KONFTEL

Conference phones for every situation

PRELIMINARY

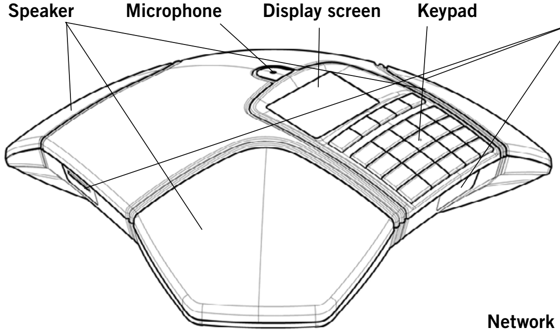
Installation and Administration of Konftel 300IP

ENGLISH

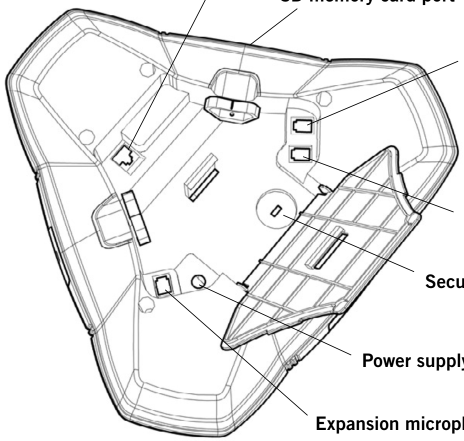
ABOUT THIS DOCUMENT

This document only includes setup, registration of accounts, and configuration. The use of the conference phone is described in the *Quick reference guide* and the *User guide*. Latest version of all documentation can be downloaded from **www.konftel.com/300ip**.

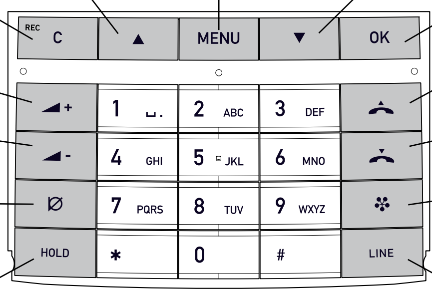
CONTENT



LEDs	
Flashing blue	Incoming call
Steady blue light	Call in progress
Flashing red	On hold, microphone and speakers turned off
Steady red light	Mute, microphone turned off



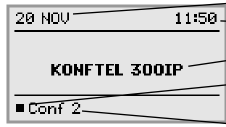
Maintenance
Clean the equipment with a soft, dry cloth. Never use liquids.



DISPLAY SCREEN

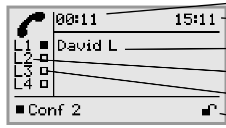
On Hook

Press to display this screen.



Off Hook

Press to display this screen.



Line status:

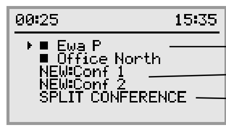
- ☐ Line free (Before account name – telephone not registered)
- ■ Line connected (Before account name – telephone registered)
- Line on hold (“HOLD” displayed on the screen – all calls on hold)
- Line (called party) busy
- Own line put on hold by other party
- Recording call
- Secure connection

Information text displays one of the following:

- Number or name of each phone line
  (The name will be displayed if a number is in the phonebook)
- Explanation of what you should do (For example **ENTER NUMBER**)
- Status (For example **HOLD** when you place all calls on hold)

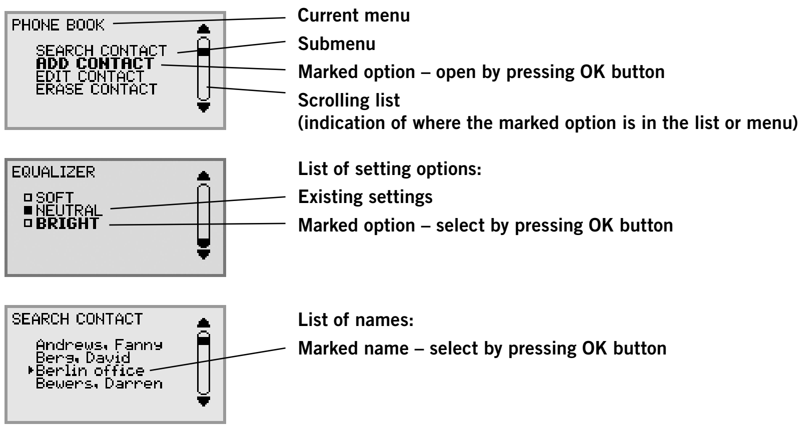
Line menu

Press **LINE** to switch to and from this menu.



Menu

Press **MENU** to switch to and from a menu.



NAVIGATION AND SELECTION IN MENUS

⇨ Press **MENU**.

⇨ Select the option you want from the menu using the arrow buttons.

⇨ Confirm by pressing **OK** to select the marked option.

⇨ Cancel the setting or go back one level in the menu by pressing **C**.

⇨ Quit the menu by pressing **MENU** again.

ⓘ Note that after you have made changes to a setting, you must press **OK** to activate the setting.

It is possible to open a menu option directly by pressing the number button that corresponds to the position of the option in the menu (e.g. 2 to open PHONEBOOK and then 3 to select EDIT CONTACT).

Writing style in instructions

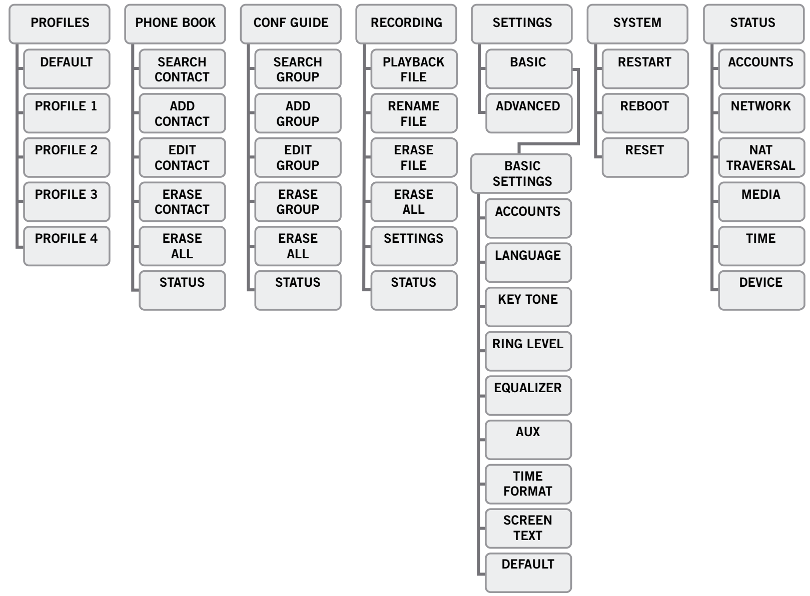
In the instructions, **MENU** > **SETTINGS** (5) means you should:

⇨ Press **MENU**.

⇨ Mark the **SETTINGS** option using the arrow buttons and confirm by pressing **OK** to open the menu (or press button number **5**).

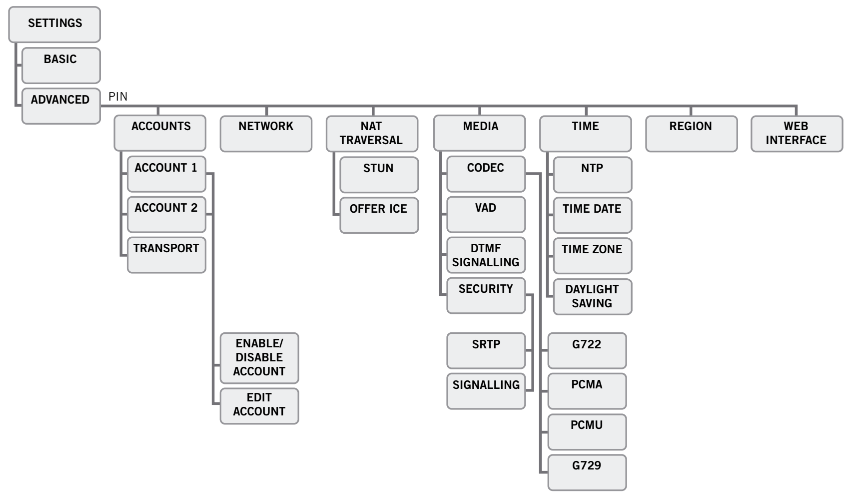
Correspondingly, **Phonebook** > **Conference Guide** in the web interface means you should select Menu Phonebook and the Conference Guide tab.

Menu tree



Menu tree, advanced settings

The advanced settings is protected by administrators PIN. The default value is **1234**.



The simplest way to make settings and edit contacts is using a PC and the Konftel 300IP web interface.

USING THE WEB INTERFACE

You can use the web browser of a PC connected to the same network to manage contacts, conference groups and settings in the Konftel 300IP.

For security reasons, recordings can only be managed directly on the Konftel 300IP. All other settings that can be made directly on the Konftel 30IP can also be made via the web interface. It is also possible to import and export contacts and conference groups, name user profiles and change PIN codes, which can only be done via the web interface. The administrator can also view logs, update software and create a configuration file.

The default setting for the PIN code is **0000** for the user account (Default, Profile 1, Profile 2, Profile 3 and Profile 4) and 1234 for the administrators account (Admin). We recommend that you change the PIN codes in order to protect the settings. The code may consist of eight digits. The administrator can always view and change the PIN codes to the user accounts. The administrator's PIN code can only be reset with a complete reset to factory settings.

Checking IP address

⇨ Press **MENU** and select the sub menu **STATUS** > **NETWORK** (7,2).

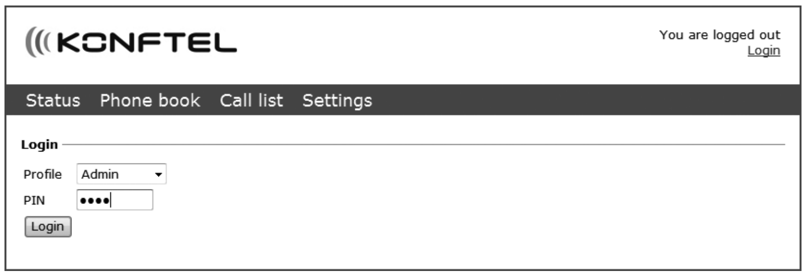
⇨ Check the conference phone's network address under the heading **IP ADDRESS**.

ⓘ Use this address to log into the web server in the conference phone.

Login

⇨ Log into the web server in Konftel 300IP by entering the phone's network address in your computer's web browser.

⇨ Select **Admin** as Profile and enter your PIN.



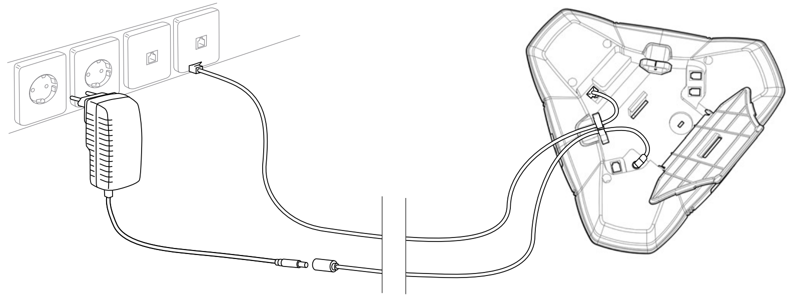
A short and simplified installation description is found in the printed Installation guide. The guide includes the basic settings for a quick start and works in most cases.

CONNECTING

⇨ Connect Konftel 300IP to the network as illustrated below.

⇨ Plug the Konftel 300 into the mains using the power adapter as illustrated below.

ⓘ Konftel 300IP can be driven directly from the network (Power over Ethernet) if the network supports this.



⇨ Place the conference phone in the middle of the table.

Konftel 300IP must obtain a network address and be registered in a SIP PBX before it can be used. To register an account and make the settings in Konftel 300IP, it is the easiest to use a computer connected to the same network and use the built-in web server.

OBTAINING A NETWORK ADDRESS

Connecting to a network with DHCP

See “Check IP address” under “USING THE WEB INTERFACE” on page 6.

Connecting to a network with static IP addresses

You need information on IP address, host name, domain, netmask, gateway, DNS 1, and DNS 2. Host name can be set freely and domain and secondary DNS can be left blank.

⇨ Press **MENU** and select **SETTINGS** > **ADVANCED** (5,2).

⇨ Enter the PIN code.

ⓘ The default code is **1234**.

⇨ Select **NETWORK** (2)

⇨ Select **STATIC IP**.

⇨ Enter values for the IP ADDRESS.

ⓘ Enter three digits (begin with 0 if necessary), press **OK**, enter three digits, and so on.

⇨ Enter HOST NAME
Default is kt300ip.

⇨ Enter DOMAIN

⇨ Enter NETMASK

⇨ Enter GATEWAY

⇨ Enter DNS 1

⇨ Enter DNS 2
The display shows DONE.

LOGIN

See “Login” under “USING THE WEB INTERFACE” on page 6.

INSTALLATION

SOFTWARE UPGRADE AND BASIC SETTINGS

The following settings should be done during installation.

Note that all settings on the Basic tab also affect the user profile Default. Other user profiles can be changed individually.

The settings on the Basic tab, except the name and PIN for Admin, can be modified by any user. Other settings require a login as Admin.

Upgrade software

See the heading “PROVISIONING – UPGRADE AND CONFIGURATION” on page 31 for a detailed description and upgrading options.

⇨ Select **Settings** > **Provisioning**.

⇨ Click on **Check Now**.

⇨ Compare the latest version, with the current version (shown on the web page).

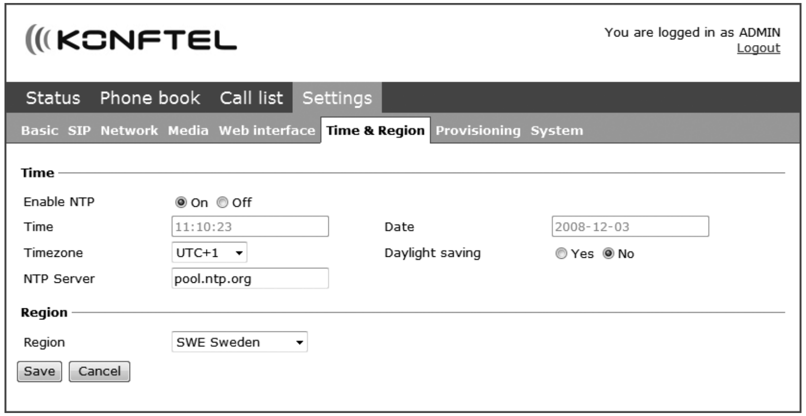
⇨ If you want to upgrade, select the desired version in the list box and click on **Upgrade**.
The browser window and the display on Konftel 300IP shows that the upgrade has begun.

ⓘ The download and installation can take several minutes. Do not interrupt the upgrade and do not disconnect any plug on Konftel 300IP during the upgrade. An interrupted upgrade can make the conference phone unusable.

⇨ When installation is complete, the text “Upgrade Complete. The unit will be rebooted.” is shown in your browser, and after a while you hear the Konftel music signature, that shows that the conference phone has started.

Setting time and region

⇨ Select **Settings** > **Time & Region**.



⇨ Select the time zone and if you want automatic correction for DST (Daylight saving).

ⓘ It is also possible to set the time and date manually or choose a different time server.

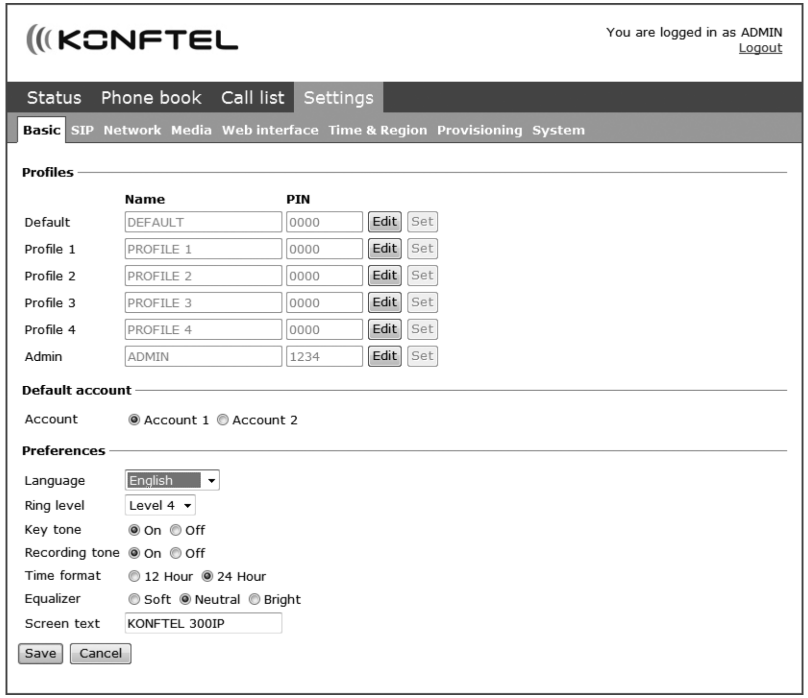
⇨ Select the region where you are.

ⓘ This setting affects the signalling.

⇨ Save the setting.
Konftel 300IP reboots with the new settings.

Changing the language

⇨ Select **Settings** > **Basic**.



⇨ Select the desired language in the list box after Language and save the setting.

Changing the PIN

PIN code for Admin should be changed from the default setting to protect the settings. Note the new PIN in a safe place. The administrator's PIN code can only be reset by a full factory reset!

⇨ Select **Settings** > **Basic** and click the **Edit** button on the Admin line.

⇨ Enter a new PIN.

ⓘ The PIN code can contain 8 digits.

⇨ Click on the **Set** and **Save** buttons.

REGISTERING AN ACCOUNT

The conference phone can be registered in a company SIP PBX or with a public IP telephony service provider. You can store settings for two accounts in Konftel 300IP. To register your phone, you must have access to the account information and all necessary settings that the SIP PBX or service provider requires.

See the heading “SIP” on page 17 for a detailed description of all settings.

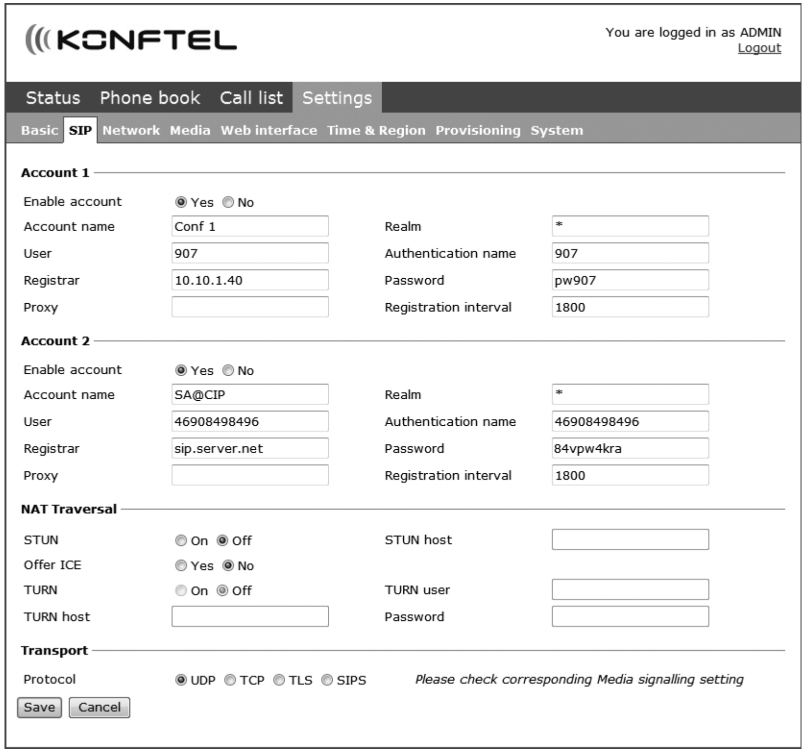
⇨ Select **Settings** > **SIP**.

⇨ Click **Yes** at Enable account under Account 1.

⇨ Enter the account information you have received.

ⓘ Account name can be chosen freely and is the name or phone number you want to appear in the phone display.

⇨ Leave the default values if you have no other information.



⇨ Select a method of NAT traversal if you got information of this.

⇨ Select a different transport protocol if you got information of this. See page 20 about using a secure transport protocol.

⇨ Save the settings by clicking the **Save** button.

Konftel 300IP responds by showing REGISTERING. Your selected account name appears at the bottom of the display with a filled square in front, if the registration is successful.

Make media settings

⇨ Select a different codec priority, if you do not accept the default settings. See page 24.

⇨ Select a SRTP option if you need a secure media protocol. See page 25. Note that this also requires a corresponding transport setting on the SIP tab.

Almost all settings can be done directly on Konftel 300IP. See “NAVIGATING THE MENUS AND MAKE SETTINGS” on page 5 for using the menu system. Because it is easier to use the web interface, we describe the settings using this interface.

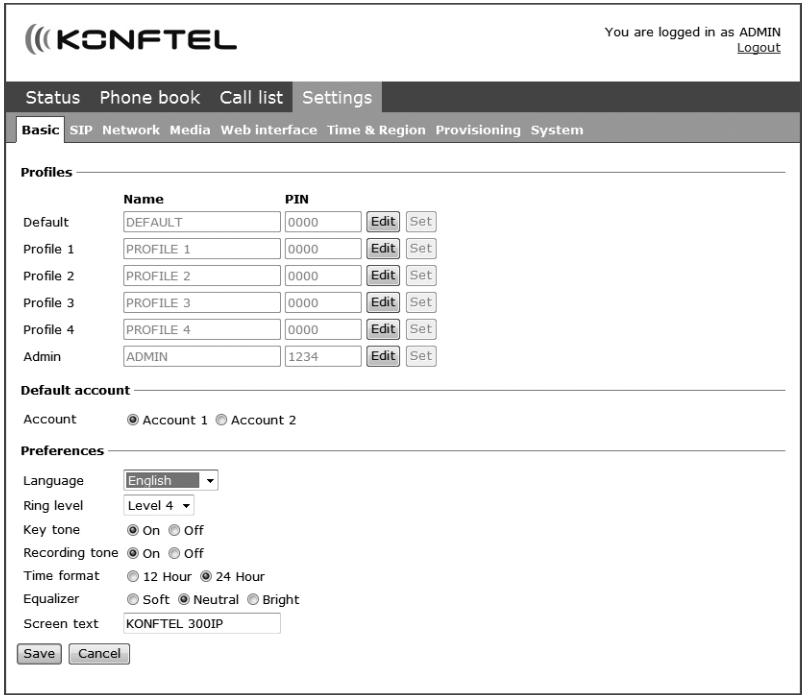
For safety reasons, recordings can only be managed directly on the Konftel 300IP. All other settings can be changed via the web interface. The web interface also allows you to import and export contacts and conference groups, rename user profiles and change PIN codes. As an administrator, you can also study logs, upgrade the software en create an XML based configuration file for easier management of a set of phones.

LOGIN

See “USING THE WEB INTERFACE” on page 6 for a description of how to log in to the web server in Konftel 300IP.

BASIC

⇨ Select **Settings** > **Basic**.



These settings affect the Admin and Default profiles. To change the basic settings of a user profile, you need to log in with that profile.

Profiles – edit name and PIN

PIN code can be changed from the default setting to protect the settings.

⇨ Select **Settings** > **Basic** and click the **Edit** button on the account you want to change.

⇨ Enter a new PIN code.

ⓘ The PIN code may consist of 8 digits.

ⓘ You can also choose to change the name of a user profile.

⇨ Click on the **Set** and **Save** buttons.

ⓘ Make a note of the new PIN code and keep it in a safe place.

ⓘ The administrator’s PIN code can only be reset with a complete reset to factory settings!

Default account

This setting determines which account to be used as default. By pressing **LINE** before dialing a number, you can choose the alternative account for the call.

⇨ Select Account 1 or Account 2 and click on the **Save** button.

On phone: **MENU** > **SETTINGS** > **BASIC** > **ACCOUNT** (5,1,1).

Language

⇨ Select language using the list box and click on the **Save** button.

On phone: **MENU** > **SETTINGS** > **BASIC** > **LANGUAGE** (5,1,2).

Ring level

There are six volume levels plus a silent mode. You will hear the ring tone for each level you select. If you select silent mode, only the blue LEDs on the phone flashes when an incoming call is received.

⇨ Select level using the list box and click on the **Save** button.

On phone: **MENU** > **SETTINGS** > **BASIC** > **RING LEVEL** (5,1,4).

Key tone

You can select whether or not you want a tone to be heard when you press a button.

⇨ Select On or Off and click on the **Save** button.

On phone: **MENU** > **SETTINGS** > **BASIC** > **KEY TONE** (5,1,3).

Recording tone

A short beep is heard every 20 seconds so that all the parties in the call know it is being recorded. This feature can be turned off.

⇨ Select On or Off and click on the **Save** button.

On phone: **MENU** > **RECORDING TONE** > **SETTINGS** (4,5).

Time format

⇨ Select 12 hour or 24 hour and click on the **Save** button.

On phone: **MENU** > **SETTINGS** > **BASIC** > **TIME FORMAT** (5,1,7).

Equalizer

The sound reproduction can be adjusted to the required pitch (SOFT, NEUTRAL or BRIGHT).

⇨ Select Soft, Neutral or Bright and click on the **Save** button.

On phone: **MENU** > **SETTINGS** > **BASIC** > **EQUALIZER** (5,1,5).

Screen text

The text on the display screen is shown when Konftel 300IP is in stand-by mode (on hook).

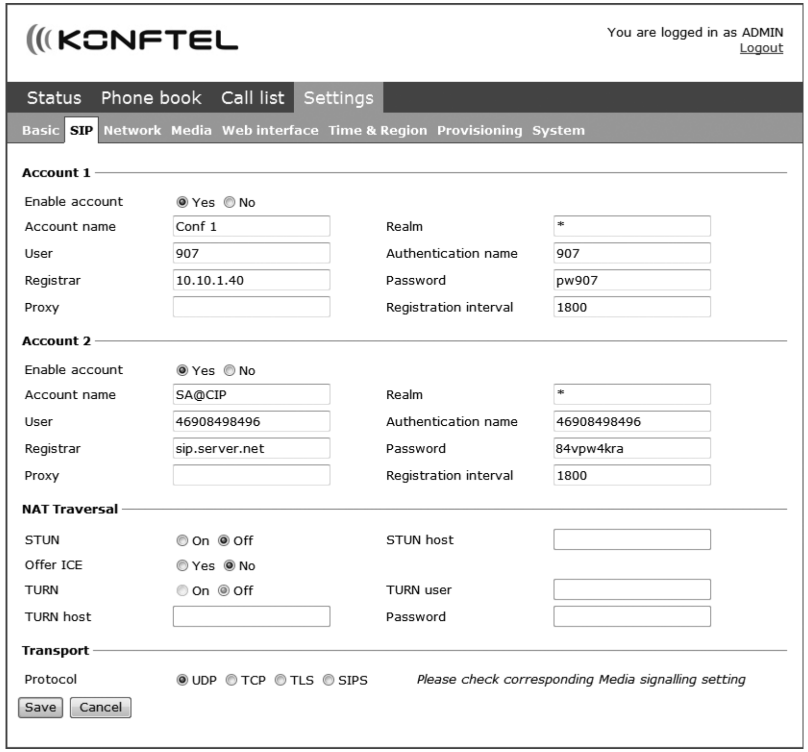
⇨ Enter your new text in the text box and click on the **Save** button.

On phone: **MENU** > **SETTINGS** > **BASIC** > **SCREEN TEXT** (5,1,8).

SETTINGS

SIP

⇨ Select **Settings** > **SIP**



Konftel 300IP can store information for two accounts, e.g. one PBX and one public service provider.

Why use two accounts?

It may be practicable to register a second account if the PBX or SIP server is located in another country than the phone. Otherwise would local calls using the PSTN (telephone network), connected through the ordinary PBX or SIP server, be connected as international calls.

Account 1 and Account 2

Enable account	It is possible to store account information for future use, but temporarily make it disabled.

Account name	This is the name showed on the display and can be set according to company standards.
User	The account (customer) name.
Registrar	Shall contain the IP address or the public name of the SIP server where the account is registered (e.g. 10.10.1.100 for a local SIP server or sip.company.net for a public VoIP service provider)
Proxy	Shall contain the proxy server used for Internet communication, if any. Can be left blank.
Realm	The protection domain where the SIP authentication (name and password) is valid. This is usually the same as the registrar. If left blank, or marked with a "*", the information is taken from the Registrar field.
Authentication name	The name used for the Realm authentication. This may be the same as the user name, but must be filled in.
Password	The password used for the Realm authentication.
Registration Interval	This is a request to the SIP server for when the registration should expire. Konftel 300IP automatically renews the registration within the time interval if the phone still is on and connected to the server. The default value is 1800 seconds.

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **ACCOUNTS** (5,2,1).

Nat traversal

NAT (*Network Address Translation*) is a firewall or router function that operates by rewriting the IP addresses in the IP headers as packets pass from one interface to the other. When a packet, for example, is sent from the inside, the source IP address and port are rewritten from the private IP address space into the address space on the outside (Internet).

NAT rewrites the addresses but leaves the packages themselves untouched. This kind of translation works just fine for many protocols, but causes a lot of trouble for SIP packages that contain address information in its content (for example an INVITE request from one IP address to another).

NAT traversal is a solution to this problem, providing a "view from the outside" that makes it possible to replace the IP address in the SIP requests with the address shown on the other side of the firewall.

Note that in some cases NAT traversal is not necessary. Some public service providers of IP telephony keep track of the actual IP address used to register a phone, and the one used in the SIP requests from the same phone, and then replaces the addresses in the SIP messages.

STUN	STUN (*Simple Traversal of UDP through NATs*) is a protocol for assisting devices behind a NAT firewall or router with their packet routing. STUN is commonly used in applications of real-time voice, video, messaging, and other interactive IP communications. The protocol allows applications operating through a NAT to discover the presence and specific type of NAT, and obtain the mapped (public) IP address (NAT address) and port number that the NAT has allocated for the application's *User Datagram Protocol* (UDP) connections to remote hosts. The protocol requires assistance from a 3rd-party network server (STUN server). STUN should be activated if an external SIP server cannot connect to the Konftel 300IP behind a firewall NAT function and the SIP server supports STUN. A suitable STUN server is usually provided by the VoIP service provider. Note: STUN might also be referred to as *Session Traversal Utilities for NAT*.
STUN host	The IP address or public name of the STUN server.
Offer ICE	ICE (*Interactive Connectivity Establishment*), is a STUN addition that provides various techniques to allow SIP-based VoIP devices to successfully traverse the variety of firewalls that may exist between the devices. The protocol provides a mechanism for both endpoints to discover the most optimized path to be used for the media traffic.
TURN	TURN (*Traversal Using Relay NAT*) TURN is an extension to the STUN protocol to facilitate NAT traversal when both endpoints are behind symmetric NAT. With TURN, media traffic for the session will have to go to a relay server. Since relaying is expensive, in terms of bandwidth that must be provided by the provider, and also additional delay for the media traffic, TURN is normally used as the last resort when endpoints cannot communicate directly.
TURN User	User authentication name on the TURN server.
TURN host	The IP address or public name of the TURN server.
Password	User authentication password on the TURN server.

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **NAT TRAVERSAL** (5,2,3).

Transport

The transport setting only concern which protocol to be used for SIP messages between the devices involved. These settings do not include the media (the actual call). The settings on the Media tab should be set accordingly.

Note that if you choose to use a secure connection, both units must support it. Otherwise they cannot negotiate a connection. If an incoming call demands a secure TLS or SIPS connection, Konftel 300IP uses the appropriate protocol even if you have set the phone to use UDP.

Protocol — **UDP** (*User Datagram Protocol*) is a protocol on the transport layer in the Internet Protocol Suite. It is a stateless protocol for short messages – datagrams. Stateless imply that it does not in advance establish any connection between sender and receiver. UDP does not guarantee reliability or ordering in the way that TCP does. Datagrams may arrive out of order or go missing without notice. The advantage is speed and efficiency.

UDP is the default protocol for SIP.

TCP (*Transmission Control Protocol*) is a protocol on the transport layer in the Internet Protocol Suite. TCP is the standard protocol for Internet communication. TCP keeps track of all individual packets of data, that they arrive to the receiver and are put together properly. TCP is not the default protocol for SIP, because it is slower and uses more bandwidth than UDP.

With UDP and TCP, SIP packets travel in plain text. **TLS** (*Transport Layer Security*) is a cryptographic protocol that provide security and data integrity for communications over TCP/IP networks. TLS encrypts the datagrams of the transport layer protocol in use. The secure connection may be to the end device or to the first server (usually the SIP server where the phone is registered). There is no guarantee that there is a secure channel to the end point, but because the SIP server is the only part receiving the user authentication, this is still a rather secure solution.

SIPS (*Secure SIP*) is a security measure that uses TLS to provide an encrypted end-to-end channel for the SIP messages. To use SIPS, however, both VoIP devices and the SIP server must support it.

ⓘ Even if Transport is set to TLS or SIPS, Konftel 300IP still accepts incoming UDP or TCP signalling.

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **ACCOUNTS** > **TRANSPORT** (5,2,1,3).

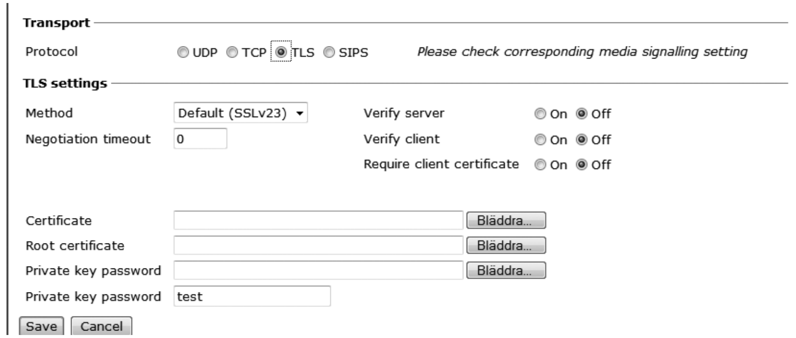
SETTINGS

TLS Settings

If you select TLS or SIPS under the transport setting, this additional settings appear on the page.

It may be possible to use secure communication without using a certificate and making any changes to this settings. In some cases the SIP server requires a certificate for user/client verification, if you choose to use TLS or SIPS. This should be specified in the account information.

You are also able to increase security furthermore by requiring verification of the server, or the client when Konftel 300IP acts as a server for incoming calls.



Method — The TLS include a variety of security measures. The methods is defined in the versions of the standard (SSL, SSL v2, SSL v3, TLS v1, TLS v2). The default method is SSLv23, which accepts both SSL v2 and v3.

Negotiation timeout — The TLS settings are negotiated during a call setup (both incoming and outgoing). If this negotiation does not succeed within the specified time (seconds) the negotiation is aborted. Timeout is disabled with 0 (zero).

Verify client — When set to On, the Konftel 300IP will activate peer verification for incoming secure SIP connections (TLS or SIPS).

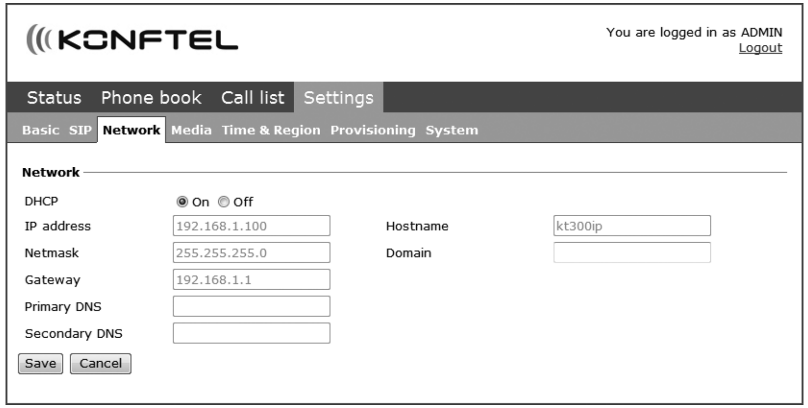
Require client certificate — When set to On, the Konftel 300IP rejects incoming secure SIP connections (TLS or SIPS) if the clients doesn’t have a valid certificate.

Verify server — When Konftel 300IP is acting as a client (outgoing connections) using secure SIP (TLS or SIPS) it will always receive a certificate from the peer. If Verify server is set to On, Konftel 300IP closes the connection if the server certificate is not valid.

Certificate	Here you can upload a certificate to the Konftel 300IP to be used for TLS or SIPS communication. A certificate is a file that combines a *public key* with information of the *owner* of the public key, all signed by a trusted third party. If you trust the third party, then you can be sure that the public key belongs to the person/organization named in that file. You can also be sure that everything you decrypt with that public key is encrypted by the person/organization named in the certificate.
Root certificate	The public key in the root certificate is used to verify other certificates. A root certificate is only needed if you have selected client or server verification. A root certificate is a certificate that is signed by the same public key that is in the certificate, a so-called "self-signed" certificate. A typical root certificate is a certificate received from a *Certificate Authority*.
Private key	Here you can upload a private key to the Konftel 300IP to be used for TLS or SIPS communication. A private key is one of the keys in a key-pair used in *asymmetric cryptography*. Message that is encrypted with the public key can only be decrypted using the private key.
Private key password	The password used for encryption of the private key, if it is encrypted.

NETWORK

⇨ Select **Settings** > **Network**.

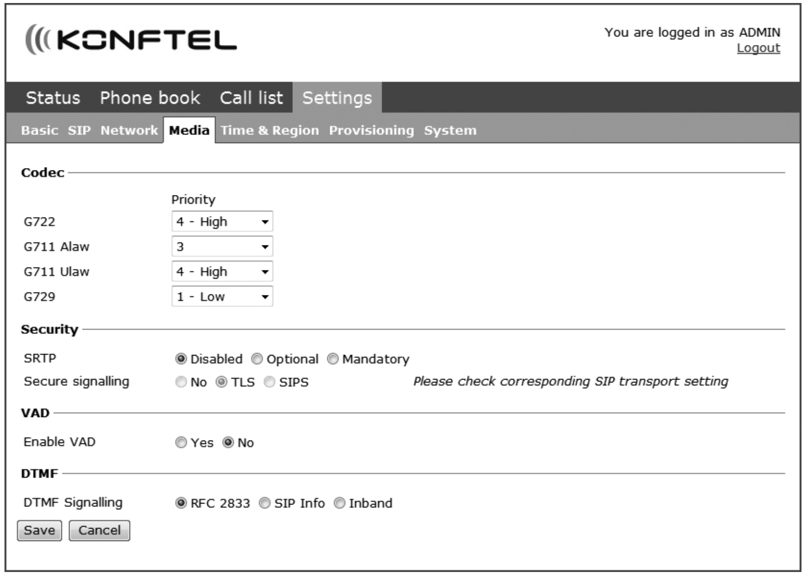


DHCP	*Dynamic Host Configuration Protocol* is a protocol used by network devices (clients) to obtain the parameters necessary for operation in the IP network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual configuration. DHCP should be set to on if no other information is given. When set to on, all other information on this page will be set automatically.
IP address	IP address of the device (Konftel 300IP). The address is provided by the network administrator or service provider if DHCP is not in use.
Hostname	Is set to kt300ip as default. Can be changed to suitable name.
Netmask	Is usually set to 255.255.255.0 to limit network traffic to the subnet.
Domain	The domain where the device is located. May be left blank.
Gateway	The device or server used for Internet communication.
Primary DNS	The address to the primary DNS (*Domain Name System*) server - a program or computer that maps a human-recognisable name to its computer-recognisable identifier (IP address).
Secondary DNS	The address to an optional secondary DNS server.

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **NETWORK** (5,2,2).

MEDIA

⇨ Select **Settings** > **Media**.



The media settings affect how the audio is sent between the devices. The involved devices perform a negotiation using SIP before a call is connected. All devices must support the same media types, codecs and security settings.

Codec

Codecs are used to convert an analogue voice signal to a digitally encoded version and vice versa. Codecs vary in the sound quality and the bandwidth required. Konftel 300IP supports the most common codecs and each codec can be given a precedence depending of if you prefer high quality audio or low bandwidth use.

The priority can be set to from 4 (high) to 1 (low) or 0 (disabled)

G722	G.722 is an *ITU-T* standard codec that provides 7 kHz wideband audio at a data rate within 64 kbit/s. It offers a significant improvement in speech quality over older narrowband codecs such as G.711, but requires a high quality network connection between the devices.
G711 Alaw	G.711 is an ITU-T standard codec that uses audio companding. Companding algorithms reduce the dynamic range of an audio signal. In analogue systems, this can increase the signal-to-noise ratio achieved during transmission, and in the digital domain, it can reduce the quantization error. There are two main compression algorithms defined in the standard, the µ-law algorithm (used in North America & Japan) and A-law algorithm (used in Europe and the rest of the world).
G711 Ulaw	See G711 µ-law above.
G729	G.729 is an ITU-T standard codec that operates at 8 kbit/s. It is mostly used in VoIP applications with low bandwidth requirement.

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **MEDIA** > **CODEC** (5,2,4,1).

Security

The media in VoIP calls is usually sent using the RTP protocol (*Real-time Transport Protocol*). RTP is a standardized packet format for delivering audio and video over the Internet.

SRTP (*Secure Real-time Transport Protocol*) is an extension to RTP to provide encryption, message authentication and integrity for the audio and video streams.

All devices must support SRTP to establish a connection, and therefore there is possible to set SRTP as disabled, optional or mandatory.

SRTP	If set to disabled, the media is sent using RTP. Note that despite this setting, Konftel 300IP will still use a secure channel if the opposite device demands it. If set to optional or mandatory, a padlock will be shown in the right lower corner on the display. If the other devices support SRTP, the padlock will be shown closed. If not it will be shown open. If set to mandatory, the call will not be connected if the other devices do not support SRTP.
Secure signalling	The SIP messages (signalling) and the SRTP cipher key are sent on a different channel than the media and are not affected by the RTP/SRTP setting. To ensure a secure connection, the signalling must be secured using **TLS** or **SIPS**, see page 20. Note that the SIP transport setting must be set accordingly.

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **MEDIA** > **SECURITY** (5,2,4,4).

VAD

Voice Activity Detection (speech detection) is a technique used in speech processing wherein the presence or absence of human speech is detected in regions of audio. In VoIP applications, the main use of VAD is to avoid unnecessary coding and transmission of silence packets, saving on computation and on network bandwidth.

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **MEDIA** > **VAD** (5,2,4,2).

DTMF

DTMF (*Dual-tone multi-frequency*) signalling is used for telephone signalling over the line to the phone switch or PBX.

If the device itself generates the tones and it is sent in the voice-frequency band, the method is called **Inband**. Using VoIP, this is not the best method. Low bit rate codecs may corrupt the signalling tones and make them hard to recognize for the switch.

RFC 2833 is a method for carrying DTMF-signalling in RTP packets using a separate RTP payload format. With this method a PSTN gateway reproduces the DTMF tones sent from the end device.

With **SIP Info** the DTMF signalling is sent as SIP requests. The SIP switch creates the tones if the call is transferred to the PSTN.

Use RFC 2833 or SIP Info as preferred methods. Switch to inband only if you encounter problems using DTMF signalling with your PBX/SIP switch.

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **MEDIA** > **DTMF SIGNALLING** (5,2,4,3).

WEB INTERFACE

⇨ Select **Settings** > **Web interface**.

The web server in the Konftel 300IP supports secure connections using HTTPS.

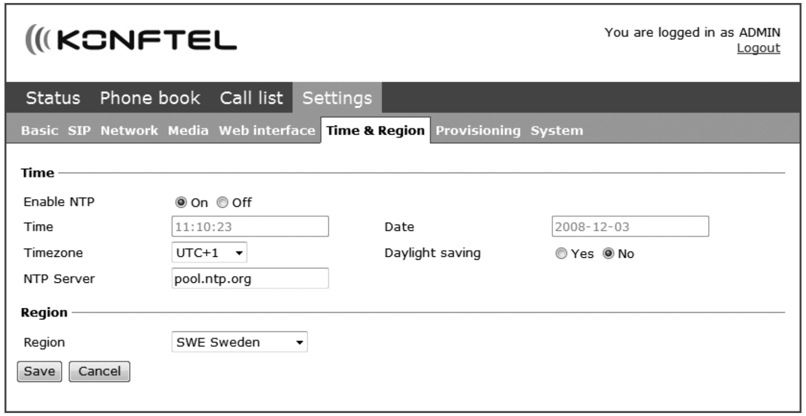
Enable HTTPS	Set *Enable HTTPS* to On if you need a secure communication between the PC used for setup and the phone.
Certificate	To use HTTPS you need to upload a certificate to the phone.

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **WEB INTERFACE** (5,2,7).

SETTINGS

TIME & REGION

⇨ Select **Settings** > **Time & Region**.



Time

Enable NTP	NTP (*Network Time Protocol*) is a protocol for distributing the *Coordinated Universal Time* (UTC) by means of synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.
Time	This field shows the actual time if NTP is enabled. Otherwise enter the correct time (hh:mm:ss) and save the setting.
Date	This field shows the actual date if NTP is enabled. Otherwise enter the correct date (yyyy-mm-dd) and save the setting.
Timezone	Select the UTC time zone in your country.
Daylight saving	Select the Yes radio button if DST (*Daylight Saving Time* or *Summer Time*) is currently used in your country. Note that this setting only adjusts the time one hour, and do not change the time automatically when the DST starts and ends.
NTP Server	The *NTP pool* is a dynamic collection of networked computers that volunteer to provide highly accurate time via NTP to clients worldwide. The machines that are ”in the pool” are part of the pool.ntp.org domain as well as of several subdomains divided by geographical zone and are distributed to NTP clients via round robin DNS.

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **TIME** (5,2,5).

Region

Select the region where you are. This setting affect the signalling (disconnect tone, busy tone, etc).

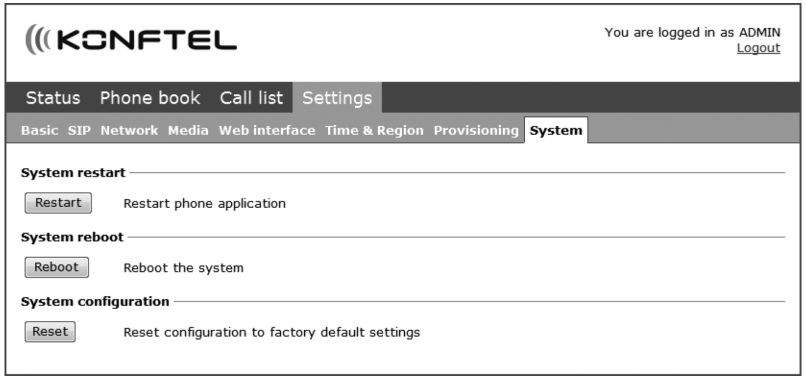
On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **REGION** (5,2,6).

PROVISIONING

See “PROVISIONING – UPGRADE AND CONFIGURATION” on page 31.

SYSTEM

⇨ Select **Settings** > **System**.



Application restart

The **Restart** button restarts the phone application. This takes less than 30 seconds.

On phone: **MENU** > **SYSTEM** > **RESTART** (6,1).

System reboot

The **Reboot** button reboots the conference phone. The starting procedure may take about two minutes.

On phone: **MENU** > **SYSTEM** > **REBOOT** (6,2).

System configuration

The **Reset** button resets Konftel 300IP to factory default settings. Every personal setting including account information is erased.

On phone: **MENU** > **SYSTEM** > **FACTORY RESET** (6,3).

Hard reset to factory settings

See page 45 about resetting the phone if you have forgotten the Admin PIN code.

⇨ Select **Settings** > **Provisioning**.

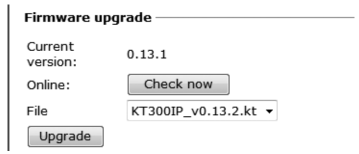
FIRMWARE UPGRADE

Konftel 300IP is easiest upgraded via a computer connected to the same network. Via the web interface, you can check if a later version is available, and then automatically install it.

It is also possible to download the latest version, via the Konftel website (**www.konftel.com/300ip**), and then install the file via the web interface.

⇨ Click on the **Check Now** button.

⇨ Compare the latest software version with the current version (shown on the same page).



⇨ If you choose to upgrade, select version in the list box and click on the **Upgrade** button.

The browser window and the Konftel 300 iP display shows that the upgrading has begun.

ⓘ The download and installation can take several minutes. Do not interrupt the upgrade and do not disconnect any plug on Konftel 300IP during the upgrade. An interrupted upgrade can make the conference phone unusable.

When installation is complete, the text “Upgrade Complete. The unit will be rebooted.” is shown in your browser, and after a while you hear the Konftel music signature, which indicates that the conference phone has started.

Upgrading from downloaded file

It is possible to download a firmware file from www.konftel.com/300ip, and install it into the Konftel 300IP from the local hard disk.

⇨ Download the firmware file from **www.konftel.com/300ip**.

⇨ Click on the **Browse...** button and locate and choose the downloaded file.

⇨ Click on the **Check Now** button.

After upgrading

If DHCP is used in the network, the IP address may have been changed. If the web browser looses contact with Konftel 300IP, check the IP address on the conference phone (see “USING THE WEB INTERFACE” on page 6).

PROVISIONING – UPGRADE AND CONFIGURATION

USING A CONFIGURATION FILE

It is possible to save a configuration xml file to be used as:

- Backup (i.e. if the system has been reset to factory default)
- Configuration interface (there are some settings that are not configurable via the web interface)
- Management tool (export, edit, and import settings to a set of phones instead of doing the settings on each phone)

The structure of the xml file is as follows:

<locale>

<region>	

<logging>

<level>	The phone application logs messages to log facility LOCAL0. Log level 1–5 (equivalent to Fatal–Trace)
<log_sip>	Log sip messages to log facility LOCAL1. Default is true.
<remote_log>	Log messages to a remote log server. Default is false.
<remote_host />	Remote log server.

<network>

<net>	
<dhcp>	Specify if DHCP should be used to obtain network settings. If so, the other network settings won’t be used.
<ip>	Specify the IP address of the KT300IP.
<netmask>	The netmask of the IP address.
<gateway>	Specify the default gateway to be used.
<dns />	Specify at most two Domain Name Servers to be used.
<dns />	
<hostname>	Specify host name.
<domain />	Specify domain name.
<time>	
<ntp>	
<timezone>	
<daylight_save>	
<ntps>	

<sip>

<udp_transport>	Specify if UDP shall be used as transport.
<udp_port>	Specify the UDP port to listen to.
<tcp_transport>	Specify if TCP shall be used as transport.
<tcp_port>	Specify the TCP port to listen to.
<tls_transport>	Specify if TLS shall be used as transport.
<sips_transport>	Specify if SIPS shall be used as transport.
<tls_port>	Specify the TLS port to listen to.
<rtp_port>	Specify the start port for RTP traffic.
<outbound_proxy />	Specify the URL of outbound proxies to visit for all outgoing requests. The outbound proxies will be used for all accounts, and it will be used to build the route set for outgoing requests. The final route set for outgoing requests will consists of the outbound proxies and the proxy configured in the account.
<use_stun>	Use Simple Traversal of UDP through NATs (STUN) for NAT traversal. Default is no.
<stun_domain />	Specify domain name to be resolved with DNS SRV resolution to get the address of the STUN servers. Alternatively application may specify stun_host and stun_relay_host instead.
<stun_host />	Specify STUN server to be used, in "HOST[:PORT]" format. If port is not specified, default port 3478 will be used.
<use_turn>	Use Traversal Using Relay NAT (TURN) for NAT traversal. Default is no.
<turn_host />	Specify TURN relay server to be used.
<turn_tcp>	Use TCP connection to TURN server. Default is false.
<turn_user />	TURN username.
<turn_passwd />	TURN password.
<nat_type_in_sdp>	Support for adding and parsing NAT type in the SDP to assist trouble-shooting. The valid values are: 0: no information will be added in SDP, and parsing is disabled 1: only the NAT type number is added 2: add both NAT type number and name
<require_100rel>	Specify whether support for reliable provisional response (100rel and PRACK) should be required by default. Note that this setting can be further customized in account configuration.
<use_srtp>	Specify default value of secure media transport usage. Note that this setting can be further customized in account configuration. 0: SRTP will be disabled, and the transport will reject RTP/SAVP offer. 1: SRTP will be advertised as optional and incoming SRTP offer will be accepted. 2: The transport will require that RTP/SAVP media shall be used.

<srtp_secure_signaling>	Specify whether SRTP requires secure signalling to be used. This option is only used when use_srtp option above is non-zero. Note that this setting can be further customized in account configuration. 0: SRTP does not require secure signalling 1: SRTP requires secure transport such as TLS 2: SRTP requires secure end-to-end transport (SIPS)
<codec>	
<type>	Codec type
<name>	Codec name
<prio>	Codec priority (0-4)
<dtmf>	DTMF signalling. Default is 2. 0: In-band 1: SIP message 2: RTP message
<no_vad>	Disable VAD? Default is VAD enabled.
<ec_tail>	Echo canceller tail length, in milliseconds.
<enable_ice>	Enable ICE?
<enable_relay>	Enable ICE relay?
<enable_presence>	Enable the use of presence signalling.

<tls>

<tls_password />	Password for the private key
<tls_method>	TLS protocol method from pjsip_ssl_method, which can be: 0: Default (SSLv23) 1: TLSv1 2: SSLv2 3: SSLv3 23: SSLv23
<tls_verify_server>	Verify server certificate.
<tls_verify_client>	Verify client certificate.
<tls_require_client_cert>	Require client certificate.
<tls_neg_timeout>	TLS negotiation timeout in seconds to be applied for both outgoing and incoming connections. If zero, no timeout is used.

<account>

<valid>	If this account information is valid or not.
<name>	User defined name of the account
<id>	The full SIP URL for the account.
<registrar>	This is the URL to be put in the request URI for the registration.

<publish_enabled>	If this flag is set, the presence information of this account will be Published to the server where the account belongs.
<initial_auth>	If this flag is set, the authentication client framework will send an empty Authorization header in each initial request.
<initial_algo />	Specify the algorithm to use when empty Authorization header is to be sent for each initial request (see above).
<pidf_tuple_id />	Optional PIDF tuple ID for outgoing PUBLISH and NOTIFY. If this value is not specified, a random string will be used.
<force_contact />	Optional URI to be put as Contact for this account. It is recommended that this field is left empty, so that the value will be calculated automatically based on the transport address.
<require_100rel>	Specify whether support for reliable provisional response (100rel and PRACK) should be required for all sessions of this account.
<proxy_uri />	Optional URI of the proxies to be visited for all outgoing requests that are using this account (REGISTER, INVITE, etc).
<reg_timeout>	Optional interval for registration, in seconds. If the value is zero, default interval will be used.
<cred>	Array of credentials. If registration is desired, normally there should be at least one credential specified, to successfully authenticate against the service provider. More credentials can be specified, for example when the requests are expected to be challenged by the proxies in the route set.
<realm>	Realm. Use "*" to make a credential that can be used to authenticate against any challenges.
<scheme />	Scheme (e.g. "digest").
<username>	Authentication name
<cred_data_type>	Type of data (0 for plaintext password).
<cred_data>	The data, which can be a plaintext password or a hashed digest.
<auto_update_nat>	This option is useful for keeping the UDP transport address up to date with the NAT public mapped address. When this option is enabled and STUN is configured, the library will keep track of the public IP address from the response of REGISTER request. Once it detects that the address has changed, it will unregister current Contact, update the UDP transport address, and register a new Contact to the registrar.
<ka_interval>	Set the interval for periodic keep-alive transmission for this account. If this value is zero, keep-alive will be disabled for this account. The keep-alive transmission will be sent to the registrar's address, after successful registration.
<ka_data />	Specify the data to be transmitted as keep-alive packets. Default: CR-LF.
<use_srtp>	Specify whether secure media transport should be used for this account. 0: SRTP will be disabled, and the transport will reject RTP/SAVP offer. 1: SRTP will be advertised as optional and incoming SRTP offer will be accepted. 2: The transport will require that RTP/SAVP media shall be used.
<srtp_secure_signaling>	Specify whether SRTP requires secure signalling to be used. This option is only used when use_srtp option above is non-zero. 0: SRTP does not require secure signalling 1: SRTP requires secure transport such as TLS 2: SRTP requires secure end-to-end transport (SIPS)

PROVISIONING – UPGRADE AND CONFIGURATION

<account>

Same as above for account 2

<provisioning>

<upgrade>

<url>	Place to find software upgrades. The supported URL types are: HTTP, FTP, and TFTP.

<www>

<enable_https>	Secure communication to the 300IP web server. Default is false.

Export configuration

⇨ Click on the **Export** button.
The configuration file is shown in the web browser.

⇨ Choose to save the page as an xml file.
The xml file is as default saved in your folder for downloaded files.

⇨ If needed, edit the xml file in a suitable editor.

Import configuration

⇨ Click on the **Browse...** button.

⇨ Select the xml file and choose to open it.

⇨ Click on the **Import** button.

IMPORTING AND EXPORTING CONTACTS

You can import contacts from a comma separated values (CSV) file. One way of creating a CSV file is using Microsoft Excel and saving the file in CSV format.

Enter the names of the contacts in the first column and their phone numbers or URIs in the second. Do not use hyphens or spaces in the number. Note that Excel ignores zeros at the beginning of numbers. The cells must therefore be formatted as text.

	A	B	C	D	E	F
1	Name	Telephone				
2	Allen, Jerry	+461517954884				
3	Anderson, Justin	+461517954955				
4	Andrews, Fanny	+461517954883				
5	Berg, David	+461517954893				
6	Berlin office	+496423687451				
7	Bewers, Darren	+461517954884				
8	Bjork, Markus	+461517954949				
9	Branshaw, Liw	+461517954871				
10	Carling, Richard	+461517954868				
11	Carlsson, Julia	+461517954884				
12	Claesson, Nicole	+461517954886				
13	Collins, David	+462380599581				
14	Cordin, Justin	+461517954898				
15	Crown, Juanito	+461517954896				
16	Evalders, Julie	+461517954881				
17	Gardelius, Stefan	+461517954950				
18	Hellberg, Mark	+461517954884				
19	Konrads, Ray	+461517954870				
20	Langdon, Steve	+461517954890				
21	Leander, Adam	+461517954879				
22	Lowendahl, Roger	+461517954885				
23	Luong, Xi	+461517954878				
24	Magret, Robin	+461517954895				
25	Mowat, Leo	+461517954872				
26	Mowji, Al	+461517954866				
27	Nelson, Mike	+461517954880				
28	Nyberg, Paul	+461517954867				

It is normally possible to export contact books stored in your PC in CSV format.

ⓘ The way the number can be written may depend on the SIP PBX being used, but normally you can use:

- Complete phone number, including country code
- Phone number, including area code
- Local phone number only
- Internal speed dial number (with company's own PBX)
- URI, e.g. **sip:user@company.com**
- URI with IP address, e.g. **sip:10.10.1.100** (within a local network)

MANAGING PHONE BOOK AND CONFERENCE GUIDE

Importing contacts

⇨ Select **Phone Book**.

⇨ Click on the **Scroll...** button under the heading Import in the web window.

⇨ Open your CSV file.

⇨ Click on **Import**.

ⓘ The name is limited to 15 characters, since the Konftel 300IP screen cannot display more than 15 characters.

Exporting contacts

You can export your contacts as a CSV document in order to import them into another phone.

⇨ Click on **Export**.

⇨ Save the document.

IMPORTING AND EXPORTING CONFERENCE GROUPS

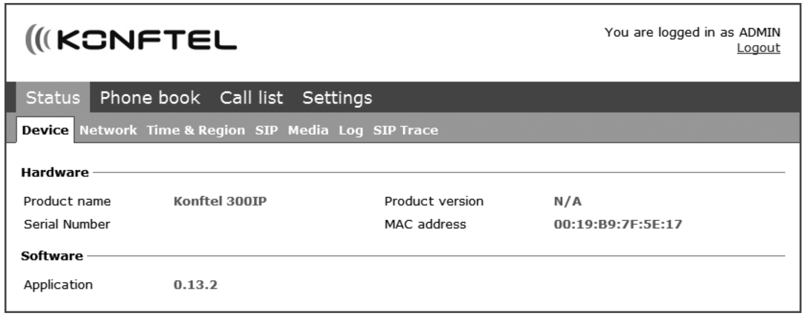
The conference groups can be imported and exported in the same way as the contacts in the phone book, but use a three column csv instead of a two column csv.

	A	B	C	D	E	F	G
1	Group	Name	Number				
2	Sales	Carlsson, Julia	+461517954884				
3	Sales	Berg, David	+461517954893				
4	Sales	Berlin office	+496423687451				
5	Sales	UK office	+441507953687				
6	Development	Bjork, Markus	+461517954949				
7	Development	Branshaw, Liw	+461517954871				
8	Development	Luong, Xi	+461517954878				
9	Development	Lowendahl, Roger	+461517954885				
10							
11							
12							
13							
14							
15							

The tabs under Status show the settings on corresponding tabs plus device info and logs.

DEVICE

⇨ Select **Status** > **Device**.

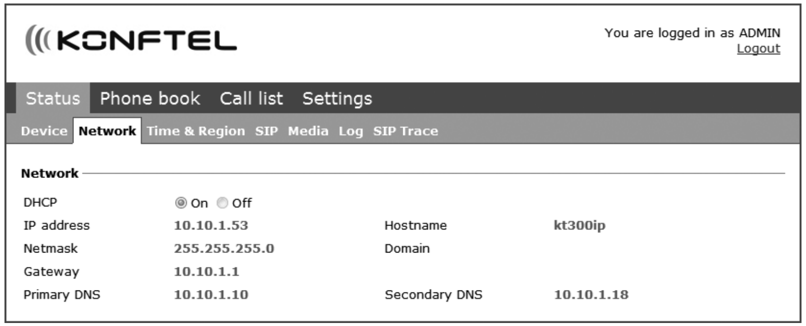


The Device tab shows phone information including serial number, network port and current software version.

On phone: **MENU** > **STATUS** > **DEVICE** (7,6).

NETWORK

⇨ Select **Status** > **Network**.

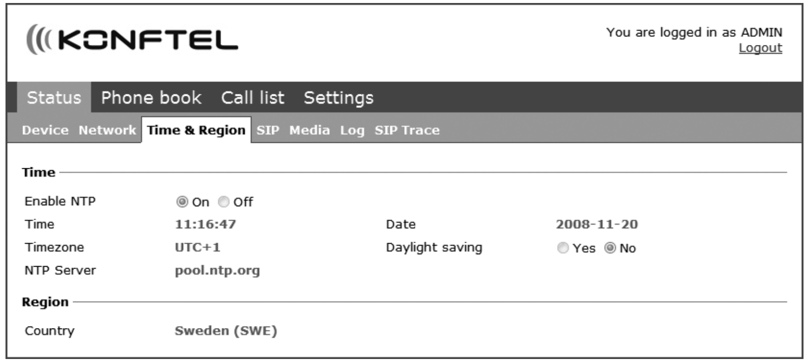


On phone: **MENU** > **STATUS** > **NETWORK** (7,2).

CHECKING STATUS AND LOGS

TIME & REGION

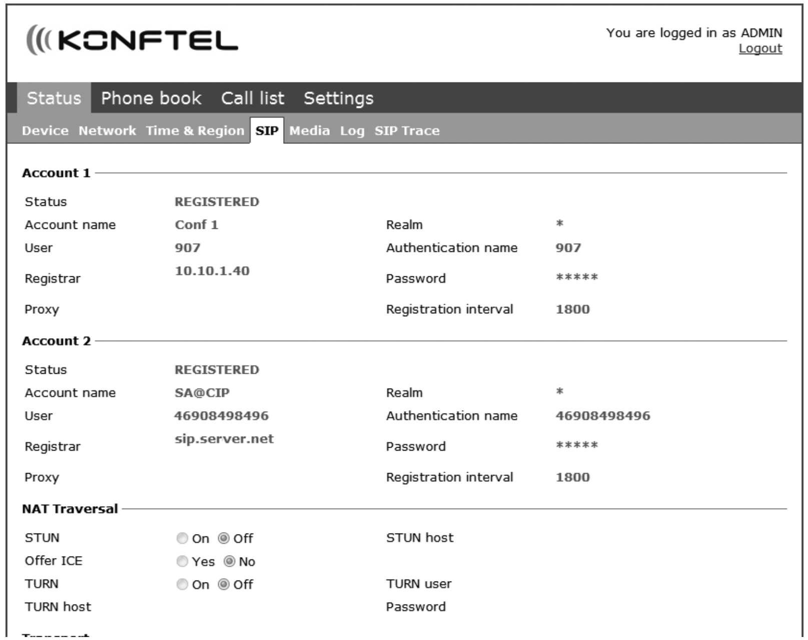
⇨ Select **Status** > **Time & Region**.



On phone: **MENU** > **STATUS** > **TIME** (7,5).

SIP

⇨ Select **Status** > **SIP**.



Account 1 and Account 2

On phone: **MENU** > **STATUS** > **ACCOUNTS** (7,1,1 and 7,1,2).

NAT traversal

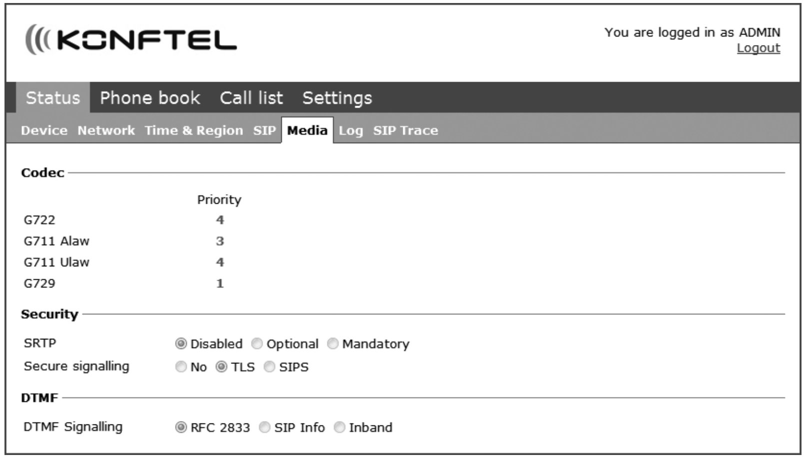
On phone: **MENU** > **STATUS** > **NAT TRAVERSAL** (7,3).

Transport

On phone: **MENU** > **STATUS** > **ACCOUNTS**> **TRANSPORT** (7,1,3).

MEDIA

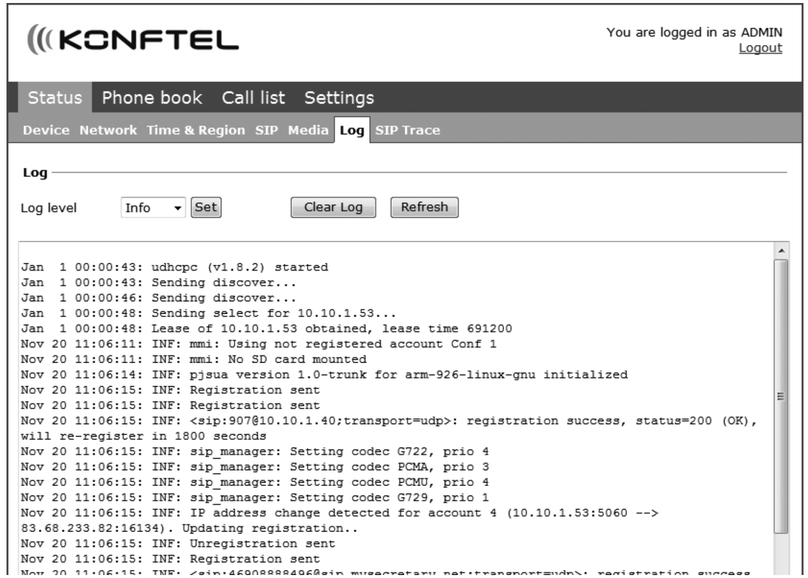
⇨ Select **Status** > **Media**.



On phone: **MENU** > **STATUS** > **MEDIA** (7,4).

LOG

⇨ Select **Status** > **Log**.

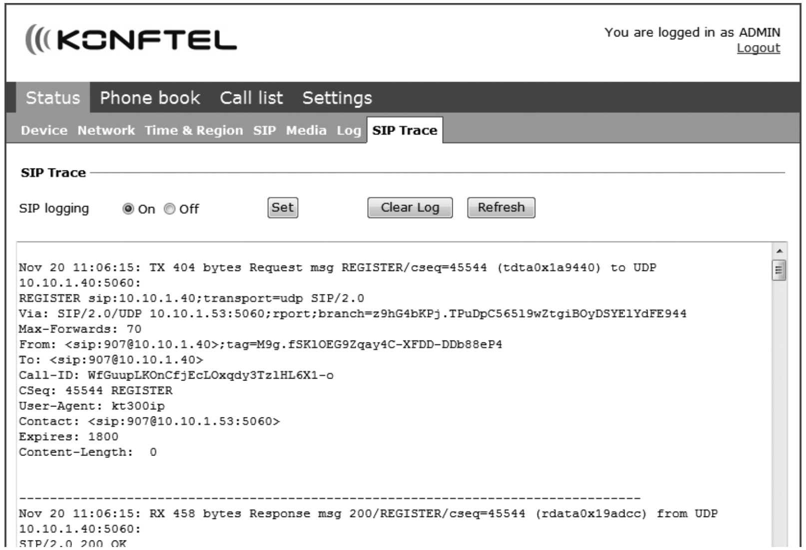


The Log tab contains a log of Konftel 300IP messages and can be useful for trouble shooting. The log can be filtered from "Fatal" (only the fatal error messages) to "Trace" (all messages).

The **Clear log** button erases all content in the log. The **Refresh** button adds all new messages sent since the Log tab was chosen.

SIP TRACE

⇨ Select **Status** > **SIP Trace**.



The SIP Trace logs the communication between the phone and the SIP PBX and can be useful for trouble shooting.

The **Clear log** button erases all content in the log. The **Refresh** button adds all new messages sent since the Log tab was chosen.

HARD RESET TO FACTORY SETTINGS

If you have forgotten the Admin PIN code, the only way to reset it to default is to do a hard factory reset.

ⓘ This erases all settings including account information and contacts!

⇨ Disconnect the power supply cable. Note that this is the same as the network cable if the phone uses Power over Ethernet.

⇨ Press and hold the **MENU** button while you connect the cable again (i.e. starts the Konftel 300IP).

⇨ Upgrade to the latest version of the software when the phone has started and redo the setup of account and other settings (see page 7).

FAULT CODES

Size	Diameter 240 mm, height 77 mm
Weight	1 kg
Colour	Liquorice black
Display screen	Illuminated graphics (LCD), 128x64
Keypad	Alphanumerical 0–9, *, on, off, mute, hold, volume up, volume down, 5 buttons for menu navigation, line mode, conference guide
Anti-theft protection	Kensington security slot
Memory	Support for SD memory cards up to 2 GB

Connectivity

Network connection	RJ45, Ethernet 10/100 Base T
Power supply	Transformer 100–240 V AC/13.5 V DC IEEE 802.3af Power over Ethernet.
Extra microphones	x2 modular 4/4
Auxiliary	Modular 4/4 for wireless headset

Network and communication

Network addressing	DHCP and static IP
NAT traversal	STUN, ICE and TURN
Connection protocol	SIP 2.0 (RFC 3261 and companion RFCs)
Transport	UDP, TCP, TLS and SIPS
Security	SRTP
Audio support	Codecs: G722, G711 A-law, G711 µ-law, G729ab
DTMF tone generation	RFC, SIP INFO, In-band
Time servers	NTP and SNTP
Configuration	Via integrated web server

Sound

Technology	OmniSound™® 2.0 Wideband
Microphone	Omni-directional
Reception area	Up to 30 metres², >10 people
Speaker	Frequency band 200–7000 Hz,
Volume	90 dB SPL 0.5 m
Equalizer	Three pitches: soft, neutral, bright

Environment

Temperature:	5°–40°C
Relative humidity:	20-80% condensation free

Recommended acoustic conditions:

	Reverberation period: 0.5 S Rt 60
	Background noise: 45 dBA

Approvals

Electrical safety	EN 60950-1:2006, ANSI/UL 60950-1-2002, CAN/CSA-C22.2, No. 60950-1-03
EMC/Radio	EN 301 489-3 V1.4.1 (2002-08), EN 301 489-1 V1.6.1 (2005-09), FCC Part 15 subpart B class A, FCC Part 15 subpart C, EN 300220-1:2000, EN 300220-2:2000 RoHS

SERVICE AND GUARANTEE

If anything is wrong with your Konftel unit, please contact the place of purchase.

Guarantee

We give a two-year guarantee on our conference telephones.

Service

Service is offered after the expiration of the guarantee. Please contact your retailer and ask for a cost estimate.

Konftel support

If you have any questions about the guarantee and service, please contact your Konftel support centre

Europe:

+46(0)90-706 489 (Monday–Friday 8.00–17.00 GMT+1)

E-mail: rma@konftel.com

USA and Canada:

+1 866-606-4728 (Monday–Friday 08.00–17.00 GMT-8)

E-mail: konftel.usa@konftel.com

Konftel is a leading company within loudspeaker communication and audio technology. We develop and sell products and technology for telephone conferences based on cutting-edge expertise within acoustics and digital signal processing. A key attribute of our products is that all the conference telephones have built-in, high-quality audio technology – OmniSound® providing crystal-clear sound. Read more about Konftel and our products on **www.konftel.com**.

Developed by Konftel AB
Box 268, SE-901 06 Umeå, Sweden
Phone: +46 90 706 489   Fax: +46 90 131 435
E-mail: info@konftel.com   Web: www.konftel.com

110047-61-001 Rev 0f