Using TLS for the Installation of Remote Phones

Contents

Overview

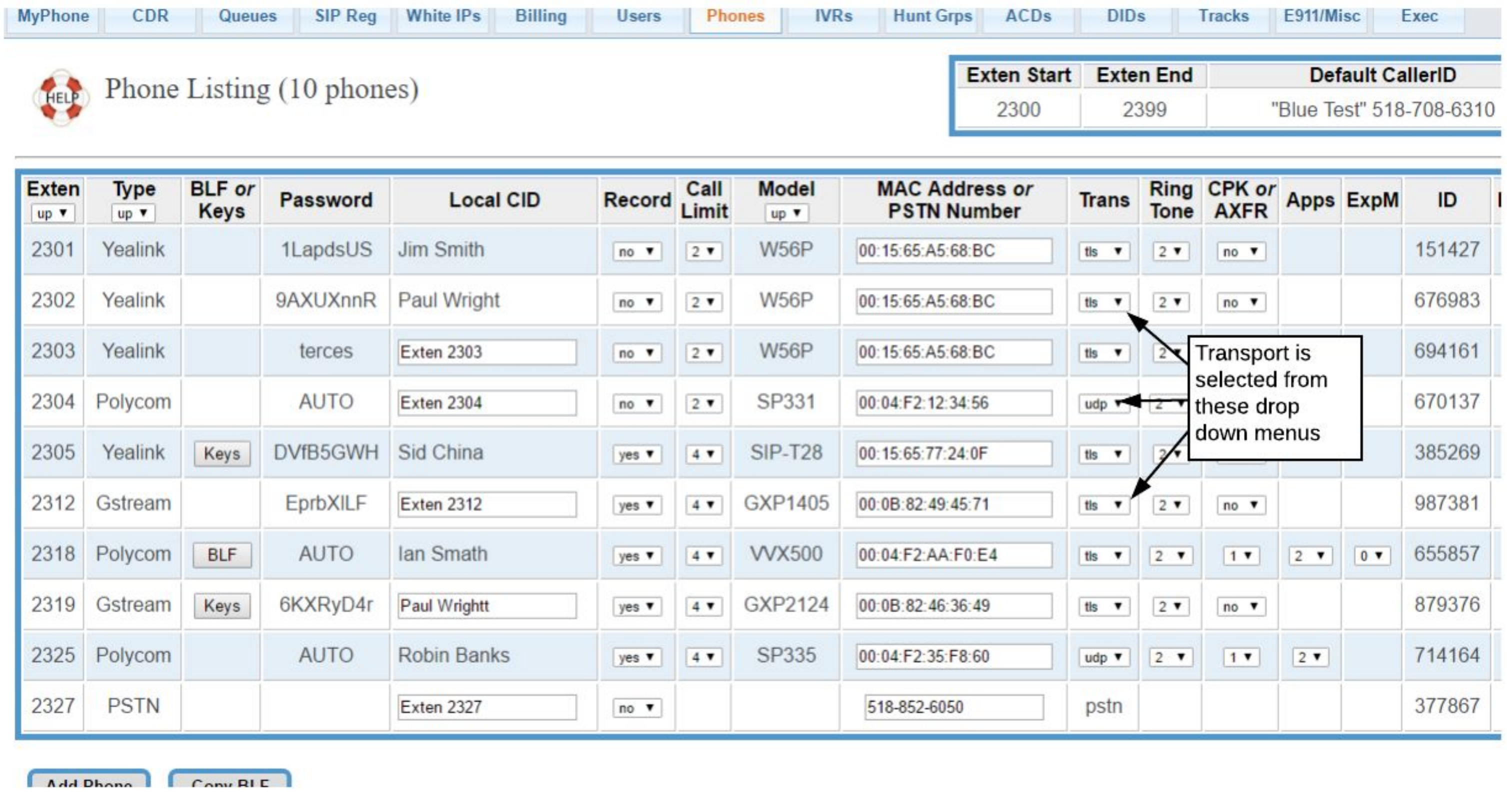
The deployment of remote phones is greatly simplified by the use of SIP over TLS (Transport Layer Security). Unlike the use of UDP which requires the white listing of the user’s IP address, TLS uses an RSA security certificate to provide the necessary verification of the user’s identity. It also uses TCP for transport which obviates the need to configure firewalls as the connection between the phone and the PBX is permanent. Bottom line, deployment is much simpler.

On a caution note if you are using one of our OSS (“On Site Servers”) units then do NOT use TLS for the local LAN based phones, use UDP transport. We infer that a phone is remote when TLS is deployed and make other modifications to the deployment such as assuming the deployment is behind NAT and provisioning a STUN/ICE server, which is not required for local phones.

The SIPS service (SIP over TLS) can be deployed to all the supported phone types (Polycom VVX, Yealink, Grandstream) and the Zoiper softphone phone. Details of how to implement this are given below.

Transport selection on Web GUI

The illustration below shows the “Phones” tab on the web GUI. The column labeled “Trans” *(Transport)* now has drop down menus to select either “tls” or “udp”. The Polycom Soundpoint family of phones will only have “udp” as an option. Other phones such as “PSTN” will have no options at all - as it is not relevant.



Phone Listing (10 phones)

Exten Start	Exten End	Default CallerID
2300	2399	"Blue Test" 518-708-6310

Exten up ▼	Type up ▼	BLF *or* Keys	Password	Local CID	Record	Call Limit	Model up ▼	MAC Address *or* PSTN Number	Trans	Ring Tone	CPK *or* AXFR	Apps	ExpM	ID
2301	Yealink		1LapdsUS	Jim Smith	no ▼	2 ▼	W56P	00:15:65:A5:68:BC	tls ▼	2 ▼	no ▼			151427
2302	Yealink		9AXUXnnR	Paul Wright	no ▼	2 ▼	W56P	00:15:65:A5:68:BC	tls ▼	2 ▼	no ▼			676983
2303	Yealink		terces	Exten 2303	no ▼	2 ▼	W56P	00:15:65:A5:68:BC	tls ▼	2 ▼				694161
2304	Polycom		AUTO	Exten 2304	no ▼	2 ▼	SP331	00:04:F2:12:34:56	udp ▼	2 ▼				670137
2305	Yealink	Keys	DVfB5GWH	Sid China	yes ▼	4 ▼	SIP-T28	00:15:65:77:24:0F	tls ▼	2 ▼				385269
2312	Gstream		EprbXILF	Exten 2312	yes ▼	4 ▼	GXP1405	00:0B:82:49:45:71	tls ▼	2 ▼	no ▼			987381
2318	Polycom	BLF	AUTO	Ian Smath	yes ▼	4 ▼	VVX500	00:04:F2:AA:F0:E4	tls ▼	2 ▼	1 ▼	2 ▼	0 ▼	655857
2319	Gstream	Keys	6KXRyD4r	Paul Wrightt	yes ▼	4 ▼	GXP2124	00:0B:82:46:36:49	tls ▼	2 ▼	no ▼			879376
2325	Polycom		AUTO	Robin Banks	yes ▼	4 ▼	SP335	00:04:F2:35:F8:60	udp ▼	2 ▼	1 ▼	2 ▼		714164
2327	PSTN			Exten 2327	no ▼			518-852-6050	pstn					377867

Transport is selected from these drop down menus

Once you have selected the desired transport protocols, rebuild the system in the usual way. All that now needs to be done is to ensure the boot server is corrected programmed into the remote phone. Instructions on how to do this are given for the various phone types below.

How to Setup a Polycom VVX Phone with a Provisioning Server

The following describes how to setup a provisioning server for a <u>REMOTE </u>Polycom phone. If the phone is local to an OSS you do not need to follow these directions. In summary we need to:

- Set the DHCP Boot Server to static
- Set the Provisioning Server Type to HTTP
- Set the Provisioning Server Address to the provisioning URL

Start by Power Cycling the Phone

Power cycle the phone and when the screen becomes active press “Cancel” and then “Setup”.

- Enter the password (default is 456)

Define “Boot Server” as “Static”

- Select “Provisioning Server” => “DHCP Menu”
- With the cursor on “Boot Server” press Edit and cycle through options until you see “Static”.
- Press “OK” and exit the DHCP menu.

Set the Provisioning Server Type to HTTP:

- On exiting the DHCP Menu the cursor will be on the “Server Type”
- Press “Edit” and cycle through until you see “HTTP”, press “OK”

Set the Provisioning Server URL:

- The cursor will now be on “Server Address”, press “Edit”
- The softkey on the left as the bottom of the screen defines the keypad mode:
    - a->1A means lower case alpha format.
    - 1->Aa means numeric format.
    - A->a1 means upper case alpha format.
- If you have been given a URL then use lower case alpha
- If you have been given an IP address use numeric format (note “*” = decimal point)
- Enter the URL/Ip and press OK

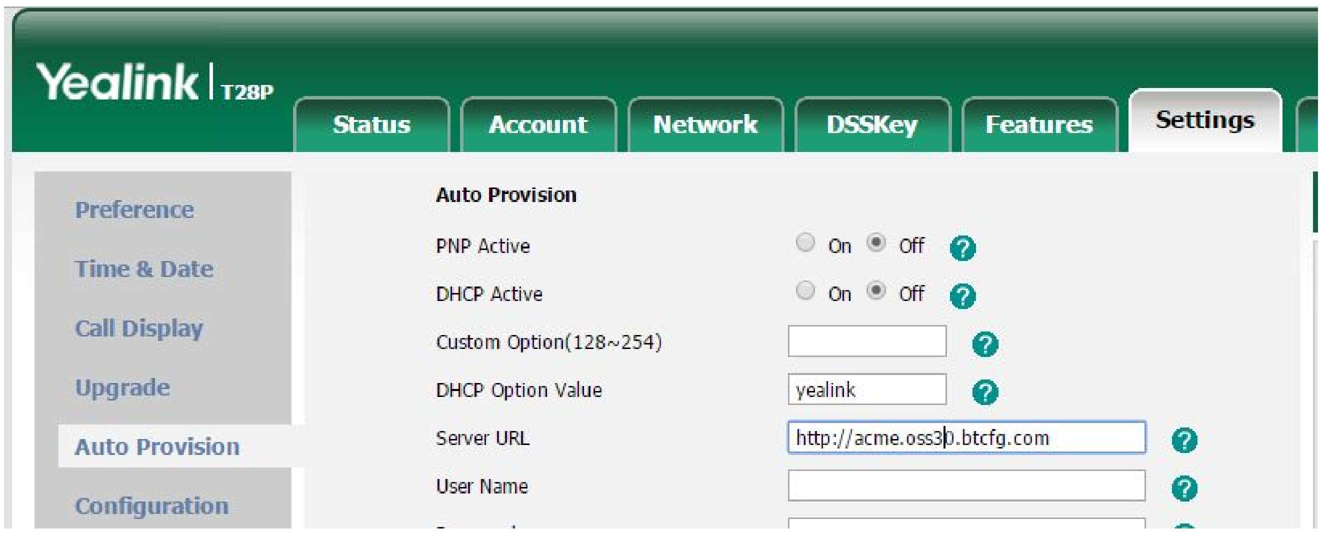
Exit and Save

- Now press “Exit” twice
- Press Save & Reboot

How to Setup a Yealink Phone with a Provisioning Server

Log into the phone by pointing a web browser at it's IP address. Enter username and password *(default is ‘admin’ and ‘admin’)* and go to Settings=>Auto_Provision *(see example illustration below).*

- Turn off “PNP Active” and “DHCP Active”.
- Add the server URL as http://<server_URL>, where <server_URL> is the URL for your server
- Press the “Confirm” button and then the “Autoprovision Now” button.



Auto Provision

PNP Active ○ On ● Off

DHCP Active ○ On ● Off

Custom Option(128~254)

DHCP Option Value yealink

Server URL http://acme.oss30.btcfg.com

User Name

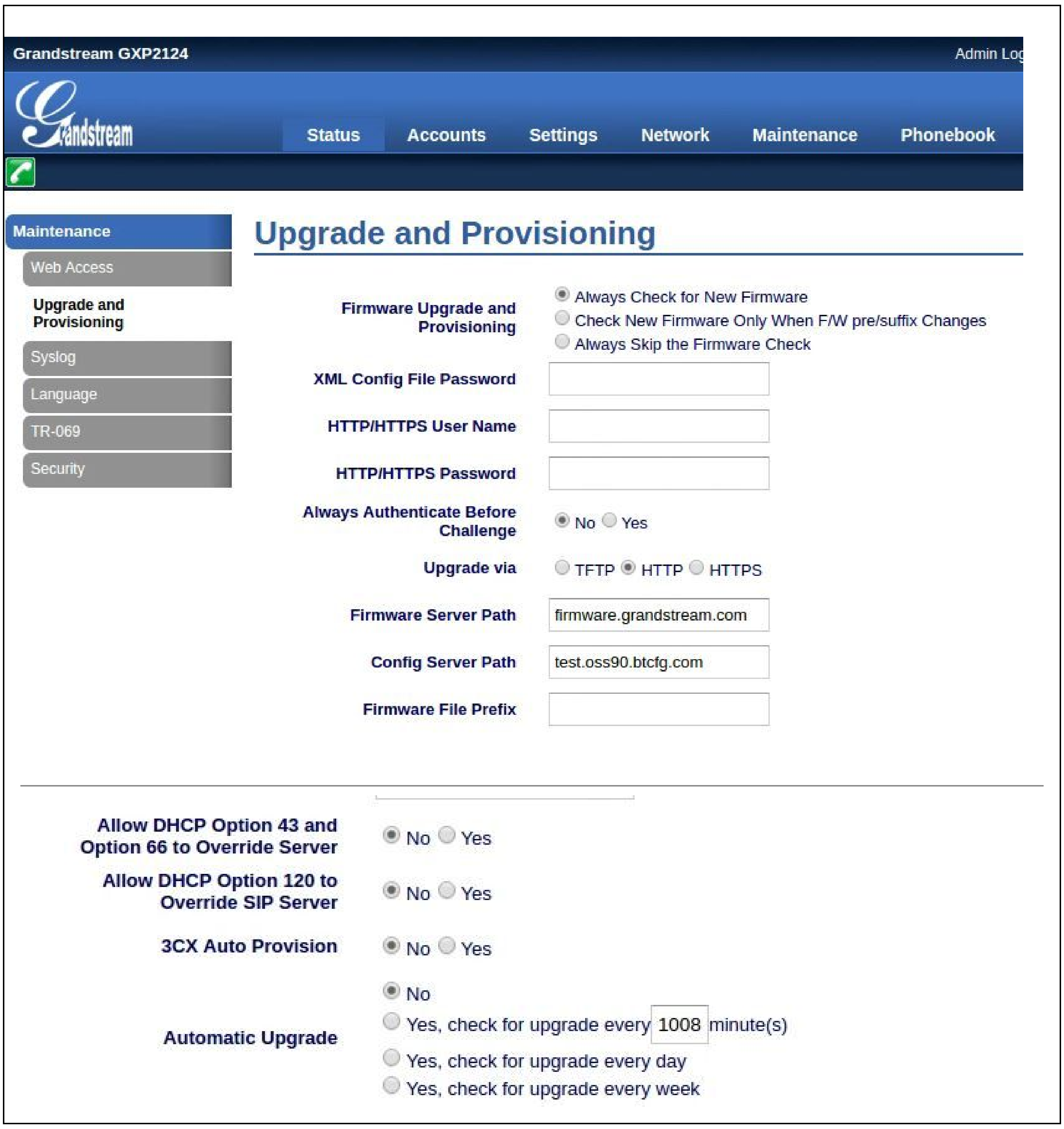
Illustration of the Provisioning Server configuration

How to Setup a Grandstream Phone with a Provisioning Server

Log into the phone by pointing a web browser at it's IP address. Enter a password *(default is ‘admin’)* and go to “Maintenance” => ”Upgrade and Provisioning” *(see example illustration below).*

- On “Upgrade Via” choose HTTP
- On “config server Path” add the server URL *(just the URL no protocol spec)*
- Finally set up the various DHCP option as shown in lower half of the illustration below.

When this has been done press “Save and Apply” and then reboot the phone



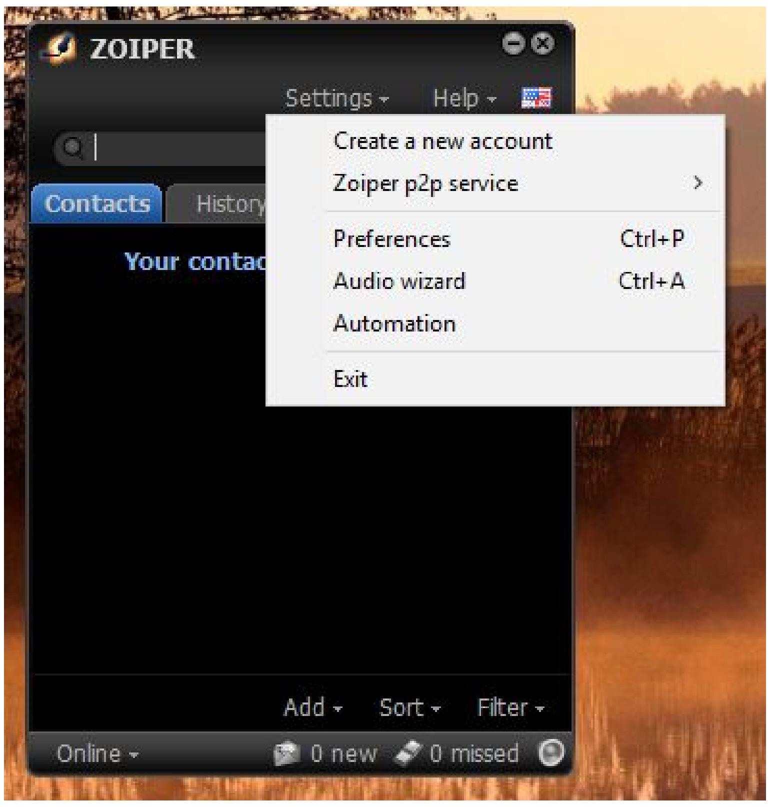
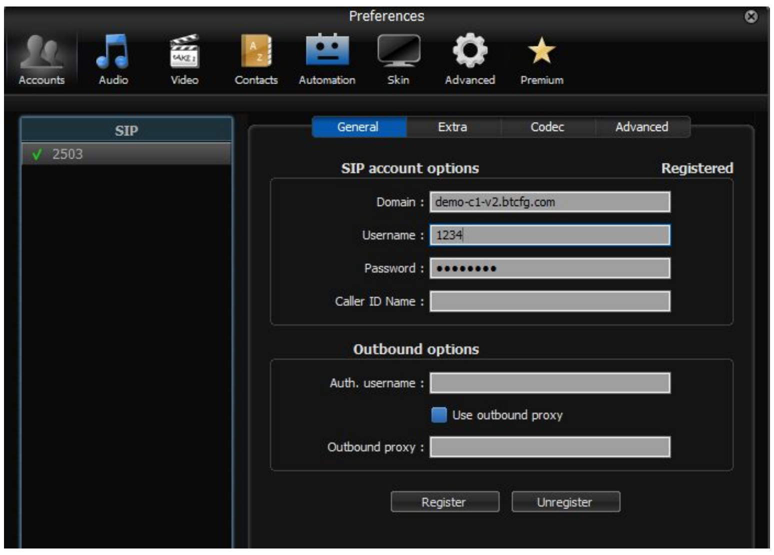
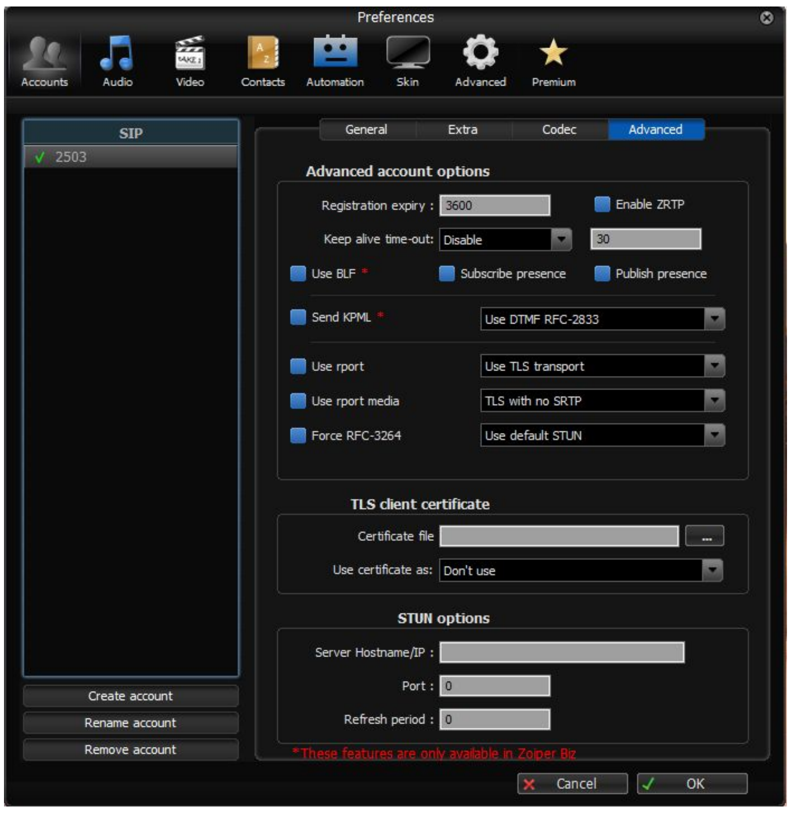
Upgrade and Provisioning

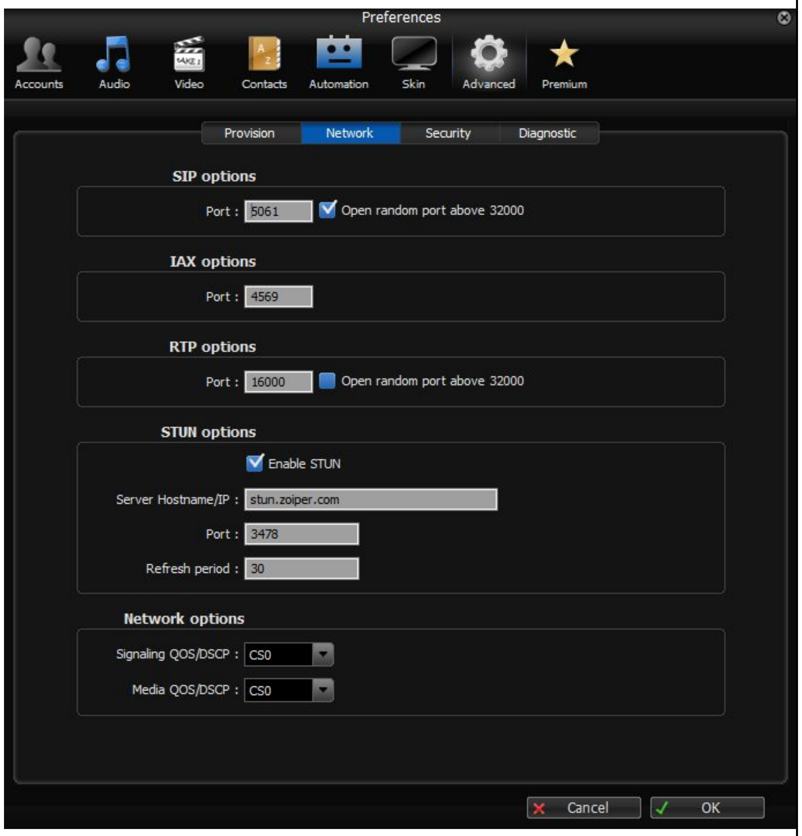
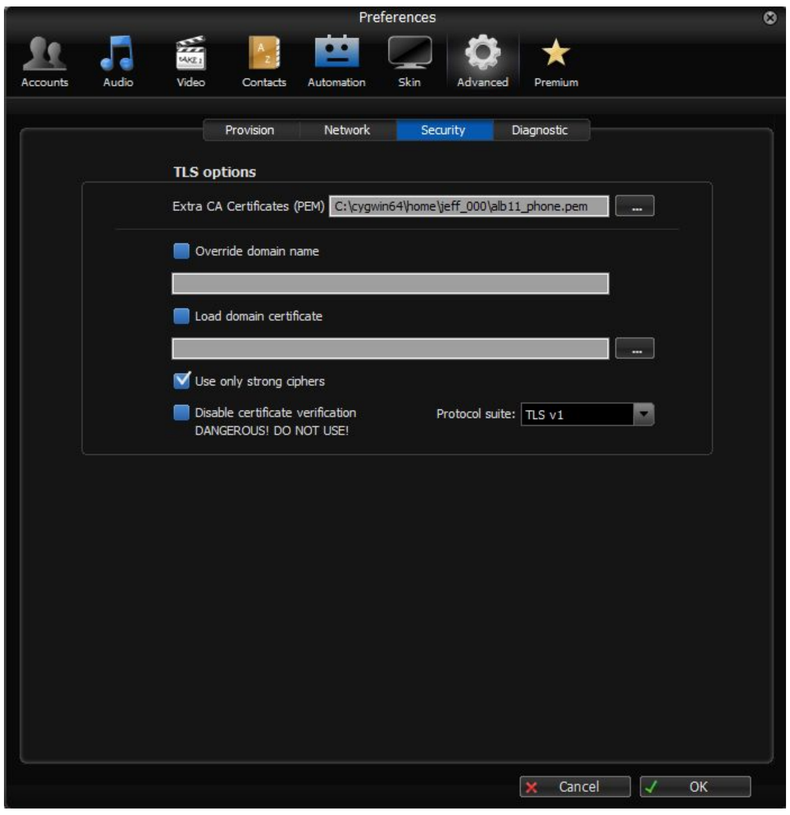
Firmware Upgrade and Provisioning	● Always Check for New Firmware ○ Check New Firmware Only When F/W pre/suffix Changes ○ Always Skip the Firmware Check
XML Config File Password	
HTTP/HTTPS User Name	
HTTP/HTTPS Password	
Always Authenticate Before Challenge	● No ○ Yes
Upgrade via	○ TFTP ● HTTP ○ HTTPS
Firmware Server Path	firmware.grandstream.com
Config Server Path	test.oss90.btcfg.com
Firmware File Prefix	
Allow DHCP Option 43 and Option 66 to Override Server	● No ○ Yes
Allow DHCP Option 120 to Override SIP Server	● No ○ Yes
3CX Auto Provision	● No ○ Yes
Automatic Upgrade	● No ○ Yes, check for upgrade every 1008 minute(s) ○ Yes, check for upgrade every day ○ Yes, check for upgrade every week

Installation of the Zoiper softphone

The Zoiper softphone is available for free from here: http://www.zoiper.com/en . This application is available for PC, Mac, Android and IOS - covers all of the most popular platforms. These installations are all similar and the one to be covered here is for the Windows OS.

Unlike the Polycom and Yealink phones the Zoiper softphone does not come with any automatic provisioning and so you will need to enter the account information as well as the security certificate, fortunately this is very straightforward. The table below progresses through four screens that you will need to enter this information into

• Click Settings => Create a new account • Select SIP, hit NEXT • Enter the credentials - you will find these on the "Phone" tab of the web GUI. An example would be: User => 1234 Password => xxxxx Domain => acme.oss10.btcfg.com • Edit the account name as need (it's unimportant) and be sure to check "Skip auto-detection" • The new account has been created.	 ZOIPER Settings Help Create a new account Zoiper p2p service Preferences Ctrl+P Audio wizard Ctrl+A Automation Exit Contacts History Your contac Add Sort Filter Online 0 new 0 missed
• Now open Settings => Preferences • You will see the account info you have just entered.	 Preferences Accounts Audio Video Contacts Automation Skin Advanced Premium SIP General Extra Codec Advanced Register Unregister ✓ 2503 SIP account options Registered Domain : demo-c1-v2.btcfg.com Username : 1234 Password : •••••••• Caller ID Name : Outbound options Auth. username : ☐ Use outbound proxy Outbound proxy :
• Click on the "Advanced Tab" • Make sure it looks identical the illustration on the right. • Note that the TLS certificate is blank here - we will configure this elsewhere. • The drop down boxes in the center right are: ○ RFC-2833 ○ Use TLS transport ○ TLS with no SRTP ○ Use default STUN	 Preferences Accounts Audio Video Contacts Automation Skin Advanced Premium SIP General Extra Codec Advanced Create account Rename account Remove account Cancel OK ✓ 2503 Advanced account options Registration expiry : 3600 ☐ Enable ZRTP Keep alive time-out: Disable 30 ☐ Use BLF * ☐ Subscribe presence ☐ Publish presence ☐ Send KPML * Use DTMF RFC-2833 ☐ Use rport Use TLS transport ☐ Use rport media TLS with no SRTP ☐ Force RFC-3264 Use default STUN TLS client certificate Certificate file ... Use certificate as: Don't use STUN options Server Hostname/IP : Port : 0 Refresh period : 0 *These features are only available in Zoiper Biz

• Now click the “Advanced” option in menu bar near the silver “gear wheel” • Make sure that screen is the same as the one to the right. • The URL for STUN is stun.zoiper.com	 Preferences Accounts Audio Video Contacts Automation Skin Advanced Premium Provision Network Security Diagnostic Cancel OKSIP options Port : 5061 ☑ Open random port above 32000 IAX options Port : 4569 RTP options Port : 16000 □ Open random port above 32000 STUN options ☑ Enable STUN Server Hostname/IP : stun.zoiper.com Port : 3478 Refresh period : 30 Network options Signaling QOS/DSCP : CS0 Media QOS/DSCP : CS0
• Finally click on the “Security” tab • In the Extra CA Certs click the [..] box and navigate to the “pem” file sent with the email. • Check “Use only strong ciphers” • Select “TLS v1” for the protocol suite. • Click “OK” at the bottom right.	 Preferences Accounts Audio Video Contacts Automation Skin Advanced Premium Provision Network Security Diagnostic ... Cancel OKTLS options Extra CA Certificates (PEM) C:\cygwin64\home\jeff_000\alb11_phone.pem □ Override domain name □ Load domain certificate ☑ Use only strong ciphers □ Disable certificate verification DANGEROUS! DO NOT USE! Protocol suite: TLS v1

That’s it, you should find the phone registers with the server and you can make and receive calls.