



SecurAccess SIP Basic Line



NOTICE D'UTILISATION

Ref: PXB41A

Cet appareil conçu et développé en France est destiné à être connecté sur un serveur VoIP ou ToIP.

Depaepe

Tel : +33 (0)1 30 25 81 60

Fax: +33 (0)1 39 98 61 24

Site Web: www.depaepe.com

Table des matières

1. PRÉSENTATION GÉNÉRALE.....	3
2. INSTALLATION.....	6
2.1. PLANS DE PERÇAGE.....	6
2.3. PASSAGE DES CÂBLES.....	9
2.3. RACCORDEMENT ET INSTALLATION.....	10
3. UTILISATION.....	12
3.1. IDENTIFICATION DES BOUTONS D'APPEL.....	12
3.2. PASSER UN APPEL.....	12
3.3. RÉPONDRE À UN APPEL.....	12
3.4. RACCROCHÉ AUTOMATIQUE.....	12
4. CONFIGURATION.....	13
4.1. ACCÉDER À L'INTERFACE WEB.....	13
4.2. STATUS.....	14
4.3. COMPTE.....	15
4.3.1. BASIQUE.....	15
4.3.2. CODEC.....	18
4.3.3. AVANCÉ.....	19
4.4. RÉSEAU.....	22
4.4.1. BASIQUE.....	22
4.4.2. AVANCÉ.....	24
4.5. RÉGLAGES.....	26
4.5.1. PRÉFÉRENCES.....	26
4.5.2. FONCTIONS.....	27
4.5.3. TONALITÉS.....	28
4.5.4. DATE & HEURE.....	29
4.6. MANAGEMENT.....	29
4.6.1. MOT DE PASSE.....	30
4.6.2. MISE À JOUR.....	30
4.6.3. AUTO-PROVISION.....	31
4.6.4. CONFIGURATION.....	33
4.6.5. TRUSTED CA.....	34
4.6.6. SERVER CA.....	34
4.6.7. OUTILS.....	35
4.6.8. REDÉMARRAGE.....	35
4.6.9. REBOOT.....	36
5. CONFIGURATION VIA UN SERVEUR CENTRAL.....	36
6. MISE À JOUR DU LOGICIEL.....	38
7. RESTAURATION DES PARAMÈTRES D'USINE.....	38
8. GABARIT D'ÉTIQUETTES.....	39
9. CARACTÉRISTIQUES.....	39
10. DÉCLARATION DE CONFORMITÉ.....	39
11. GARANTIE ET S.A.V.....	40

1. Présentation générale

Les portiers **SecurHD IP** sont des téléphones IP compatibles avec tous les serveurs VoIP et ToIP.

Ils sont conformes aux indices de protection **IP65 (étanchéité)** et **IK09 (mécanique)**, et destinés à être installés :

- en encastré ou en saillie,
- à l'intérieur d'un bâtiment comme à l'extérieur, à des emplacements où la notion de sécurité est importante (locaux non surveillés, lieux ouverts au public, risque de vandalisme, intempéries).

Ces fonctions ne nécessitent pas d'être alimentées par une source extérieure supplémentaire.

Dans tous les cas, l'appareil est alimenté soit via une alimentation externe (non fournie), soit via grâce à la technologie PoE (Power over Ethernet).

Ces deux sources ne doivent pas être connectées en même temps sur le SecurHD IP. Votre administrateur réseau pourra vous indiquer la solution la plus appropriée.

Les principales fonctions :

1. Appel

P2P (sur adresse IP fixe) / SIP (sur numéro direct compte SIP).

Modèles sans clavier, 1, 2, 3, ou 4 boutons d'appels programmables.

Modèles à clavier, numérotation libre, et de 1 à 4 boutons.

2. Décrochage automatique

Sur appel entrant, le SecurHD IP décroche automatiquement pour établir une communication audio. Le décrochage se fait automatiquement après un appel.

3. Raccrochage automatique

Par détection de fin de communication.

4. Administration via WebAccess

La programmation se fait par l'interface web du portier ou par provisioning.

Modèles avec clavier



Modèles sans clavier



Vis de fixation

Haut-parleur

Boutons mémoire

Microphone

Vis de fixation

2. Installation

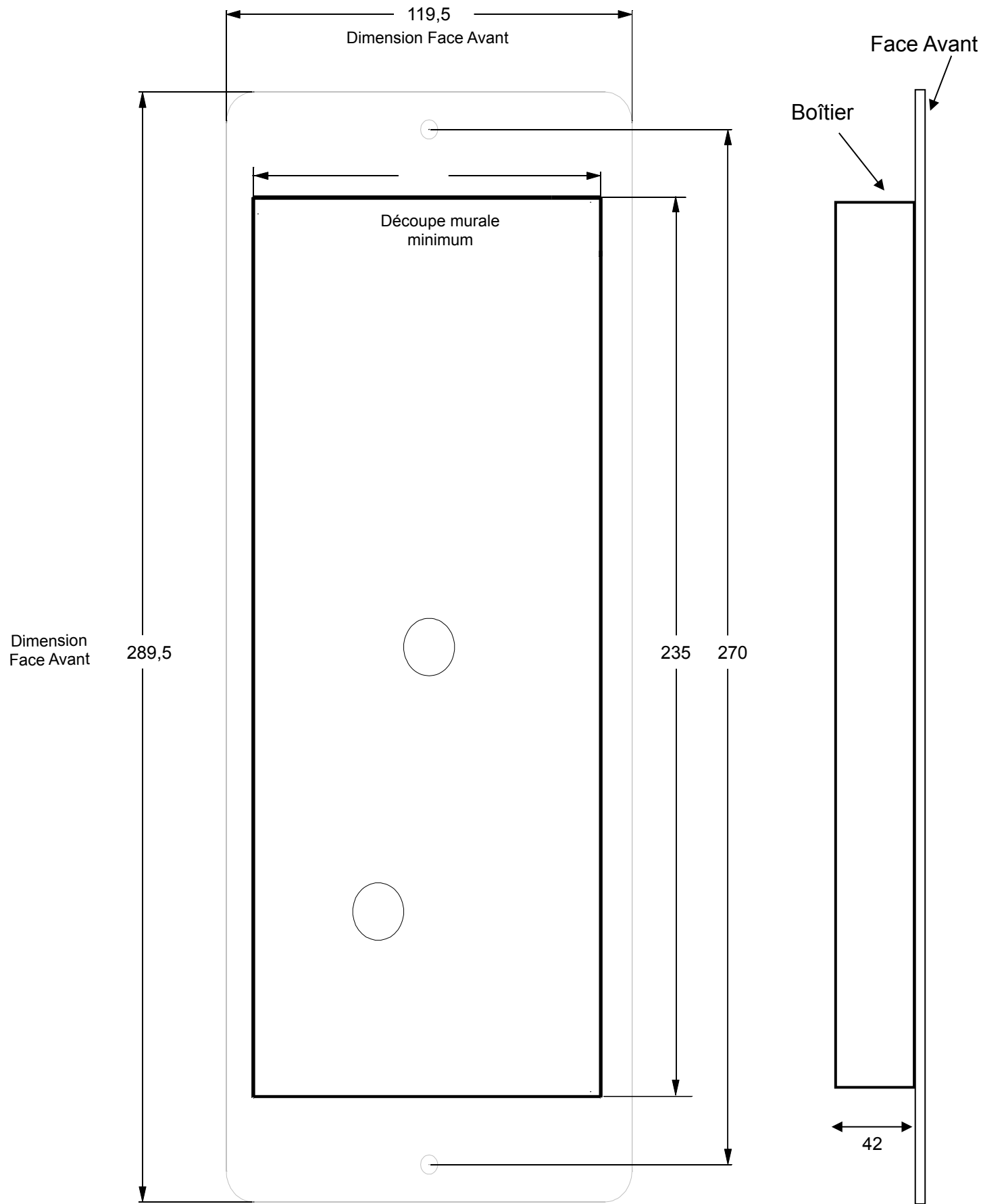
L'installation, le raccordement et la configuration doivent être effectués par du personnel qualifié (installateur, électricien, ...). Toutes les opérations nécessitant une ouverture de l'appareil doivent s'effectuer en prenant toutes les précautions nécessaires pour éviter les chocs électriques.



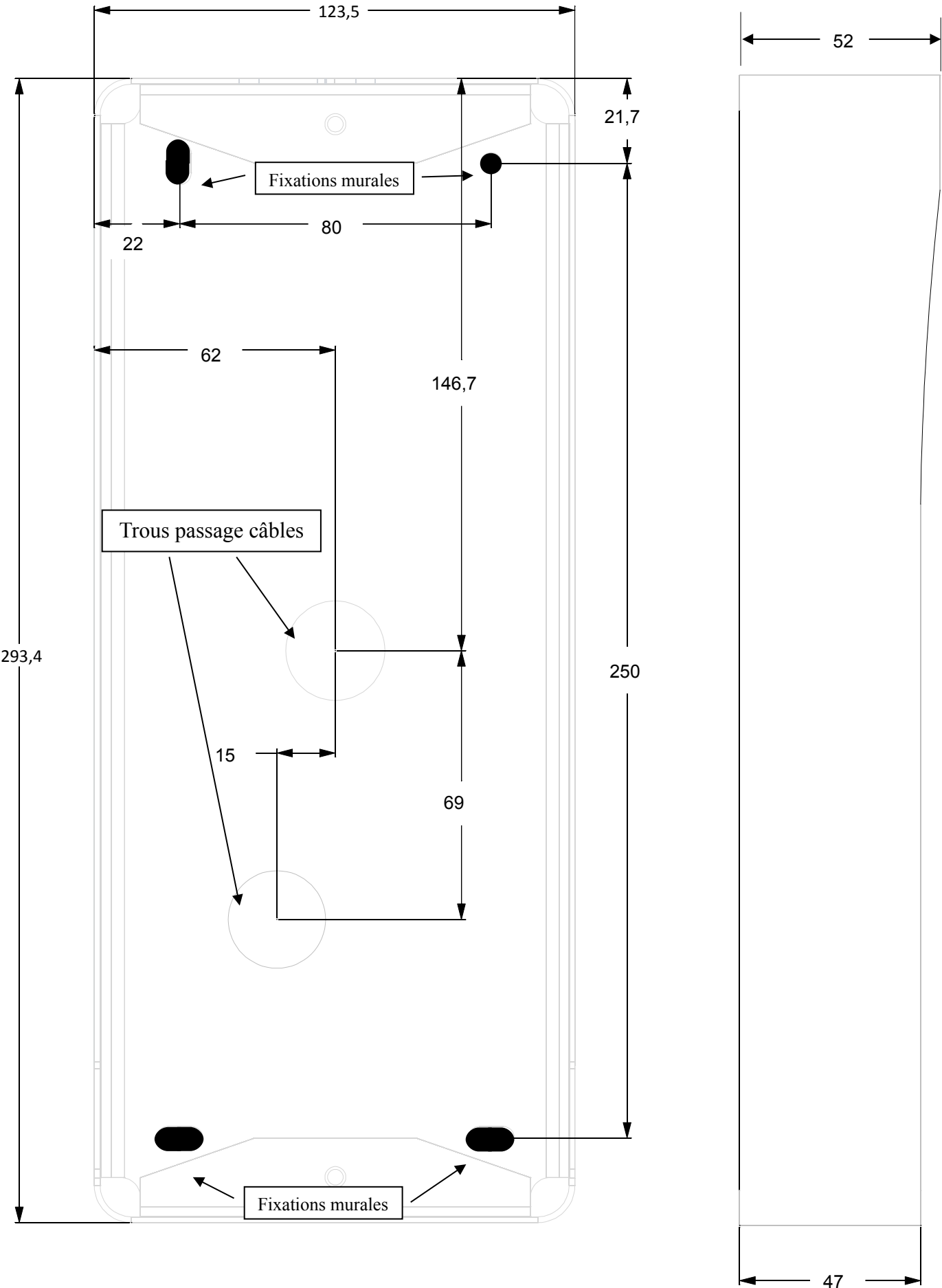
2.1. Plans de perçage

Voir pages 8 et 9.

Plans de perçage mural



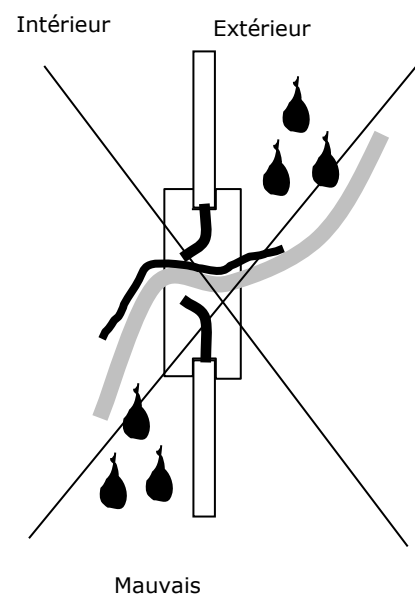
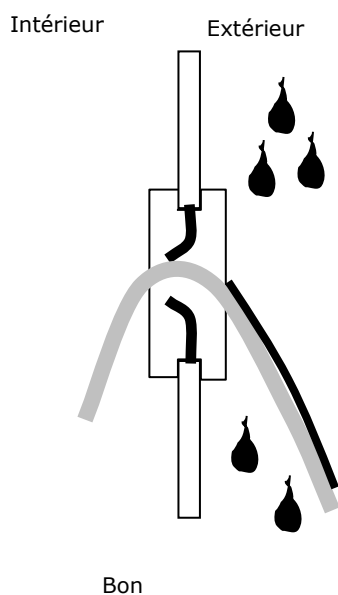
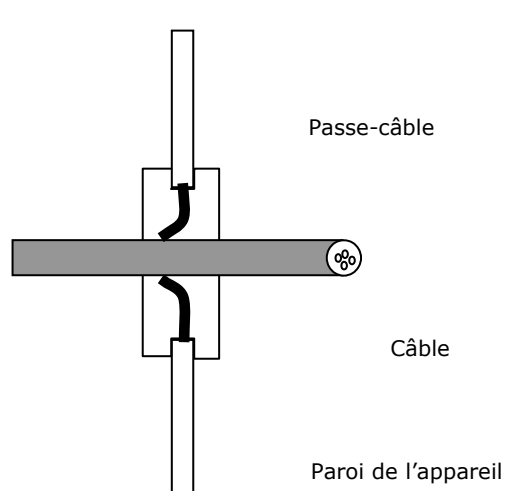
Plans de découpe pour le montage encastré



2.3. Passage des câbles



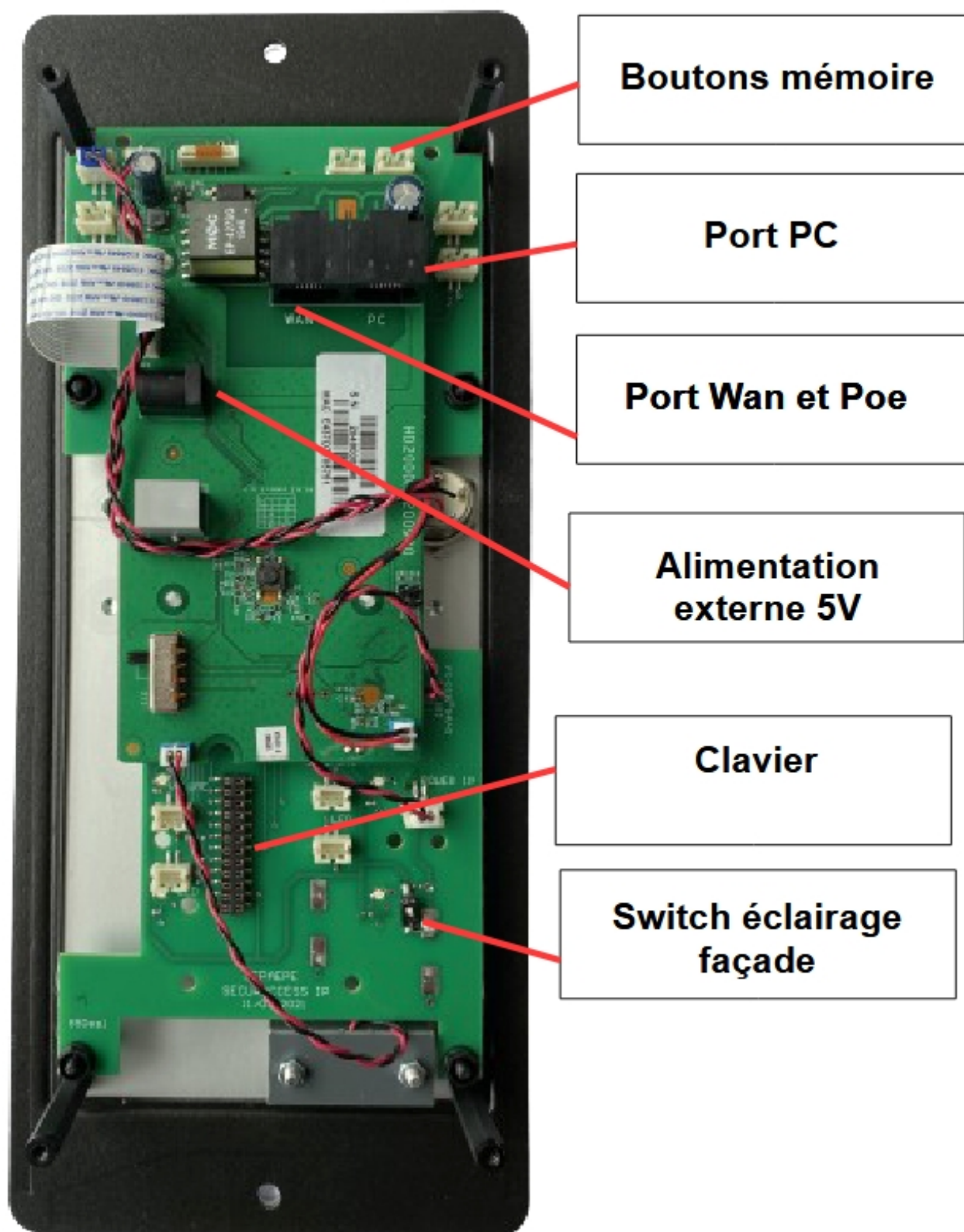
Afin d'obtenir la meilleure étanchéité souhaitée :
percer les passes câbles avec une dimension inférieure à celle du câble, orienter la
sortie du câble vers le bas afin de ne pas favoriser le stockage et l'écoulement
d'eau (par son stockage) à l'intérieur du produit.



Les boîtiers ont été percés à plusieurs endroits afin de permettre
une ventilation naturelle.
Veiller à ne pas obturer ces trous de ventilation !

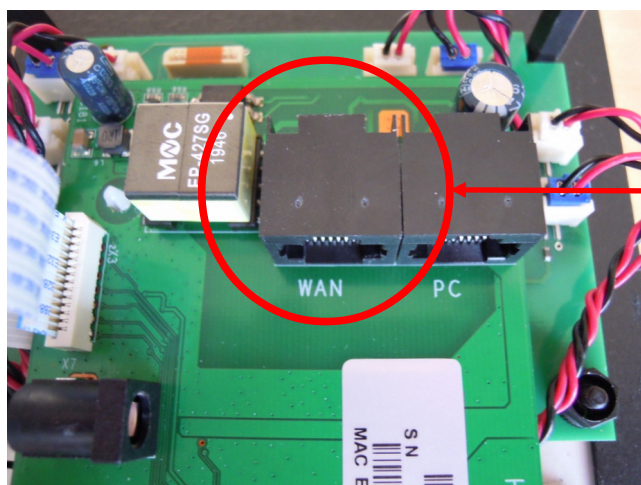
2.3. Raccordement et installation

Modèles avec clavier



Réseau Ethernet et PoE

Une embase RJ45 prévoit le raccordement du SecurHD IP au **réseau Ethernet** avec la possibilité d'une alimentation **PoE** (Power Over Ethernet) par le biais du câble Ethernet.

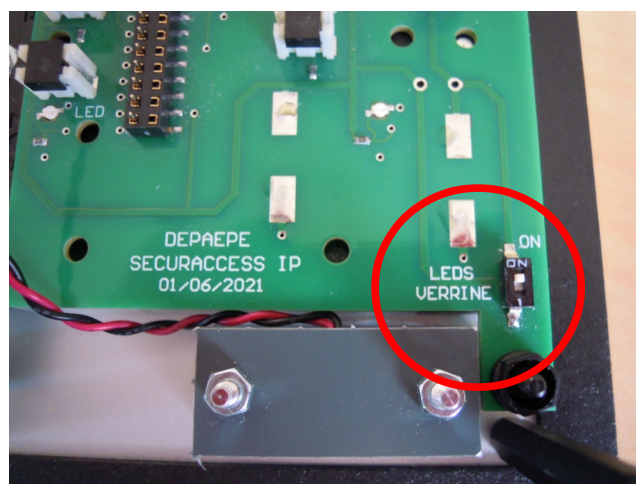


Accès TRT3 (TNV-3)

Embase RJ45 pour
raccordement Ethernet

La fonction d'éclairage ne nécessite pas d'alimentation supplémentaire.

Elle peut être activée ou désactivée grâce à un interrupteur situé sur la carte.



Ce terminal est conçu pour être raccordé sur un réseau téléphonique (Classé TRT3 au sens de la norme EN 60950 amendements 1 à 11).

Ces deux sources ne doivent pas être connectées en même temps sur le SecurHD IP. Votre administrateur réseau pourra vous indiquer la solution la plus appropriée.

3. Utilisation

3.1. Identification des boutons d'appel

Les boutons d'appel en façade sont toujours numérotés de Droite à Gauche et de Haut en Bas, de Bt1 à Bt4, quelque soit le nombre de boutons disponibles.

3.2. Passer un appel

1) Par bouton d'appel direct (numérotation automatique)

Pour appeler, appuyer sur un des boutons d'appel, le numéro principal en mémoire sera composé automatiquement (après paramétrage des mémoires des boutons d'appel (cf §4.5.2 page 31)).

Lorsque la communication est établie, l'appareil passe en mode conversation « Mains-libres » et vous entendez votre interlocuteur.

Le raccrochage se fait soit automatiquement lorsque la conversation est terminée, ou soit en appuyant de nouveau sur le bouton d'appel.

2) Par composition clavier (numérotation manuelle – modèle à clavier uniquement)

Le clavier du SecurHD IP fonctionne en mode numérotation libre.

Pour appeler, composer le numéro et attendre 4 secondes (pause par défaut, réglable) avant que la numérotation soit lancée ou valider par la touche « # ».

NOTE : En mode « P2P » (peer to peer), l'adresse IP d'un poste peut être utilisée pour réaliser un appel à condition d'être sur le même segment réseau. Pour cela, composer depuis le clavier l'adresse IP du poste en remplaçant les « . » par des « * ».

Exemple : pour l'adresse IP 192.168.92.100, on composera 192*168*92*100.

3.3. Répondre à un appel

Lorsque le portier est appelé, il décroche automatiquement.

Lorsque la communication est établie, l'appareil passe en mode conversation.

Le raccrochage se fait sur appui du bouton d'appel ou lorsque l'appelé met fin à la conversation.

3.4. Raccroché automatique

Lorsque vous êtes en numérotation ou en conversation, le portier est susceptible de mettre fin à la communication en fonction de certains paramètres.

Le SecurHD IP raccrochera automatiquement dans le cas où un nouvel appui sera fait sur le bouton d'appel.

4. Configuration

Le SecurHD IP intègre un serveur Web et des pages HTML qui permettent aux utilisateurs de configurer le SecurHD IP via une interface de navigateur Web facile à utiliser.

4.1. Accéder à l'interface web

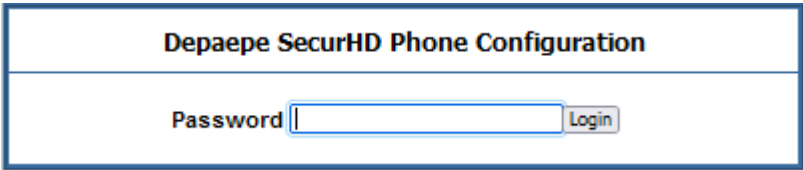
Connectez le SecurHD IP à un réseau via un câble Ethernet standard, par défaut, le SecurHD IP est en mode DHCP.

Utilisez un analyseur de protocole réseau standard (par exemple Wireshark) pour obtenir l'adresse IP allouée à l'unité de base par le serveur DHCP. Vous pouvez également contacter votre administrateur pour obtenir l'adresse IP allouée au SecurHD IP par le serveur DHCP.

La page de configuration du SecurHD IP est accessible via votre navigateur Web en saisissant l'adresse IP WAN: **HTTP://adresseIP**

Assurez-vous que votre PC est connecté au même réseau que le SecurHD IP.

À partir de votre navigateur Web, le SecurHD IP affichera l'écran de connexion suivant:



The screenshot shows a web interface titled "Depaepe SecurHD Phone Configuration". Below the title, there is a label "Password" followed by a text input field and a "Login" button.

Par défaut, le mot de passe est : **admin**

4.2. Status

Après avoir validé le mot de passe dans l'écran de connexion, le serveur Web intégré au SecurHD IP affichera la page de configuration suivante, qui est expliquée en détails ci-dessous :

Status

- Version**
 - Product Model: SecurHD IP
 - Firmware Version:
 - BOOT--2.0.5.16(2018-07-30 18:43:00)
 - IMG--1.0.4.32(2021-09-06 17:27:00)
 - ROM--1.0.4.32(2021-09-06 17:27:00)
 - DSP--9.0.3(Patch 1.0.16M)
- Account Status**
 - Account: Registered
- Network**
 - WAN Port Type: Static IP
 - WAN IP Address: 192.168.100.218
 - Subnet Mask: 255.255.255.0
 - Gateway: 192.168.100.2
 - Primary DNS: 0.0.0.0
 - Secondary DNS: 0.0.0.0
 - MAC Address: e4:37:d7:10:57:24
 - Device Type: Bridge
- Memory Free**: 53724 KB
- System Up Time**: 11 day(s) 22 hour(s) 59 min(s) 22 sec(s)
- Restart**: Restart

NOTE

Version:
It shows product type and the version of firmware.

Account Status:
It shows the registered status of accounts.

Network:
It shows the information of WAN port and LAN ports.

System Up Time:
It shows the running time after device power up.

Restart:
This button will restart the voip application

Product Model	Contains the product model info.
Firmware Version	• Boot: Booting code version number. • IMG: This is the main software (firmware) release number, always used to identify the software (firmware) system of the phone. • ROM: This is the main software (firmware) release number, always used to identify the software (firmware) system of the phone. • DSP: Powerful Digital Signal Processing (DSP) technology to ensure superior audio quality.
Account	Indicates whether account are registered to the related SIP server(s).
WAN Port Type	This field shows type of IP address of SecurHD IP.
WAN IP Adess	This field shows IP address of SecurHD IP.
Subnet Mask	This field shows Subnet Mask address of SecurHD IP.
Gateway	This field shows Gateway address of SecurHD IP.
Primary DNS	This field shows Primary DNS address of SecurHD IP.
Secondary DNS	This field shows Secondary address of SecurHD IP.
MAC Address	This field shows MAC address of SecurHD IP.

4.3. Compte

4.3.1. Basique

Basic

Codec

Advanced

Account Status

* Account Active ☐ No ☒ Yes

* Primary SIP Server ?

Failover SIP Server ?

Second Failover SipServer ?

Prefer Primary SIP Server ☒ No ☐ Yes ?

Outbound Proxy ?

Backup Outbound Proxy ?

* SIP Transport ☐ UDP ☒ TCP ☐ TLS ?

NAT Traversal ☐ No ☒ No, but send keep alive ☐ STUN

Label ?

* SIP User ID ?

* Authenticate ID ?

* Authenticate Password ?

Name ?

Registered

DNS Mode ☒ A Record ☐ SRV ☐ NAPTR/SRV

User ID Is Phone Number ☐ No ☒ Yes

SIP Registration ☐ No ☒ Yes

Unregister On Reboot ☒ No ☐ Yes

Register Expiration ?

Outgoing Call Without Registration ☐ No ☒ Yes

Local SIP Port ?

Use Random Port ☒ No ☐ Yes

Voice Mail UserID ?

RPort ☒ No ☐ Yes

RFC 2543 Hold ☐ No ☒ Yes

SaveSet

Restart

NOTE

* fields must be filled and require a phone restart

Basic:
The Basic Parameters set for administrator

Codecs:
Choose the codecs you want to use.

Advanced:
The Advanced parameters for administrator.

Account Status	Indicates whether accounts are registered to the related SIP server(s).
Account Active	When set to Yes the FXS port is activated Sip.mycompany.com or IP Adress.
Primary SIP Server	This field contains the URI string or the IP address (and port, if different from 5060) of the SIP primary server. Examples : sip.my-voip-provider.com, or sip:my-company-sip-server.com, or 192.168.1.200:5066
Failover SIP server	Optional, used when primary server no response. This field contains the URI string or the IP address (and port, if different from 5060) of the SIP failover server. Examples : sip.my-voip-provider.com, or sip:my-company-sip-server.com, or 192.168.1.200:5066

Second Failover Sip Server	Optional, used when failover SIP Server no response. This field contains the URI string or the IP address (and port, if different from 5060) of the SIP Second failover server. Examples : sip.my-voip-provider.com, or sip:my-company-sip-server.com, or 192.168.1.200:5066
Prefer Primary SIP Server	Optional, used when failover SIP Server no response. Yes – will register to primary server if failover registration expires.
Outbound proxy	This field contains the URI string or the IP address (and port, if different from 5060) of the outbound proxy. If there is no outbound proxy, this field SHOULD be left blank. If not blank, all outgoing requests will be sent to this outbound proxy. proxy.myprovider.com or IP Address.
Backup Outbound Proxy	This is usually set as IP Address
SIP Transport	Default is UDP.
NAT Transersal	This parameter defines whether or not the SecurHD IP NAT traversal mechanism is activated. If activated (by choosing “Yes”) and a STUN server is also specified, then the SecurHD IP performs according to the STUN client specification. Using this mode, the embedded STUN client will detect if and what type of firewall/NAT is being used. If the detected NAT is a Full Cone, Restricted Cone, or a Port-Restricted Cone, the SecurHD IP will use its mapped public IP address and port in all of its SIP and SDP messages. If the NAT Traversal field is set to “Yes” <i>with no specified STUN server</i> , the SecurHD IP will periodically (every 20 seconds or so) send a blank UDP packet no payload data) to the SIP server to keep the “hole” on the NAT open.
Label	The name show on the LCD of the current device.
SIP User ID	SIP service subscriber’s User ID.
Authenticate ID	SIP service subscriber’s Authenticate ID. Can be identical to or different from SIP User ID.
Authenticate Password	SIP service subscriber’s account password.
Name	SIP service subscriber’s Label which will be used for Caller ID display.
DNS Mode	Choice of the DNS mode.
User ID is Phone Number	If the SecurHD IP has an assigned PSTN telephone number, this field should be set to “Yes”. Otherwise, set it to “No”. If “Yes” is set, a “user=phone” parameter will be attached to the “From” header in SIP request.
SIP Registration	This parameter controls whether the SecurHD IP needs to send REGISTER messages to the proxy server. The default setting is “Yes”.
Unregister On Reboot	Default is “No.” If set to “Yes”, then the SIP user will be unregistered on reboot.
Register Expiration	This parameter allows the user to specify the time frequency (in minutes) the SecurHD IP refreshes its registration with the specified registrar. The default interval is 60 minutes (or 1 hour). The maximum interval is 65535 minutes (about 45 days).
Outgoing call without registration	Default is No . If set to “Yes,” user can place outgoing calls even when not registered (if allowed by ITSP) but is unable to receive incoming calls.
Local SIP Port	This parameter defines the local SIP port the SecurHD IP will listen and

	transmit. The default value for FXS port is 5060. The default value for FXO port is 5062.
Use Random port	This parameter, when set to Yes, will force random generation of both the local SIP and RTP ports. This is usually necessary when multiple SecurHD IP are behind the same NAT.
Voice Mail User ID	The number for check voice mail.
RPort	RPort in RFC 3581.
RFC 2543 Hold	By default is Yes. Enable if Yes or disable if No : Hold

4.3.2. Codec

Preferred Vocoder In listed order:

Choice 1:

Choice 2:

Choice 3:

Choice 4:

Choice 5:

Choice 6:

PTime(ms):

G723 Rate: ☒ 6.3kbps encoding rate
☐ 5.3kbps encoding rate

iLBC mode: ☒ 20ms mode
☐ 30ms mode

iLBC Payload Type: ?

NOTE

Basic:
The Basic Parameters set for administrator.

Codecs:
Choose the codecs you want to use.

Advanced:
The Advanced parameters for administrator.

Preferred Vocoder In listed order	The SecurHD IP supports up to 7 different Vocoder types including G.711 A-/U-law , G.723.1, G.726, G.729A/B, G.722, iLBC, GSM_FR . Depending on the product model, some of these Vocoders may not be provided in standard release. Users can configure Vocoders in a preference list that will be included with the same preference order in SDP message. The first Vocoder in this list can be entered by choosing the appropriate option in "Choice 1". Similarly, the last Vocoder in this list can be entered by choosing the appropriate option in "Choice 7".
Voice Frames Per TX	This field contains the number of voice frames to be transmitted in a single packet. When setting this value, the user should be aware of the requested packet time (used in SDP message) as a result of configuring this parameter. This parameter is associated with the first vocoder in the above vocoder Preference List or the actual used payload type negotiated between the 2 conversation parties at run time. Examples : if the first vocoder is configured as G723 and the "Voice Frames per TX" is set to be 2, then the "ptime" value in the SDP message of an INVITE request will be 60ms because each G723 voice frame contains 30ms of audio. Similarly, if this field is set to be 2 and if the first vocoder chosen is G729 or G711 or G726, then the "ptime" value in the SDP message of an INVITE request will be 20ms. If the configured voice frames per TX exceeds the maximum allowed value, the SecurHD IP will use and save the maximum allowed value for the corresponding first vocoder choice. The maximum value for PCM is 10(x10ms) frames; for G726, it is 20 (x10ms) frames; for G723, it is 32 (x30ms) frames; for G729/G728, 64

	(x10ms) and 64 (x2.5ms) frames respectively.
G723 Rate	This defines the encoding rate for G723 vocoder. By default, 6.3kbps rate is chosen.
iLBC mode	from 96 to 127. By default, it is 97

4.3.3. Avancé

Basic

Codec

Advanced

DTMF Payload Type	101
DTMF Type	RFC2833
Send Flash Event	☒ No ☐ Yes ?
Enable Call Features	☐ No ☒ Yes ?
Proxy Require	
Use NAT IP	?
SRTP Mode	☒ Disabled ☐ Enabled but not forced ☐ Enabled and forced
VAD	☒ No ☐ Yes
Symmetric RTP	☒ No ☐ Yes
Jitter Buffer Type	☐ Fixed ☒ Adaptive
Jitter Buffer Length	☐ Low ☒ Medium ☐ High
Account Ring Tone	Ring3.bin
Ring Volume	4 ?
Ring Timeout	60 ?
Dial Plan	{[*^]+}
Subscribe for MWI	☒ No, do not send SUBSCRIBE for Message Waiting Indication ☐ Yes, send periodical SUBSCRIBE for Message Waiting Indication
Send Anonymous	☒ No ☐ Yes ?
Anonymous Call Rejection	☒ No ☐ Yes
Check SIP User ID	☒ Don't Check ☐ Always Check ☐ Automatic
Auto Answer	☒ No ☐ Yes
Allow Auto Answer By Call-Info	☐ No ☒ Yes
Turn off Speaker on remote disconnect	☒ No ☐ Yes
Session Expiration	180 ?
Min-SE	90 ?
Caller Request Timer	☒ No ☐ Yes ?
Callee Request Timer	☒ No ☐ Yes ?
Force Timer	☒ No ☐ Yes ?
UAC Specify Refresher	☐ UAC ☐ UAS ☒ Omit(Recommended)
UAS Specify Refresher	☒ UAC ☐ UAS(When UAC did not specify refresher tag)
Force Invite	☒ No ☐ Yes ?
Hook Flash Timing	minimum: 50 maximum: 100 ?
Refuse-Return-Code	486(Busy Here)
Caller Display Source	From Only

NOTE

Basic:
The Basic Parameters set for administrator

Codecs:
Choose the codecs you want to use.

Advanced:
The Advanced parameters for administrator.

DTMF Payload Type	This parameter sets the payload type for DTMF using RFC2833.
DTMF Type	Send DTMF as inband (in-audio), via RTP (According to RFC 2833), or via SIP INFO message.
Send Flash event	This parameter allows users to control whether to send an SIP NOTIFY message indicating the Flash event, or just to switch to the voice channel when users press the Flash key.
Enable Call Feature	Default is No. If set to Yes, Call Forwarding & Do-Not-Disturb are supported locally (see P.17) if Yes, call features using star codes will be supported locally
Proxy Require	SIP Extension to notify SIP server that the unit is behind the NAT/Firewall.
Use NAT IP	NAT IP address used in SIP/SDP message. Default is blank.
SRTP Mode	Secure Real-Time Transport Protocol (SRTP) encrypts the RTP during VoIP phone.
VAD	Default is No . VAD allows detecting the absence of audio and conserve bandwidth by preventing the transmission of "silent packets" over the network.
Symmetric RTP	Default is No . When set to Yes the device will change the destination to send RTP packets to the source IP address and port of the inbound RTP packet last received by the device.
Jitter Buffer Type	Select either Fixed or Adaptive based on network conditions.
Jitter Buffer Lengh	Select Low, Medium or High based on network conditions.
Account Ring Tone	There are 8 uniquely defined ring tones.
Ring Timeout	Incoming call will stop ringing when not picked up given a specific period of time.
Dial Plan	Dial Plan Rules:- 1. Accept Digits: 1,2,3,4,5,6,7,8,9,0 2. Grammar: x - any digit from 0-9; a. xx+ - at least 2 digit number; b. ^ - exclude; c. [3-5] - any digit of 3, 4, or 5; d. [147] - any digit 1, 4, or 7; e. <2=011> - replace digit 2 with 011 when dialing • Example 1: {[369]11 1617xxxxxxx} - Allow 311, 611, 911, and any 10 digit numbers of leading digits 1617 • Example 2: {^1900x+ <=1617>xxxxxxx} - Block any number of leading digits 1900 and add prefix 1617 for any dialed 7 digit numbers • Example 3: {1xxx[2-9]xxxxxxx <2=011>x+} - Allow any length of number with leading digit 2 and 10 digit-numbers of leading digit 1 and leading exchange number between 2 and 9; If leading digit is 2, replace leading digit 2 with 011 before dialing 3. Default: Outgoing - {x+}
Subscribe for MWI	Default is No. If set to "Yes" a SUBSCRIBE for Message Waiting Indication will be sent periodically.
Send Anonymous	If this parameter is set to "Yes", the "From" header in outgoing INVITE message will be set to anonymous, essentially blocking the Caller ID from displaying.
Anonymous Call Rejection	Default is No .

	If set to Yes, incoming calls with anonymous Caller ID will be rejected with 486 Busy message.
Check SIP User ID	When the phone receive INVITE, at first it will check if it is right the 'To' in the message.
Auto answer	Enable or disable the 'auto answer' feature
Allow Auto Answer By Call-Info	Enable or disable 'auto answer' when some call use Call-info to activate this feature.
Turn off Speaker on remote disconnect	When the remote user hang up, the phone will disable the speaker.
Session Expiration	The SIP Session Timer extension enables SIP sessions to be periodically "refreshed" via a SIP request (UPDATE, or re-INVITE). Once the session expires, if there is no refresh via a UPDATE or re-INVITE message, the session is terminated. Session Expiration is the time (in seconds) at which the session is considered timed out, provided no successful session refresh transaction occurs before hand. The default value is 180 seconds.
Min-SE	Defines the minimum session expiration (in seconds). Default is 90 seconds .
Caller Request Timer	If set to "Yes", the phone will use session timer when it makes outbound calls if remote party supports session timer.
Callee Request Timer	If selecting "Yes", the phone will use session timer when it receives inbound calls with session timer request.
Force Timer	If set to "Yes", the phone will use session timer even if the remote party does not support this feature. If set to "No", the session timer is enabled only when the remote party supports this feature. To turn off Session Timer, select "No" for Caller Request Timer, Callee Request Timer, and Force Timer.
UAC Specify Refresher	As a Caller, select UAC to use the phone as the refresher, or UAS to use the Callee or proxy server as the refresher.
UAS Specify Refresher	As a Callee, select UAC to use caller or proxy server as the refresher, or UAS to use the phone as the refresher.
Force Invite	Session Timer can be refreshed using INVITE method or UPDATE method. Select "Yes" to use INVITE method to refresh the session timer.
Hook Flash Timing	The time break for hook flash
Refuse-Return-Code	This setting decide the response when you reject a call automatically or manually, phone will reject as Busy here (Phone is busy can't answer), or Not found, or Temporarily unavailable.
Caller Display Source	Setting caller name display source, contain "FROM", "PAI-FROM", "PAI-RPID-FROM", "RPID-PAI-FROM", "RPID-FROM"

4.4. Réseau

4.4.1. Basique

Basic

Advanced

● **WAN**

☐ DHCP

DHCP HostName

DHCP Domain

DHCP Vendor Class Id

DHCP User Class

☒ Static IP Address

IP Address

Subnet Mask

Default Gateway

Static DNS ☒ No ☐ Yes

Primary DNS

Secondary DNS

☐ PPPoE

Account ID

PassWord

Service Name

Preferred DNS Server

Reply To ICMP ☐ No ☒ Yes

WAN Http Access ☐ No ☒ Yes

?

?

?

● **PC Port**

☒ As Bridge

☐ As Router

IP Address

Subnet Mask

IP Lease Time

DHCP Server

SaveSet

Restart

NOTE

DHCP:
The network configuration will be acquired from DHCP server.

Static IP Address:
Specify the IP address
SubnetMask Default Gateway
Primary DNS Secondary DNS
fields manually.

PPPoE:
Contact your ISP if it should be used.

WAN	The SecurHD IP operates in three modes: DHCP mode: All the field values for the Static IP mode are not used (even though they are still saved in the Flash memory.) The SecurHD IP acquires its IP address from the first DHCP server it discovers on its LAN. The DHCP option is reserved for NAT router mode. Static IP mode: Configure all of the following fields: IP address, Subnet Mask, Default Gateway address, Primary DNS , Secondary DNS. PPPoE: To use the PPPoE feature, set the PPPoE account settings. The SecurHD IP establishes a PPPoE session if any of the PPPoE fields are set.
Reply To ICMP	If set to “Yes”, the SecurHD IP will respond to the PING command from other computers, but it also is vulnerable to the DOS attack. Default is No .
WAN Http Access	If this parameter is set to “No”, the HTML configuration update via WAN port is disabled.
PC Port	Allow to use the internet port as bridge or as router.

4.4.2. Avancé

Basic

Advanced

● LLDP

Active Disable ▾

Packed Interval 120 (15~3600s)

● CDP

Active Disable ▾

Packed Interval 60 (1~3600s)

● VLAN

WAN Port	Active	Enable ▾			
	VID	0			
	Priority	0			
PC Port	Active	Enable ▾			
	VID	0			
DHCP VLAN	Active	Disable ▾			?

Voice Qos [] ?

SIP Qos [] ?

● VPN

Active ☐ Yes ☒ No

Upload VPN Config

Choisissez un fichier

Aucun... oisi

Import

● Web Server

HTTP Port 80 ?

HTTPS Port 443

Type HTTP&HTTPS ▾

● 802.1X

802.1X Mode Disable ▾

Identity []

MD5 Password []

● Local RTP Port

Max Rtp Port 12200 ?

Min Rtp Port 12100 ?

● VQRTCP Report

RTCP Support Disable ▾ ?

Voice Quality Report Collector [] ?

RTCP-XR Report Format [] ?

● Others

STUN Server [] ?

Keep-alive Interval 20 ?

SaveSet

Restart

NOTE

QoS:

When the network capacity is insufficient, QoS could provide priority to users by setting the value.

LLDP	Active : select the desired value from the pull-down list of Active. Packed interval : enter the desired time (in seconds) in the Packet interval (1~3600s) field.
CDP	Active to use the Cisco Discover Protocol
VPN	Active : Upload VPN Config :
DHCP VLAN	Active : yes or no (DHCP option 132).
Web Server	HTTP Port : default for http is 80. HTTPS Port : Type :
802.1X	802.1X Mode : Identity : MD5 Password :
Local RTP Port	Max Rtp Port : The Largest RTP Port : Should be large than (Min-RTP-Port +100) and less than 65535. Min Rtp Port : The Lowest RTP Port : Port >= 1024
VQ RTCP Report	RTCP Support : If Enable, Phone will statistic analysis RTP Info, then Report to Collector if Need. Voice Quality Report Collector : The RTCP Collector Info. Examples : sip:account@sample.com:8765. RTCP-XR-report Format : The Format of Reported PUBLISH In
Others	STUN Server : URL or IP:port Keep-alive interval : default 20 seconds.

4.5. Réglages

4.5.1. Préférences

The screenshot shows the 'Préférences' (Preferences) configuration page. On the left is a blue sidebar with buttons for 'Preference', 'Features', 'Tones', and 'Date & Time'. The main area contains the following settings:

- Web Language:** English (dropdown menu)
- Keypad DTMF Tone:** On (radio buttons)
- Volume Amplification:** -6dB (dropdown menu)
- HandSet Send Volume:** 4 (text input)
- NO Key Entry Timeout(seconds):** 4 (text input)
- Dial-now Time-out (seconds):** 0 (text input)
- Watch Dog Enable:** Off (radio buttons)
- Customer Set User Agent:** (empty text input)
- Voice Mail Tone:** On (radio buttons)
- Busy Tone Timer (0~5s):** 4 (text input)
- Open Keypad Tone:** Off (radio buttons)
- Use # As Dial Key:** Yes (radio buttons)
- Send # as %23:** No (radio buttons)

At the bottom are 'SaveSet' and 'Cancel' buttons. On the right, there is a 'NOTE' box.

Web Language	Select the displayed language for web page
Keypad DTMF Tone	Enable or disable the sound when press a key
HandSet Send Volume	Allow the amplification of the volume.
No Key Entry Timeout	In seconds, 0 means never timeout, default is 0 second.
Dial-now Time-out	In seconds, Interval for DialNow, default is 0 second.
Watch Dog Enable	Prevent phone freeze, so that it can be automatically reset when it run error.
Customer Set User Agent	When phone send SIP data it will make User Agent in the packet, default use its model info.
Voice Mail Tone	
Busy Tone Timer	
Open Keypad Tone	
Use # As Dial Key	This parameter allows users to configure the “#” key to be used as the “Send” (or “Dial”) key. If set to “Yes”, pressing this key will immediately trigger the sending of dialed string collected so far. In this case, this key is essentially equivalent to the “(Re)Dial” key. If set to “No”, this “#” key will then be included as part of the dial string to be sent out.
Send # as %23	Allow to send the DTMF of # as a command %23.

4.5.2. Fonctions

Preference

Features

Tones

Date&Time

[-] Forward: ?

Always
☐ On ☒ Off

Target
?

On Code
?

Off Code
?

Busy
☐ On ☒ Off

Target
?

On Code
?

Off Code
?

No Answer
☐ On ☒ Off

After Ring Time(seconds)
60 ?

Target
?

On Code
?

Off Code
?

[-] Call Waiting

Call Waiting
☒ On ☐ Off

[-] Speed Dial

Index	Type	Label	Value
M1	Speed Dial ▼		1001
M2	Speed Dial ▼		1002
M3	Speed Dial ▼		1003
M4	Speed Dial ▼		1005

[-] Distinctive Ring Tone

Index	Ring Id	User ID
1	Custom Ring Tone 1	
2	Custom Ring Tone 2	
3	Custom Ring Tone 3	

SaveSet
Cancel

NOTE

Forward::

This feature allows you to forward an incoming call to another phone number.

Target:

The number to which the incoming calls will be forwarded.

On Code:

The code that will be sent to PBX when it is switched On.

Off Code:

The code that will be sent to PBX when it is switched Off.



Forward : Always	Target : Target number for transfer. On Code : The feature code to enable all incoming calls forward, the phone will send the feature code directly to open all incoming calls forward. Off Code : The feature code to disable all incoming calls forward, the phone will send the feature code directly to close all incoming calls forward.
Forward : Busy	Target : transferred to target number. On Code : The feature code to enable busy call forward, the phone will send the feature code directly to open busy call forward. Off Code : The feature code to disable busy call forward, the phone will send the feature code directly to close busy call forward.
Forward : No answer	After Ring Time(seconds) : waiting time for NoAnswer forward. Target : number for transfer. On Code : The feature code to enable no answer call forward, the phone will send the feature code directly to open no answer call forward. Off Code : The feature code to disable no answer call forward, the phone will send the feature code directly to close no answer call forward.
Call Waiting	Enable if On or Disable if Off call waiting.
Speed Dial (M1 to M4)	SecurHD IP has defined 4 speed dial keys. After you program numbers for this key. You can push a speed dial key and then the call will be originated.
Distinctive Ring Tone	Caller ID must be configured. Select a Distinctive Ring Tone 1 through 3 for a particular Caller ID. The SecurHD IP will ONLY use selected ring tones for particular Caller IDs. For all other calls, the SecurHD IP will use System Ring Tone. When selected and no Caller ID is configured, the selected ring tone will be used for all incoming calls.

4.5.3. Tonalités

NOTE

Select Country:
Choose the country you are in. In custom mode, you can write the tones manually in this format.

Syntax: f1=val,f2=val[,c=on1/off1[-on2/off2[-on3/off3]]];
(Frequencies are in Hz and cadence on and off are in 10ms)
ON is the period of ringing ("On time" in ms) while OFF is the period of silence.
In order to set a continuous ring, OFF should be zero.
Otherwise it will ring ON ms and a pause of OFF ms and then repeat the pattern.
Up to three cadences are supported.

Select Country	Choice of the tones in function of the country.
Dial Tone, Ringback Tone, Busy Tone, Reorder Tone, Confirmation Tone, Call Waiting Tone	Using these settings, users can configure ring or tone frequencies based on parameters from local telecom. By default, they are set to North American standard. Frequencies should be configured with known values to avoid uncomfortable high pitch sounds. Syntax: f1=val,f2=val[,c=on1/off1[-on2/off2[-on3/off3]]]; (Frequencies are in Hz and cadence on and off are in 10ms) ON is the period of ringing ("On time" in ms) while OFF is the period of silence. In order to set a continuous ring, OFF should be zero. Otherwise it will ring ON ms and a pause of OFF ms and then repeat the pattern. Up to three cadences are supported.

4.5.4. Date & Heure

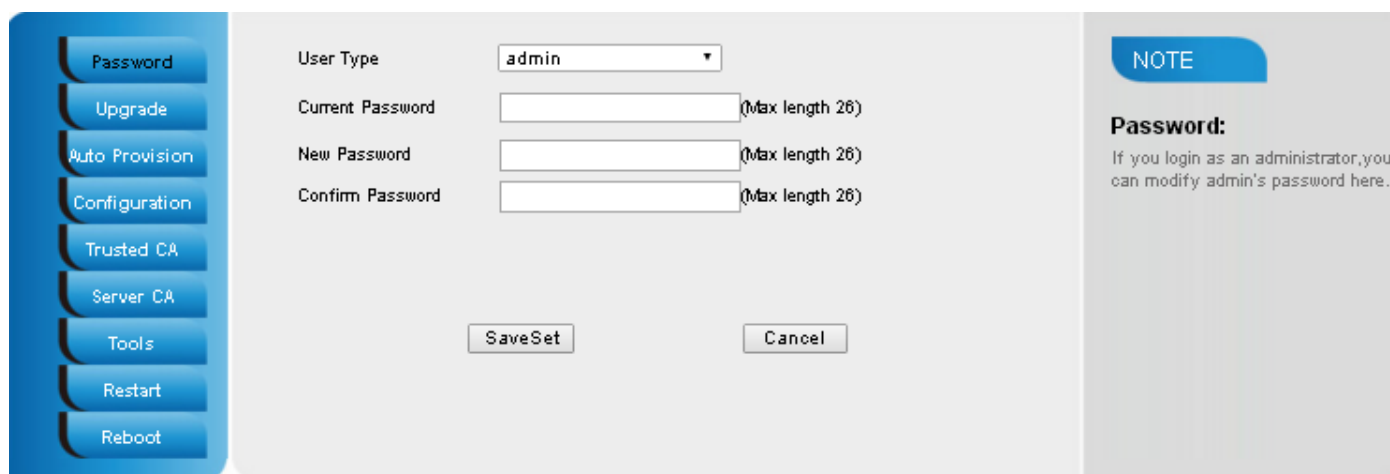
NOTE

Time Zone:
Choose the time zone you are in.

DHCP Time	Allow to active or deactivate the DHCP time.
Time Zone	Current local time in cities worldwide.
NTP Server is Covered with DHCP	Allow DHCP Option 42 to override NTP server.
NTP Server	Adress of NTP server.
Backup NTP Server	Adress of the backup NTP server.

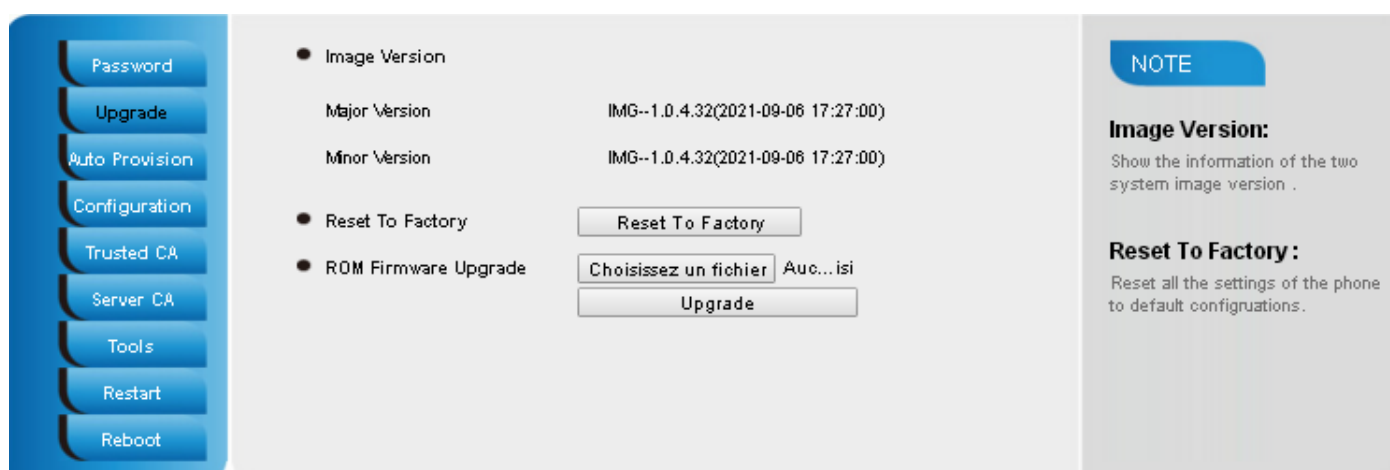
4.6. Management

4.6.1. Mot de passe



User Type	Choose between : Admin: The administrator access level. With this access level, all configurations on interface. The authentication identity for this access level is admin. And the default password is admin. Var: The value-added reseller access level. Generally, with this access level, most on the web user interface and phone user interface can be read and written. The authentication identity
Current password	Enter the current password.
New password	Enter the new password.
Confirm password	Confirm the new password.

4.6.2. Mise à jour



Major Version	Major Version of the firmware.
Minor Version	Minor Version of the firmware.
Reset To Factory	Reset factory setting.
ROM Firmware Upgrade	Permit to select a firmware to upgrade

4.6.3. Auto-provision

- Password
- Upgrade
- Auto Provision**
- Configuration
- Trusted CA
- Server CA
- Tools
- Restart
- Reboot

● **Firmware Upgrade**

PnP Active ☐ No ☒ Yes

Upgrade Mode ☐ TFTP ☒ HTTP ☐ FTP ☐ HTTPS

Firmware Server Path

Config Server Path

Allow DHCP Option

To Override Server: ☐ No ☒ Yes

AUTO Upgrade: ☐ No ☒ Yes

Check for upgrade every Minutes

HTTP/FTP/HTTPS UserName

HTTP/FTP/HTTPS Password

Firmware/Config File Prefix

Firmware/Config File Postfix

Upgrade Check Mode :

☒ Always Check For New Firmware

☐ check new firmware only when F/W/ pre/suffix changes

☐ Always Skip The Firmware Check

Authenticate Cfg File ☒ No ☐ Yes

Set Common AES Key

Autoprovision Now

?

● **SNMP Service**

SNMP Service Enable ☒ No ☐ Yes

SNMP Get Community

SNMP Set Community

SNMP Manager IP 1

SNMP Manager IP 2

SNMP Manager IP 3

SNMP Manager IP 4

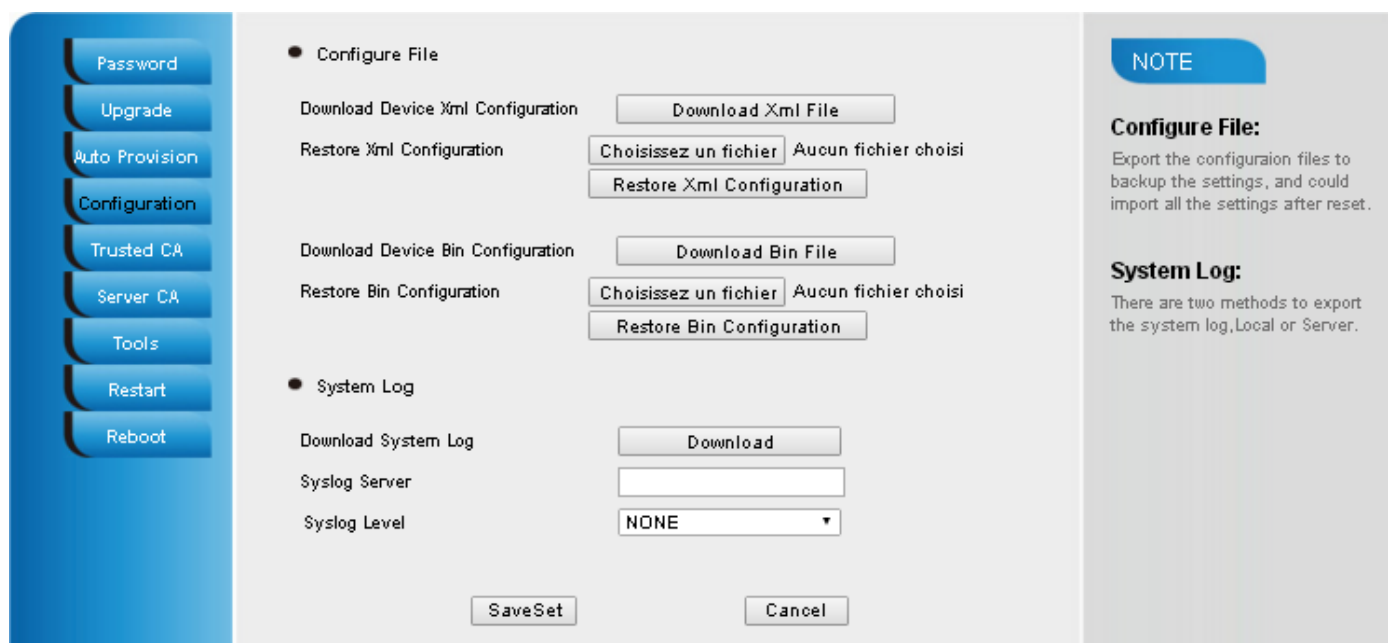
NOTE

Firmware Upgrade :

The detail sets about the firmware upgrade for the system.

PnP Active	The request to the server to obtain a support URL for upgrade.
Upgrade Mode	Type of the provider : TFTP/HTTP/FTP/HTTPS
Firmware Server Path	needs to be set to be a valid URL of a provider server, server name can be in either FQDN or IP address format. Below are examples of some valid URLs. e.g. firmware.mycompany.com:5688/Depaepe e.g. www.mycompany.com:5688/fm/Depaepe e.g. 218.2.83.110 By default address_ip_server_provider/fm
Config Server Path	needs to be set to be a valid URL of a provider server, server name can be in either FQDN or IP address format. Below are examples of some valid URLs. e.g. firmware.mycompany.com:5688/Depaepe e.g. www.mycompany.com:5688/cfg/Depaepe e.g. 218.2.83.110 By default : address_ip_server_provider/cfg
Allow DHCP Option	Allow DHCP Option (128 or 150 or 66).
To Override Server	
Auto Upgrade	
Check for upgrade every	Check for upgrade every X minutes.
HTTP/FTP/HTTPS UserName	HTTP/FTP/HTTPS UserName
HTTP/FTP/HTTPS Password	HTTP/FTP/HTTPS Password
Firmware/Config File Prefix	Firmware Prefix allows device to download the firmware name with the matching Prefix.
Firmware/Config File Postfix	Firmware Postfix allows device to download the firmware name with the matching Postfix.
Upgrade Check Mode	
Authenticate Cfg File	Enable if Yes or disable if No Cfg File.
Set Common AES Key	The XML configuration file could be encrypted in AES-128-CBC algorithm. The encryption password is defined in P8631 (Management->Auto Provision->Set Common AES Key) of the configuration file. The Password length is from 1-16, and password must be[0-9,A-F].
Autoprovision Now	

4.6.4. Configuration



NOTE

Configure File:
Export the configuraion files to backup the settings, and could import all the settings after reset.

System Log:
There are two methods to export the system log, Local or Server.

Download Device Xml Cfg	Export the XML configuration files to backup the settings.
Restore Xml Cfg	Import the XML configuration files to restore the settings.
Download System Log	Allow to download the system log.
Syslog Server	The IP address or URL of System log server. This feature is especially useful for the ITSP (Internet Telephone Service Provider)
Syslog Level	Select the SecurHD IP to report the log level. Default is NONE. The level is one of DEBUG, INFO, WARNING or ERROR. Syslog messages are sent based on the following events: 1. product model/version on boot up (INFO level) 2. NAT related info (INFO level) 3. sent or received SIP message (DEBUG level) 4. SIP message summary (INFO level) 5. inbound and outbound calls (INFO level) 6. registration status change (INFO level) 7. negotiated codec (INFO level) 8. Ethernet link up (INFO level) 9. SLIC chip exception (WARNING and ERROR levels) 10. memory exception (ERROR level) The Syslog uses USER facility. In addition to standard Syslog payload, it contains the following components: GS_LOG: [device MAC address][error code] error message <i>Example:</i> May 19 02:40:38 192.168.1.14 GS_LOG: [00:0b:82:00:a1:be] [000] Ethernet link is up

4.6.5. Trusted CA

Password
Upgrade
Auto Provision
Configuration
Trusted CA
Server CA
Tools
Restart
Reboot

Index	Issued TO	Issued By	Expiration	Delete
1				☐
2				☐
3				☐
4				☐
5				☐
6				☐
7				☐
8				☐
9				☐
10				☐

Delete

Import Trusted Certificate Files

Choisissez un fichier
Aucun fichier choisi

Import Trusted Certificates

Only Accept Trusted Certificates
☐ On
☒ Off

Common Name Validation
☐ On
☒ Off

Trusted Certificates
☒ Default Certificates
☐ Custom Certificates
☐ All Certificates

SaveSet

Cancel

NOTE

Trusted CA:
you can import TLS certificate file here.

Import Trusted Certificates Files	
Trusted Certificates	

4.6.6. Server CA

Password
Upgrade
Auto Provision
Configuration
Trusted CA
Server CA
Tools
Restart
Reboot

Issued TO	Issued By	Expiration	Delete
			☐

Delete

Import Server Certificate Files

Choisissez un fichier
Aucun fichier choisi

Import Server Certificates

Device Certificates
☒ Default Certificates
☐ Custom Certificates

SaveSet

Cancel

NOTE

Server CA:
you can import TLS certificate file here.

Import Server Certificates Files	
Device Certificates	

4.6.7. Outils



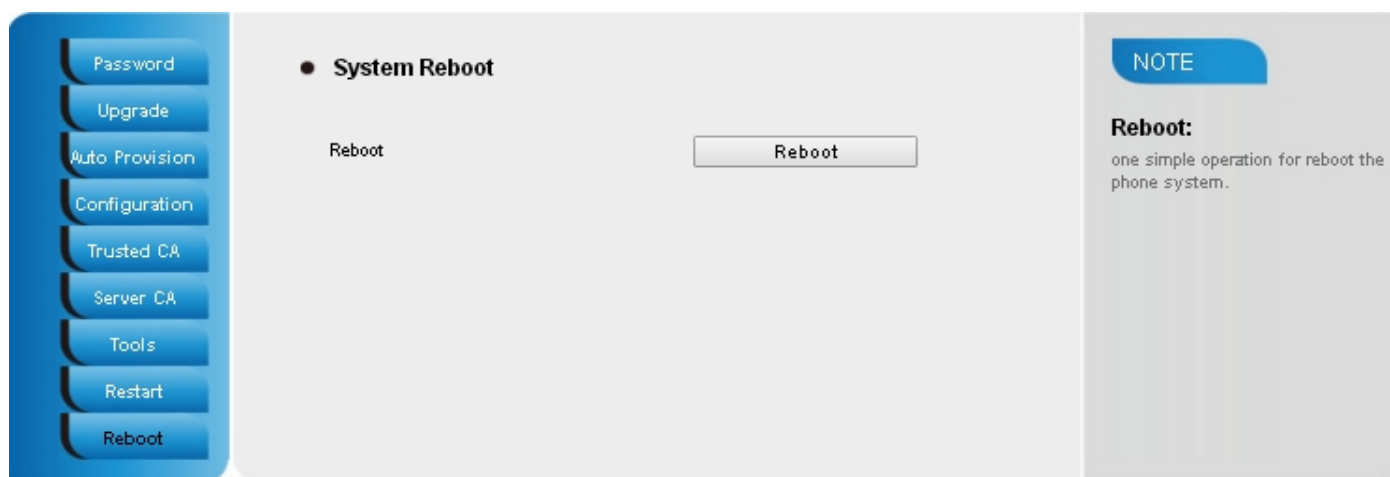
Pcap Feature	Allow to capture network frames.
--------------	----------------------------------

4.6.8. Redémarrage



Le redémarrage permet de relancer l'application SIP.

4.6.9. Reboot



Vous pouvez redémarrer le SecurHD IP en cliquant sur le bouton «Reboot» après chaque mise à jour de la page de configuration.

Vous pouvez également redémarrer en débranchant l'alimentation du SecurHD IP, puis en le rallumant.

Si votre SecurHD IP devient «bloqué» ou ne répond plus, vous pouvez débrancher l'alimentation pour le redémarrer.

Un redémarrage fréquent en débranchant l'alimentation n'est pas recommandé et ne devrait pas être nécessaire.

5. Configuration via un serveur central

Les SecurHD IP peuvent être automatiquement configurés à partir d'un système d'approvisionnement central.

Lorsque le SecurHD IP démarre, il enverra une requête TFTP ou HTTP pour télécharger les fichiers de configuration.

Il existe deux fichiers de configuration, l'un est «cfg.txt» et l'autre est «cfg001fc1xxxxxx», où «001fc1xxxxxx» est l'adresse MAC du SecurHD IP.

Pour plus d'informations sur le format du fichier de configuration, veuillez consulter la documentation technique associée.

Le fichier de configuration peut être téléchargé via TFTP ou HTTP à partir du serveur central.

Un fournisseur de services ou une entreprise avec un grand déploiement de SecurHD IP peut facilement gérer la configuration et la fourniture de services de périphériques individuels à distance et automatiquement à partir d'un serveur central.

Le système d'approvisionnement central utilise TFTP ou HTTP amélioré (compatible NAT donc pas de problèmes de NAT) et d'autres protocoles de communication pour communiquer individuellement avec chaque SecurHD IP pour la mise à niveau du micrologiciel, etc...

A propos des options DHCP prises en charge.

À l'heure actuelle, le SecurHD IP prend en charge les options DHCP : 2/12/15/42/43/60/66/128/150

1. Option 2 – Time Offset

Basic Option → Time Zone : Allow DHCP Option 2 to override Time Zone setting

2. Option 12 – Host Name

Basic Option → dynamically assigned via DHCP: DHCP hostname

3. Option 15 – Domain Name

Basic Option → dynamically assigned via DHCP: DHCP domain

4. Option 60 – Class-identifier

Basic Option → dynamically assigned via DHCP: DHCP vendor class ID

5. Option 43 – Vendor specific information

Basic Option → dynamically assigned via DHCP: DHCP vendor specific information

6. Option 42 – NTP servers

SUPER OPTIONS → NTP Server : Allow DHCP Option 42 to override NTP server

Note below,

SUPER OPTIONS → Firmware Upgrade and Provisioning : Allow DHCP Option

If you fill in 66, mean DHCP option 66; fill in 128, mean DHCP option 128; fill in 150, mean DHCP option 150.

7. Option 66

TFTP server name (if you select SUPER OPTION → Upgrade Via → TFTP)

HTTP server name (if you select SUPER OPTION → Upgrade Via → HTTP)

8. Option 128

TFPT Server IP address (if you select SUPER OPTION->Upgrade Via->TFTP)

HTTP Server IP address (if you select SUPER OPTION->Upgrade Via->HTTP)

9. Option 150

TFTP server address (if you select SUPER OPTION->Upgrade Via->TFTP)

HTTP server address (if you select SUPER OPTION->Upgrade Via->HTTP)

6. Mise à jour du logiciel

Pour mettre à niveau le logiciel, le SecurHD IP peut être configuré avec un serveur TFTP où se trouve la nouvelle image de code.

La mise à niveau TFTP peut fonctionner en mode IP statique ou DHCP en utilisant une adresse IP privée ou publique. Il est recommandé de définir l'adresse du serveur TFTP dans une adresse IP publique ou sur le même LAN avec le SecurHD IP.

Il existe deux façons de configurer le serveur TFTP pour mettre à niveau le micrologiciel, à savoir via l'invite du menu vocal ou via l'interface de configuration Web du SecurHD IP.

Pour configurer le serveur TFTP via l'invite vocale, suivez la section 8.1, une fois l'adresse IP TFTP configurée, éteignez et rallumez le SecurHD IP, le micrologiciel sera récupéré une fois le SecurHD IP démarré.

Pour configurer le serveur TFTP via l'interface de configuration Web, ouvrez votre navigateur pour pointer sur l'adresse IP du SecurHD IP.

Saisissez le mot de passe administrateur pour accéder à l'écran de configuration. De là, entrez l'adresse du serveur TFTP dans le champ désigné vers le bas de l'écran de configuration.

Une fois le serveur TFTP configuré, veuillez redémarrer le SecurHD IP.

Le processus TFTP peut prendre jusqu'à 1 à 2 minutes sur Internet, ou juste 20 secondes et plus s'il est effectué sur un réseau local.

Il est recommandé aux utilisateurs d'effectuer la mise à niveau TFTP dans un environnement LAN contrôlé si possible. Pour ceux qui n'ont pas de serveur TFTP local, DEPAEPE fournit un serveur TFTP compatible NAT sur l'Internet public pour la mise à niveau du micrologiciel. Veuillez consulter la section Service du site Web de DEPAEPE pour obtenir l'adresse IP de ce serveur TFTP.

REMARQUES : Lorsque le téléphone IP DEPAEPE démarre, il enverra une requête TFTP ou HTTP pour télécharger les fichiers de configuration, il y a deux fichiers de configuration, l'un est «cfg.txt» et l'autre est «cfg001fc1xxxxxx», où «001fc1xxxxxx» est l'adresse MAC du SecurHD IP. Ces deux fichiers sont uniquement à des fins de provisionnement automatique initial, pour la mise à niveau normale du micrologiciel TFTP ou HTTP, les messages d'erreur suivants dans un journal de serveur TFTP ou HTTP peuvent être ignorés.

7. Restauration des paramètres d'usine

Avertissement:

La restauration des paramètres d'usine par défaut supprimera toutes les informations de configuration de l'appareil.

Vous pouvez réinitialiser le SecurHD IP :

- soit via la page Web.

Aller sur la page « Management », puis dans l'onglet « Upgrade », cliquer ensuite sur le bouton « Reset To Factory ».

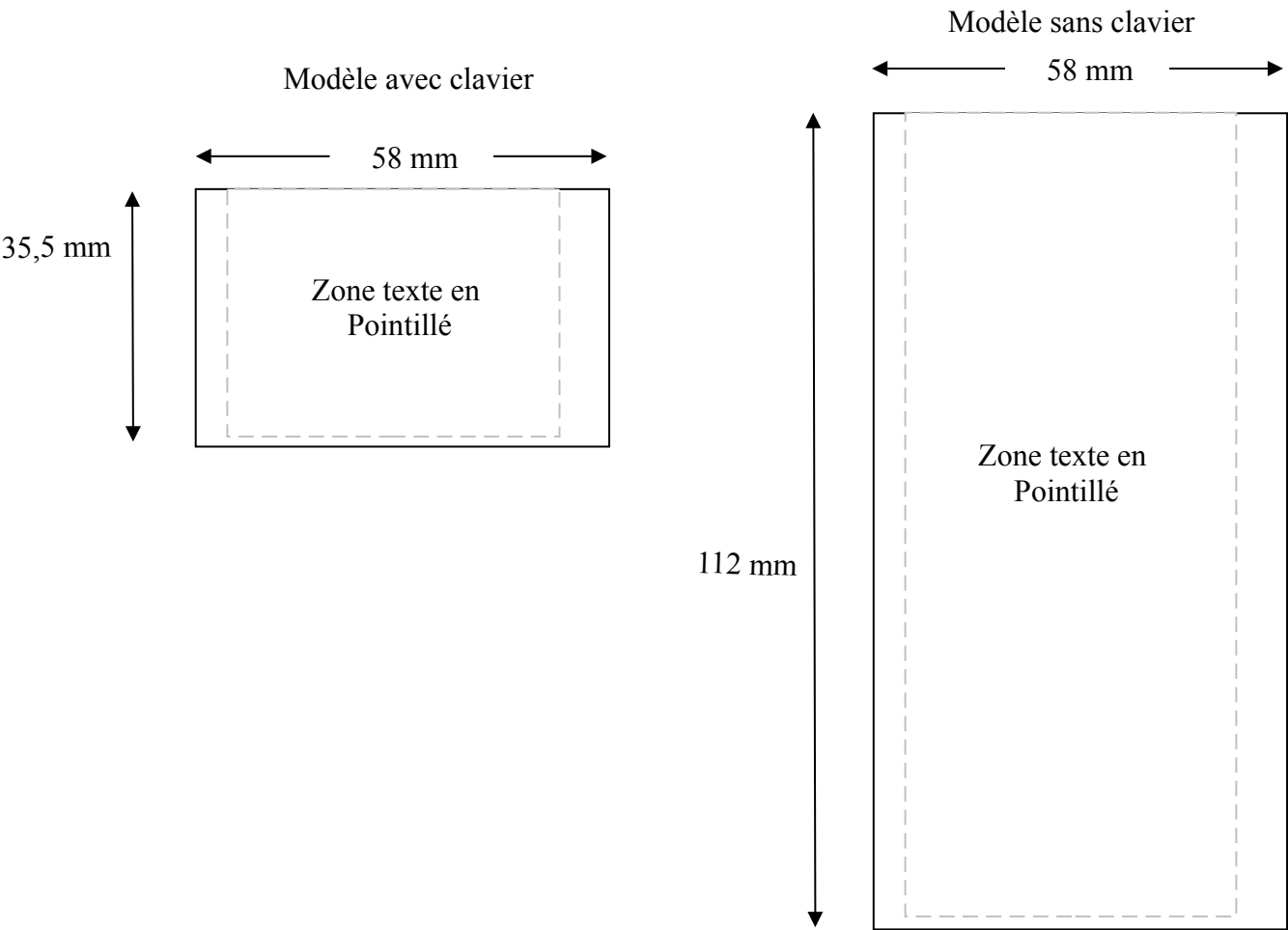
- soit via le bouton Reset situé sur la carte.

Maintenez le bouton pendant 10 secondes et relâcher pour effectuer la restauration.

Après la manipulation choisie, l'appareil sera restauré et redémarré.

8. Gabarit d'étiquettes

Modèle avec ou sans clavier



9. Caractéristiques

Codecs voix :	G.711, G.722, G.723, G.726, G.729, iLBC
Indice de protection :	IP65 et IK9
Température de fonctionnement :	-20°C à +50°C
Alimentation externe :	5V DC 1000 mA
PoE :	IEEE 802.3af
Consommation en courant :	90mA avec alimentation PoE

10. Déclaration de conformité

Nom et Siège social : **Henri Depaepe SAS**

Téléphone : +33 (0) 1 30 25 81 60

Adresse : 14, Rue Georges Méliès

Télécopie : +33 (0) 1 39 98 61 24

Localité : CORMEILLES-EN-PARISIS

Code postal : 95240

Identification du produit :

- Nature : Terminal de Télécommunications
- Type : Interphone
- Référence commerciale : SecurAccess BasicLine SIP
- Autres informations : Communications mains-libres

Déclare sous son entière responsabilité que le produit décrit ci-dessus est en conformité avec les exigences essentielles applicables et en particulier celles de la directive 1999/5/CE) suivantes :

Article 3.1 a : (protection de la santé et de la sécurité de l'utilisateur)

.....EN 60950

Article 3.1 b : (exigences de protection en ce qui concerne la compatibilité électromagnétique)

..... EN 55022 et EN 55024.

Conçu et fabriqué en France



Ce produit est conforme à la directive Européenne 2002/95/CE relative à la limitation de l'utilisation de certaines substances dangereuses dans les équipements électriques et électroniques. (RoHS)



Ce symbole signifie que ce produit est conforme à la directive de l'Union Européenne sur les déchets des équipements électriques et électroniques. (WEEE), 2002/96/EC. Il ne doit pas être jeté en fin de vie comme un déchet ménager afin de préserver l'environnement et la santé humaine.

L'élimination des équipements électriques et électroniques nécessite l'intervention de services désignés par le gouvernement ou les collectivités locales. Pour plus d'informations sur le traitement des appareils en fin de vie, contacter le revendeur du produit ou notre service commercial.

Document non contractuel. Le constructeur se réserve le droit d'apporter toutes les modifications qu'il jugera utiles, sans préavis.

11. Garantie et S.A.V.

Cet appareil a été conçu pour être utilisé conformément aux opérations décrites dans la présente notice. Toute utilisation différente est susceptible d'atteindre à votre santé ou au

fonctionnement de l'appareil. Pour un usage optimal, en toute sécurité, et pour éviter d'endommager le produit, nous vous recommandons de lire attentivement et d'observer les précautions suivantes :

- N'utilisez jamais cet appareil durant un orage.
- Ne pas obstruer les orifices servant à l'aération naturelle du poste.

Le non-respect de ces précautions, ainsi qu'une utilisation différente de celles décrites dans la présente notice peut entraîner le refus de prise en charge de la garantie.

Depaepe Telecom garantit ce produit contre les défauts et dysfonctionnements durant une période d'un (1) an à partir de la date d'achat initiale. En cas de défaut ou de dysfonctionnement, Depaepe Telecom procédera gratuitement, selon son choix et à titre exclusif, soit à la réparation, soit au remplacement du téléphone s'il est renvoyé durant la période de garantie.

Les éventuelles pièces de rechange utilisées pour les réparations peuvent être des pièces révisées ou contenir des éléments révisés. Si le remplacement du téléphone est nécessaire, celui-ci peut être remplacé par un appareil révisé du même aspect et de la même couleur.

Exclusions

Depaepe Telecom ne garantit pas la compatibilité de ses téléphones avec la totalité des équipements présents sur le marché. La garantie est valable pour un usage normal de l'appareil tel qu'il est défini dans la notice d'utilisation. Les fournitures utilisées avec l'appareil ne sont pas couvertes par la garantie. Cette garantie ne couvre pas les dommages aux produits dues à une cause étrangère à l'appareil ou résultant d'une installation, d'un entreposage ou d'une utilisation inappropriés, du vieillissement, d'un accident, d'une négligence, d'un abus, d'une mauvaise utilisation, d'un incendie ou imputables aux éléments naturels tels que des orages, des tempêtes ou des inondations dès lors que le téléphone est en votre possession.

Service de réparation sous garantie et S.A.V.

Vous pouvez contacter notre S.A.V. au : 01 30 25 81 74. Pour les produits achetés auprès d'un revendeur (installateur ou distributeur), les retours en SAV devront être effectués par son intermédiaire.

Tout retour à notre service après-vente ne pourra être accepté qu'accompagné, au choix, de la copie de notre bordereau de livraison ou de la copie de notre facture, notamment pour l'identification et la traçabilité des produits. Les matériels à réparer doivent être adressés aux frais de l'expéditeur à l'adresse suivante :

SADITEC
Service SAV Depaepe
ZA de la Croix Boissée
91810 VERT LE GRAND

Les matériels dont la panne peut être prise au titre de la garantie générale seront réexpédiés une fois réparés, à nos frais. Dans tous les autres cas, un devis de réparation sera envoyé et la réparation ne pourra être effectuée qu'après acceptation écrite du devis ou du bon de commande s'y référant.

NB : Les réparations de ce produit ne doivent être effectuées que par le fabricant ainsi que par d'autres prestataires légalement habilités. Cette restriction s'applique pendant et après la période de garantie. Une réparation par une personne non autorisée annulera la garantie.