD10X will get its IP address, Gateway, and DNS Server(s) from the network. When Auto Configuration is disabled, you must enter a static IP address for the HD10X, as well as addresses for the Gateway and DNS Server(s).
Static IP	When Static IP is selected, you must enter a static IP address for the HD10X, as well as an IPv6 address prefix, Gateway, and DNS Server(s).
IP Address	If Auto Configuration is disabled, enter a static IP address for the HD10X.
Prefix (0–128)	Enter the IPv6 address prefix length (0 to 128 bits).
Gateway	Enter the address of the default gateway (in this case, your router).
Manually Configure DNS	Select to enable manual DNS configuration.
Primary DNS	If Auto Configuration is disabled, enter addresses for the primary and secondary DNS servers.
Secondary DNS	

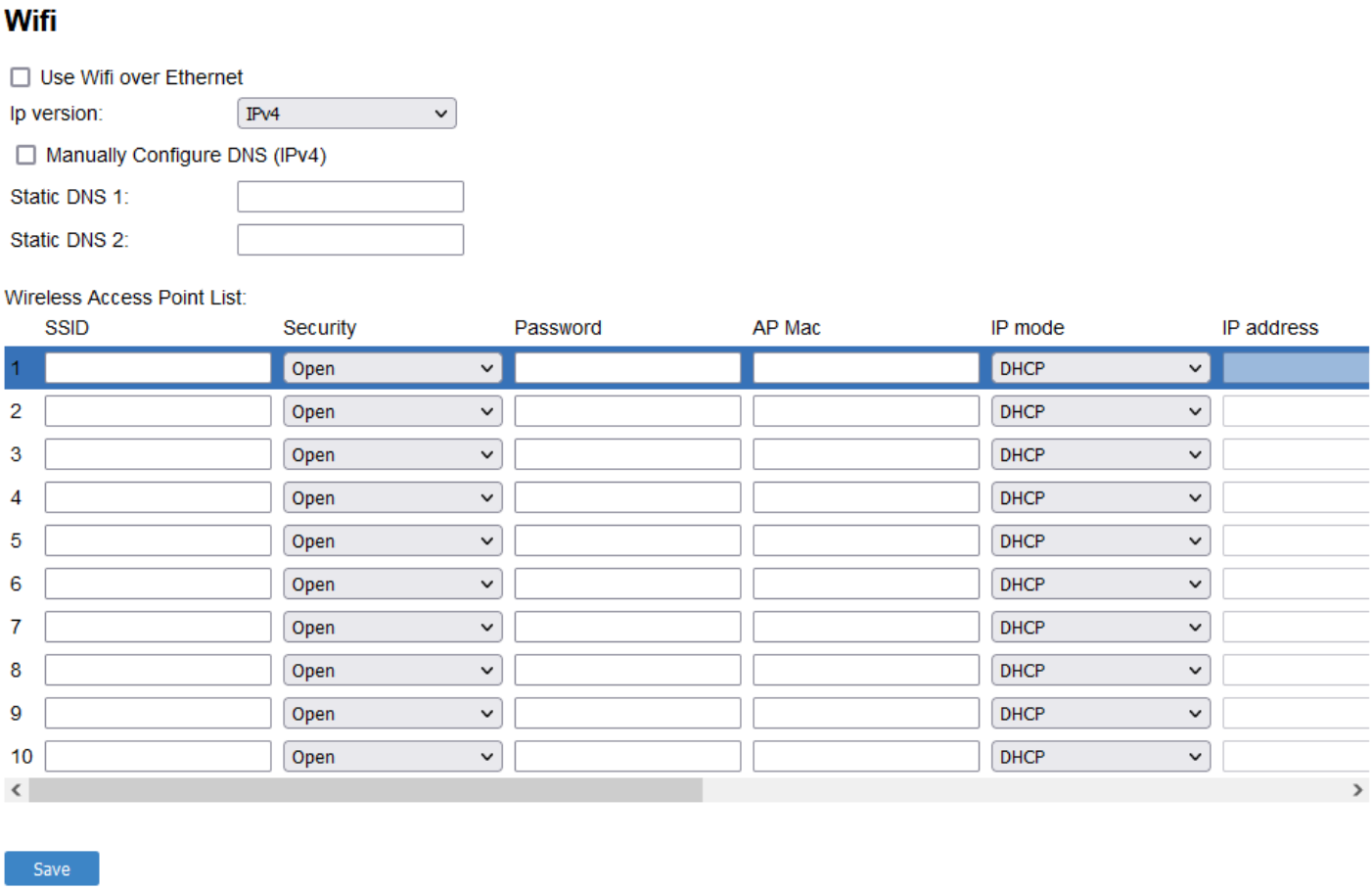
3.3.1.3 Wi-Fi

HD350W and HD351W support Wi-Fi feature.

Wi-Fi Access Points Setting

At least one Wi-Fi access point that can carry the Wi-Fi networks at the location is required.

Up to 10 Wi-Fi access points can be added.

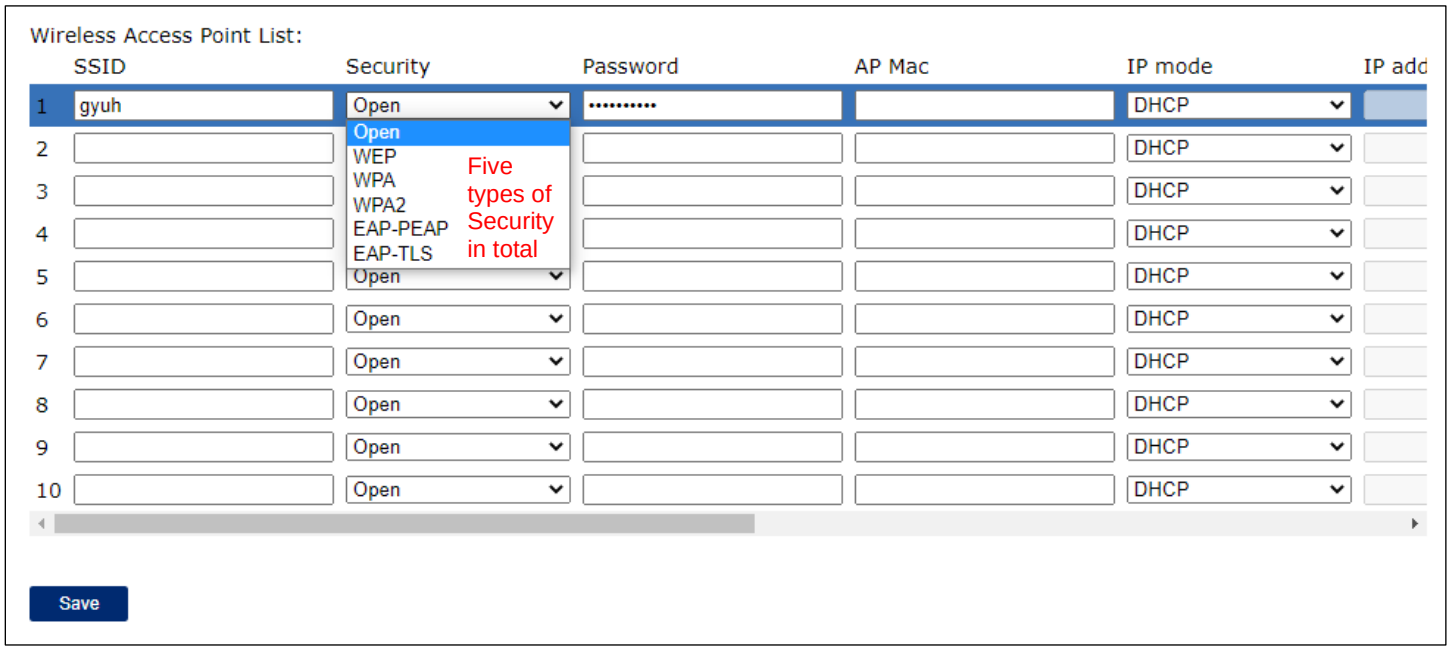


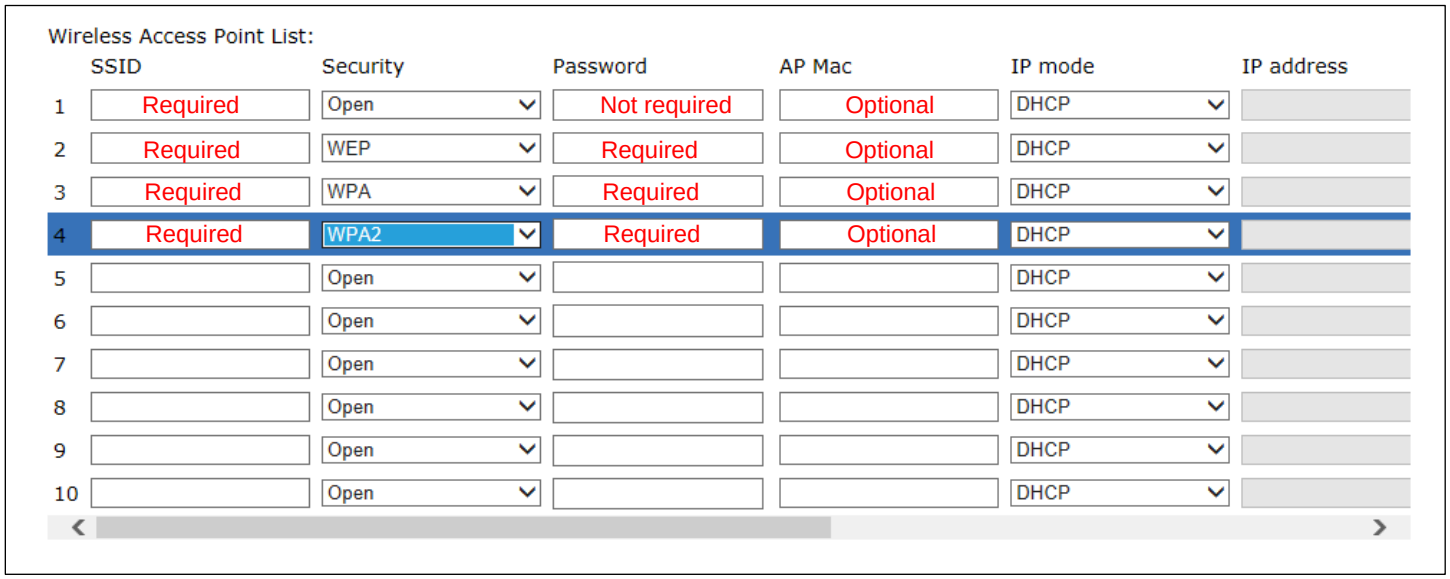
Wireless Access Point List:

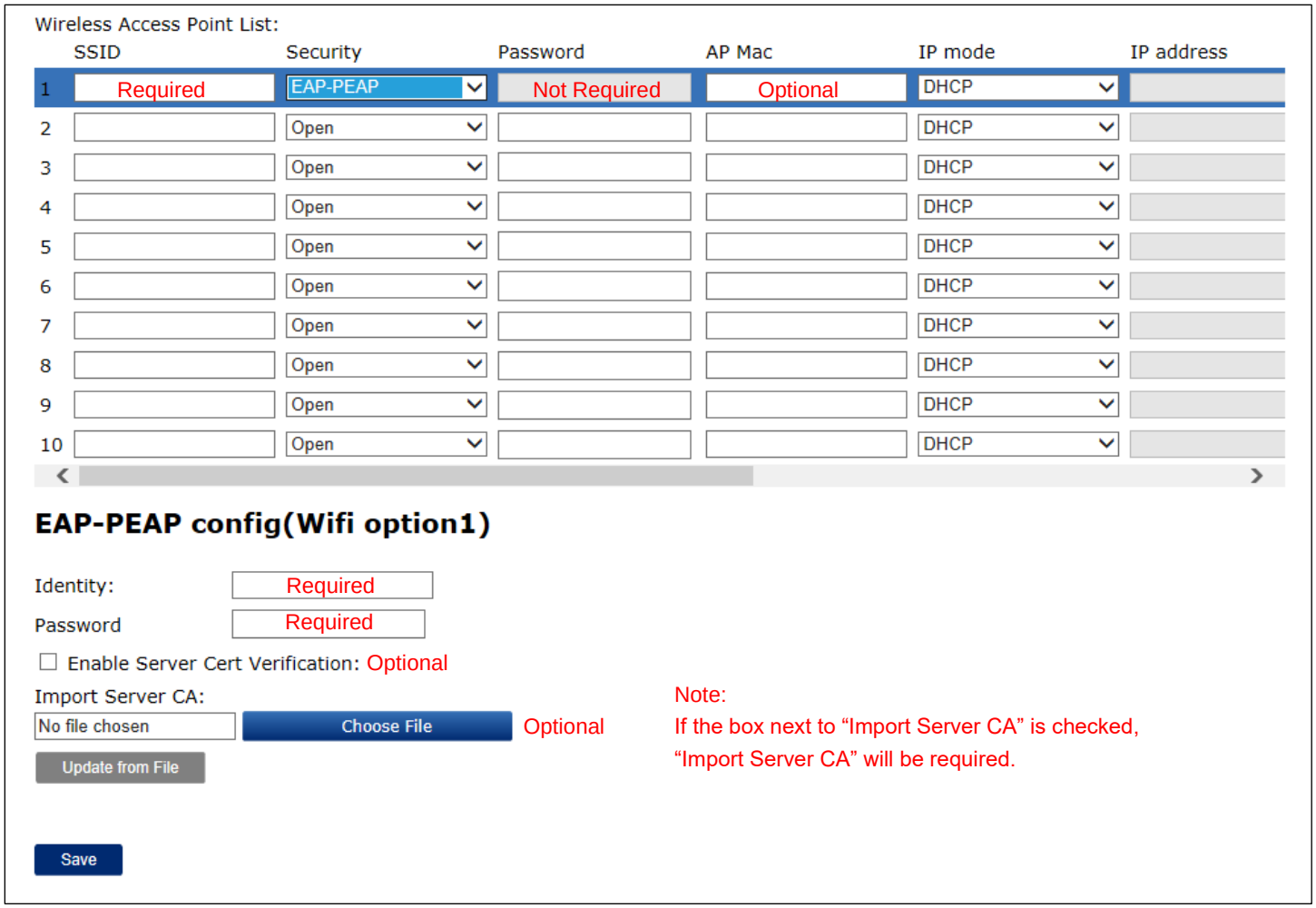
Entry	SSID	Security	Password	AP MAC	IP Mode
Value / Option		Open			DHCP
		WEP			
		WPA			
		WPA2			Static IP
		EAP-PEAP			
		EAP-TLS			
Description	Wi-Fi Access Point's SSID	Open: No authentication		Wi-Fi Access Point's MAC Address	
		WEP: Wired Equivalent Privacy			
		WPA: Wi-Fi Protected Access			
		WPA2: Wi-Fi Protected Access 2			
		EAP-PEAP: Extensible Authentication Protocol -			

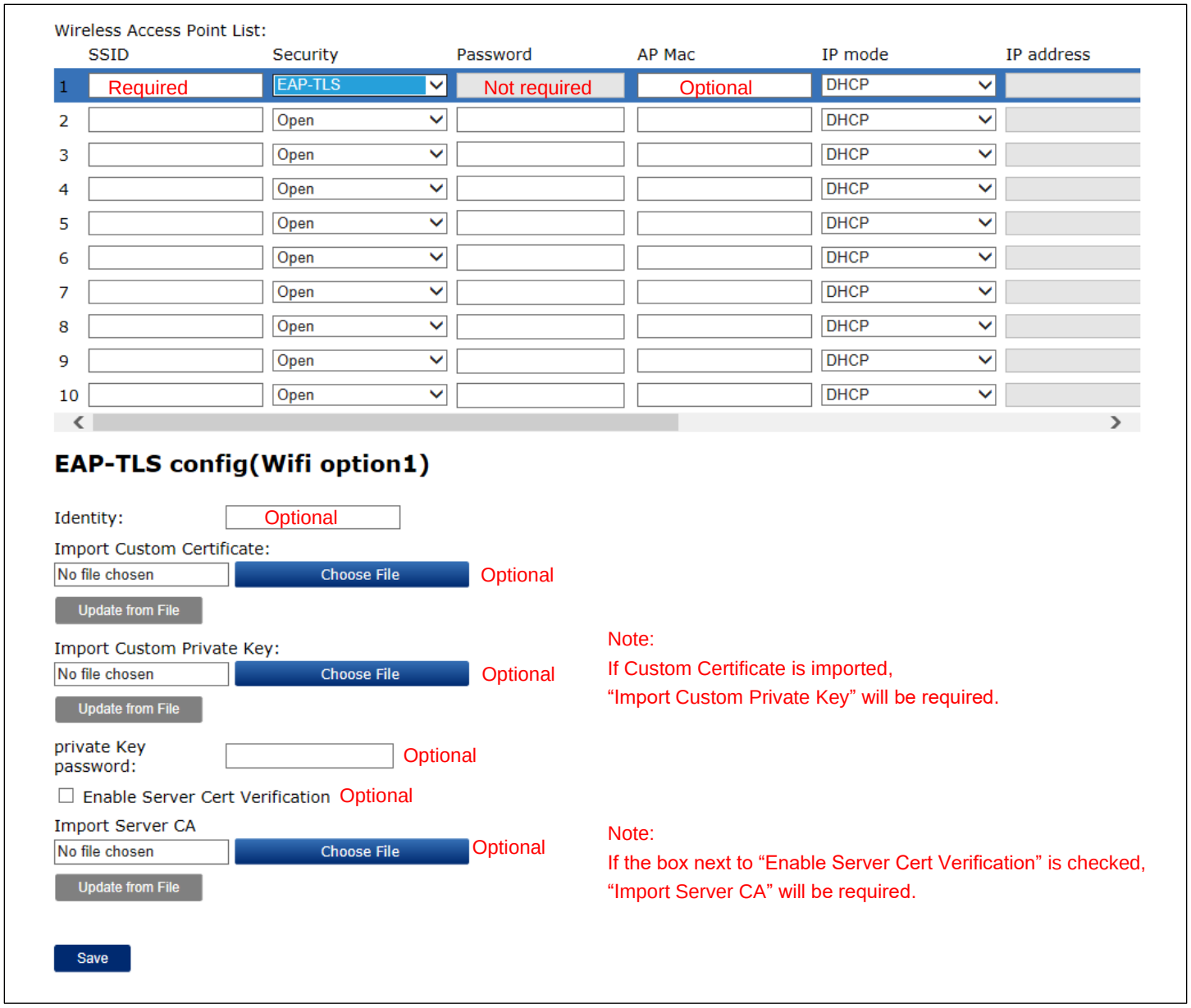
		Protected Extensible Authentication Protocol			
		EAP-TLS: Extensible Authentication Protocol - Transport Layer Security			

Entry	IP Address	Gateway	Subnet Mask	DNS 1	DNS 2
Value	Phone IP	Gateway IP	Phone subnet	DNS IP	
Description	Apply to Static IP Mode only				






Wireless Access Point List:
SSID
Security
Password
AP Mac
IP mode
IP address
1
Required
EAP-PEAP
Not Required
Optional
DHCP
2
Open
DHCP
3
Open
DHCP
4
Open
DHCP
5
Open
DHCP
6
Open
DHCP
7
Open
DHCP
8
Open
DHCP
9
Open
DHCP
10
Open
DHCP
EAP-PEAP config(Wifi option1)
Identity:
Required
Password
Required
Enable Server Cert Verification: Optional
Import Server CA:
No file chosen
Choose File
Optional
Update from File
Note:
If the box next to “Import Server CA” is checked,
“Import Server CA” will be required.
Save



Enable Wi-Fi Connection

Enable by Web Portal

1. Check the box next to “Use Wi-Fi over Ethernet”, and then Ethernet port is disabled.
2. Click **Save** to reboot the phone.

Enable by Configuration

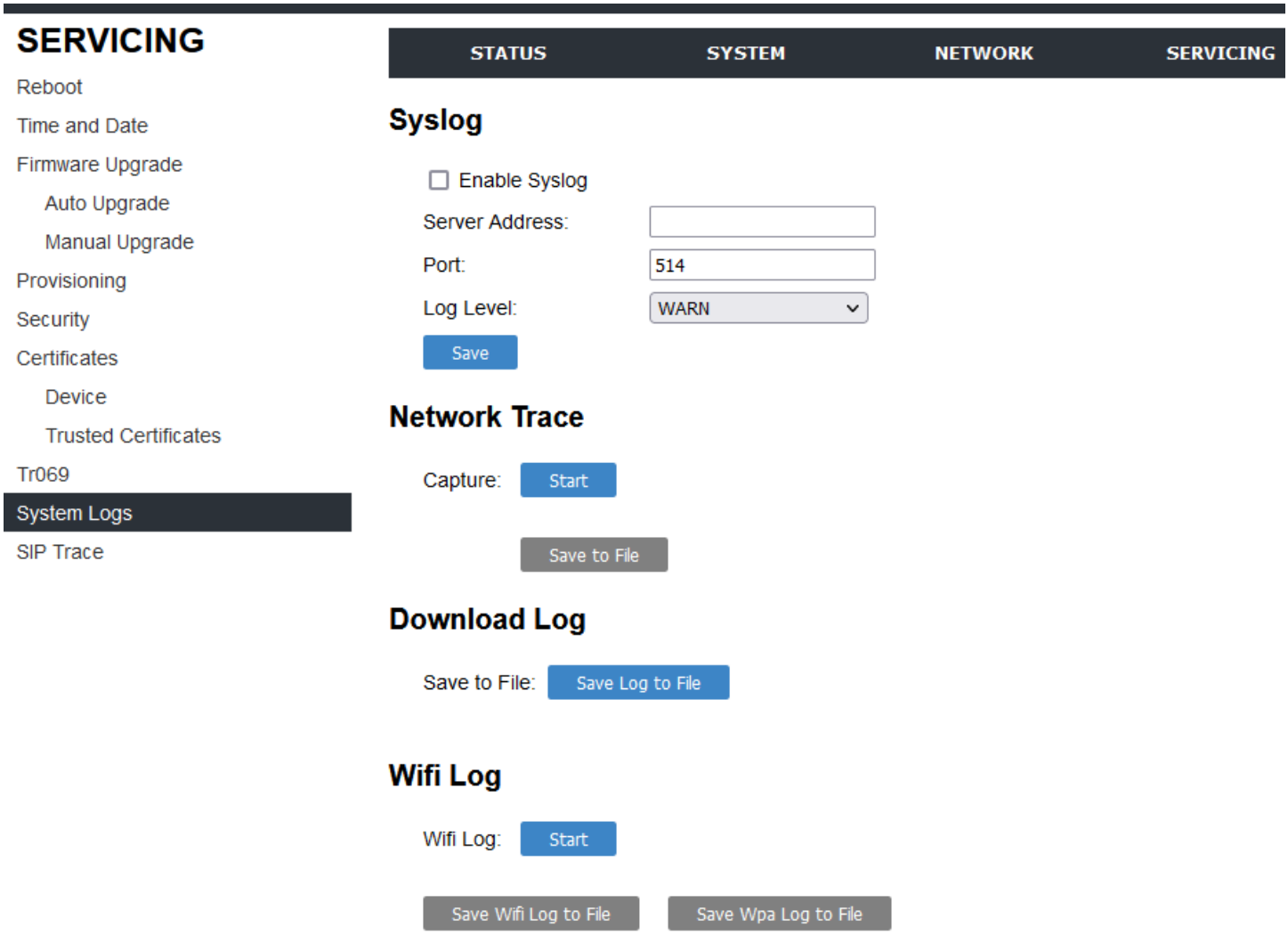
1. Set the network configuration by referring to Section 6.6.3 Network Module.
2. Reboot the phone manually.

Enable by Voice menu

1. Follow the steps of voice menu by referring to Chapter 5 Configure with Voice Menu - 1 Network Configuration.

2. When you are finished with the Voice menu, place the handset in the cradle.

Note: If you change any network settings, your phone will automatically reboot. This will enable your new settings to take effect.

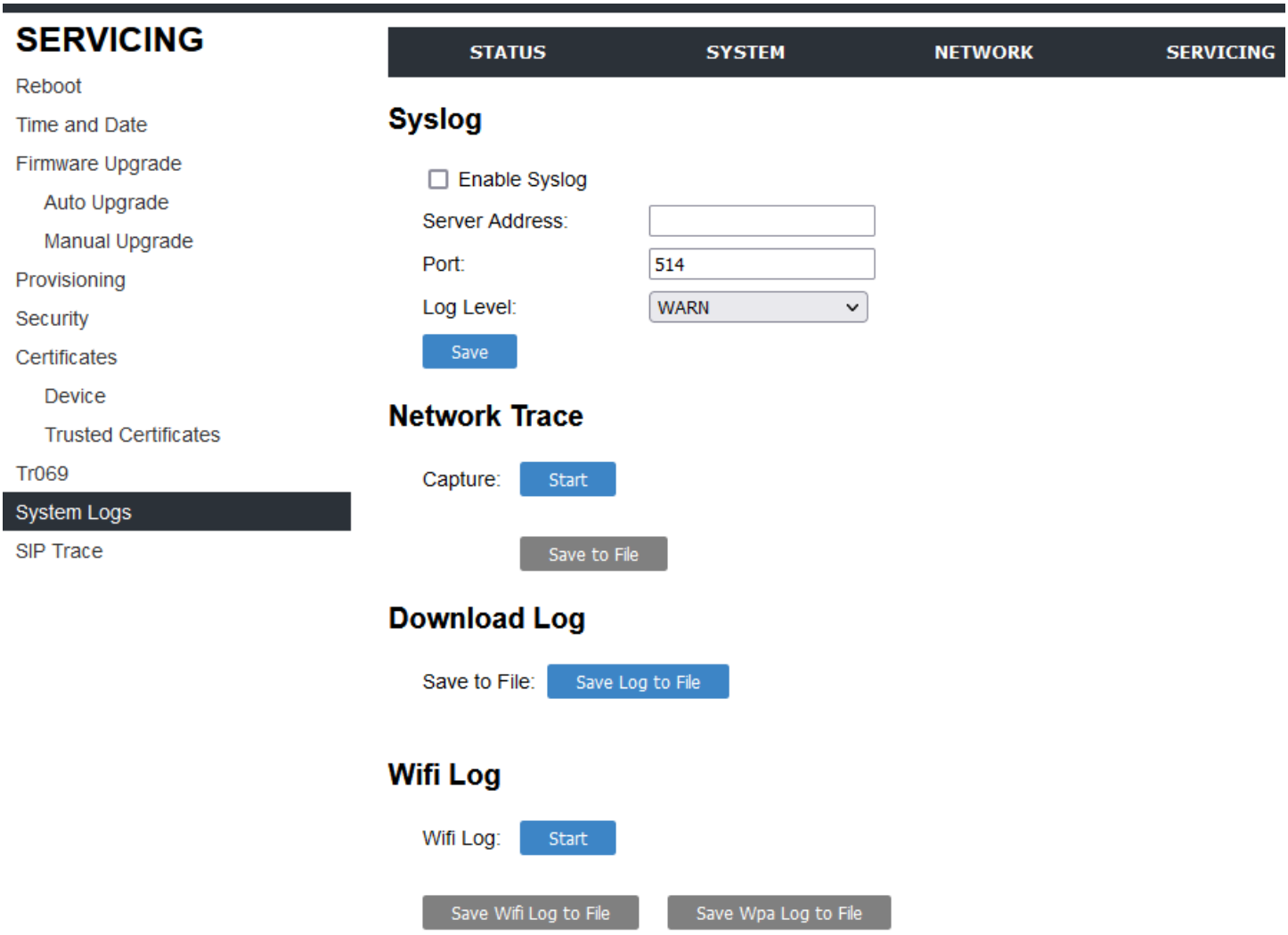


3.3.1.4 Note on Wi-Fi Access Point Setting for SIP Network

1. Use bridge mode not NAT mode
2. Enable SIP ALG (Application Layer Gateway) if available
3. Use Dual band (2.4G & 5G)
4. Disable DFS setting (dynamic frequency selection)

3.3.1.5 Download Wi-Fi log

If the phones cannot connect to the Wi-Fi network, please download a Wi-Fi log under **System Logs** and send it to technical support.

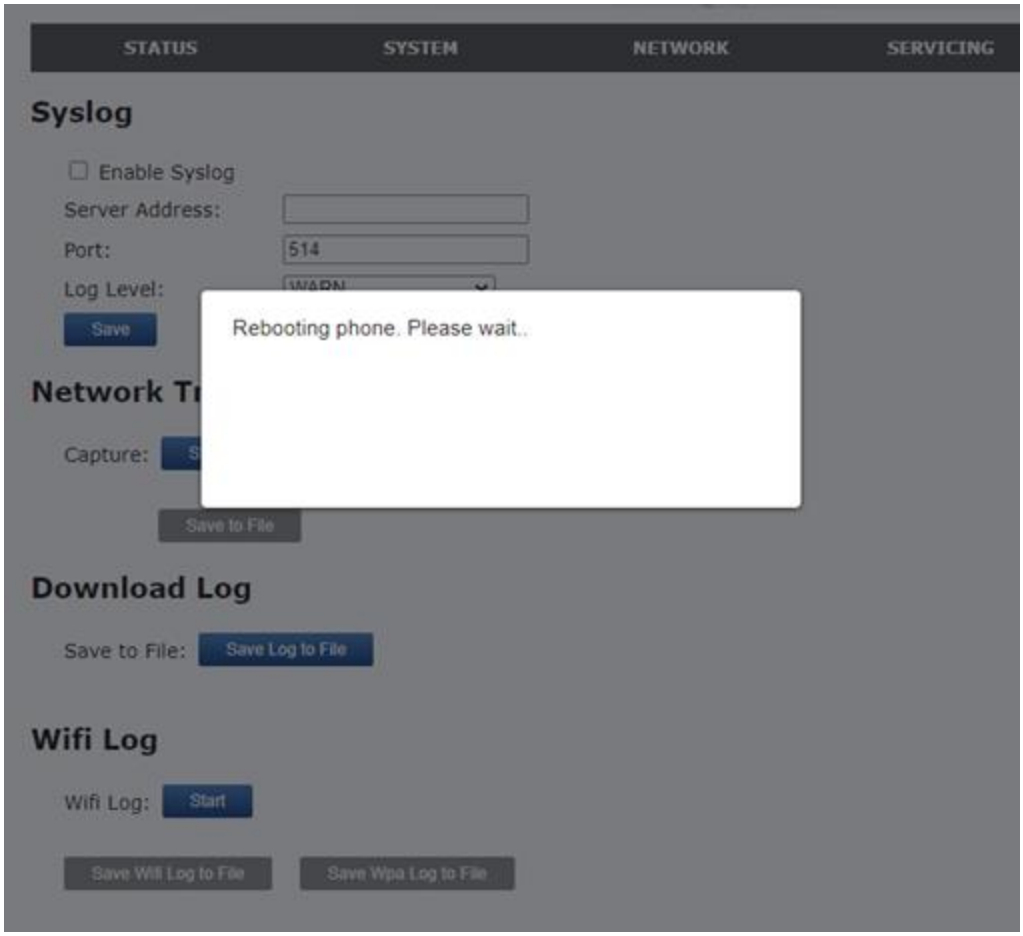


To download a Wi-Fi log:

1. Disable Wi-Fi connection by Voice menu:

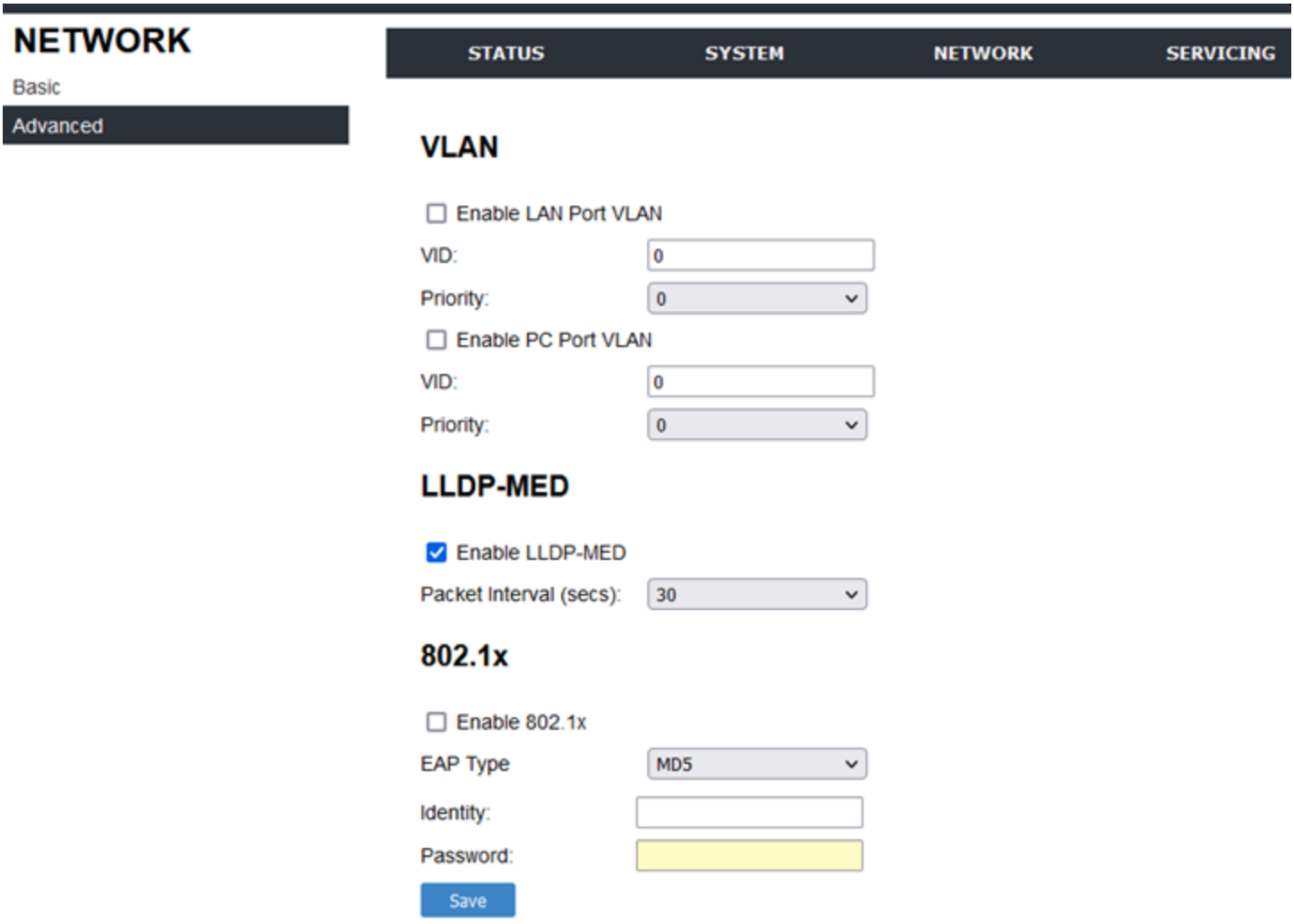
   Follow the steps of voice menu by referring to Chapter 5 Configure with Voice Menu - 1 Network Configuration.

2. Click **Start**. A window says “Rebooting phone. Please wait...” pops up. Wait until the system automatically logs out.



3. Log in the system and visit the **System Logs** page again. The text on the **Start** button switches to **Stop**.
4. Click **Save Wifi log to file** and then **Save Wpa log to File**.
5. Click **Stop**.

3.3.2 Advanced Network Settings



3.3.2.1 VLAN

You can organize your network and optimize VoIP performance by creating a virtual LAN for phones and related devices.

Click the link for each setting to see the matching configuration file parameter in Section 6.6.3 Network Settings ("network" Module). Default values and ranges are listed there.

Setting	Description
Enable LAN Port VLAN	Enable if the phone is part of a VLAN on your network. Select to enable.
VID	Enter the VLAN ID (vlan 5, for example).
Priority	Select the VLAN priority that matches the Quality of Service (QOS) settings that you have set for that VLAN ID. Outbound SIP packets will be marked and sent according to their priority. 7 is the highest priority. Note • To configure QOS settings for your router or switch is a subject outside the scope of this document.

3.3.2.2 LLDP-MED

Setting	Description
Enable LLDP-MED	Enables or disables Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED). LLDP-MED is a standards-based discovery protocol supported on some network switches. It is required for auto-configuration with VLAN settings.
Packet Interval (sec)	Set the LLDP-MED packet interval (in seconds).

3.3.2.3 802.1x

This section has been updated.

Setting	Description
Enable 802.1x	Enables or disables the 802.1x authentication protocol. This protocol allows the phone to attach itself to network equipment that requires device authentication via 802.1x.
Identity	Enter the 802.1x EAPOL identity
MD5 Password	Enter the 802.1x EAPOL MD5 password

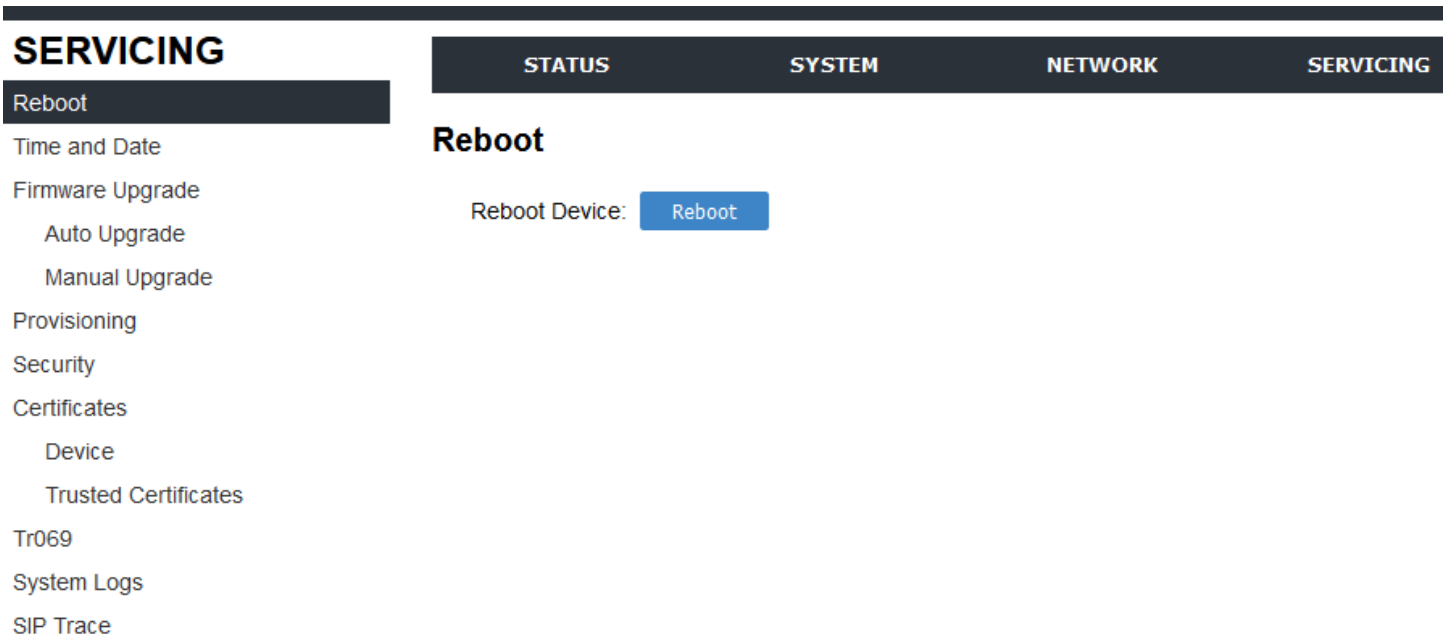
3.4 Configure Servicing Pages

On the Emergency Dialing Settings page, you can enable/disable and configure the Emergency Dialing feature.

If enabled, and the telephone goes off-hook for a period of time specified by the Delay timer, the pre-defined Phone Number will automatically be dialed.

3.4.1 Reboot

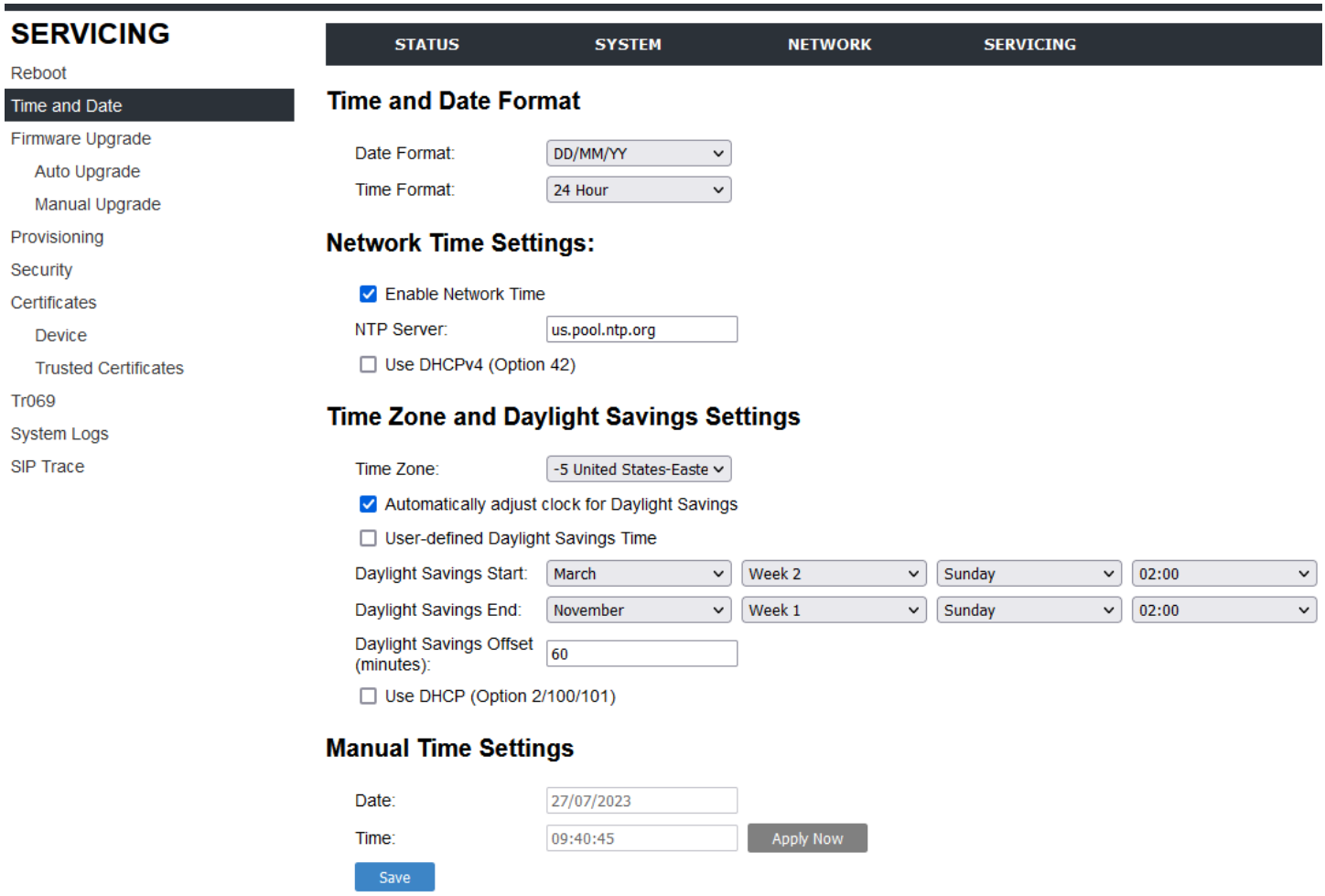
To manually reboot the HD10X and apply settings that you have updated, click **REBOOT**.



3.4.2 Time and Date

On the Time and Date page, you can manually set the time and date, and the time and date formats. You can also set the system time to follow a Network Time Protocol (NTP) Server (recommended) or you can set the time and date manually.

The time and date settings are also available as parameters in the configuration file. See Section 6.6.5 Time and Date Settings ("time_date" Module).



3.4.2.1 Time and Date Format

Click the link for each setting to see the matching configuration file parameter in Section 6.6.5 Time and Date Settings ("time_date" Module). Default values and ranges are listed there.

Setting	Description
Date Format	Set the date format.
Time Format	Set the clock to a 24-hour or 12-hour format.

3.4.2.2 Network Time Settings

Setting	Description
Enable Network Time	Enables or disables getting time and date information for your phone from the Internet.
NTP Server	If Enable Network Time is selected, enter the URL of your preferred time server.
Use DHCP (Option 42)	If Enable Network Time is selected, select to use DHCP to locate the time server. Option 42 specifies the NTP server available to the phone. When enabled, the phone obtains the time in the following priority: 1. Option 42 2. NTP Server 3. Manual time

3.4.2.3 Time Zone and Daylight Savings Settings

Setting	Description
Time Zone	Select your time zone from the list.
Automatically adjust clock for Daylight Savings	Select to adjust the clock for daylight savings time according to the NTP server and time zone setting. To disable daylight savings adjustment, disable both this setting and User-defined Daylight Savings Time.
User-defined Daylight Savings Time	Select to set your own start and end dates and offset for Daylight Savings Time. To disable daylight savings adjustment, disable both this setting and Automatically adjust clock for Daylight Savings
Daylight Savings Start: • Month • Week • Day • Hour	If User-defined DST is enabled, set the start date and time for daylight savings: Month, week, day, and hour.
Daylight Savings End: • Month • Week • Day • Hour	If User-defined DST is enabled, set the end date and time for daylight savings: Month, week, day, and hour.
Daylight Savings Offset (minutes)	If User-defined DST is enabled, this will specify the daylight savings adjustment (in minutes) to be applied when the current time is between Daylight Savings Start and Daylight Savings End.
Use DHCP (Option 2/100/101)	If Enable Network Time is selected, select to use DHCP to determine the time zone offset. Options 2, 100 and 101 determine time zone information.

3.4.2.4 Manual Time Settings

If Enable Network Time is disabled or if the time server is not available, use **Manual Time Settings** to set the current time.

Setting	Description
Date	Select the current year, month, and day. Click the Date field and select the date from the calendar that appears.
Time	Set the current hour, minute, and second. Click the Time field, and enter the current time. You can also refresh the page to update the manual time settings.

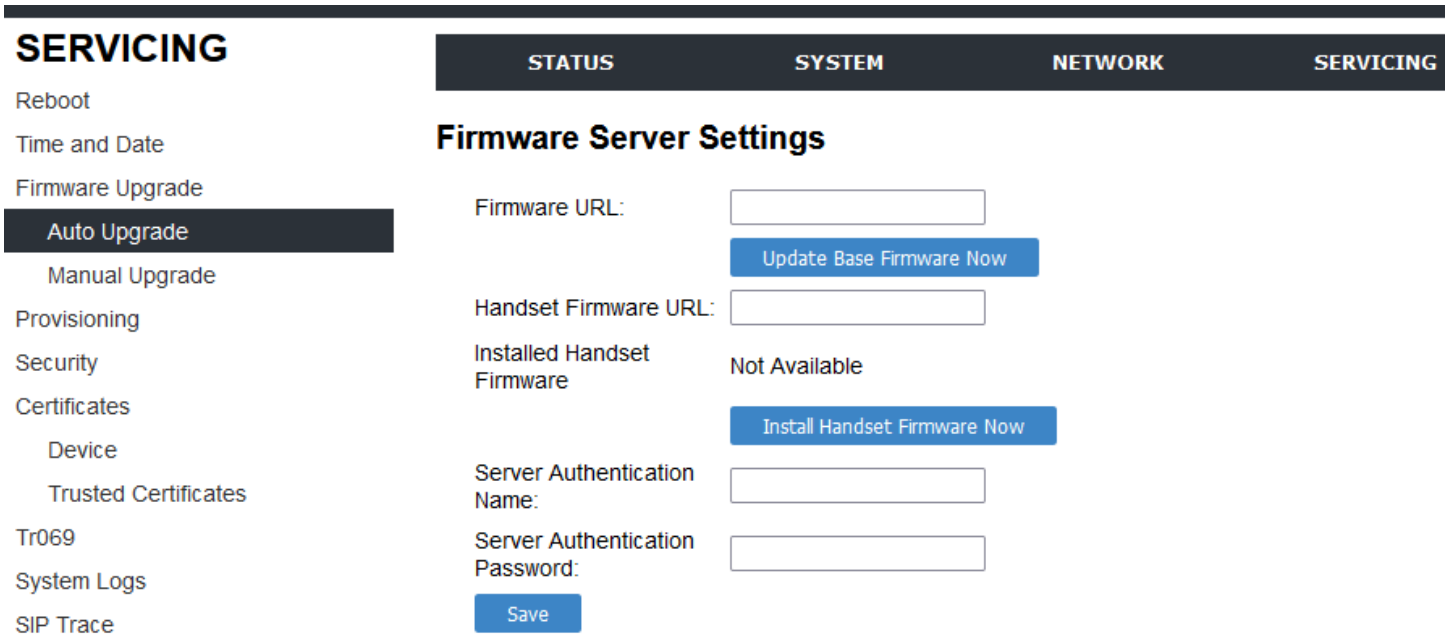
Click **Apply Now** to start the HD10X using the manual time settings.

3.4.3 Firmware Upgrade

You can update the HD10X with new firmware using the following methods:

- Retrieving a firmware update file from a remote host computer and accessed via a URL. This central location may be arranged by you, an authorized dealer, or your SIP service provider. Enter the URL under **Firmware Server Settings**.
- Using a file located on your computer or local network. No connection to the Internet is required. Consult your dealer for access to firmware update files. Click **Manual Upgrade** to view the page. where you can manually upgrade the HD10X firmware.

The firmware upgrade settings are also available as parameters in the configuration file. See Section 6.6.4 Provisioning Settings ("provisioning" Module).



3.4.3.1 Firmware Server Settings

Click the link for each setting to see the matching configuration file parameter in Section 6.6.4 Provisioning Settings ("provisioning" Module). Default values and ranges are listed there.

Setting	Description
Firmware URL	The URL where the HD10X telephone base firmware update file resides. This should be a full path, including the file name of the firmware file.
Handset Firmware URL	The URL where the HD10X cordless handset firmware update file resides. This should be a full path, including the file name of the firmware file.
Installed Handset Firmware	The version number of handset firmware currently installed.
Installed Color Handset Firmware	The version number of color handset firmware currently installed.
Server authentication name	Authentication username for the firmware server
Server authentication password	Authentication password for the firmware server

To update the firmware immediately:

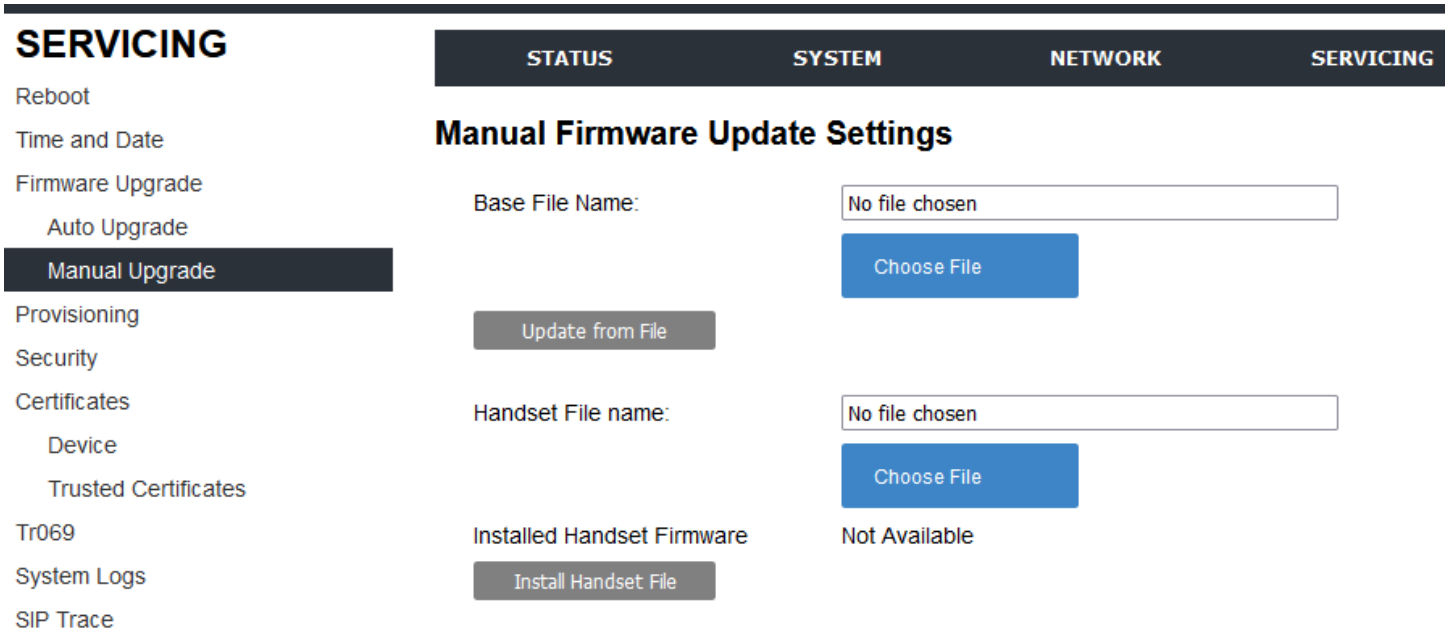
- Click **Update Base Firmware Now** or **Install HS Firmware Now**.

Note

- You can also configure the HD10X to check for firmware updates at regular intervals. See Section 3.4.4.Provisioning.

3.4.3.2 Manual Firmware Update and Upload

On the Manual Firmware Update Settings page, you can upgrade the HD10X / HM201 telephone base and cordless handset firmware using a file located on your computer or local network. To upload color handset firmware, the base's software version should be 2.22.6.0 or later.



To update the firmware using a file on your computer or local network:

1. On **Manual Firmware Update** page, click **CHOOSE FILE** to locate and open the firmware update file.
2. Click **UPDATE FROM FILE** or **INSTALL HS FILE**.

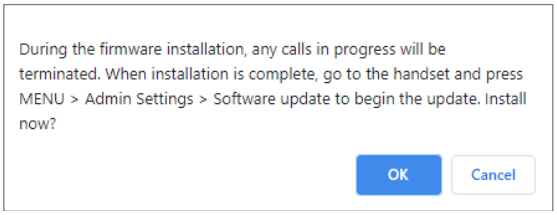
After clicking **UPDATE FROM FILE**, the HD10X will update its firmware and restart. If you are updating handset firmware, you must perform one more procedure after clicking **INSTALL HS FILE**. See Section 3.4.3.3 Updating a Cordless Handset below.

3.4.3.3 Updating a Cordless Handset

Updating DECT cordless handset firmware using the Web Portal is a two-step process. First, you must download the handset firmware and install it on the telephone base. Second, you must install the handset firmware on the handset. The handset downloads the firmware over the air from the telephone base.

To install the handset firmware on the telephone base:

1. To install the handset firmware: Click **INSTALL HS FIRMWARE NOW** on the Firmware Server update page, or **INSTALL HS FILE** on the **Manual Firmware update** page. The confirmation dialog box shown below appears.



2. To begin installing the handset firmware, click **OK**. The message "Installing handset firmware. Please wait... "appears. To cancel the download, click **CANCEL**.
   After clicking **OK**, the message System update in progress. "Please wait... " appears on the handset. After a successful update, the message Firmware installation successful appears on the Web Portal.

An error message appears if:

- The handset firmware is already up to date.
- The handset firmware URL is incorrect, or the file cannot be retrieved for any other reason.
- The handset firmware file is corrupted.
- The handset doesn't recognize the firmware file. For example, the firmware file may belong to a different product.

To install the firmware on the cordless handset:

Note

- Your cordless handset will automatically initiate the firmware update after a short period of time, as long as there are no active calls on the base station. If you wish to manually start the firmware update, perform the steps below.
  1. On the handset, press **MENU**, and then select Admin settings.
  2. Enter the admin password. The default is admin. To switch between entering upper or lower- case letters, press the ***** key.
  3. On the Admin settings menu, select Firmware update. The handset checks for new firmware. If new firmware is found, the handset screen asks you to proceed with the update.

Note

- Only one handset at a time can perform a firmware update. The base LEDs flash to indicate the base is busy and all incoming calls are rejected while the update is in progress.

3.4.4 Provisioning

Provisioning refers to the process of acquiring and applying new settings for the HD10X using configuration files retrieved from a remote computer. After a HD10X is deployed, subsequent provisioning can update the HD10X with new settings; for example, if your service provider releases new features. See also Section 6.6.4 Provisioning Settings ("provisioning" Module).

With automatic provisioning, you enable the HD10X to get its settings automatically - the process occurs in the background as part of routine system operation. Automatic provisioning can apply to multiple devices simultaneously.

With manual provisioning on the Web Portal, you update the HD10X settings (configuration and/ or firmware) yourself via SERVICING > Provisioning > Import Configuration and/or SERVICING > Firmware Upgrade > Manual Upgrade. Manual provisioning can only be performed on one HD10X at a time.

On the Provisioning page, you can enter settings that will enable the HD10X to receive automatic configuration and firmware updates. The Provisioning page also allows you to manually update HD10X configuration from a locally stored configuration file using an Import function. You can also export the HD10X configuration - either to back it up or apply the configuration to another HD10X in the future - to a file on your computer.

The provisioning process functions according to the Resynchronization settings and Provisioning Server Settings. The HD10X checks for the provisioning URL from the following sources in the order listed below:

1. PnP - Plug and Play Subscribe and Notify protocol
2. DHCP Options
3. Preconfigured URL - Any HD10X updated to the latest firmware release will have the Redirection Server URL available as the default Provisioning Server URL (see Section 3.4.4.1 Provisioning Server.)

Note

- Using the Redirection Service requires contacting the support team for an account.

If one of these sources is disabled, not available, or has not been configured, the HD10X proceeds to the next source until reaching the end of the list.

The provisioning settings are also available as parameters in the configuration file. See Section 6.6.4 Provisioning Settings ("provisioning" Module).

3.4.4.1 Provisioning Server

Setting	Description
Server URL	URL of the provisioning file(s). The format of the URL must be RFC 1738 compliant, as follows: "<schema>://<user>:<password>@ <host>:<port>/<url-path>" "<user>:<password>@" may be empty. "<port>" can be omitted if you do not need to specify the port number.
Server Authentication Name	User name for access to the provisioning server
Server Authentication Password	Password for access to the provisioning server

3.4.4.2 Plug-and-Play Settings

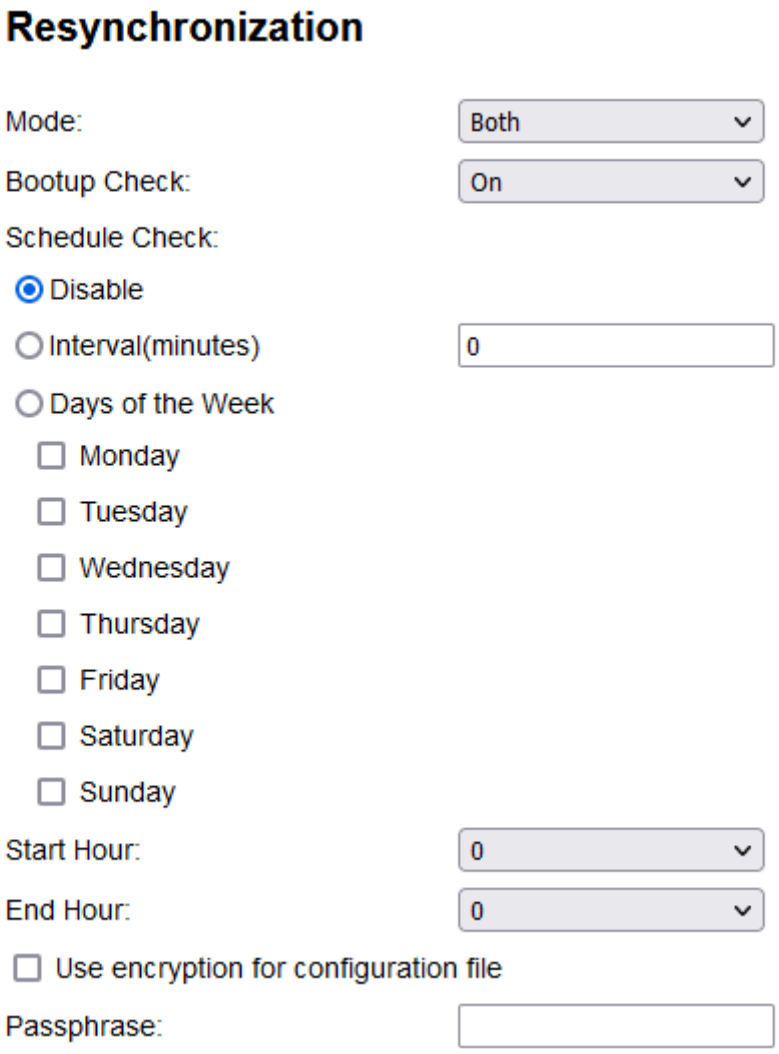
Setting	Description
Enable PnP Subscribe	Select to enable the HD10X to search for the provisioning URL via a SUBSCRIBE message to a multicast address (224.0.1.75). The HD10X expects the server to reply with a NOTIFY that includes the provisioning URL. The process times out after five attempts.

3.4.4.3 DHCP Settings

Setting	Description
Use DHCP Options	Enables the HD10X to use DHCP options to locate and retrieve the configuration file. When selected, the HD10X automatically attempts to get a provisioning server address, and then the configuration file. If DHCP options do not locate a configuration file, then the server provisioning string is checked. Note • Ensure that DHCP is also enabled on the Basic Network Settings page.
DHCP Option Priority 1	If DHCP is enabled, Set the DHCP Option priority. Select the highest priority option.
DHCP Option Priority 2	If DHCP is enabled, Set the DHCP Option priority. Select the second highest priority option.
DHCP Option Priority 3	If DHCP is enabled, Set the DHCP Option priority. Select the third highest priority option.
Vendor Class ID (DHCP 60)	DHCP Option 60 is available to send vendor-specific information to the DHCP Server.
User Class Info (DHCP 77)	DHCP Option 77 is available to send vendor-specific information to the DHCP Server.

3.4.4.4 Resynchronization

On the Resynchronization page, you can select how and when the phone checks for updated firmware and/or configuration files.

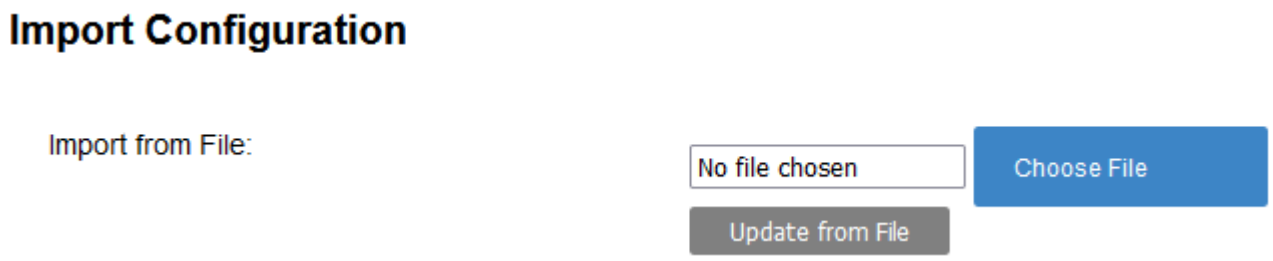


Setting	Description
Mode	Sets which files for which the HD10X checks. It can check for configuration files, firmware update files (from the URL entered on the Firmware Server Settings page), or both. Note • Ensure that DHCP is also enabled on the Basic Network Settings page: When checking for both configuration and firmware files, the firmware URL can be within the config file. This firmware URL precedence over the URL on the Firmware Server Settings page. It will also update the URL on the Firmware Server Settings page. This allows you to change the firmware URL automatically.
Bootup Check	Sets the HD10X to check the provisioning URL for new configuration and/ or firmware files upon bootup. The update is applied as part of the reboot process.

Schedule Check: Disable	When selected, disables regularly scheduled file checking.
Schedule Check: Interval	Sets an interval for checking for updates. After selecting Interval, enter the interval in minutes between update checks.
Schedule Check: Days of the Week	Select to enable weekly checking for updates on one or more days. After selecting Days of the Week, select the day(s) on which the HD10X checks for updates.
Start Hour	Select the hour of the day on which the HD10X checks for updates.
End Hour	Select the hour of the day on which the HD10X stops checking for updates.
Use encryption for configuration file	Enables an AES-encrypted configuration file to be decrypted before being applied to the HD10X. Select if the configuration file has been secured using AES encryption.
Passphrase	If the configuration file has been secured using AES encryption, enter the 16-bit key.

3.4.4.5 Import Configuration

You can configure the HD10X by importing a configuration file from your computer or your local network. For more information about configuration file types and configuration file formatting, see Chapter 6 Provisioning Using Configuration Files.



To import a configuration file:

1. Click **CHOOSE FILE** to locate and open the configuration file.
2. Click **UPDATE FROMFILE**.

The HD10X will update its configuration.

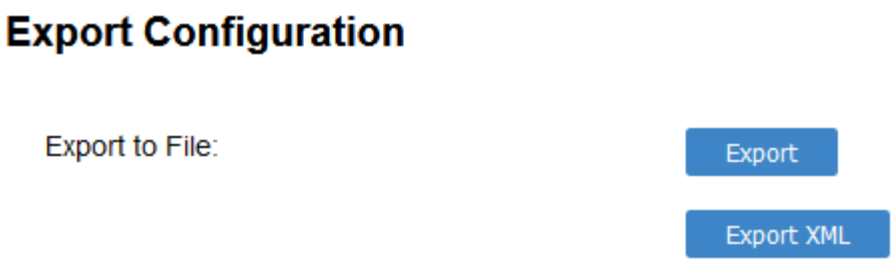
Manually importing a configuration file differs from the auto-provisioning process in that:

- The HD10X does not check whether the file has been loaded before. The configuration file is processed whether or not it is different from the current version.
- The HD10X will restart immediately after importing the configuration file, without waiting for one minute of inactivity.

3.4.4.6 Export Configuration

You can export all the settings you have configured on the Web Portal and save them as a configuration file on your computer. You can then use this configuration file as a backup, or use it to update other phones.

Under **Export Configuration**, you can also reset the phone to its default configuration.



The exported configuration file will contain the following passwords in plain text:

- SIP account authentication password
- EAPOL password
- Firmware server password
- Provisioning server password
- Encryption passphrase
- LDAP server password

Please ensure that you save the exported configuration file in a secure location.

To export the configuration file:

- Click **EXPORT**.

The format of the exported file is <model name>_<mac address>.cfg. For example, HD10X_00041367803C.cfg

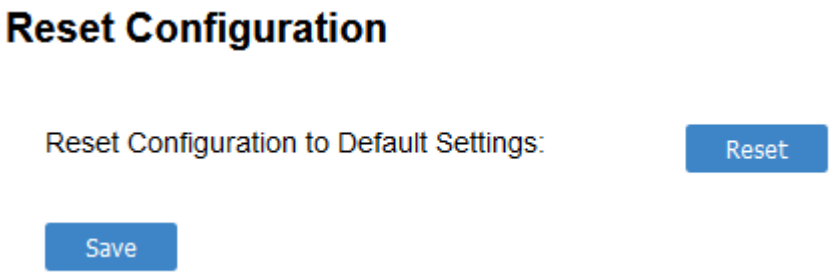
Exporting a configuration file generates two header lines in the configuration file. These header lines provide the model number and software version in the following format:

#Model Number = xxxxxxx
#SW Version = xxxxxxx

You can use the exported file as a general configuration file, and duplicate the settings across multiple units. However, ensure that you edit the file to remove any MAC-specific SIP account settings before applying the general configuration file to other units.

3.4.4.7 Reset Configurations

You can reset the phone to its default settings.



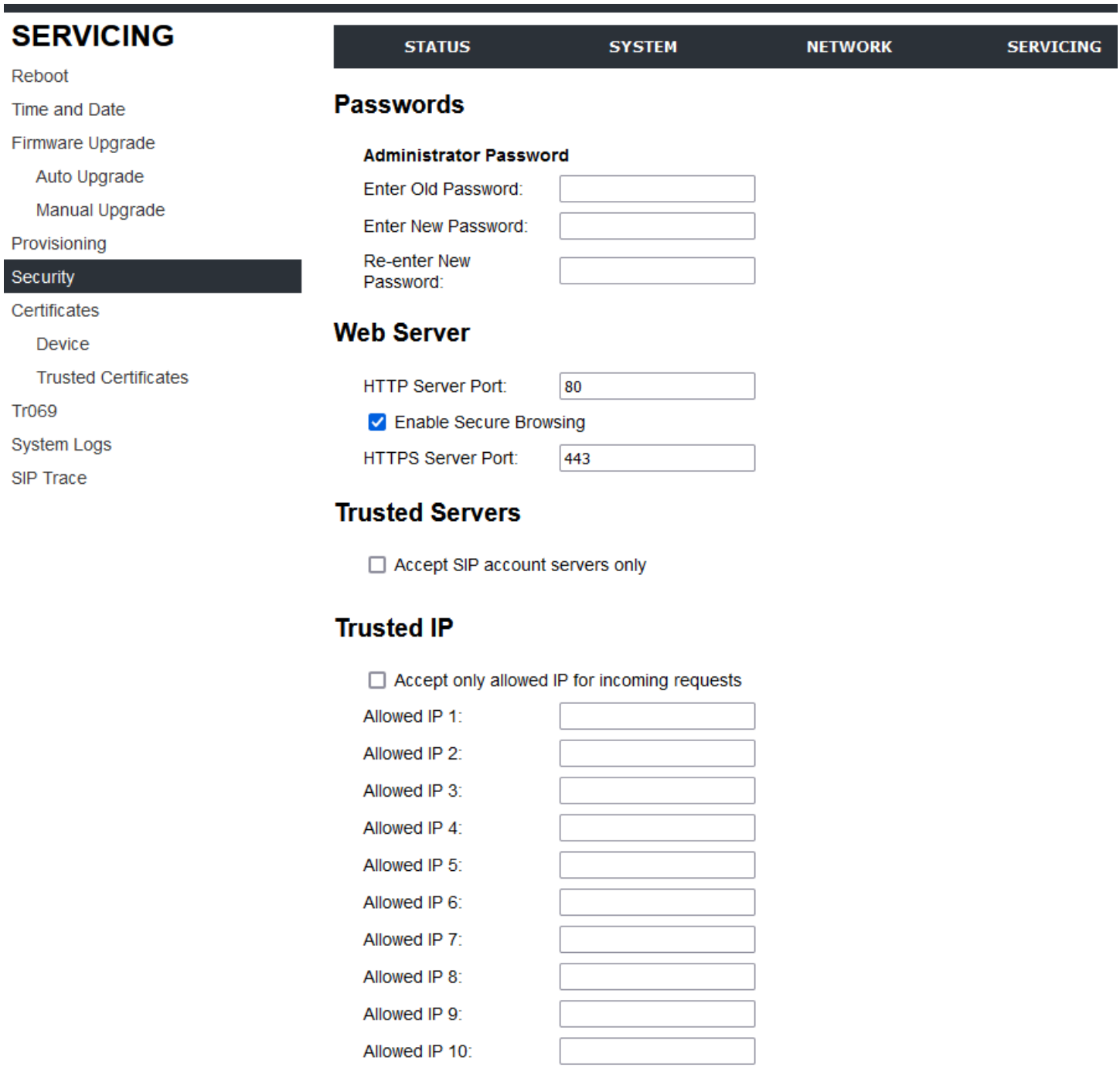
To reset the HD10X to its default configuration:

1. Under **Reset Configuration**, click **RESET**.
2. When the confirmation box appears, click **OK**.

3.4.5 Security

On the Security page you can reset the admin password, reset the user password, and enter web server settings.

The security settings are also available as parameters in the configuration file. See Section 6.6.7 Web Settings ("web" Module).



3.4.5.1 Passwords

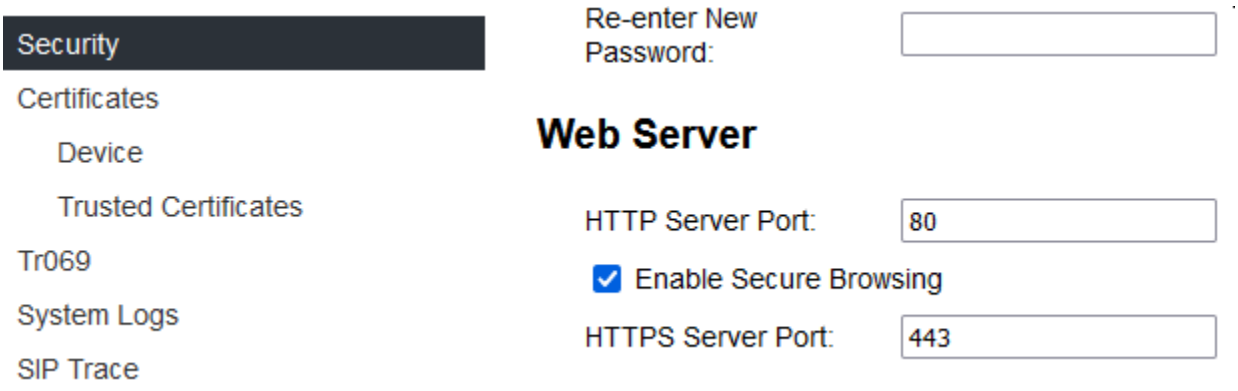
You can set the administrator password and user password on the Web Portal or by using provisioning.

To change the admin password:

1. Enter the old password (for a new HD10X, the default password is admin).
2. Enter and re-enter a new password. The password is case sensitive and can consist of both numbers and letters (to a maximum of 15 characters).
3. Click **SAVE**.

3.4.5.2 Web Server

You can set the administrator password and user password on the Web Portal or by using provisioning.



Setting	Description
HTTP Server Port	Port used by the HTTP server.
Enable Secure Browsing	Set the server to use the HTTPS protocol.
HTTPS Server port	Port used by the HTTPS server.

To configure Web Server Settings:

1. Enter the HTTP Server port number. The default setting is 80.
2. Enable or Disable Secure Browsing. When enabled, the HTTPS protocol is used, and you must select the HTTPS server port in the next step.
3. Enter the HTTPS server port number. The default setting is 443.

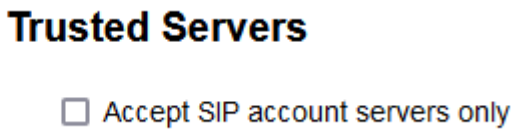
Note: Changing the Web Server settings will reboot the HD10X.

3.4.5.3 Trusted Servers

The Trusted Servers setting provides a means of blocking unauthorized SIP traffic. When enabled, each account's Registration server, SIP server, Outbound Proxy server and Backup Outbound Proxy server will be used as sources for trusted SIP traffic. All unsolicited SIP traffic (for example, INVITE, NOTIFY, unsolicited MWI, OPTIONS) will be blocked unless it is from one of the trusted servers with the enabled

accounts.

If additional trusted sources are required beyond what has been specified with the enabled accounts (for example, if IP dialing or other types of server traffic need to be secured), use the **Trusted IP settings** on the Security page.



Setting	Description
Accept SIP account servers only	Enable or disable using the account servers as sources for trusted SIP traffic.

3.4.5.4 Trusted IP

In addition to the Trusted Servers setting, incoming IP traffic can be filtered using an **Allowed IP** list of IP addresses. When this means is enabled, all unsolicited IP traffic will be blocked unless it is from one of the trusted IP addresses on the **Allowed IP** list.

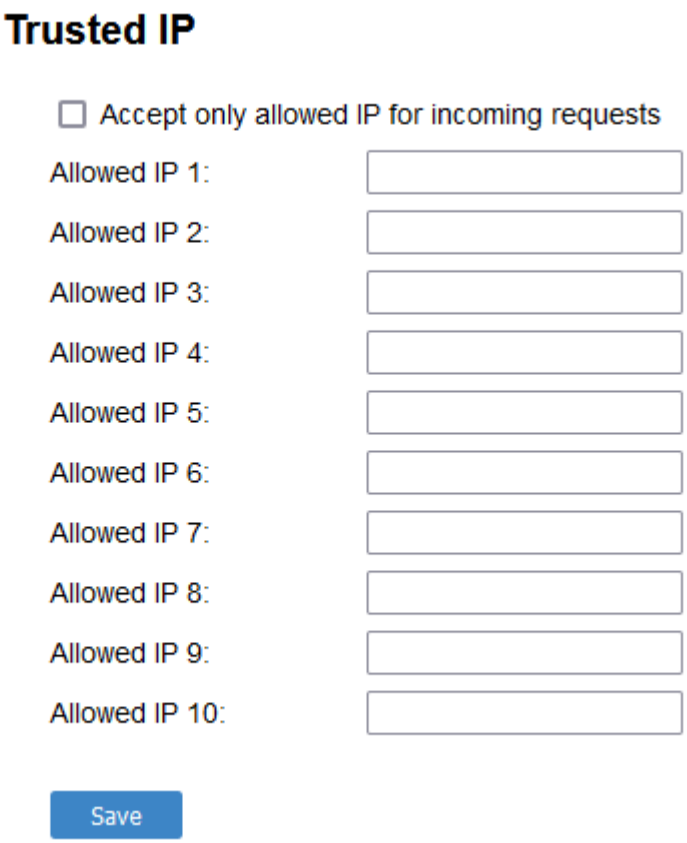
You can enter the **Allowed IP** list in the 10 fields on the **Trusted IP** section. Entries on the **Allowed IP** list must be specified as IP addresses (IPv4 or IPv6).

Three formats are supported for entries on the **Allowed IP** list:

1. IP range specified using CIDR notation (defined in rfc4632). IPv4 or IPv6 address followed by a prefix, for example, 192.168.0.1/24.
2. IP range specified with a pair of starting and ending IPv4 or IPv6 addresses, separated by '-' (for example, 192.168.0.1-192.168.5.6).
   - No space before or after '-'
   - Both starting IP & ending IP have to be with the same IP version
   - Starting IP has to be smaller than the ending IP; otherwise, all traffic will be dropped.
3. Single IP address in IPv4 or IPv6.

Note

- Changing the Web Server settings will reboot the HD10X.



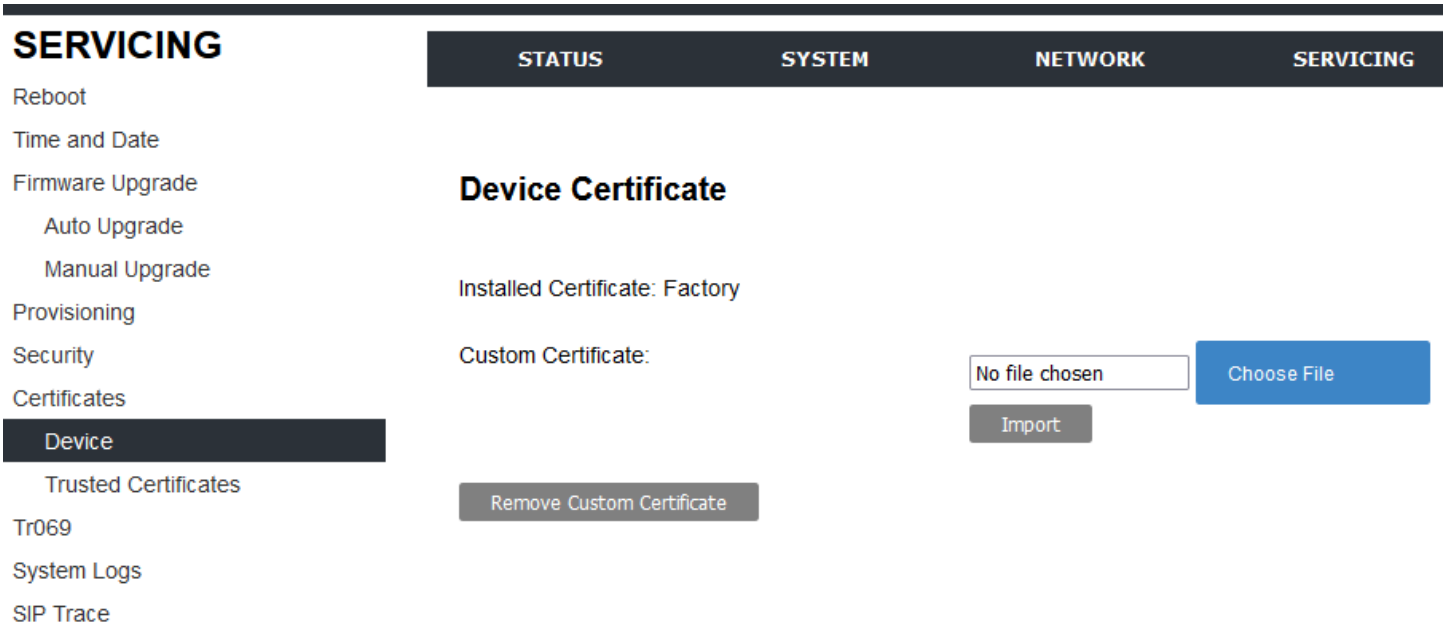
Setting	Description
Accept only allowed IP for incoming requests	Enable or disable using the **Allowed IP** list to filter all IP traffic.
Allowed IP 1-10	Enter IP addresses or address ranges to be used as sources of authorized IP traffic.

3.4.6 Certificates

You can add two types of certificates using the Web Portal or the provisioning file. The two types of certificates are:

- Device - A single Device Certificate can be uploaded so that other parties can authenticate the phone in the following cases:
  - When the phone acts as a web server for the user to manage configuration.
  - When the phone acts as a client for applications where HTTP is supported.
- Trusted - Trusted Certificates are for server authentication with secured HTTP transaction in the following applications: SIP signalling, Provisioning, Firmware, and LDAP directory service. Up to 20 trusted certificates can be installed.

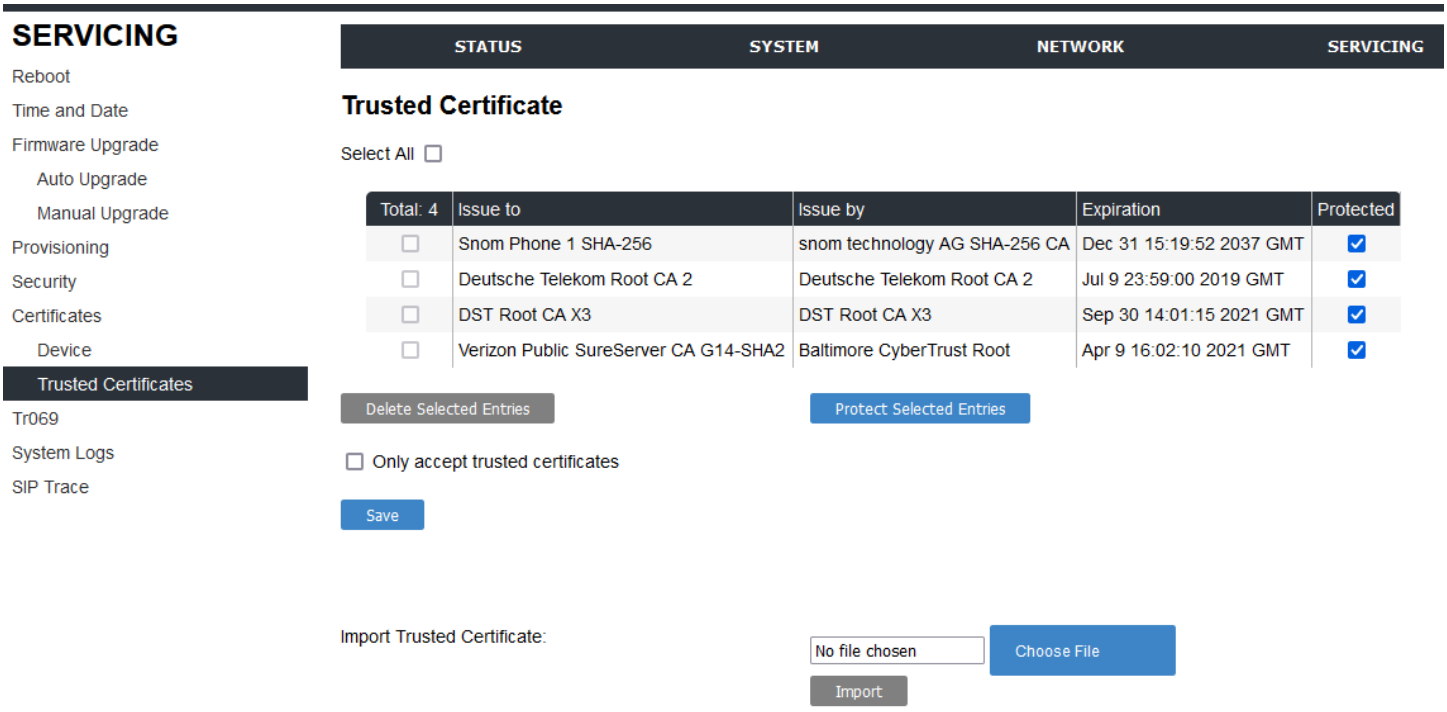
3.4.6.1 Device Certificate



To upload a Device certificate:

1. On the Device Certificate page, click **CHOOSE FILE**.
2. Locate the certificate file and click **OPEN**.
3. On the Device Certificate page, click **IMPORT**.

3.4.6.2 Trusted Certificate



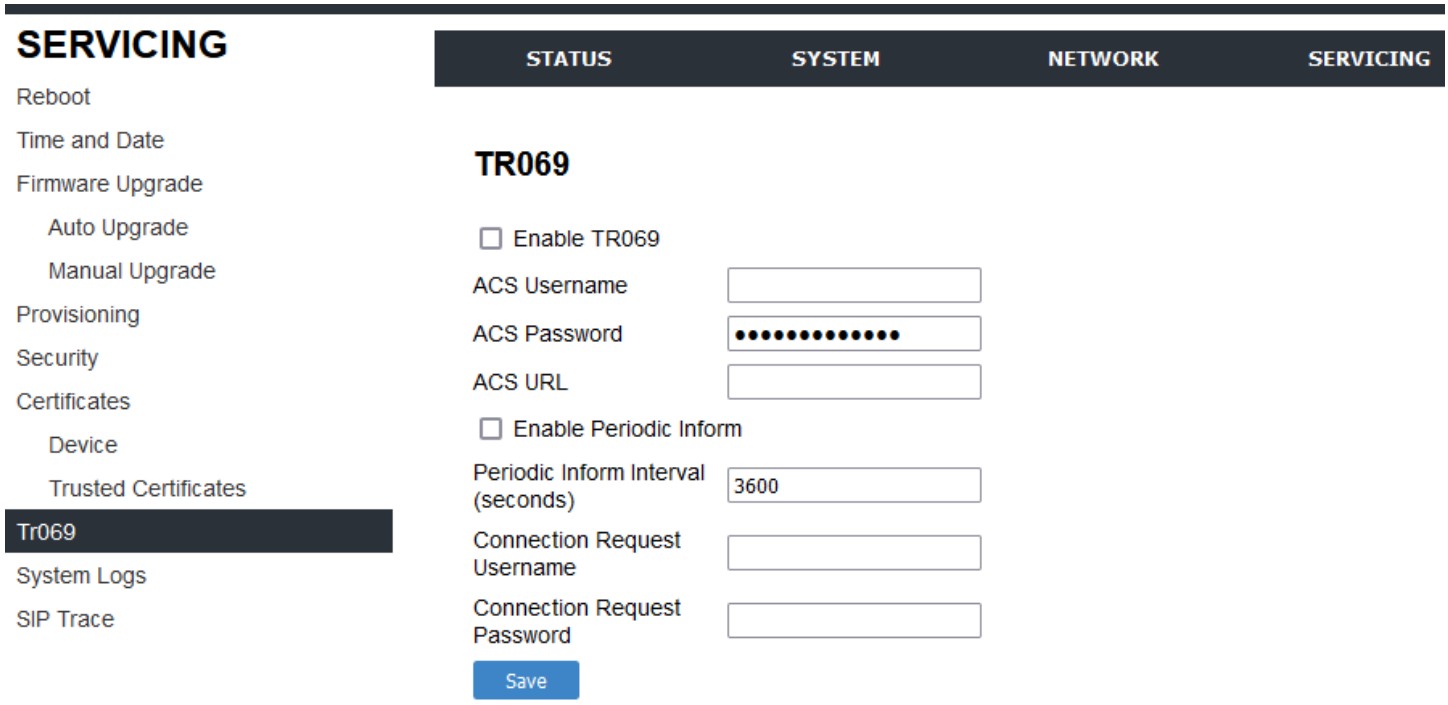
On the **Trusted Certificate** page, you can:

- Import up to 20 trusted certificates.
- Delete individual (or all) certificates.
- Protect certificates by check the box next to **Protected**, and then clicking **PROTECT SELECTED ENTRIES**. Protected certificates cannot be selected for deletion and are not removed during a reset to factory defaults.

Select **Only accept trusted certificates** to enable server authentication. Deselecting this option disables server authentication.

3.4.7 TR-069 Settings

The Broadband Forum's Technical Report 069 (TR-069) has defined a protocol for remote management and secure auto-configuration of compatible devices. On the **Tr069** page, you can enable TR-069 and configure access to an auto-configuration server (ACS).



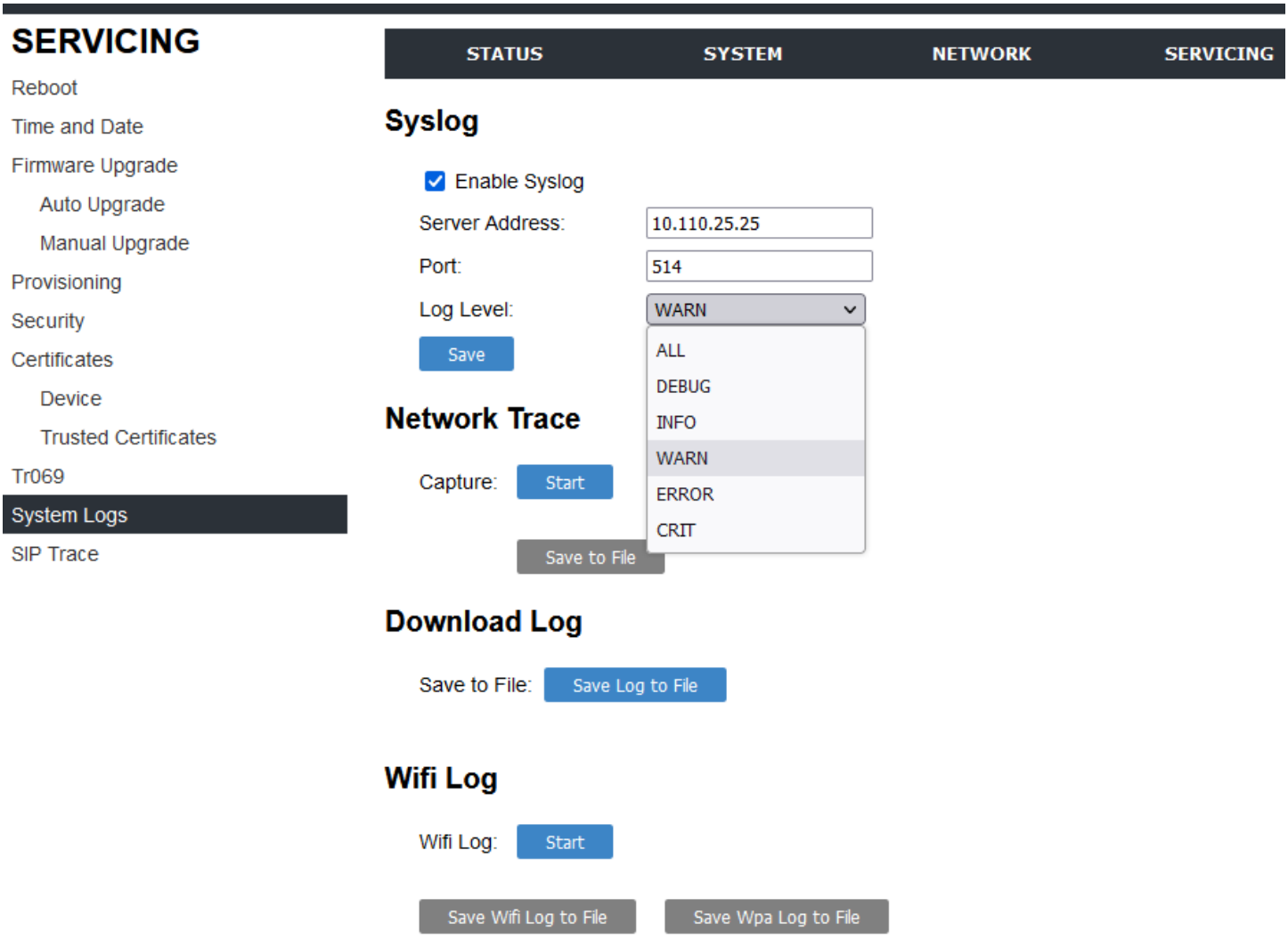
Setting	Description
Enable TR069	Enable/Disable TR-069 subsystem.
ACS Username	User name used for ACS authentication.
ACS Password	Password used for ACS authentication.
ACS URL	URL used to contact the ACS (for example, http://my.acs:9675/path/to/somewhere/).
Enable Period Inform	Enable/Disable periodic informs method calls.
Periodic Inform Interval (seconds)	Periodic inform method calls interval.
Connection Request Username	If the ACS wants to communicate with the device, it must offer the matching Connection Request user name. When the device sends the report to ACS for the first time, it contains information for this.
Connection Request Password	If the ACS wants to communicate with the device, it must offer the matching Connection Request password. When the device sends the report to ACS for the first time, it contains information for this.

3.4.8 System Logs

On the **Syslog Settings** page, you can enter settings related to system logging activities. It supports the following logging modes:

- Syslog server
- Volatile file

Under **Network Trace**, you can capture network traffic related to the phone's activity and save the capture as a .pcap file. The file can be used for diagnostic and troubleshooting purposes.



Under **Download Log**, you can save the system log to a file.

The Syslog settings are also available as parameters in the configuration file. See Section 6.6.6 Log Settings ("log" Module).

3.4.8.1 Syslog Settings

Setting	Description
Enable Syslog	Enable log output to syslog server.
Server Address	Syslog server IP address.
Port	Syslog server port.
Log Level	Set the log level. The higher the level, the larger the debug output. 5 - ALL 4 - DEBUG 3 - INFO 2 - WARNING 1 - ERROR 0 - CRITICAL

The logging levels are:

- CRITICAL: Operating conditions to be reported or corrected immediately (for example, an

internal component failure or file system error).
- ERROR: Non-urgent failures - unexpected conditions that won't cause the device to malfunction.
- WARNING: An indication that an error or critical condition can occur if action is not taken.
- INFO: Normal operational messages.
- DEBUG: Developer messages for troubleshooting/debugging purposes.

3.4.8.2 Network Trace

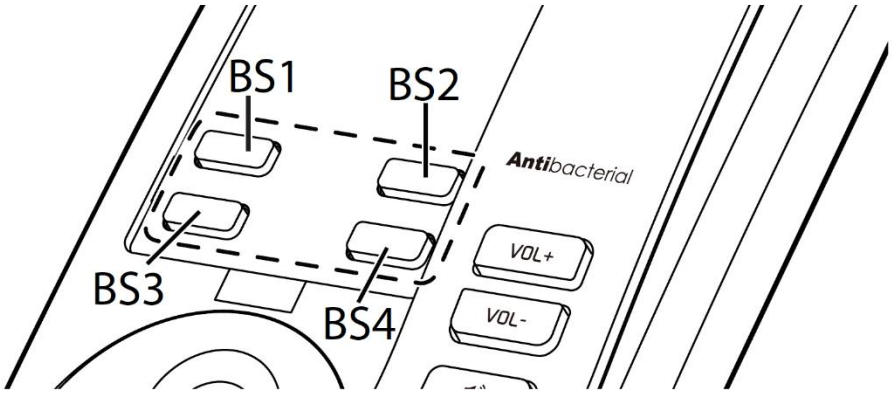
To perform a network trace:

Start a network trace by clicking **START**. The button changes to **STOP**. Stop the network trace by clicking **STOP**.

Save the trace by clicking **SAVE TO FILE**. Your browser should prompt you to save the capture a .pcap file.

4 Configure via Star Code

4.1 Base Star Codes Provisioning HD100, HD100W, HD101, HD101W



- [VOL+] [VOL-] [VOL+] [VOL-] [VOL+] [VOL-] [BS1] [BS2] [BS3] --> IP Address read back
- [VOL+] [VOL-] [VOL+] [VOL-] [VOL+] [VOL-] [BS1] [BS2] [BS1] --> Set factory default
- [VOL+] [VOL-] [VOL+] [VOL-] [VOL+] [VOL-] [BS2] [BS3] [BS2] --> Delete all hs
- [VOL+] [VOL-] [VOL+] [VOL-] [VOL+] [VOL-] [BS2] [BS3] [BS1] --> Base start registration mode
- [VOL+] [VOL-] [VOL+] [VOL-] [VOL+] [VOL-] [BS3] [BS3] [BS1] --> Set Wi-Fi On
- [VOL+] [VOL-] [VOL+] [VOL-] [VOL+] [VOL-] [BS3] [BS3] [BS2] --> Set Wi-Fi Off

Note

1st [VOL+] Long press >5s

4.2 Handset Star Codes Provisioning HD101, HD101W

- *883247#Mute/Hold --> Set factory default
- 123Mute/Hold/Hold --> HS Start Registration Mode
- *331734#Mute/Hold --> to de-registration

4.3 Handset Star Codes Provisioning HD100, HD100W

1. idle mode long press [VOL+] > 5s
2. *234234#{extension}#
3. e.g. *234234#12345# => 12345.cfg will be provision after reboot.

4.4 Handset Star Codes Provisioning HD101, HD101W

1. HS off hook (have dial tone or busy tone)
2. *234234#{extension}# (maximum 32 digits for whole star code)
3. e.g. *234234#12345# => 12345.cfg will be provision after reboot

4.5 Base Star Codes Provisioning HD151

- *990000# --> Set factory default
- *331734# --> Delete all hs
- 123[Mute] --> Base start registration mode
- 123[Hold] --> Base start registration mode
- *782842# --> Set the IP mode to Static

- *463427# --> Set the IP mode to DHCP
- *471233# --> IP Address readback
- *234[Mute]<extension># --> Set provisioning to get <extension>.cfg

4.6 Handset Star Codes Provisioning HD151

- 123Mute/Hold/Hold --> HS Start Registration Mode

4.7 Base Star Codes Provisioning HD130, HD150

- *990000# --> Set factory default
- *782842# --> Set the IP mode to Static
- *463427# --> Set the IP mode to DHCP
- *471233# --> IP Address readback
- *234[Mute]<extension># --> Set provisioning to get <extension>.cfg

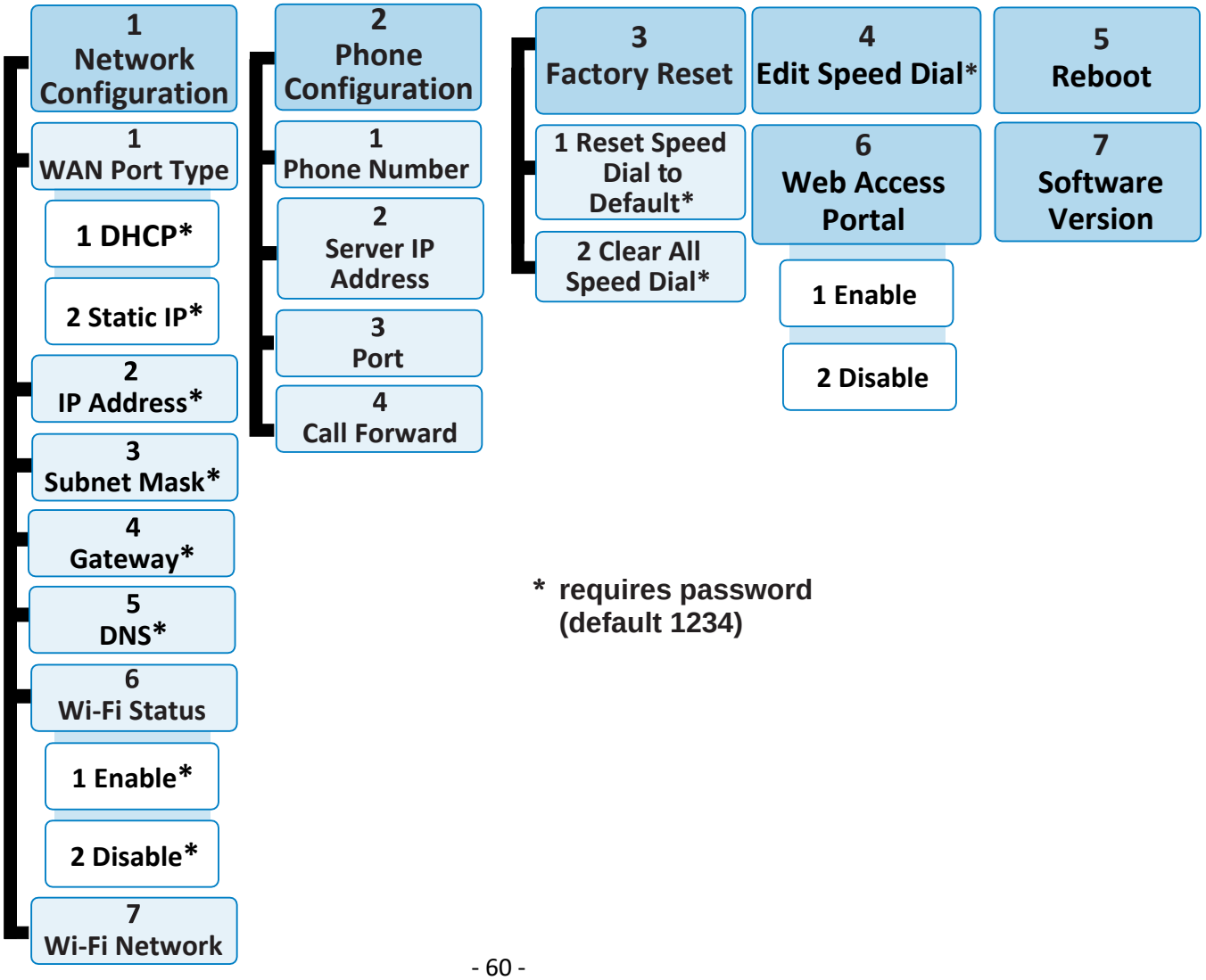
5 Configure with Voice Menu

The Voice menu enables you to use the handset to query and change phone settings. To accomplish this, follow the below steps:

1. **Access Voice Menu:**
   - HD100:
     When the phone is idle, press this key sequence on the handset: *** * * *.**
     A digitized voice on the handset will announce Voice Menu options.

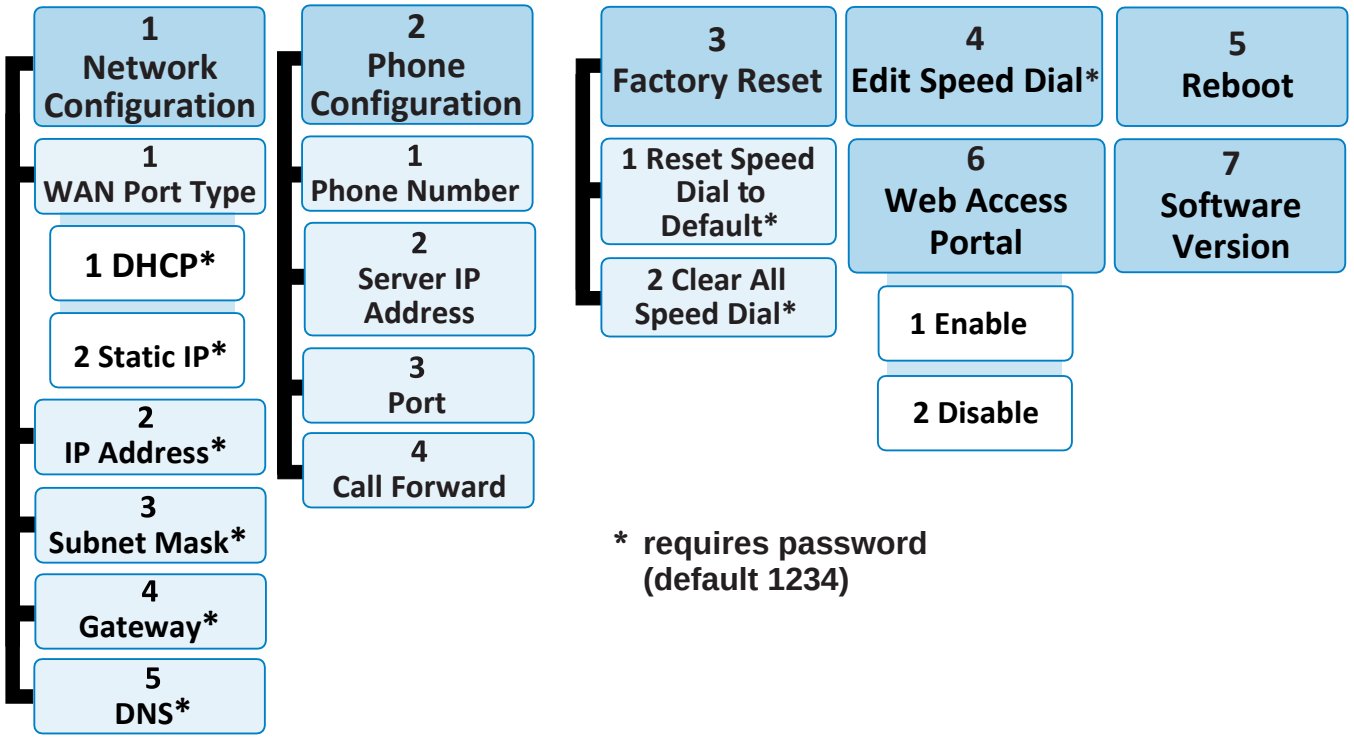
     -OR-

     HD101:
     When the phone is idle, press this key sequence on the handset: **TALK * * * *.**
     A digitized voice on the handset will announce Voice Menu options.
2. **Query or configure with Voice menu:**
   - Press the number key on the handset to select the desired menu option, or enter information, a list of menu options will be shown in the diagram below:
     - HD100W, HD101:



-OR-

- HD100, HD101:



- Example 1: to find out the IP address of the phone, press 1 for Network Configuration, and then press 2 for IP Address.
- Example 2: to disable Wi-Fi connection, press 1 for Network Configuration, then press 6 for Wi-Fi status and then press 2 for Disable.

3. Exit Voice menu:

When you have done querying or configuring with the Voice menu,

- HD100 (corded):
  Place the handset in the cradle.

  -OR-

- HD101 (cordless phone on base):
  Place the handset in the cradle or press **OFF**.

  Note: If you change any network settings, your phone will automatically reboot. This will enable your new settings to take effect.

6 Provisioning Using Configuration Files

Provisioning using configuration files is the quickest way to configure multiple HD10X phones. You can place configuration files on a provisioning server, where the HD10X phones retrieve the files and update their configuration automatically.

Configuration files have the extension **.cfg** and contain settings that will apply to HD10X phones. To edit a configuration file, open it with a text editor such as Notepad.

The settings within a configuration file are grouped into modules. Most of the modules group their settings in the same way that settings are grouped on the HD10X Web Portal. For example, the "time_date" module in the configuration file contains the same settings that are on the **Time and Date** Web Portal page. For a complete list of HD10X configuration file modules and their associated parameters, see Section 6.6 Configuration File Parameter Guide.

Using the Web Portal, you can also import a configuration file and apply the configuration file settings to the HD10X. For more information, see Section 3.4.4.5 Import Configuration.

This chapter covers:

- Provisioning Process
- Configuration File Types
- Data Files
- Configuration File Tips and Security

6.1 Provisioning Process

The automatic provisioning process is as follows:

Check for new or updated configuration files. For file-checking options, see Section 3.4.4.Provisioning.

1. The HD10X maintains a list of the last loaded provisioning files. The HD10X compares its current configuration against the files it finds on the provisioning server.

   If provisioning has been triggered by the resync timer expiring or by remote check-sync, HD10X checks for updated files after one minute of inactivity.

2. Download the configuration files.

   If any file on the provisioning server has changed, the HD10X treats it as a new file and downloads it.

   If the provisioning URL specifies a path only with no filename, then by default the HD10X looks for and retrieves the following file:

   - General file: **<model>.cfg**.

     The <model> variable is the product model: HD10X, for example.
     If the provisioning URL specifies both a path and filename, then the HD10X retrieves only the configuration file specified.

3. The HD10X restarts after one minute of inactivity.

   During provisioning, the HD10X reads the configuration file and validates each module and setting. The HD10X considers a setting valid if it is:
   - a valid data type
   - formatted as a valid setting
   - within a valid data range

- Part of a module that passes an integrity check. That is, the module's settings are consistent and logical. For example, in the "network" module, if DHCP is disabled, but no static IP address is specified, the module will fail the integrity check and none of the settings will apply.

Invalid modules or invalid settings are skipped and logged as ERROR messages in the system log, but will not interrupt the provisioning process. The system log will include the module parameters that have not been applied. A recognized module with unrecognized settings will cause all other settings in that module to be skipped.

A successful configuration or firmware update is reported as an INFO message in the system log.

See Section 6.6 Configuration File Parameter Guide for the options and value ranges available for each configuration file setting.

6.1.1 Resynchronization: Configuration File Checking

You can select several options that determine when the HD10X checks for new configuration files. This process of checking for configuration files is called Resynchronization. Resynchronization options are available on the Web Portal **Provisioning** page, but you can also include them in a configuration file.

The resynchronization options are:

- Mode - sets the HD10X to check for a configuration file only, a firmware update file only, or both types of files.
- Never - configuration file checking is disabled
- Bootup - the HD10X checks for new configuration files when it boots up. Any updates are applied during the bootup process.
- Remote check-sync - enables you to start a resynchronization remotely using your hosted server's web portal. The Remote check-sync settings are available only in the configuration file, not the Web Portal.
- Repeatedly, at a defined interval from 60 to 65535 minutes (45 days).

6.1.2 HD10X Reboot

If the HD10X needs to restart after an auto-update, the restart happens only after the device has been idle for one minute.

To prevent users from delaying the update process (auto-updates cannot begin until the HD10X has been idle for one minute), or to avoid device restarts that might interfere with incoming calls:

- Set the resynchronization interval to a suitable period
- Upload any new configuration file(s) to your provisioning server after work hours so that the HD10X will download the file(s) when there is no call activity.

When you update the HD10X by importing a configuration file using the Web Portal, the device restarts immediately after applying the new settings, regardless of whether the HD10X is idle.

6.2 Configuration File Types

The HD10X can retrieve and download two types of configuration file. Depending on your requirements, you may want to make both types of configuration file available on your provisioning server.

The configuration file type is a general configuration file. The types differ in name only. The formatting of the files' content is the same.

The general configuration file contains settings that are required by every HD10X in the system. The filename format is: General file: **<model>.cfg**

If the provisioning URL specifies a path only with no filename, then by default the HD10X will fetch both files.

However, if the provisioning URL specifies both a path and filename, then the HD10X will only fetch the single configuration file specified.

The general files can contain any of the available configuration settings. A setting can appear in the general configuration file. If a setting appears in the file, the setting that is read last is the one that applies.

You can configure a setting for most of your HD10X phones in the general file, and then overwrite that setting for just a few HD10X phones.

6.3 Data Files

The configuration file can also include links to data files for product customization. Allowed data types include the following:

- Directory (contacts, blacklist) in .xml format
- Certificates (server, provisioning) in .pem format

Links to data files are in the configuration file's "file" module. This is where you enter any URLs to the data files that the HD10X phone may require.

None of the data files is export when you export a configuration file from the HD10X. However, you can export a Directory or Blacklist .xml file using the Web Portal. After modifying the .xml file, you can use the configuration file "file" module to have the HD10X import the new file.

6.4 Configuration File Tips and Security

All configuration settings are initially stored in a configuration template file. Copy, rename, and edit the template file to create a general configuration file. You can store the general configuration file on your provisioning server.

Do not modify the configuration file header line that includes the model and firmware version.

To save your time and effort, consider which settings will be common to all (or the majority of) HD10X phones. Such settings might include call settings, language, and NAT settings. You can then edit those settings in the configuration template and save it as the general configuration file.

6.4.1 Clearing Parameters with %NULL in Configuration File

For configuration file parameters that can have a text string value, you can clear the value of the parameter by applying the value %NULL in the configuration file.

For example: sip_account.1.display_name = %NULL

However, the following parameter is an exception. Applying the value %NULL to this parameter will reset it to its default value.

- **file.hs_idle_logo** - applying %NULL restores the default value (logo)

6.5 TFTP Pull Down Method

Another way to configure your phone is to use the TFTP Pull Down Method. With this method, you can update your phone with a configuration file from one of the following sources:

- DHCP option 66 server

- Redirect server

To configure your phone using the TFTP Pull Down Method:

Please see Chapter 4 Configure via Star Code for complete information of how enter star codes.

If a DHCP option 66 server is present:

- The phone will do a GET request for the configuration file from the DHCP option 66 server. For example, DHCP option 66 server address = 192.168.1.200, the phone will do a GET request for 192.168.1.200/1388.cfg.
- Your phone will reboot after installing the configuration file.

If you do NOT have DHCP option 66:

- The phone will do a GET request for the configuration file from the Redirection server. For example, Redirection server address = https://provisioning.snom.com/hotel01/, the phone will do a GET request for https:// provisioning.snom.com/hotel01/1388.cfg
- Your phone will reboot after installing the configuration file.

6.6 Configuration File Parameter Guide

This chapter lists the available options for all the settings within the HD10X configuration file. Most settings in the configuration file have an equivalent in the Web Portal (see the settings tables in Chapter 3 Configure via Web Portal). However, the options you must enter when editing the configuration file have a different syntax and format.

The settings are divided into modules. Most modules correspond to a page on the HD10X Web Portal. You may wish to reorganize the modules within the configuration file itself. The configuration file settings can be listed in any order, and the configuration file will still be valid.

The modules included in the configuration file are:

6.6.1 SIP Account Settings ("sip_account" Module)

The SIP Account settings enable you to set up individual accounts for each user. Each account requires you to configure the same group of SIP account settings. The SIP account settings for each account are identified by the account number.

For example, for account 1 you would set:

sip_account.1.sip_account_enable = 1

sip_account.1.label = Line 1

sip_account.1.display_name = 1001

sip_account.1.user_id = 2325551001

and so on.

For account 2, you would set:

sip_account.2.sip_account_enable = 1

sip_account.2.label = Line 2

sip_account.2.display_name = 1002

sip_account.2.user_id = 2325551002

and so on, if you have additional accounts to configure.

All these settings are exported when you manually export the configuration from the HD10X.

General configuration file settings

Setting:	**sip_account.1.dial_plan**		
Description:	Sets the dial plan for account 1. See Section 3.2.1.2 Dial Plan.		
Values:	Text string	**Default:**	x+P

Setting:	**sip_account.1.call_restrict_dial_plan**		
Description:	Enter call restriction dial plan, to prevent users from completing calls to certain numbers for this account.		
Values:	text string (dial plan syntax)	**Default:**	Blank

Setting:	**sip_account.1.inter_digit_timeout**		
Description:	Sets the inter-digit timeout (in seconds) for account 1. The inter-digit timeout sets how long the HD10X waits after the last digit is entered before dialing the number.		
Values:	1-10	**Default:**	3

Setting:	**sip_account.1.dtmf_transport_method**		
Description:	Sets the transport method for DTMF signaling for account 1.		
Values:	auto, rfc2833, inband, info	**Default:**	auto

Setting:	**sip_account.1.unregister_after_reboot_enable**		
Description:	Enables or disables the HD10X to unregister account 1 after rebooting.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**sip_account.1.primary_sip_server_address**		
Description:	Sets the SIP server IP address for account 1.		
Values:	Text string	**Default:**	Blank

Setting:	**sip_account.x.primary_sip_server_port**

Description: Sets the SIP server port for account 1.

Values: 1–65535 **Default:** 5060

Setting: **sip_account.x.primary_registration_server_address**

Description: Sets the registration server IP address for account 1.

Values: IPv4, IPv6 or FQDN **Default:** Blank

Setting: **sip_account.x.primary_registration_server_port**

Description: Sets the registration server port for account 1.

Values: 1–65535 **Default:** 5060

Setting: **sip_account.x.primary_registration_expires**

Description: Sets the expiration time (in seconds) of the current registration for account 1.

Values: 30–7200 **Default:** 3600

Setting: **sip_account.x.registration_retry_time**

Description: Sets the retry frequency of the current registration for account 1.

Values: 1–1800 **Default:** 10

Setting: **sip_account.x.primary_outbound_proxy_server_address**

Description: Sets the outbound proxy server IP address for account 1.

Values: IPv4, IPv6 or FQDN **Default:** Blank

Setting: **sip_account.x.primary_outbound_proxy_server_port**

Description: Sets the outbound proxy server port for account 1.

Values: 1–65535 **Default:** 5060

Setting: **sip_account.x.backup_outbound_proxy_server_address**

Description: Sets the backup outbound proxy server IP address for account 1.

Values: IPv4, IPv6 or FQDN **Default:** Blank

Setting: **sip_account.x.backup_outbound_proxy_server_port**

Description: Sets the backup outbound proxy server port for account 1.

Values: 1-65535 **Default:** 5060

Setting: **sip_account.x.codec_priority.1**

Description: Sets the highest-priority codec for account 1.

Values: g711u, g711a, g729, g726, g722, g723_1, ilbc **Default:** g711u

Setting: **sip_account.x.codec_priority.2**

Description: Sets the second highest-priority codec for account 1.

Values: none, g711u, g711a, g729, g726, g722, g723_1, ilbc **Default:** g711a

Setting: **sip_account.x.codec_priority.3**

Description: Sets the third highest-priority codec for account 1.

Values: none, g711u, g711a, g729, g726, g722, g723_1, ilbc **Default:** g729

Setting: **sip_account.x.codec_priority.4**

Description: Sets the fourth highest-priority codec for account 1.

Values: none, g711u, g711a, g729, g726, g722, g723_1, ilbc **Default:** g726

Setting: **sip_account.x.codec_priority.5**

Description: Sets the fifth highest-priority codec for account 1.

Values: none, g711u, g711a, g729, g726, g722, g723_1, ilbc **Default:** g722

Setting: **sip_account.x.codec_priority.6**

Description:	Sets the highest-priority codec for account 1.		
Values:	none, g711u, g711a, g729, g726, g722, g723_1, ilbc	**Default:**	g723_1

Setting:	**sip_account.x.codec_priority.7**		
Description:	Sets the highest-priority codec for account 1.		
Values:	none, g711u, g711a, g729, g726, g722, g723_1, ilbc	**Default:**	ilbc

Setting:	**sip_account.x.voice_encryption_enable**		
Description:	Enables or disables SRTP voice encryption for account 1.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**sip_account.x.g729_annexb_enable**		
Description:	Enables G.729 Annex B, with voice activity detection (VAD) and bandwidth-conserving silence suppression. This setting applies only when G.729a/b is selected in a **sip_account.x.codec_priority** parameter.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**sip_account.x.ilbc_payload_type**		
Description:	Set the default payload type for the ilbc codec.		
Values:	96-127	**Default:**	98

Setting:	**sip_account.x.dscp**		
Description:	Sets the Voice Quality of Service Layer 3 - DSCP for account 1.		
Values:	0–63	**Default:**	46

Setting:	**sip_account.x.sip_dscp**		
Description:	Sets the Signaling Quality of Service Layer 3 - DSCP for account 1.		
Values:	0–63	**Default:**	26

Setting: **sip_account.x.local_sip_port**

Description: Sets the Local SIP port for account 1.

Values: 1-65535 **Default:** Account 1: 5060 Account 2: 5070 Account 3: 5080 Account 4: 5090

Setting: **sip_account.x.transport_mode**

Description: Sets the Signaling Transport Mode for account 1.

Values: udp, tcp, tls **Default:** udp

Setting: **sip_account.x.mwi_enable**

Description: Enables or disables message waiting indicator subscription for account 1. Enable if SUBSCRIBE and NOTIFY methods are used for MWI.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **sip_account.x.mwi_subscription_expires**

Description: Sets the MWI subscription expiry time (in seconds) for account 1.

Values: 15–65535 **Default:** 3600

Setting: **sip_account.x.mwi_ignore_unsolicited**

Description: Enables or disables ignoring of unsolicited MWI notifications - notifications in addition to, or instead of, SUBSCRIBE and NOTIFY methods - for account 1. Disable if MWI service is configured on the voicemail server and does not involve a subscription to a voicemail server.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **sip_account.x.stutter_dial_tone_enable**

Description: Enables or disables MWI stutter dial tone for account 1.

Values: 0 (disabled), 1 (enabled) **Default:** 1

Setting: **sip_account.x.nat_traversal_stun_enable**

Description: Enables or disables STUN (Simple Traversal of UDP through NATs) for account 1. STUN enables clients, each behind a firewall, to establish calls via a service provider hosted outside of either local network.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **sip_account.x.nat_traversal_stun_server_address**

Description: Sets the STUN server IP address.

Values: IPv4, IPv6 or FQDN **Default:** Blank

Setting: **sip_account.x.nat_traversal_stun_server_port**

Description: Sets the STUN server port.

Values: 1-65535 **Default:** 3478

Setting: **sip_account.x.nat_traversal_stun_keep_alive_enable**

Description: Enables or disables UDP keep-alives. Keep-alive packets are used to maintain connections established through NAT.

Values: 0 (disabled), 1 (enabled) **Default:** 1

Setting: **sip_account.x.nat_traversal_stun_keep_alive_interval**

Description: Sets the interval (in seconds) for sending UDP keep-alives.

Values: 0-65535 **Default:** 30

Setting: **sip_account.x.keep_alive_enable**

Description: Enable SIP keep alive for NAT traversal and monitoring SIP server status.

Values: 0 (disabled),
1 (enabled) **Default:** 0

Setting: **sip_account.x.keep_alive_interval**

Description: Sets the interval (in seconds) for sending keep-alives.

Values: 1-3600 **Default:** 15

Setting: **sip_account.x.keep_alive_ignore_failure**

Description: Enable the phone to ignore keep-alive failure, if failure triggers re-subscription (and calls are dropped).

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **sip_account.x.music_on_hold_enable**

Description: Enables or disables a hold-reminder tone that a far-end caller hears when put on hold during a call on account 1.

Values: 0 (disabled), 1 (enabled) **Default:** 1

Setting: **sip_account.x.sip_session_timer_enable**

Description: Enables or disables the SIP session timer.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **sip_account.x.sip_session_timer_min**

Description: Sets the session timer minimum value (in seconds) for account 1.

Values: 90-65535 **Default:** 90

Setting: **sip_account.x.sip_session_timer_max**

Description: Sets the session timer maximum value (in seconds) for account 1.

Values: 90-65535 **Default:** 1800

Setting: **sip_account.x.check_trusted_certificate**

Description: Enables or disables accepting only a trusted TLS certificate for account 1.

Values: 0 (disabled),
1 (enabled) **Default:** 0

Setting: **sip_account.x.preferred_ptime**

Description: Enter the packetization interval time in milliseconds.

Values:	10, 20, 30, 40, 50, 60	**Default:**	20

Setting: **sip_account.x.cid_src_priority.1**

Description: Sets the first priority of the caller ID source to be displayed on the incoming call screen.

Values:	from, pai, rpid	**Default:**	pai

Setting: **sip_account.x.cid_src_priority.2**

Description: Sets the second priority of the caller ID source to be displayed on the incoming call screen.

Values:	none, from, pai, rpid	**Default:**	rpid

Setting: **sip_account.x.cid_src_priority.3**

Description: Sets the third priority of the caller ID source to be displayed on the incoming call screen.

Values:	none, from, pai, rpid	**Default:**	from

Setting: **sip_account.x.call_rejection_response_code**

Description: Select the response code for call rejection. This code applies to the following call rejection cases:

- User rejects an incoming call
- DND is enabled
- Phone rejects a second incoming call with Call Waiting disabled
- Phone rejects an anonymous call with Anonymous Call Rejection enabled
- Phone rejects call when the maximum number of calls is reached

Values:	480, 486, 603	**Default:**	486

Setting: **sip_account.x.dtmf_payload_type**

Description: Set the configurable RTP payload type for in-call DTMF.

Values:	96-127	**Default:**	101

Setting: **sip_account.x.use_register_route_header**

Description: Use Route header for REGISTER

Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting: **sip_account.dirty_host_ttl**

Description: Specify the “Time to Live” (TTL) for dirty hosts in seconds. This means that, when a phone was unable to reach a host, the phone will not try to reach this host again until the time specified in this field has elapsed.
If this setting is 0 or empty, it has no effect (the host is set as "dirty" but only for 0 seconds, which means it will have no effect on future requests)

Values:	0,1	**Default:**	0

Setting: **sip_account.dns_query_option**

Description: Select DNS query option for SIP traffic only:
0 (DNS query with A record only)
1 (DNS query with NAPTR/SRV/A)
DNS query for all other traffic (e.g. HTTP) should always perform A record only.

Values:	0, 1	**Default:**	1

Setting: **sip_account.shared_local_sip_port**

Description: Defines the local SIP port to be used by all accounts, if enabled by parameter **sip_account.shared_local_sip_port_enable**.

Values:	1-65535	**Default:**	5060

Setting: **sip_account.shared_local_sip_port_enable**

Description: Enables shared local SIP port.

Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting: **sip_account.x.sip_account_enable**

Description: Enables account 1 to be used by the device.

Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting: **sip_account.x.label**

Description: Room Number (Admin Tools)

Values:	Text string	**Default:**	Blank

Setting: **sip_account.x.display_name**

Description: Sets the text portion of the caller ID that is displayed for outgoing calls using account 1.

Values:	Text string	**Default:**	Blank

Setting: **sip_account.x.user_id**

Description: Sets the account ID for account 1. Depending on your service provider's specifications, this could be an extension number.

Note:
Do not enter the host name (e.g. "@sipservice.com"). The configuration file automatically adds the default host name.

Values:	Text string	**Default:**	Blank

Setting: **sip_account.x.authentication_name**

Description: Sets the authentication name for account 1. Depending on your service provider's specifications, this could be identical to the user ID.

Values:	Text string	**Default:**	Blank

Setting: **sip_account.x.authentication_access_password**

Description: Sets the authentication password for account 1.

Values:	Text string	**Default:**	Blank

Setting: **sip_account.x.access_code_retrieve_voicemail**

Description: Sets the voicemail retrieval feature access code for account 1.

Values:	Text string	**Default:**	Blank

Setting: **sip_account.x.share_line_enable**

Description: Sets the account type for account 1. If the shared line type is enabled, multiple HD10X phones can be configured with shared line appearances.

Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting: **sip_account.x.mwi_uri**

Description: Sets the MWI URI that will be used for MWI subscription. If this setting is left blank, the HD10X uses the account 1 user ID for MWI subscription.

Values: SIP URI text string **Default:** Blank

6.6.2 Handset Settings ("hs_settings" Module)

The Handset Settings allow you to configure account assignments and names for the cordless handsets that are registered to the base station. For more information on registering cordless handsets, see HD101 User Guide.

General configuration file settings

Setting: **hs_settings.rf_power**

Description: Sets the DECT RF Power: 0 (low), 1 (high)

Values: 0,1 **Default:** 0

Setting: **hs_settings.x.handset_name**

Description: Sets the name for handset x. You can use up to 11 letters and/or numbers. Use alphanumeric characters only-no symbol characters are allowed.

Values: Text string **Default:** HANDSET

Setting: **hs_settings.x.default_account**

Description: Only one account is allowed. For future use.

Values: 1 **Default:** 1

Setting: **hs_settings.x.assigned_account**

Description: Only one account is allowed. For future use.

Values: 1 **Default:** 1

6.6.3 Network Settings ("network" Module)

The network settings follow the format: network.[element].

General configuration file settings

Setting: **network.vlan.wan.enable**

Description: Enables or disables the WAN VLAN.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **network.vlan.wan.id**

Description: Sets the WAN VLAN ID.

Values: 0-4095 **Default:** 0

Setting: **network.vlan.wan.priority**

Description: Sets the WAN port priority.

Values: 0-7 **Default:** 0

Setting: **network.lldp_med.enable**

Description: Enables or disables LLDP-MED.

Values: 0 (disabled), 1 (enabled) **Default:** 1

Setting: **network.lldp_med.interval**

Description: Sets the LLDP-MED packet interval (in seconds).

Values: 1-30 **Default:** 30

Setting: **network.eapol.enable**

Description: Enables or disables 802.1x EAPOL.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **network.eapol.identity**

Description: Sets the 802.1x EAPOL identity.

Values: Text string **Default:** Blank

Setting: **network.eapol.access_password**

Description: Sets the 802.1x EAPOL MD5 password.

Values:	Text string	**Default:**	Blank

Setting: **network.vendor_class_id**

Description: Sets the vendor ID for DHCP option 60.

Values:	Text string	**Default:**	Hotel SIP HD10X

Setting: **network.user_class**

Description: Sets the user class for DHCP option 77.

Values:	Text string	**Default:**	Hotel SIP HD10X

Setting: **network.ip.mode**

Description: Sets the IPv4 network mode.

Values:	disable, dhcp, static, pppoe	**Default:**	dhcp

Setting: **network.ip.static_ip_addr**

Description: Sets a static IP address for the network.

Values:	Text string (IPv4)	**Default:**	Blank

Setting: **network.ip.subnet_mask**

Description: Sets the subnet mask for the network.

Values:	Text string (IPv4)	**Default:**	Blank

Setting: **network.ip.gateway_addr**

Description: Sets the Gateway IP address.

Values:	Text string (IPv4)	**Default:**	Blank

Setting: **network.ip.dns1**

Description: Sets the primary DNS server IP address.

Values:	Text string (IPv4)	**Default:**	Blank

Setting: **network.ip.dns2**

Description: Sets the secondary DNS server IP address.

Values:	Text string (IPv4)	**Default:**	Blank

Setting: **network.ip.manually_configure_dns**

Description: Enable or disable manual DNS configuration.

Values:	0 (disable), 1 (enable)	**Default:**	0

Setting: **network.ip.pppoe.service_name**

Description: If IPv4 mode is PPPoE, enter the name of the applicable PPPoE provider, in case more than one is available.

Values:	Text string	**Default:**	Blank

Setting: **network.ip.pppoe.username**

Description: If IPv4 mode is PPPoE, enter your PPPoE account username.

Values:	Text string	**Default:**	Blank

Setting: **network.ip.pppoe.access_password**

Description: If IPv4 mode is PPPoE, enter your PPPoE account password.

Values:	Text string	**Default:**	Blank

Setting: **network.ip6.mode**

Description: Set the IPv6 network mode, depending on how the device will be assigned an IP address.

Values:	disable, auto, static	**Default:**	disable

Setting: **network.ip6.static_ip_addr**

Description: When IPv6 mode is static, enter the static IP address for the network.

Values: Text string (IPv6) **Default:** Blank

Setting: **network.ip6.prefix**

Description: When IPv6 mode is static, enter the IPv6 address prefix length.

Values: 0-128 **Default:** 64

Setting: **network.ip6.gateway_addr**

Description: When IPv6 mode is static, enter the default gateway address.

Values: Text string (IPv6) **Default:** Blank

Setting: **network.ip6.dns1**

Description: If manual DNS configuration is enabled, enter the address for the primary DNS server.

Values: Text string (IPv6) **Default:** Blank

Setting: **network.ip6.dns2**

Description: If manual DNS configuration is enabled, enter the address for the secondary DNS server.

Values: Text string (IPv6) **Default:** Blank

Setting: **network.ip6.manually_configure_dns**

Description: Enable or disable manual DNS configuration for IPv6.

Values: 0 (disable), 1 (enable) **Default:** 0

Setting: **network.wifi_enable**

Description: Enables or disables the Wi-Fi.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **network.wifi_diagnostic_mode**

Description: Enable or disable the Wi-Fi diagnostic mode.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **network.wifi_master_ip_mode**

Description: Sets the network Wi-Fi IP mode type.

Values: Text string (ipv4 or ipv6) **Default:** ipv4

Setting: **network.wifi_manually_configure_dns**

Description: Enable or disable manual Wi-Fi DNS configuration.

Values: 0 (disable), 1 (enable) **Default:** 0

Setting: **network.wifi_mannually_dns1**

Description: Sets the primary Wi-Fi DNS server IP address.

Values: Text string **Default:** Blank

Setting: **network.wifi_mannually_dns2**

Description: Sets the secondary Wi-Fi DNS server IP address.

Values: Text string **Default:** Blank

Setting: **network.wifi_ip6.manually_configure_dns**

Description: Enable or disable manual Wi-Fi IPV6 DNS configuration.

Values: 0 (disable), 1 (enable) **Default:** 0

Setting: **network.wifi_ip6_mannually_dns1**

Description: Sets the primary Wi-Fi IPV6 DNS server IP address.

Values: Text string **Default:** Blank

Setting: **network.wifi_ip6.mannually_dns2**

Description: Sets the secondary Wi-Fi IPV6 DNS server IP address.

Values: Text string **Default:** Blank

Setting: **network.x.wifi_ssid**

Description: Sets the Wi-Fi Access Point's SSID. x ranges from 1 to 10.

Values: Text string **Default:** Blank

Setting: **network.x.wifi_apMac**

Description: Sets the Wi-Fi Access Point's MAC Address. x ranges from 1 to 10.

Values: Text string **Default:** Blank

Setting: **network.x.wifi_security**

Description: Sets Wi-Fi security type. x ranges from 1 to 10.

Values: OPEN, WEP, WPA, WPA2, EAP-PEAP, EAP-TLS **Default:** OPEN

Setting: **network.x.wifi_access_password**

Description: Sets the password for WEP, WPA and WPA2. x ranges from 1 to 10.

Values: Text string **Default:** Blank

Setting: **network.x.wifi_peap_verify_server_cert**

Description: Enable or disable the request to authenticate PEAP Server Certificate. x ranges from 1 to 10.

Values: 0 (disable), 1 (enable) **Default:** 0

Setting: **network.x.wifi_peap_identity**

Description: Sets EAP-PEAP identity. x ranges from 1 to 10.

Values: Text string **Default:** Blank

Setting: **network.x.wifi_peap_password**

Description: Sets EAP-PEAP password. x ranges from 1 to 10.

Values: Text string **Default:** Blank

Setting: **network.x.wifi_tls_verify_server_cert**

Description: Enable or disable the request to authenticate TLS Server Certificate. x ranges from 1 to 10.

Values: 0 (disable), 1 (enable) **Default:** 0

Setting: **network.x.wifi_tls_private_key_password**

Description: Sets the private key password for TLS. (Optional, depends on customer key management). x ranges from 1 to 10.

Values: Text string **Default:** Blank

Setting: **network.x.wifi_tls_identity**

Description: Sets the identity for TLS. (Optional for most servers). x ranges from 1 to 10.

Values: Text string **Default:** Blank

Setting: **network.x.wifi_ip_mode**

Description: Sets the IP mode of wireless access point to dhcp or static. x ranges from 1 to 10.

Values: Text string (dhcp or static) **Default:** dhcp

Setting: **network.x.wifi_static_dns1**

Description: Sets the static parameters for primary Wi-Fi IPV4 DNS server. x ranges from 1 to 10.

Values: Text string **Default:** Blank

Setting: **network.x.wifi_static_dns2**

Description: Sets the static parameters for secondary Wi-Fi IPV4 DNS server. x ranges from 1 to 10.

Values: Text string **Default:** Blank

Setting: **network.x.wifi_static_gateway_addr**

Description: Sets the static gateway address for Wi-Fi IPV4. x ranges from 1 to 10.

Values: Text string **Default:** Blank

Setting: **network.x.wifi_static_ip_addr**

Description: Sets the static IP address for Wi-Fi IPV4. x ranges from 1 to 10.

Values: Text string **Default:** Blank

Setting: **network.x.wifi_static_subnetmask**

Description: Sets the static subnet mask for Wi-Fi IPV4. x ranges from 1 to 10.

Values: Text string **Default:** Blank

Setting: **network.x.wifi_ip6.mode**

Description: Sets the IP mode of wireless access point to auto or static. x ranges from 1 to 10.

Values: Text string (auto or static) **Default:** Auto

Setting: **network.x.wifi_ip6.dns1**

Description: Sets the static parameters for primary Wi-Fi IPV6 DNS server. x ranges from 1 to 10.

Values: Text string **Default:** Blank

Setting: **network.x.wifi_ip6.dns2**

Description: Sets the static parameters for secondary Wi-Fi IPV6 DNS server. x ranges from 1 to 10.

Values: Text string **Default:** Blank

Setting: **network.x.wifi_ip6.gateway_addr**

Description: Sets the gateway address for Wi-Fi IPV6. x ranges from 1 to 10.

Values: Text string **Default:** Blank

Setting:	**network.x.wifi_ip6.prefix**		
Description:	Sets the prefix for Wi-Fi IPV6. x ranges from 1 to 10.		
Values:	Text string	**Default:**	Blank

Setting:	**network.x.wifi_ip6.static_ip_addr**		
Description:	Sets the static IP address for Wi-Fi IPV6. x ranges from 1 to 10.		
Values:	Text string	**Default:**	Blank

6.6.4 Provisioning Settings ("provisioning" Module)

The provisioning settings follow the format: provisioning.[element].

All these settings are exported when you manually export the configuration from the HD10X.

General configuration file settings

Setting:	**provisioning.dhcp_option_enable**		
Description:	Enables or disables using DHCP options for locating the configuration and firmware files.		
Values:	0 (disabled), 1 (enabled)	**Default:**	1

Setting:	**provisioning.dhcp_option_priority_1**		
Description:	Sets the first priority DHCP option for the provisioning/firmware file check.		
Values:	66, 159, 160	**Default:**	66

Setting:	**provisioning.dhcp_option_priority_2**		
Description:	Sets the second priority DHCP option for the provisioning/firmware file check.		
Values:	66, 159, 160	**Default:**	159

Setting:	**provisioning.dhcp_option_priority_3**		
Description:	Sets the third priority DHCP option for the provisioning/firmware file check.		
Values:	66, 159, 160	**Default:**	160

Setting: **provisioning.resync_mode**

Description: Sets the mode of the device's provisioning/firmware file check. This determines which files the device retrieves when the resync process begins.

Values: config_only, firmware_only, config_and_firmware **Default:** config_and_firmware

---

Setting: **provisioning.bootup_check_enable**

Description: Enables or disables bootup check for configuration and firmware files.

Values: 0 (disabled), 1 (enabled) **Default:** 1

Setting: **provisioning.schedule_mode**

Description: Sets the type of schedule check for configuration and firmware files.

Values: disable, interval, weekday **Default:** disable

Setting: **provisioning.resync_time**

Description: Sets the interval (in minutes) between checks for new firmware and/or configuration files.

Values: 0-65535 **Default:** 0 (OFF)

Setting: **provisioning.weekdays**

Description: Sets the day(s) when the device checks for new firmware and/or configuration files. Enter a comma-delimited list of weekdays from 0 (Sunday) to 6 (Saturday). For example, 5,6,0 means the provisioning check will be performed on Friday, Saturday and Sunday.

Values: text string **Default:** Blank

Setting: **provisioning.weekdays_start_hr**

Description: Sets the hour when the device checks for new firmware and/or configuration files.

Values: 0-23 **Default:** 0

Setting: **provisioning.weekdays_end_hr**

Description: Sets the hour when the device stops checking for new firmware and/or configuration files.

Values: 0-23 **Default:** 0

Setting: **provisioning.remote_check_sync_enable**

Description: Enables or disables remotely triggering the device to check for new firmware and/or configuration files. The file checking is triggered remotely via a SIP Notify message from the server containing the **check-sync** event.

Values: 0 (disabled), 1 (enabled) **Default:** 1

Setting: **provisioning.crypto_enable**

Description: Enables or disables encryption check for the configuration file(s). Enable if you have encrypted the configuration file(s) using AES encryption.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **provisioning.crypto_passphrase**

Description: Sets the AES encryption passphrase for decrypting the configuration file(s). Enter the key that was generated when you encrypted the file.

Values: Text string **Default:** Blank

Setting: **provisioning.check_trusted_certificate**

Description: Enables or disables accepting only a trusted TLS certificate for access to the provisioning server.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **provisioning.pnp_enable**

Description: Enables or disables the HD10X checking for the provisioning URL using the Plug-and-Play Subscribe and Notify protocol.

Values: 0 (disabled), 1 (enabled) **Default:** 1

Setting: **provisioning.pnp_response_timeout**

Description: Sets how long the HD10X repeats the SUBSCRIBE request if there is no reply from the PnP server.

Values: 1-60 **Default:** 10

Setting: **provisioning.pwd_export_enable**

Description: Enables or disables passwords from being exported in plain text. This parameter is not available on the Web Portal. The passwords affected are:

- network.eapol.access_password
- provisioning.fw_server_access_password
- provisioning.server_access_password
- profile.admin.access_password
- sip_account.x.authentication_access_password
- remoteDir.ldap_access_password
- remoteDir.broadsoft_access_password

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **provisioning.provision_priority_1**

Description: Sets the provsioning priority order.

Values: pnp, dhcp_option,url **Default:** pnp

Setting: **provisioning.provision_priority_2**

Description: Sets the provsioning priority order.

Values: pnp, dhcp_option,url **Default:** dhcp_option

Setting: **provisioning.provision_priority_3**

Description: Sets the provsioning priority order.

Values: pnp, dhcp_option,url **Default:** url

Setting: **provisioning.firmware_url**

Description: Sets the URL for the server hosting the firmware file.

Values: Text string **Default:** Blank

Setting: **provisioning.handset_firmware_url**

Description: Sets the URL for the server hosting the handset firmware file.

Values: Text string **Default:** Blank

Setting: **provisioning.cordless_deskset_firmware_url**

Description: Sets the URL for server hosting the color handset firmware file.

Values: Text string **Default:** Blank

Setting: **file.hs_idle_logo**

Description: Set URL for server hosting the color handset background wall paper bmp file.

Values: Text string **Default:** Blank

Setting: **provisioning.fw_server_username**

Description: Sets the authentication name for the server hosting the firmware file.

Values: Text string **Default:** Blank

Setting: **provisioning.fw_server_access_password**

Description: Sets the authentication password for the server hosting the firmware file.

Values: Text string **Default:** Blank

Setting: **provisioning.server_address**

Description: Sets the provisioning server IP address.

Values: Text string **Default:** http://et.phones.com/redirectserver

Setting: **provisioning.server_username**

Description: Sets the authentication name for the provisioning server.

Values: Text string **Default:** Blank

Setting: **provisioning.server_access_password**

Description: Sets the authentication password for the provisioning server.

Values: Text string **Default:** Blank

6.6.5 Time and Date Settings ("time_date" Module)

The time and date settings follow the format: time_date.[element].

All these settings are exported when you manually export the configuration from the HD10X.

All the time and date settings are included in the general configuration file.

Setting: **time_date.date_format**

Description: Sets the format for displaying the date.

Values: DD/MM/YY, MM/DD/YY, YY/MM/DD **Default:** DD/MM/YY

Setting: **time_date.24hr_clock**

Description: Enables or disables 24-hour clock.

Values: 0 (disabled), 1 (enabled) **Default:** 1

Setting: **time_date.ntp_server**

Description: Enables or disables NTP server to set time and date.

Values: 0 (disabled), 1 (enabled) **Default:** 1

Setting: **time_date.ntp_server_addr**

Description: Sets the URL for the NTP server.

Values: IPv4, IPv6 or FQDN **Default:** us.pool.ntp.org

Setting: **time_date.ntp_dhcp_option**

Description: Enables or disables DHCP option 42 to find the NTP server.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **time_date.selected_timezone**

Description: Sets the local time zone.

Values: Pacific/Pago_Pago, Pacific/Honolulu, America/Adak, America/Anchorage, America/Vancouver, America/Tijuana, America/Los_Angeles, America/Edmonton, America/Chihuahua, America/Denver, America/Phoenix, America/Winnipeg, Pacific/Easter, America/Mexico_City, America/Chicago, America/Nassau, America/Montreal, America/Grand_Turk, America/Havana, America/New_York, America/Caracas, America/Halifax, America/Santiago, America/Asuncion, Atlantic/Bermuda, Atlantic/Stanley, America/Port_of_Spain, America/St_Johns, America/Godthab, America/Argentina/Buenos_Aires, America/Fortaleza, America/Sao_Paulo, America/Noronha, Atlantic/Azores, GMT, America/Danmarkshavn, Atlantic/Faroe, Europe/Dublin, Europe/Lisbon, Atlantic/Canary, Europe/London, Africa/Casablanca, Europe/Tirane, Europe/Vienna, Europe/Brussels, Europe/Zagreb, Europe/Prague, Europe/Copenhagen, Europe/Paris, Europe/Berlin, Europe/Budapest, Europe/Rome, Europe/Luxembourg, Europe/Skopje, Europe/Amsterdam, Africa/Windhoek, Europe/Tallinn, Europe/Helsinki, Asia/Gaza, Europe/Athens, Asia/Jerusalem, Asia/Amman, Europe/Riga, Asia/Beirut, Europe/Chisinau, Europe/Kaliningrad, Europe/Bucharest, Asia/Damascus, Europe/Istanbul, Europe/Kiev, Africa/Djibouti, Asia/Baghdad, Europe/Moscow, Asia/Tehran, Asia/Yerevan, Asia/Baku, Asia/Tbilisi, Asia/Aqtau, Europe/Samara, Asia/Aqtobe, Asia/Bishkek, Asia/Karachi, Asia/Yekaterinburg, Asia/Kolkata, Asia/Almaty, Asia/Novosibirsk, Asia/Krasnoyarsk, Asia/Bangkok, Asia/Shanghai, Asia/Singapore, Australia/Perth, Asia/Seoul, Asia/Tokyo, Australia/Adelaide, Australia/Darwin, Australia/Sydney, Australia/Brisbane, Australia/Hobart, Asia/Vladivostok, Australia/Lord_Howe, Pacific/Noumea, Pacific/Auckland, Pacific/Chatham, Pacific/Tongatapu

Default: America/New_York

Setting: **time_date.daylight_saving_auto_adjust**

Description: Sets the device to automatically adjust clock for daylight savings.

Values: 0 (disabled), 1 (enabled)

Default: 1

Setting: **time_date.daylight_saving_user_defined**

Description: Enables or disables manual daylight savings configuration.

Values: 0 (disabled), 1 (enabled)

Default: 0

Setting:	**time_date.daylight_saving_start_month**		
Description:	Sets the month that daylight savings time starts.		
Values:	January, February, March, April, May, June, July, August, September, October, November, December	**Default:**	March

Setting:	**time_date.daylight_saving_start_week**		
Description:	Sets the week that daylight savings time starts.		
Values:	1-5	**Default:**	2

Setting:	**time_date.daylight_saving_start_day**		
Description:	Sets the day that daylight savings time starts.		
Values:	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday	**Default:**	Sunday

Setting:	**time_date.daylight_saving_start_hour**		
Description:	Sets the hour that daylight savings time starts.		
Values:	00:00, 01:00, 02:00, 03:00, 04:00, 05:00, 06:00, 07:00, 08:00, 09:00, 10:00, 11:00, 12:00, 13:00, 14:00, 15:00, 16:00, 17:00, 18:00, 19:00, 20:00, 21:00, 22:00, 23:00	**Default:**	02:00

Setting:	**time_date.daylight_saving_end_month**		
Description:	Sets the month that daylight savings time ends.		
Values:	January, February, March, April, May, June, July, August, September, October, November, December	**Default:**	November

Setting:	**time_date.daylight_saving_end_week**		
Description:	Sets the week that daylight savings time ends.		
Values:	1-5	**Default:**	1

Setting:	**time_date.daylight_saving_end_day**

Description: Sets the day that daylight savings time ends.

Values: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday **Default:** Sunday

---

Setting: **time_date.daylight_saving_end_hour**

Description: Sets the hour that daylight savings time ends.

Values: 00:00, 01:00, 02:00, 03:00, 04:00, 05:00, 06:00, 07:00, 08:00, 09:00, 10:00, 11:00, 12:00, 13:00, 14:00, 15:00, 16:00, 17:00, 18:00, 19:00, 20:00, 21:00, 22:00, 23:00 **Default:** 02:00

Setting: **time_date.daylight_saving_amount**

Description: Sets the daylight savings time offset in minutes.

Values: 0-255 **Default:** 60

Setting: **time_date.timezone_dhcp_option**

Description: Enables or disables DHCP option 2/100/101 for determining time zone information.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **time_date.ntp_server_update_interval**

Description: Sets the delay between NTP server updates, in seconds.

Values: 0-4294967295 **Default:** 1000

Setting: **time_date.time_and_date**

Description: Manually sets the date and time. Use the format <year>-<month>-<day>T<hour>:<minute>:<second>

Values: <year>-<month>-<day>T<hour>:<minute>:<second> **Default:** 2016-03-01T12:00:00

6.6.6 Log Settings ("log" Module)

The log settings control system logging activities. System logging may be required for troubleshooting purposes. The following logging modes are supported:

* Syslog server—output to a log file on a separate server (Syslog server)

The log settings follow the format: log.[element].

All the log settings are included in the general configuration file.

Setting:	**log.syslog_enable**		
Description:	Enables or disables log output to syslog server.		
Values:	0 (disabled), 1 (enabled)	**Default:**	0

Setting:	**log.syslog_server_address**		
Description:	Sets the syslog server IP address.		
Values:	Text string (IPv4 or IPv6)	**Default:**	Blank

Setting:	**log.syslog_server_port**		
Description:	Sets the syslog server port.		
Values:	1-65535	**Default:**	514

Setting:	**log.syslog_level**		
Description:	Sets the log level. The higher the level, the larger the debug output. 5 - all 4 - debug 3 - info 2 - warning 1 - error 0 - critical		
Values:	0-5	**Default:**	2

6.6.7 Web Settings ("web" Module)

The web settings control the web server IP, port, and security settings.

The web settings follow the format: web.[element].

All the web settings are included in the general configuration file.

Setting: **web.server_enable**

Description: Enables or disables the availability of the phone's embedded Web Portal.

Values: 0 (disabled), 1 (enabled) **Default:** 1

Setting: **web.http_port**

Description: Sets the http port when http is enabled.

Values: 1-65535 **Default:** 80

Setting: **web.https_enable**

Description: Sets server to use the https protocol.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **web.https_port**

Description: Sets the https port when https is enabled.

Values: 1-65535 **Default:** 443

6.6.8 Trusted IP Settings ("trusted_ip" Module)

The trusted_ip settings provide enhanced security for the HD10X. When enabled, these settings can filter network traffic and reject any traffic from unauthorized sources.

The trusted_ip settings follow the format: trusted_ip.[element].

All the trusted_ip settings are included in the general configuration file.

Setting: **trusted_ip.only_accept_allowed_ip**

Description: Enables or disables using the Allowed IP list to filter network traffic. When enabled, all unsolicited IP traffic will be blocked unless it is from one of the trusted IP addresses on the "Allowed IP" list.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **trusted_ip.x.allow_ip**

Description: Enter an IP address or address range for one instance of the “Allowed IP” list. x ranges from 1 to 10. See Section 3.4.5.4 Trusted IP for more information.

Values: Text string (IPv4 or IPv6, IP range in IPv4 or IPv6) **Default:** Blank

6.6.9 Trusted Server Settings (“trusted_servers” Module)

The trusted_servers settings provide enhanced security for the HD10X. When enabled, these settings can filter network traffic and reject any traffic from unauthorized sources.

The trusted_servers settings follow the format: trusted_servers.[element].

All the trusted_servers settings are included in the general configuration file.

Setting: **trusted_servers.only_accept_sip_account_servers**

Description: Enables or disables using each enabled account's Registration server, SIP server, Outbound Proxy server and Backup Outbound Proxy server as sources for trusted SIP traffic.

Values: 0 (disabled), 1 (enabled) **Default:** 0

6.6.10 User Preference Settings ("user_pref" Module)

The user settings are accessible to the HD10X user. These settings are useful for initial setup. You may wish to remove these settings from auto-provisioning update files so that users do not have their own settings overwritten.

The user preference settings follow the format: user_pref.[element].

General configuration file settings

Setting: **user_pref.account.1.ringer**

Description: Sets the ring tone for account 1.

Values: 1-10 **Default:** 3

Setting: **user_pref.call_terminated.busy_tone_enable**

Description: Enables the HD10X to play a busy tone when the far-end party ends the call, or when a network error condition (keep-alive failure) occurs.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **user_pref.ringer_volume**

Description: Sets the ringer volume (0 is OFF).

Values: 0-9 **Default:** 5

Setting: **user_pref.absent_timeout**

Description: Sets the absent timeout (the interval after going off hook with no action taken) in seconds. After the absent timeout, the phone returns to idle mode.

Values: 10-60 **Default:** 30

Setting: **user_pref.speaker_volume**

Description: Sets the speakerphone volume.

Values: 1-9 **Default:** 5

Setting: **user_pref.moh_timeout**

Description: Sets music on hold timeout.

Values: 1-9 **Default:** 2

6.6.11 Call Settings ("call_settings" Module)

Setting: **call_settings.account.1.block_anonymous_enable**

Description: Enables or disables anonymous call blocking.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **call_settings.account.1.fwd_always_enable**

Description: Enables call forward always

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **call_settings.account.1.fwd_always_target**

Description: Call forward target number

Values: TEXT **Default:** Empty

Setting: **call_settings.hotline_enable**

Description: Enables or disables the hotline (Emergency Dialing) feature.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **call_settings.hotline_number**

Description: Sets the number dialed by the hotline (Emergency Dialing) feature.

Values: number or alpha-numeric ID, with or without the host part of the SIP URI are accepted; IP entry has to be supported if IP dialing is supported **Default:** Blank

Setting: **call_settings.hotline_delay**

Description: Sets the delay (in seconds) between the phone going off hook and the hotline (emergency) number being dialed.

Values: 0-10 **Default:** 0

Setting: **call_settings.account.1.cfna_enable**

Description: Enables call forward when no answer

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **call_settings.account.1.cfna_target**

Description: Call forward when no answer target number

Values: TEXT **Default:** Empty

Setting: **call_settings.account.1.cfna_delay**

Description: Set when no answer delay before call forward (number of rings)

Values: 1-10 **Default:** 6

6.6.12 Programmable Feature Key Settings ("pfk" Module)

The programmable feature key (PFK) settings store the data associated with each programmable feature key.

The programmable feature key settings follow the format: pfk.x.[element], where x is the programmable feature key ID, ranging from 1 to 10, and 13-14. All the programmable feature key settings are included in the general configuration file.

Setting: **pfk.x.quick_dial**

Description: Sets the quick dial string to use if quick dial is assigned to PFK x.

- x = 1-10 for speed dial keys 1-10 on telephone base
- x = 13 for Service key (HS SER.) on cordless handset
- x = 14 for Emergency key (HS EMER.) on cordless handset

Values: Text string (SIP URI) **Default:** Blank

Setting: **pfk.x.account**

Description: Sets the SIP account used for the assigned feature (if applicable).

- x = 1-10 for speed dial keys 1-10 on telephone base
- x = 13 for Service key (HS SER.) on cordless handset
- x = 14 for Emergency key (HS EMER.) on cordless handset

Values: 1 **Default:** 1

6.6.13 Audio Settings (“audio” Module)

The audio settings include jitter buffer parameters and RTP port settings.

All the audio settings are included in the general configuration file.

Setting: **audio.x.jitter_mode**

Description: Select the desired mode for the jitter buffer: fixed (static) or adaptive. This setting depends on your network environment and conditions.

Values: fixed, adaptive **Default:** adaptive

Setting: **audio.x.fixed_jitter.delay**

Description: When in fixed jitter buffer mode, set the delay (in ms) desirable to provide good audio quality with the minimal possible delay.

Values: 30-500 **Default:** 70

Setting: **audio.x.adaptive_jitter.min_delay**

Description: When in adaptive jitter buffer mode, set the minimum delay (in ms) desirable to maintain data packet capture and audio quality.

Values: 20-250 **Default:** 60

Setting: **audio.x.adaptive_jitter.target_delay**

Description: When in adaptive jitter buffer mode, set the target delay (in ms) desirable to provide good audio quality with the minimal possible delay.

Values: 20-500 **Default:** 80

Setting: **audio.x.adaptive_jitter.max_delay**

Description: When in adaptive jitter buffer mode, set the maximum delay (in ms) desirable to maintain data packet capture and audio quality.

Values: 180-500 **Default:** 240

Setting: **audio.x.rtp.port_start**

Description: Sets the Local RTP port range start.

Values: 1-65535 **Default:** 18000

Setting: **audio.x.rtp.port_end**

Description: Sets the Local RTP port range end.

Values: 1-65535 **Default:** 19000

Setting: **audio.rtcp_xr.enable**

Description: Enables or disables reporting of RTCP XR via SIP to a collector server. RTP Control Protocol Extended Reports (RTCP XR) are used for voice quality assessment and diagnostics.

Values: 0 (disabled), 1 (enabled) **Default:** 0

6.6.14 TR-069 Settings ("tr069" Module)

The Broadband Forum's Technical Report 069 (TR-069) defines a protocol for remote management and secure auto-configuration of compatible devices. The TR-069 settings allow you to enable TR-069 and configure access to an auto-configuration server (ACS).

All the TR-069 settings are included in the general configuration file.

Setting: **tr069.enable**

Description: Enable/disable the TR-069 subsystem.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **tr069.acs.url**

Description: Enter the URL to the auto configuration server (ACS).

Values: Text string **Default:** Blank

Setting: **tr069.acs.username**

Description: Enter user name for ACS authentication.

Values: Text string **Default:** Blank

Setting: **tr069.acs.access_password**

Description: Enter password for ACS authentication.

Values: Text string **Default:** Blank

Setting: **tr069.periodic_inform.enable**

Description: Enable/disable the phone sending Inform messages to the server.

Values: 0 (disabled), 1 (enabled) **Default:** 0

Setting: **tr069.periodic_inform.interval**

Description: Set the interval (in seconds) between sending Inform messages.

Values: 1-65535 **Default:** 3600

Setting: **tr069.connection_request.username**

Description:	Set the user name for authenticating the connection sent from the ACS.		
Values:	Text string	**Default:**	Blank

Setting:	**tr069.connection_request.access_password**		
Description:	Set the password for authenticating the connection sent from the ACS.		
Values:	Text string	**Default:**	Blank

Setting:	**user_pref.voice_guide_password = 4 digits of Number**		
Description:	Set the password for voice menu and only 4 digits allowed.		
Values:	4 digits	**Default:**	Blank

7 Troubleshooting

If you have difficulty with your H-series phones, please try the suggestions below.

For customer service or product information, contact the person who installed your system. If your installer is unavailable, visit our website at *www.snom.com* for contact and support information.

7.1 Common Troubleshooting Procedures

Follow these procedures to resolve common issues. For more troubleshooting information, see the phone specific setup guide for your product.

The DECT handset doesn't register. "Registration failed" appears on the screen.

- Ensure the handset is fully charged and in the charger. Remove and replace the handset in its charger before selecting **Register** on the HD10X.
- Ensure the handset is not already registered to another base. If it has been registered to another base, deregister it.

The firmware upgrade or configuration update is not working.

- Before using the Web Portal, ensure you have the latest version of your web browser installed. Some menus and controls in older browsers may operate differently than described in this manual.
- Ensure you have specified the correct path to the firmware and configuration files on the **SERVICING > Firmware Upgrade > Auto Upgrade** page and the **SERVICING > Provisioning** page.

8 Appendix

The configuration methods below are only applied to HM201.

8.1 Upload / Update Handset Screen Wallpaper for HD1

HD1 is the color display handset of HM201.

Handset Screen Wallpaper Requirements

- File format: bmp (e.g. wallpaper1.bmp)
- Resolution: 240x320 / Color depth: 24bit
- Example:

Set Wallpaper's URL

- Set the new wallpaper's URL (See Setting: file.hs_idle_logo on page 89 in Section 6.6.2 Handset Settings ("hs_settings" Module)
- Example: file.hs_idle_logo = http://www.yourcompany.com/wallpaper1.bmp

Upload/Change Wallpaper

- Import a configuration file with the line of the new wallpaper's URL via web portal from your computer or your local network (See Section 3.4.4.5 Import Configuration)

  OR

- Use auto-provisioning (See Section 3.4.4 Provisioning)

8.2 Upload/Update Firmware for HM201 Only

Upload/update by

- Color handset firmware box (See Section 3.4.3.2 Manual Firmware Update and Upload)

  OR

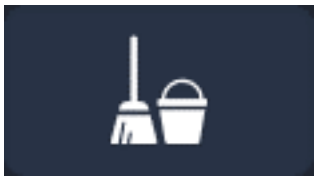
- Auto-provisioning (See Section 3.4.4 Provisioning)

8.3 Speed Dial Settings for HM201

- image pending till product is available

Icon List for HD1

Icon	Description	Icon Index
	Front Desk	1
	Guest Service	2
	Room Service	3
	Restaurant	4
	Concierge	5
	Message	6
	Ticket Booking	7

	Emergency	8
	Wake Up	9
	House Keeping	10
	Laundry	11
	Valet	12
	SPA	13

Note:

1. Input icon name in the Description column, which will be displayed in the color screen of HD1.
2. Input speed dial number in the Value column. User will dial the speed dial numbers when he/she presses these speed dial numbers' corresponding icons on the color screen of HD1.
3. Choose Icon Index from the drop-down menu.
4. Set the three hard keys named **Emergency**, **Front Desk** and **Message** in the first three rows highlighted by green box above. They can be also added to the speed dial list on handset color screen in the other rows of this table.

- image pending till product is available

Note:

1. The fourth row of the Speed Dial Settings is for setting the middle soft key of HD1, both of which are highlighted by red box above.

   ***** Soft keys perform the action indicated by the on-screen labels.

   ***** When user presses the middle soft key highlighted by red box, the telephone number input in value column of the fourth row in the Speed Dial Settings will be dialed.

2. When user presses **SpdDial**, the right soft key highlighted by blue box, the speed dial icon list will appear on the handset color screen. Press ^ or v to select a speed dial entry. Press **OK**, then its corresponding speed dial number will be dialed.

snom

SIP Phone Configuration Guide_2023.02.23