KONFTEL.COM

Installation & Administration of Konftel 800

ENGLISH

KONFTEL GET TOGETHER]

CE

Konftel AB hereby declares that this conference phone is in conformity with all the essential requirements and other relevant provisions of Directive 1999/5/EC.

Please visit **www.konftel.com** to view the complete declaration of conformity.

Warning!

Do not expose the Konftel 800 to water or moisture.

Warning!

Do not open the casing of the Konftel 800.

Table of contents

Table of contents

INTRODUCTION

PURPOSE

This document provides checklists and procedures for installing, configuring, and administering Konftel 800. It is intended primarily for implementation engineers and administrators.

OVERVIEW

PHONE OVERVIEW

Konftel 800 is a SIP conference phone that you can use to make calls and hold conferences with a great audio quality. It provides an improved user experience and ensures an easier connection to audio conference bridges. The phone is based on a multi-connectivity platform to leverage the “Bring your own device” approach.

The features of the conference phone include a simple-to-use 4.3 inch graphical LCD with a backlight and volume up/down and mute buttons. Two more mute key buttons are located along the perimeter of the device. You can attach additional expansion microphones or cascade three Konftel 800 devices in a daisy chain to expand the audio distribution and pickup in the room.

SAFETY GUIDELINES

Ensure that you are familiar with the following safety guidelines before installing, configuring, and administering Konftel 800.

ⓘ This conference phone is not designed for making emergency telephone calls when the power fails. Make alternative arrangements for access to emergency services.

- Read, understand, and follow all the instructions.
- Do not place this phone on an unstable cart, stand, or table. Konftel 800 may fall, causing serious damage to the device.
- Do not drop, knock, or shake the phone. Rough handling can break internal circuit boards.
- Ensure that the power cord or plug is not damaged.
- Do not overload wall outlets and extension cords as this can result in the risk of fire or electric shock.
- Avoid wetting the device to prevent fire or electrical shock hazard.
- Unplug the device from the wall outlet before cleaning. Do not use liquid or aerosol cleaners, harsh chemicals, cleaning solvents, or strong detergents to clean the device. Use a damp cloth for cleaning.
- Avoid exposing the phone to high temperatures above 40°C (104°F), low temperatures below 0°C (32°F), or high humidity.
- Do not block or cover slots and openings of the phone. These openings are provided for ventilation, to protect the phone from overheating.

- Never push objects of any kind into this phone through cabinet slots as they might touch dangerous voltage points or short out parts that could result in a risk of fire or electric shock.
- Do not disassemble this product to reduce the risk of electric shock. Opening or removing covers may expose you to dangerous voltages or other risks. Incorrect reassembly can cause electric shock during subsequent use.
- Do not use the phone to report a gas leak in the vicinity of the leak.
- Do not use the phone near intensive care medical equipment or close to persons with pacemakers.
- Do not place the phone too close to electrical equipment such as answering machines, TV sets, radios, computers, and microwave ovens to avoid interference.

ⓘ In case Konftel 800 and the corresponding accessories are damaged, the device does not operate normally or exhibits a distinct change in performance, refer for servicing to the qualified service personnel.

PHYSICAL LAYOUT

Figure 1: Front view of Konftel 800 IP Conference Phone

The following table lists the buttons and the other elements of Konftel 800 IP Conference Phone.

Callout number	Description
1	Mute buttons

Callout number	Description
2	Volume down button
3	Volume up button
4	NFC tag
5	Touch screen
6	LED status indicators

CONNECTION LAYOUT

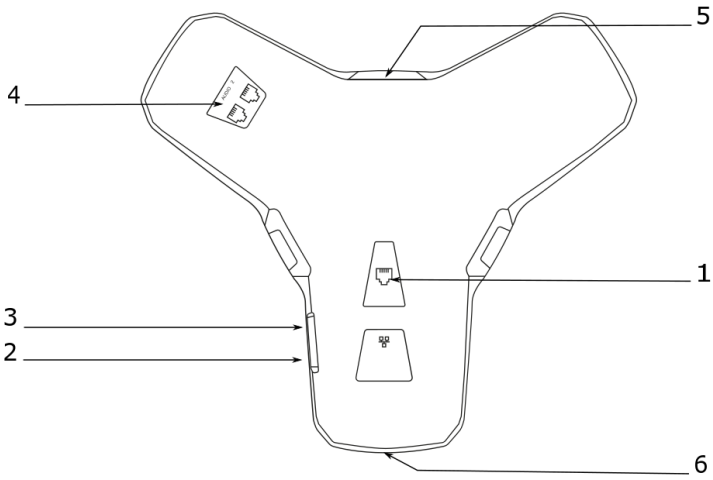

Figure 2: Connection layout of Konftel 800 IP Conference Phone

The following table lists the sockets and ports available on Konftel 800 IP Conference Phone for connection.

Callout number	Description
1	PoE/Ethernet connection socket
2	USB Type A
3	Micro-USB Type B
4	Audio expansion ports
5	Kensington® security lock port
6	NFC tag for Bluetooth

DIMENSIONS

The following table shows the dimensions of Konftel 800 IP Conference Phone.

Parameter	Dimension
Width	326.41 mm
Length	369.87 mm
Height	74.7 mm

ICONS

Icons on the main screen of Konftel 800 IP Conference Phone

Icon	Name	Description
	Recent	To check the call list. The phone provides the following information about the calls: • **Number**. You can view the number or the name of the contact from the phone book.

Icon	Name	Description
		• **Date**. You can view the information when the phone received the call. This applies only to the calls preceding the current day. • **Time**. For the current day the phone shows the time of the call in `hh:mm` format. • **Direction**. You can view the incoming, outgoing and missed calls.
	Unite	To access the Konftel Unite settings.
	Dialpad	To dial phone numbers and codes for telephone operations or Konftel Unite connection.
	Settings	To check and configure the settings from the phone. You can view the phone's status and reach the menu.
	Mute	To mute and unmute the phone.
	Volume up	To increase the phone's volume level.
	Volume down	To decrease the phone's volume level.

Other icons of Konftel 800 IP Conference Phone

Icon	Name	Description
	Call/Answer	To indicate the phone's off-hook status and answer an incoming call.

Icon	Name	Description
	Hang up	To indicate the phone's on-hook status and end a call.
	Incoming call	To show an incoming call.
	Outgoing call	To show an outgoing call.
	Missed call	To indicate a missed call.
	Hold/On Hold	To put a call on hold or to indicate that a call is on hold.
	Conference	To organize a conference call.
	Split	To split a conference call into several separate calls.
	Add participant	To add a participant to a conference call.
	Talk private	To organize a private discussion with a participant of a conference call.
	Caps	To capitalize the letters.

Icon	Name	Description
	Delete	To delete an unneeded number or letter.
	Visibility	To mark if the characters must stay visible to the user, for example during the log in with the password.
	Invisibility	To mark if the characters must stay invisible to the user, for example during the log in with the password.
	Logged in	To indicate that the user logged in as the administrator.
	Microphone muted	To indicate that the phone is in muted state.
	Enter	To confirm the input of information.
	Confirm	To confirm the information.
	Reject	To discard the information.
	Arrow down	To move to the sections below.
	Arrow up	To move to the sections above.

Icon	Name	Description
	Arrow left	To return to the previous page.
	Arrow right	To move to subsections of a section.
	USB	To indicate an active USB connection.
	Konftel Unite connected	To show the connection of the phone to Konftel Unite.
	Daisy chain	To indicate that the phone is in a daisy chain mode.
	Loading	To show that the phone is loading the new version of the firmware.

PREREQUISITES

Konftel 800 is based on a multi-connectivity platform to support the “Bring your own device” use case. You can connect Konftel 800 to a SIP server using the Ethernet.

The following checklist describes tasks you must perform before setting up your Konftel 800:

No.	Task	Notes	✔
1	Review prerequisite information.	If you do not have all the required software and hardware, Konftel 800 might not function as expected.	
2	Gather pre-installation data.	Pre-installation data is required to perform initial parameter setup and to create user accounts for Konftel 800.	
3	Ensure that the Konftel 800 package contains all the required components and accessories.	You can connect optional components and accessories to Konftel 800. Perform this task if you want to use the optional components and accessories with your device.	
4	Connect Konftel 800 to a power supply and to the network.		

Software and hardware prerequisites

Install and configure:

- A DHCP server for providing dynamic IP addresses
- A file server, an HTTP/HTTPS for downloading software distribution packages and the settings file
- Konftel Unite

Konftel 800 requires the current version of Konftel Unite to be installed.

Server configuration checklist

The following checklist describes the tasks related to server configuration that you must perform for the initial installation of Konftel 800.

No.	Task	Notes	✔
1.	Ensure that you have all required licenses for the DHCP and file server software.	Contact your server software vendors to obtain information about server licensing.	
2.	Ensure that a DHCP server is installed and configured.	Contact your DHCP server vendor to obtain installation documentation.	
3.	Ensure that a file server is installed and configured.	Contact your file server vendor to receive installation documentation.	

Power supply connectivity

Konftel 800 uses 10/100/1000 Mbit Ethernet and supports PoE Type 1 and Type 2 power supply, which means either 15W or 30W at the power distribution unit.

Operation modes:

- PoE 802.3af 15W
- PoE 802.3at 30W

ⓘ If your LAN does not support the PoE 802.3af 15W/PoE 802.3at 30W specification, you can use the AC power adaptor, which can be purchased with the device.

Connection to other devices

Konftel 800 is based on a multi-connectivity platform and uses the following features and ports to connect to devices such as a personal computer, expansion microphones, and another Konftel 800:

- Built-in Bluetooth LE
- Built-in NFC tag
- USB Type A
- Micro-USB Type B
- Audio expansion ports

SPECIFICATIONS

The following specifications are supported on Konftel 800:

Name	Description
Power	• PoE 802.3af • PoE 802.3at • PoE injector available as an accessory
Connectivity	• Ethernet RJ45 10/100/1000 Mbps, PoE 802.3af and PoE 802.3at • Built-in Bluetooth LE • USB 2.0 Device • Daisy Chain (audio) ports (6-pin RJ-type)
Screen	Graphical touch screen with a resolution of approximately 480x800 and size of 4.3”
Acoustics	• 3 symmetrically placed MEMS microphones • Full range speaker in the sealed enclosure
Music	• PoE 802.3at: 91 dB and bass boost • PoE 802.3af: 87 dB • Daisy Chain: 91 dB
Speech	• PoE 802.3at: 91 dB • PoE 802.3af: 87 dB • Daisy Chain: 91 dB
USB	• Micro-USB Type B
Bluetooth	• Bluetooth LE
Accessories	You can additionally purchase the following accessories: • Konftel PoE kit • Konftel Smart Microphones • Konftel Daisy Chain kit

Name	Description
User interface	• Simplified user interface • Functional keypad and dial pad • LED indicators for mute/hold

INITIAL SETUP AND CONFIGURATION

CONFIGURATION OF KONFTEL 800

You can configure Konftel 800 directly from the phone or adjust the settings through the web interface. You can use the web browser of a PC connected to the same network to conduct the initial setup of the phone, its registration in the network, and settings in Konftel 800. You can view logs, update software, and create configuration files in the web interface.

ⓘ

The administrator can always change the administrator password. By default, the administrator password is not set. You must set it when you first activate the phone or reset Konftel 800 to its factory settings.

ⓘ You must enter correct administrator password to change the phone's configuration. For that, you must always remember your password.

Setting the password for Konftel 800

Use this procedure to set the password for your Konftel 800 when you first activate the phone or after a reset to the phone factory settings.

Connect the PoE cable to ensure the phone power supply.

⇨ Wait for the following message to appear on the phone screen:

`For full functionality, please set administration password.`

⇨ Tap **Yes** to set the password.

⇨ Optional: Tap **Skip** to avoid setting the password. In this case Konftel 800 will be functioning in the user mode with the restricted number of configuration options.

⇨ Using the keyboard on the phone screen, type your password. It can contain letters, numbers, and special characters.

The password must contain at least 4 characters. When the user enters the password, the phone hints if the password is bad or good.

⇨ Type the password again to confirm it.

⇨ Return to the Home screen by tapping the < icon.

The phone reboots.

Setting up a DHCP server

Konftel 800 supports any DHCP server software as long as the software is correctly configured.

Contact your server software vendor to obtain server software installation and configuration instructions.

⇨ Install the DHCP server software according to the server software vendor's instructions.

⇨ Configure the IP address for the phone.

You must configure the required DHCP options to connect to the network with DHCP. The detailed description of the available DHCP options is provided in Network settings on page 30.

Connecting to a network with DHCP

Use this procedure to connect to a network with DHCP from your phone or through the web interface.

To connect to the network with DHCP from Konftel 800, do the following:

- Tap **Settings** > **Network**.
- Enable **DHCP**.

To connect to the network with DHCP through the web interface, do the following:

- On the web interface, click **Network**.
- Enable **DHCP**.
- Click **Save**.

  The phone reboots.

Viewing the IP address

Use this procedure to view the IP address of your Konftel 800. You can use this address to log into the web interface of the conference phone and manage the settings in the device through the web browser.

⇨ On the phone's screen, tap **Settings**.

⇨ Tap **Status** or the › icon.

The phone displays the following hardware details:

- IP address
- MAC address
- Bluetooth MAC Address
- Hardware revision

- Software version
- Software version of the Smart Mics

⇨ Tap the < icon twice to return to the Home screen.

Setting a static IP address

Use this procedure to connect to the network using a static IP address, and not with DHCP.

Get the IP address, netmask, gateway, DNS 1, and DNS 2.

To set the static IP address from the phone, do the following:

- On the phone screen, tap **Settings** > **Network**.
- Tap **Static IP**, and enter the following:
  - IP address
  - Netmask
  - Gateway
- Return to the home screen to save the changes.

To set the static IP address through the web interface, do the following:

- On the web interface, select **Network**.
- In the **Static IP** section, enter the following:
  - IP address
  - Network mask
  - Gateway
- Click **Save**.

  The phone reboots.

Logging in to Konftel 800

Use this procedure to log into the web server of your Konftel 800 from your web browser.

Note that when you log in to the web server for the first time, you must check that the web browser has the IP address of you phone in `https://111.222.33.44` format. The phone only supports `https://` format and does not work with http://.

⇨ On your web browser, type the IP address of your phone.

⇨ Press **Enter**.

⇨ In the **Password** field, enter your password.

⇨ Click **Login** or press **Enter**.

Logging out from Konftel 800

Use this procedure to log out from the web server of your Konftel 800 from your web browser.

You must be logged in to the web interface of your conference phone.

On your web browser, tap **Logout**.

You are forwarded to the Login page and see the prompt that you are not logged in.

Registering an account on the phone

Use this procedure to register an account on the phone.

Konftel 800 supports three accounts: the primary account, the secondary account and the fallback account. The phone uses the primary account to make and receive calls. You can register the secondary account simultaneously with the primary account but the phone uses it only to receive calls. The secondary account can be used to make call if the phone fails to register to the primary account. You must register the fallback account only if the phone fails to register to both primary and secondary accounts.

You must have access to the account information and all necessary settings that the SIP PBX requires.

⇨ On the phone screen, tap **Settings** > **SIP**.

⇨ Tap **Primary Account**, and enter the following information:

- **Account name**: The name that the phone shows on the screen. You can set it based on your corporate standards.
- **User**: The account name. The phone uses the content of this field to construct the user Universal Resource Identifier (URI). Note that if **User** is not specified, the phone is not able to make a registration request.
- **Registrar Address**: The IP address or the public name of the SIP server where the account is registered. It can be **10.10.1.100** for a local SIP server or **sip.company.net** for a public VoIP service provider.
- **Proxy**: The proxy server used for Internet communication by the company. This field can be left blank.

⇨ Enable **Keep Alive**.

This will ensure a persistent connection for this account.

⇨ Tap **Credentials**, and enter the following:

- Realm

- Authentication name. If **Authentication name** is not specified, the phone uses the content of the **User** field to authenticate.
- Password. The phone uses this password for the Realm authentication.

⇨ Tap < to return to the account registration menu.

⇨ Optional: Enter **Registration Timeout** in seconds.

This is a request to the SIP server that specifies when the registration must expire. Konftel 800 automatically renews the registration within the set period if the phone is still on and connected to the server. By default it is 300 seconds.

⇨ Tap < to return to the SIP menu.

Repeat Steps 2 to 7 for the secondary and fallback accounts.

Registering an account through the web interface

Use this procedure to register an account for Konftel 800 through the web interface.

You must have access to the account information and all necessary settings that the SIP PBX requires.

⇨ On the web interface, click **SIP**.

⇨ Under **Primary account status**, enter the following account information:

- **Account name**
- **User**
- **Registrar**
- **Proxy**: This field can be left blank.
- **Registration timeout**
- **Realm**: A protection domain where the SIP authentication name and password is valid.

  The realm is usually the same as the registrar. If you enter an asterisk (*), the phone responds to any realm. If there is a specific realm, the phone responds only to that realm when asked for credentials.
- **Authentication name**
- **Password**: The password for the Realm authentication.

⇨ Enable **Keep alive**.

⇨ Optional: Repeat Steps 2 to 3 for the secondary and fallback accounts.

SETTINGS CONFIGURATION AND MANAGEMENT

CONFIGURATION OF KONFTEL 800

You can configure almost all settings directly on Konftel 800. For that you need to navigate through the menu and select the options you need. Using the web interface make the settings configuration easier. This guide provides the explanations of both options for you to choose the more convenient one.

The basic settings, such as the phone name, language, and ring level, can be modified by any user. To configure other settings you must login as the Administrator.

CONFIGURATION OF THE BASIC SETTINGS

You can configure the basic settings during the installation of Konftel 800 or any time after it. The basic settings include the following:

- Phone name
- Language
- Ringtone level
- Reboot device
- Webapp debug
- Daisy chain mode
- Factory reset
- Security
- Time and region settings

For more information about the basic settings, see Basic settings on page 25.

Configuring the basic settings on the phone

Use this procedure to configure the basic settings on the phone.

⇨ On the phone screen, tap **Settings** > **Phone**.

⇨ Optional: For time settings, tap **Settings** > **Time**.

⇨ Choose the parameter that you want to configure and proceed to the options available.

You must log in as the administrator to change the password, choose the daisy chain mode or reset the phone to factory settings.

⇨ After the choices are made, return to the home screen.

Depending on what parameters you change, the phone restarts the application or reboots.

Configuring the settings by using the web interface

Use this procedure to configure the settings through the web interface of your Konftel 800. Note that only administrator can configure all the settings.

⇨ Log in to the web interface of Konftel 800.

⇨ Click **Basic**.

⇨ Choose the parameter that you want to configure and proceed to the options available.

⇨ Click the **Save** button.

Basic settings

The following are the basic settings of Konftel 800 available through the web interface in the **Basic** tab or on the phone in **Settings** > **Phone** and **Settings** > **Time**.

Name	Description
Phone	
Phone name	To specify the name of the phone, which is visible on the home screen when the phone is in a stand-by or on hook mode.

Table continued…

Name	Description
Language	To select the appropriate language. The options are: • English • Swedish • Danish • Norwegian • Finnish • Italian • German • French • Spanish • Portuguese • Dutch
Ringtone level	To choose from six volume levels and a silent mode. If you select the silent mode, only the green LEDs on the phone flash when a call is received.
Reboot device	To reboot the phone in case of a need. ⓘ You can find the **Reboot device** button only in the web interface. You can also activate the **Reboot device** function on the phone when you change some of the phone settings in the phone user interface.
Webapp debug	To enable or disable the debugging function for the web application. It activates the web application logging available in the **System logs** tab. ⓘ You can use this function only through the web interface.

Table continued…

Name	Description
Daisy chain mode	To choose a mode, in which your Konftel 800 operates in case of a daisy chain arrangement. The following options are available: • Master • Slave ⓘ You can configure this parameter in case of logging in with the administrator's password.
Security	To change the administrator's password. ⓘ You can configure this parameter in case of logging in with the administrator's password. ⓘ For security reasons, you can change the administrator's password only on the phone.
Factory reset	To reset the phone to its factory settings. By resetting the phone to its factory setting, you remove all the configurations set, exported and installed in course of the phone's use. ⓘ You can do the factory reset only if you log in with the administrator's password and only on the phone.
Time and region	
NTP enable	To enable or disable the Network Time Protocol (NTP). ⓘ You can configure this parameter in case of logging in with the administrator's password.
NTP server	To specify the NTP server when NTP is enabled. By default the phone uses the following NTP server: `0.pool.ntp.org`. ⓘ You can configure this parameter in case of logging in with the administrator's password.

Table continued…

Name	Description
Date	To set the current date. The date is set in the `mm/dd/yyyy` format. You can specify it by doing the following: • Manually enter the date in the field. • Use the up and down arrows to move through a set of fixed values for the date, month, and year. • Select a date from the drop-down calendar. You can also click the ✕ icon to delete the value that is available and enter the date you want.
Time	To set the current time. The time is set in the `hh:mm:ss` format. You can see the time on the Home screen of the phone. ⓘ The interface provides the time using the 12–hour clock approach, that is you see an AM or PM abbreviation to specify the time. You can specify the time by doing the following: • Manually enter the time value in the field. • Use the up and down arrows to move through a set of fixed values for the hours, minutes, and seconds.
Geo timezone (auto DST)	To enable or disable the Daylight saving time (DST) mode based on the selected geographical timezone.
Timezone	To select a timezone from a drop-down list. The available timezone is based on **Geo timezone** being enabled or disabled. With **Geo timezone** disabled, the phone sets the time as a difference with the Coordinated Universal Time (UTC). With **Geo timezone** enabled, the phone specifies the timezone based on the country and the city observing the DST.

After you click **Save** in the web interface, the phone saves the changes and restarts the application or reboots, depending on what parameters you changed. To save changes on the phone, you must return to the Home screen, and the phone restarts the application or reboots to apply them.

CONFIGURATION OF THE NETWORK SETTINGS

The network settings of Konftel 800 include the following:

- DHCP
- Hostname
- Domain
- DNS1
- DNS2
- VLAN
- Static IP
- LLDP
- 802.1x

You can configure the network settings on the phone or through the web interface of Konftel 800.

For more information about the network settings, see Network settings on page 30.

Configuring the network settings on the phone

Use this procedure to configure the network settings of your Konftel 800 on the phone.

Log in as the administrator.

⇨ On the phone screen, tap **Settings** > **Network**.

⇨ Choose the parameter that you want to configure and proceed to the options available.

⇨ Tap < to return to the main screen.

The phone reboots to apply the changes.

Configuring the Network settings through the web interface

Use this procedure to configure the Network settings of your Konftel 800 through the web interface.

⇨ Log in to the web interface.

⇨ Click **Network**.

⇨ Choose the parameter that you want to configure and proceed to the options available.

⇨ Click **Save**.

The phone reboots to apply the changes.

Network settings

The following are the network setting of Konftel 800 available through the web interface in the **Network** tab or on the phone in **Settings** > **Network**.

Name	Description
Network	
DHCP	To enable or disable Dynamic Host Configuration Protocol (DHCP) on your phone. DHCP is used by network devices to obtain the parameters necessary for operation in the IP network. You must enable DHCP if no other specific information is given. ⓘ When DHCP option is enabled, all other information on this page is set automatically.
Hostname	To specify the hostname of your phone in the network. By default, it is set to konftel800. You can change it to another name.
Domain	To specify the domain where the device is located. ⓘ You can leave his field blank.
DNS 1	To specify the address to the primary Domain Name System (DNS) server. ⓘ Leave the field blank for DHCP default settings.
DNS 2	To specify the address to an optional secondary DNS server. ⓘ Leave the field blank for DHCP default settings.

Table continued…

Name	Description
VLAN	To enable or disable the Virtual Local Area Network (VLAN). By enabling this option, all communication to and from Konftel 800 goes through the specified VLAN. ⓘ The phone also uses this VLAN to communicate through the web interface.
VLAN ID	To specify the ID number to be used for all IP telephony communication through VLAN on your phone.
Static IP	
IP address	To specify the IP address of the phone if DHCP is disabled. In this case, the address is provided by the network administrator or the service provider.
Network mask	To specify the network mask for your phone. Usually it is set to `255.255.255.0` to limit network traffic to the subnet.
Gateway	To specify the gateway for your phone. The gateway is the address of the device or server used for Internet communication.
LLDP	
LLDP enable	To enable and disable specification of the phone location settings. Konftel 800 uses Link Layer Discovery Protocol—Media Endpoint Discovery (LLDP-MED) as a data link protocol to send information about itself and receive data about other devices in the same network. You can specify a part of the parameters if some information is unavailable. ⓘ You can configure LLDP settings only through the web interface.
Country subdivision	To specify the part of the country.

Table continued…

Name	Description
Country	To specify the country.
City	To specify the city.
City division	To specify the city district or area.
Block	To specify the block within the city district.
Street	To specify the street.
Direction	To specify the direction of moving along the street.
Number	To specify the house number.
Landmark	To specify the reference point for the location.
Additional	To specify additional reference points.
Name	To specify the name of the company.
ZIP	To specify the ZIP-code of the location.
Building	To specify the name or number of the building.
Unit	To specify the unit within the building.
Floor	To specify the floor of the building.
Room	To specify the room in the building.
802.1x	
Enable 802.1x	To enable or disable **Enable 802.1x**. When enabled, Konftel 800 asks an authentication server for permission when connected to the LAN.
Username	To specify your name in the network.

Table continued…

Name	Description
EAP MD5 enable	To enable or disable Extensible Authentication Protocol (EAP) MD5 method.
Enable EAP TLS	To enable or disable the EAP Transport Layer Security (TLS) method.
EAP MD5	
EAP password	To set EAP password.
EAP TLS	
EAP TLS Certificate	To specify the certificate for the phone to use for authentication in case of TLS applied.
EAP TLS CA Certificate	To specify the public key in the root certificate which the phone uses to verify other certificates in case of TLS applied. Root certificate is also known as the Certificate Authority (CA) certificate.
EAP TLS Private key	To specify the private key which the phone uses to verify other certificates in case of TLS applied.
Private key password	To specify the password for encryption of the private key when using TLS.

LLDP Data Units

When Konftel 800 uses LLDP, it sends the information as LLDP Data Units. Each LLDP Data Unit is a sequence of Time-Length-Value (TLV) strings.

The phone supports LLDP on primary Ethernet interfaces. The following table lists the TLVs typical for Konftel 800:

Category	TLV Name	String length	TLV String Value
BASIC MANDATORY	CHASSIS ID	7	MAC ADDRESS OF THE PHONE

Category	TLV Name	String length	TLV String Value
BASIC MANDATORY	PORT ID	7	IP ADDRESS OF THE PHONE
BASIC MANDATORY	TIME TO LIVE	2	LLDP_TTL
BASIC OPTIONAL	SYSTEM NAME	22	LLDP_SYSTEM_NAME
BASIC OPTIONAL	SYSTEM DESCRIPTION	28	VENDOR INFORMATION AND FIRMWARE VERSION
BASIC OPTIONAL	SYSTEM CAPABILITIES	4	THE PHONE IS WITHIN THE SYSTEM CAPABILITIES OCTET. IF THE PHONE IS REGISTERED, BIT 5 THAT IS EQUAL TO THE PHONE IS WITHIN THE ENABLED CAPABILITIES OCTET.
BASIC OPTIONAL	MANAGEMENT ADDRESS	12	MGMT ADDR STRING LENGTH = 5; MGMT ADDRESS SUBTYPE = 01; (IPV4) MGMT ADDRESS = IPADD; INTERFACE NUMBER SUBTYPE = 2; INTERFACE NUMBER = 3
ORGANIZATIO N SPECIFIC	IEEE - VLAN NAME	11	OUC = 00-80-C2; IEEE 802.1 SUBTYPE = 3; VLAN IDENTIFIER = VLAN ID; VLAN NAME LENGTH = LENGTH OF VLAN NAME; VLAN NAME = NAME OF VLAN
ORGANIZATIO N SPECIFIC	IEEE 802.3 - LINK AGGREGATIO N	9	OUC = 00-12-0F; IEEE 802.3 SUBTYPE = LINK AGGREGATION 3;

Category	TLV Name	String length	TLV String Value
			AGGREGATION STATUS = 1; AGGREGATED PORT ID = 0
ORGANIZATION SPECIFIC IEEE 802.3	MAC/PHY/ CONFIGURATION STATUS	9	802.3 OUC = 00-12-0F (HEX); 802.3 SUBTYPE = 1; AUTONEGOTIATION SUPPORT/ STATUS = VALUE SENT DURING AUTO-NEGOTIATION; OPTIONAL MAU TYPE = LLDP_MAU
TIA LLDP MED	LLDP-MED CAPABILITIES	7	TIA OUC = 00-12-BB (HEX); LLDP CAPABILITIES SUBTYPE = 1; LLDP-MED CAPABILITIES = 00-3F (MED CAPS, NETWORK POLICY, LOCATION ID, EXTENDED POWER, INVENTORY); LLDP-MED DEVICE TYPE = 3 (CLASS III)
ORGANIZATION SPECIFIC	CIVIC LOCATION IDENTIFICATION	63	TIA OUC = 00-12-BB; LOCATION DATA FORMAT = CIVIC ADDRESS LCI
ORGANIZATION SPECIFIC	ELIN LOCATION IDENTIFICATION	5	TIA OUC = 00-12-BB; LOCATION DATA FORMAT = ECS ELIN
TIA LLDP MED	NETWORK POLICY - VOICE	8	TIA OUC = 00-12-BB (HEX); NETWORK POLICY SUBTYPE = 2; APPLICATION TYPE = 1 (VOICE) U = 0 (NETWORK POLICY IS DEFINED) T = TAGGING X = 0 (RESERVED BIT) VLAN ID = VLAN_IN_USE

Category	TLV Name	String length	TLV String Value
TIA LLDP MED	INVENTORY - SOFTWARE REVISION	5–36	TIA OUC = 00-12-BB (HEX); SOFTWARE REVISION SUBTYPE = 7; SOFTWARE REVISION = VALUE
ORGANIZATIO N SPECIFIC	EXTENDED POWER-VIA-MDI	7	OUC = 00-12-BB; AVAILABLE PARAMETERS = POWER TYPE, POWER SOURCE, POWER PRIORITY, POWER VALUE
BASIC MANDATORY	END-OF-LLDPU	0	NA

CONFIGURATION OF THE MEDIA SETTINGS

You can configure the media settings during the installation of Konftel 800 or any time after it. The media settings include the following:

- Security
- Audio codecs

For more information about the basic settings, see Media settings on page 37.

Configuring the media settings on the phone

Use this procedure to configure the media settings of your Konftel 800 on the phone.

Log in as the administrator.

⇨ On the phone screen, tap **Settings** > **Media**.

⇨ Choose the parameter that you want to configure and proceed to the options available.

⇨ Tap < to return to the main screen.

The phone restarts application to apply the changes.

Configuring the media settings through the web interface

Use this procedure to configure the media settings of your Konftel 800 through the web interface.

⇨ Log in to the web interface.

⇨ Click **Media**.

⇨ Choose the parameter that you want to configure and proceed to the options available.

⇨ Click **Save**.

The phone restarts application to apply the changes.

Media settings

The following are the media setting of Konftel 800 available through the web interface in the **Media** tab or on the phone in **Settings** > **Media**.

Name	Description
Security	
SRTP	To select Secure Real-time Transport Protocol (SRTP) parameters to provide encryption, message authentication, and integrity for the audio and video streams. The options are: • Disabled: Konftel 800 does not use SRTP. • Optional: If selected, the phone uses SRTP If other devices support it. • Mandatory: The call is not connected if the other devices do not support SRTP.
SRTCP	To enable or disable the Secure Real Time Control Protocol (SRTCP). Enabled SRTCP means using the encrypted protocol.
Capability Negotiation (RFC5939)	To enable or disable the Session Description Protocol (SDP) capability negotiation. If Capability Negotiation is enabled, the phone can negotiate transport protocols and attributes.

Table continued…

Name	Description
Audio Codecs	To set the priorities to your codec preferences, where `6` is high, `1` is low, and `Disabled` is also possible.
ILBC	This is a high-complexity speech codec suitable for robust voice communication over IP. ILBC is designed for narrow band speech. It uses a block-independent linear-predictive coding algorithm and has support for two basic frame lengths: 20 ms at 15.2 kbit/s and 30 ms at 13.33 kbit/s.
OPUS	This is an audio coding format used in interactive real-time applications on the Internet. It can switch between various codecs depending on the bandwidth available. OPUS adapts to low bit-rate, narrowband speech and to high-quality stereo music.
PCMU	This is an ITU-T standard codec with U-law compression algorithm also known as G711 U-law. It is used in North America and Japan. By default it is set to `4`.
PCMA	This is an ITU-T standard codec with A-law compression algorithm also known as G711 A-law. It is used in Europe and the rest of the world, except North America and Japan. Companding algorithms reduce the dynamic range of an audio signal. In analog systems, this can increase the signal-to-noise ratio achieved during transmission, and in the digital domain, it can reduce the quantization error.
G722	This is an ITU-T standard codec that provides 7 kHz wideband audio at a data rate within 64 kbit/s. It offers an improved speech quality but requires a high quality network connection between the devices.
G729	This is an ITU-T standard codec that operates at 8 kbit/s. It is mostly used in VoIP applications with low bandwidth requirement. By default it is set to `3`.

After you click **Save**, the phone saves the changes and restarts application.

CONFIGURATION OF THE SIP SETTINGS

The SIP settings can be configured during the installation of Konftel 800. The SIP settings include the following:

- Primary account
- Secondary account
- Fallback account
- Source port
- Transport protocol
- Transport Layer Security (TLS)
- Advanced SIP settings
- DTMF
- NAT Traversal

The SIP settings can be configured on the phone or through the web interface of Konftel 800.

Configuring the SIP settings on the phone

Use this procedure to configure the SIP settings of your Konftel 800 on the phone.

Log in as the administrator.

⇨ On the phone screen, tap **Settings** > **SIP**.

⇨ Choose the parameter that you want to configure and proceed to the options available.

⇨ Tap < to return to the main screen.

The phone restarts application to apply the changes.

Configuring the SIP settings through the web interface

Use this procedure to configure the SIP settings of your Konftel 800 through the web interface.

⇨ Log in to the web interface.

⇨ Click **SIP**.

⇨ Choose the parameter that you want to configure and proceed to the options available.

⇨ Click **Save**.

The phone restarts application to apply the changes.

SIP settings

The following are the SIP setting of Konftel 800 available through the web interface in the **SIP** tab or on the phone in **Settings** > **SIP**.

Name	Description
Transport	
Transport protocol	To choose one of the following protocols: • UDP. This is the default setting. • TCP • TLS • SIPS ⓘ Even if you choose TLS, Konftel 800 still accepts incoming UDP or TCP signalling.
Source port	To specify the local User Datagram Protocol (UDP) port to ensure stable bidirectional traffic.
TLS	
ⓘ This section is available in the web interface if you choose TLS or SIPS transport protocol.	
TLS method	To choose the security methods to be applied. The options are: • **TLS v1.** • **TLS v1.1.** • **TLS v1.2.** This is the default setting.
Verify client	To enable or disable **Verify client**. The options are: • Yes: The phone activates peer verification for incoming secure SIP connections. • No: This is the default setting.

Table continued…

Name	Description
Verify server	To enable or disable **Verify server**. The options are: • Yes: When Konftel 800 is acting as a client for outgoing connections with secure SIP, it always receives a certificate from the peer. If you select this, the phone closes the connection in case of a non-valid server certificate. • No: This is the default setting.
Require client certificate	To enable or disable client certificate verification. The options are: • Yes: The phone rejects incoming secure SIP connections if the client does not have a valid certificate. • No: This is the default setting.
TLS negotiation timeout	To specify the timeout for the TLS settings negotiation during a call setup. You must define the time in seconds in this field. If this negotiation is not successful within the specified time, the phone aborts the negotiation. You can disable the timeout by entering `0`. The default setting is `0` seconds.
TLS certificate	To upload a certificate for TLS or SIPS communication. A certificate is a file that combines a public key with information about the owner of the public key, 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 named in that file. You can also be sure that everything you decrypt with that public key is encrypted by the person named in the certificate.
TLS CA certificate	To upload a certificate for TLS or SIPS communication received from a Certificate Authority (CA). You can use it to verify other certificates. You need the CA certificate if you have **Verify server** or **Verify client** enabled.

Table continued…

Name	Description
TLS private key	To upload a private key for TLS or SIPS communication. A private key is one of the keys in a key pair in asymmetric cryptography. Messages encrypted using the public key can only be decrypted using the private key.
Password	To specify the password used for encryption of the private key if it is encrypted.
Primary account	
Account name	To set the name for the primary account displayed on the screen according to the existing corporate standards.
User	To set the account or customer name for the primary account.
Registrar	To specify the IP address or the public name of the SIP server where the primary account is registered. For example, **10.10.1.100** for a local SIP server or **sip.company.net** for a public VoIP service provider.
Proxy	To specify the Universal Resource Identifier (URI) of the proxy server used by the primary account.
Keep alive	To make the phone maintain an active connection to the network. The options are: • Yes: If you select this, the phone renews the connection of the phone's primary account to the network. • No: This is the default setting.
Realm	To specify the protection domain where the SIP authentication of the primary account with the name and password is valid. If the field is left blank, or marked with an asterisk (*), the phone responds to any realm. If specified, the phone only responds to the specific realm when asked for credentials.

Table continued…

Name	Description
Authentication name	To specify the number that is assigned to the user in the primary account.
Password	To define the password for the **Realm** authentication in the primary account. On the phone, the password can be configured in **Settings** > **SIP** > **Primary account** > **Credentials**
Registration timeout	To specify the time when the registration of the primary account expires and the SIP server is sent a corresponding request. Konftel 800 automatically renews the registration within the time interval if the phone is still on and connected to the server. The default value is `300` seconds.
Secondary account	
Account name	To set the name for the secondary account displayed on the screen according to the existing corporate standards.
User	To set the account or customer name for the secondary account.
Registrar	To specify the IP address or the public name of the SIP server where the secondary account is registered.
Proxy	To specify the URI of the proxy server used by the secondary account.
Keep alive	To make the phone maintain an active connection to the network with the secondary account.
Realm	To specify the protection domain where the SIP authentication of the secondary account with the name and password is valid.
Authentication name	To specify the number that is assigned to the user in the secondary account.

Table continued…

Name	Description
Password	To define the password for the **Realm** authentication in the secondary account. On the phone, the password can be configured in **Settings** > **SIP** > **Secondary account** > **Credentials**
Registration timeout	To specify the time when the registration of the secondary account expires and the SIP server is sent a corresponding request. The default value is `300` seconds.
Fallback account	
Account name	To set the name for the fallback account displayed on the screen according to the existing corporate standards.
User	To set the account or customer name for the fallback account.
Registrar	To specify the IP address or the public name of the SIP server where the fallback account is registered.
Proxy	To specify the URI of the proxy server used by the fallback account.
Keep alive	To make the phone maintain an active connection to the network with the fallback account.
Realm	To specify the protection domain where the SIP authentication of the fallback account with the name and password is valid.
Authentication name	To specify the number that is assigned to the user in the fallback account.
Password	To define the password for the **Realm** authentication in the fallback account. On the phone, the password can be configured in **Settings** > **SIP** > **Fallback account** > **Credentials**

Table continued…

Name	Description
Registration timeout	To specify the time when the registration of the fallback account expires and the SIP server is sent a corresponding request. The default value is `300` seconds.
DTMF	
DTMF method	To define the Dual-tone multi-frequency (DTMF) signalling method. The options are: • **RFC 4733**. This is a method of carrying DTMF signals in RTP packets by using a separate RTP payload format. It is set by default. • **SIP Info**. In this case, the DTMF signals are sent as SIP requests. The SIP switch creates the tones if the call is transferred to the PSTN. • **In-band**. The phone itself generates the tones and sends them in the voice frequency band. ⓘ Use **RFC 4733** or **SIP Info** as the preferred methods as they are more consistent with other tones available. Switch to **In-band** only if you encounter problems using DTMF signalling with your PBX/SIP switch.
RFC 4733 payload type	To specify the type of audio traffic. By default it is `101`.
Advanced	
Disable rport	To enable or disable remote port forwarding. The default setting is disabled.
Session timers	To set a time-related mechanism to disconnect the sessions that the phone establishes. The options are: • Disable. This is the default setting. • Optional • Mandatory

Table continued…

Name	Description
Session expiration	To specify the session expiration time in seconds. The default setting is `1800` seconds.
Outbound proxy	To specify the IP address of the outbound proxy, if available.
Enable SIP traces	To enable or disable provision of key information for troubleshooting. The default setting is disabled.
Allow contact rewrite	To enable or disable storing the IP address from the response of the register request. If a change is detected, the phone unregisters the available SIP URI (contact), and updates it with the new address.
Network Address Translation (NAT) Traversal	
ICE	To enable or disable the Interactive Connectivity Establishment (ICE) 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 the endpoints to identify the most optimal path for the media traffic to follow. The default setting is disabled.
STUN	To enable or disable the Simple Traversal of UDP through the NAT (STUN) is a protocol that assists devices behind a NAT firewall or router with their packet routing. STUN is commonly used in real-time voice, video, messaging, and other interactive IP communication applications. The protocol allows applications operating through the NAT to discover the presence and specific type of the NAT and obtain a public IP address (NAT address) and port number that the NAT allocated for the application's User Datagram Protocol (UDP) connections to remote hosts. You must enable STUN if an external SIP server cannot connect to the phone behind a firewall NAT function and the SIP server supports STUN. ⓘ Another definition of STUN is the Session Traversal Utilities for NAT.

Table continued…

Name	Description
STUN server	To enter the IP address or the public name of the STUN server.
TURN	To enable or disable the Traversal Using Relay NAT (TURN). TURN is an extension of the TURN protocol that enables 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 additional delay for the media traffic, you must use TURN as a last resort when endpoints cannot communicate directly. ⓘ To enable TURN, you must enable ICE.
TURN server	To enter the IP address or the public name of the TURN server.
User	To specify the user authentication name on the TURN server.
Password	To enter the user authentication password on the TURN server.

After you click **Save**, the phone saves the changes and restarts application.

CERTIFICATES APPLICATION

You can use certificates to authenticate Konftel 800 using TLS. You can do it when configuring the advance settings of your phone.

The application of a certificate involves the following:

- Download of the root certificate from the Certificate Server
- Creation of the server certificate from the Certificate Server
- Generation of the private key
- Conversion of the certificates and the private key to .PEM format
- Import of the .PEM files to the phone

Downloading the root certificate

Use this procedure to download the root certificate that the phone will apply for authentication by using TLS/SIPS and EAP-TLS.

Connect to Microsoft Server Certification Authority.

⇨ On the **Microsoft Server Certification Authority** page, click **Download a CA certificate, certificate chain, or CRL**.

⇨ Click **Download CA certificate**.

Creating the server certificate

Use this procedure to create the server certificate that the phone will apply for authentication by using TLS/SIPS and EAP-TLS.

Connect to Microsoft Server Certification Authority.

⇨ On the **Microsoft Server Certification Authority** page, click **Request a certificate**.

⇨ Click **Advanced certificate request**.

⇨ Enter the following information:

a) In **Identifying information**, specify the name, email, company name, department, and city, state, and country of your location.
b) In **Type of Certificate Needed**, click **Client Authentication Certificate**.
c) In **Key option**, click **Create new key set**.
d) In **CSP**, select **Microsoft Enhansed Cryptographic Provider v 1.0**.
e) In **Key usage**, select **Both**.
f) In **Key Size**, specify `1024`.
g) Select **Automatic key container name**.
h) Select **Mark keys as exportable**.
i) Select **Enable strong private key protection**.
j) In **Request Format**, select **PKCS10**.
k) In **Hash Algorithm**, select **SHA-1** from the list.
l) Enter the short name of the phone.

⇨ Click **Submit**.

The system saves the certificate to the location specified while creating the CA.

Installing the certificate

Use this procedure to install the certificate that the phone will apply for authentication using TLS/SIPS and EAP-TLS. You can do it from your regular web

browser. Here you can find the procedure for Mozilla Firefox. For information about other web browser application, see the instructions provided by the software manufacturers.

Open your web browser.

- To install the certificate from Mozilla Firefox, do the following:
  a) In Mozilla Firefox, click the **Options** menu and click **Privacy&Security**.
  b) Click **Certificate** and then click the **View certificates** button.
  c) In the **Certificate Manager** window, click the **Authorities** tab.
  d) Click **Import**.
  e) Find the saved certificate file and click **Open**.
  f) In the **Downloading Certificate** window, select all the check boxes, and click **OK**.

Exporting the private key

Use this procedure to export the private key that the phone will apply for authentication using TLS/SIPS and EAP-TLS. You can do it from your regular web browser. Here you can find the procedure for Internet Explorer and Mozilla Firefox. For information about other web browser application, see the instructions provided by the software manufacturers.

Open your web browser.

To export the private key from Internet Explorer, do the following:

- Click **Tools** > **Internet Options** > **Content**.
- Click **Certificates** to show the list of the certificates installed.
- Click **Export**.
- Click **Yes** to export the private key.
- Click **Next**.
- Select the format in which you want to export the private key file and click **Next**.
- Specify the file name and choose the location to export the certificate.
- Click **Finish**.

To export the private key from Mozilla Firefox, do the following:

- In Mozilla Firefox, click the **Options** menu and select **Privacy&Security**.
- Select **Certificate** and click the **View certificates** button.
- In the **Certificate Manager** window, click the **Authorities** tab.
- Click **Export**.
- Specify the file name and choose the location to export the certificate.
- Click **OK**.

Converting the certificates to .PEM format

Use this procedure to convert the certificates for the phone to .PEM format. Konftel 800 supports certificates in the .PEM format only.

⇨ Use the following Openssl commands to convert the files:

a) From .DER to .PEM:

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

b) From .PFX to .PEM:

```
openssl pkcs12 -in certificate.pfx -out certificate.cer -nodes
```

⇨ On the web interface, browse to the .PEM files to use TLS mode of authentication.

FEATURES AND ACCESSORIES

KONFTEL UNITE

You can manage your Konftel 800 from a mobile phone or a tablet if you have Konftel Unite installed on the device. You can download and install Konftel Unite free from App Store and Google Play like any other application. You can use the NFC tag to easily start downloading the application. For that, you must bring the mobile device with the NFC enabled to the NFC tag on the conference phone, and the web browser on the mobile device opens the web page with the application in App Store or Google Play.

With Konftel Unite, you can call contacts from your local address book, create conference groups, and control a call (you can answer and hang up the call, mute the microphone, dial a number, adjust the volume level, and etc.).

The mobile device with Konftel Unite is connected to the phone over the built-in Bluetooth LE. Konftel 800 is always discoverable for this connection.

You can configure Konftel Unite parameters on the phone and from the mobile device with the application installed.

Pairing and connecting devices

Use this procedure to pair your Konftel 800 with Konftel Unite on your mobile device the first time when you use them together. After that, they connect with one touch when you run the application near the conference phone.

The connection range is up to 20 meters. The connection breaks if this range is exceeded. You see a request to reconnect when Konftel Unite is within the range of Konftel 800. Reconnection requires only one touch.

ⓘ You can pair up to 100 mobile phones or tablets with your Konftel 800. But only one user connection is active at a time.

Install Konftel Unite on your mobile device.

⇨ On your mobile device, open Konftel Unite.

The mobile phone displays the closest Konftel 800.

⇨ To select the phone you want to connect, perform one of the following actions:

- If your mobile device displays Konftel 800 you want to connect, tap **Connect** on the mobile device screen.

- If your mobile device does not display Konftel 800 you want to connect, tap **Skip** and then tap the connection symbol in the upper left corner of your mobile device screen.

  The mobile device displays the list of available conference phones.

The mobile phone displays a pairing code on the screen.

⇨ Enter the code with the keypad on the conference phone.

⇨ Press **OK** on the conference phone to start pairing.

When the devices are paired, both Konftel Unite and Konftel 800 display a connection symbol.

The conference phone and Konftel Unite remain paired while they are close to one another.

Disconnecting devices

Use this procedure to disconnect your Konftel 800 from the mobile device with Konftel Unite installed.

Ensure that Konftel 800 is connected to a mobile device with Konftel Unite installed.

- To disconnect from the mobile device, do the following:
  a) In Konftel Unite, tap the connection symbol in the upper left corner of the screen.
  b) Optional: Under **Change device**, select another conference phone to connect to. Note that you can do it if there are other conference phones available nearby.

     The application starts connecting to the selected conference phone.
  c) Tap the **Disconnect** button near the highlighted connected device name.

     The connection symbol in the upper left corner of the screen becomes inactive.
- To disconnect from the conference phone, do the following:
  a) On Konftel 800, tap **Settings** > **Unite**.
  b) Tap **Disconnect device**.

     The phone shows the Konftel Unite icon and informs that the application is disconnected.

Deleting pairing

Use this procedure to delete the pairing between the conference phone and the mobile device. You can delete the paring only from the conference phone.

Pair Konftel 800 with a mobile device with Konftel Unite.

⇨ To delete the pairing from the conference phone, on the Home screen, do one of the following:

- Tap **Unite**.
- Tap **Settings** > **Unite**.

⇨ Tap **Remove bonding information**.

This function both disconnects the current connection and deletes the pairing. You must start a new pairing process the next time you want to connect to the phone.

Configuring the Konftel Unite settings

Use this procedure to configure the Konftel Unite settings from the application installed on a mobile device.

⇨ Run Konftel Unite on your mobile device.

⇨ Optional: Connect to Konftel 800.

The phone displays a connection symbol on the screen.

⇨ Tap **Settings** and proceed with configuration.

Konftel Unite settings

You can set the following parameters for Konftel 800 from the Konftel Unite interface:

Name	Description
Connection	To enable or disable the connection to Konftel 800. The options are: • **On**: The default option. • **Off**: To use Konftel Unite without connection to any Konftel 800. You can use the conferencing application from your mobile device within your mobile phone subscription.

Table continued…

Name	Description
Moderator code	To join the scheduled conference calls as a moderator. You must enter respective codes in the following fields: • **Use moderator code**: To host conference calls over a bridge service. For every call you join, Konftel Unite uses your moderator code instead of your guest code. • **Instead of guest code**: To specify the guest code instead of which Konftel Unite uses your moderator code.
Dial prefix	To enter the prefix digits in the **Use prefix** field.
My bridge	To enter the phone number and optional PIN code of the most frequently used conference service. You can use the **My Bridge** button to join the conference call. The **My bridge** button appears in the calendar view.
Meeting notification	To set a reminder about a call. The options are: • 5 minutes before • 10 minutes before • 15 minutes before • Never
Calendars to show	To select the calendars in the mobile phone from which you want Konftel Unite to take the information.
Tell a colleague	To share information about Konftel Unite with a person that you want. You can do it by using an email application. After you confirm that Konftel Unite can get access to your email application, you see a message created. Along with the description of the application, it contains links to Konftel Unite in App Store and Google play so that the person can easily start the download.
Read more about Unite	To get additional information about Konftel Unite. The application forwards you to the web site with the corresponding information.

Table continued…

Name	Description
Feedback and support	To share your experience of using the application and request for support. The options are: • A messenger, for example, Viber, WhatsApp, Telegram, and etc. • An email application • Connection by Bluetooth
Diagnostics	To select a log of the events for Konftel Unite. You can send the created log by tapping **Send** through an email application. The log can be used in troubleshooting. You can also delete the logs from the application by tapping **Clear**.
Show tutorial	To read information about Konftel Unite features.
About Konftel Unite	To check the version of the application installed on your mobile device

EXPANSION OF THE PHONE COVERAGE

You can use your Konftel 800 on larger conference tables or when the number of a meeting participants is greater than 10. In this case you can ensure high-level quality of audio signal by expanding the phone coverage in the room without a PA system. You can do it by connecting Smart Mic expansion microphones to the phone or by cascading several Konftel 800 devices in a daisy chain.

Expansion of the phone coverage helps to improve the audio quality in large rooms. The conference phone and two Smart Mics increase the capture range from 30 square meters to up to 70 square meters. Three phones in a daisy chain increase the range from 30 square meters to up to 90 square meters.

Expansion coverage arrangement

You can organize a daisy chain with your conference phone and another Konftel 800 or connect Smart Mic expansion microphones. The maximum number of devices connected in a daisy chain is 3. One Konftel 800 phone acts as a central device (a “master”) and one or two other units act as expansion devices (“slaves”).

The typical arrangements when the phone's coverage is expanded are the following:

- Master phone — Slave phone
- Slave phone — Master phone — Slave phone
- Master phone — Expansion microphone
- Expansion microphone — Master phone — Expansion microphone

When Konftel 800 acts as a master, it performs all its configured functions.

When Konftel 800 is in a subordinate position (a "slave"), it performs the following functions:

- Play audio received from the master device. The master phone defines the audio characteristics.
- Send its microphone audio to the master device.
- Receive and indicate mute state changes made on the master device.
- Send information to the master device, when you tap **Mute**.
- Send information to the master device when you adjust the volume on it.

ⓘ It is not possible to make calls between the master and the slave devices.

In a daisy chain each phone is powered by its own PoE injector. The phone powers the Smart Mics when these are connected. The power available from each port is around 5W.

Arranging a daisy chain

Use this procedure to arrange a daisy chain of one master Konftel 800 phone and one or two slave conference phones or expansion microphones.

If you arrange the daisy chain made of several conference phones, prepare the connection cables. The cables in the Daisy Chain kit are 5 and 10 meters. You can purchase the Daisy Chain kit as an accessory.

The cable of the Smart Mic is 3 m long.

⇨ Connect the cable to the audio expansion port on the phone.

There are 2 audio expansion ports on Konftel 800.

⇨ Connect the other end of the cable to the audio expansion port of the other phone.

In case of expansion microphones, the other end of the cable is fixed in the device.

Defining the mode of the phone

Use this procedure to define the mode of your Konftel 800 in a daisy chain.

Log in as the administrator.

- To define the mode of your conference phone on the phone, do the following:
  a) On the phone screen, tap **Settings** > **Phone** > **Daisy chain**.
  b) Select the required mode.

     The following options are available:

     - Master
     - Slave

  The phone restarts the application.
- To define the mode of your Konftel 800 through the web interface, do the following:
  a) On the web interface, click **Basic**.
  b) In **Daisy chain mode**, select the required mode from the drop-down list.

     The following options are available:

     - Master. This is the default mode.
     - Slave

  c) Click **Save**.

  After the return to the Home screen, the phone restarts the application.

  The slave unit shows the following message on the screen: “Daisy chain slave”. This message remains for the period when the phone is in the slave mode within the daisy chain arrangement.

Disabling the daisy chain mode

You can disable the daisy chain mode through the web interface or from the phone.

Ensure that the phone displays the Daisy chain icon.

- To disable the daisy chain mode from the web interface, do the following:
  a) On the web interface, click **Basic**.
  b) In **Daisy chain mode**, select **Master**.
  c) Click **Save**.
- To disable the daisy chain mode from the phone, do the following:
  a) Touch the phone screen and enter the administrator password.

b) Click **Phone** > **Daisy chain**.
c) Select the **Master** mode.
d) Return to the Home screen by tapping the < icon.

Application restarts and restores the Master status.

MAINTENANCE

PROVISIONING ON KONFTEL 800

To ensure effective operation of your Konftel 800, you can check and download the latest version with the software update packages to the phone. The easiest way to upgrade Konftel 800 is through a PC connected to the same network.

You can export and import a configuration file, check the new firmware and upload a firmware version only through the web interface. The device management settings are available both on the phone and through the web interface.

Upgrading firmware by using the downloaded file

Use this procedure to upgrade your Konftel 800 from the local hard disk.

Save the appropriate firmware file in a specified location on your PC.

⇨ On the web interface, select **Provisioning**.

⇨ Go to the **Firmware** section.

⇨ Under **Firmware upload** and click the **Choose file** button.

⇨ Locate and select the downloaded file.

You can see the name of the chosen file near the **Choose file** button.

⇨ Click **Save**.

The system displays the upgrade in your browser window and on the screen of Konftel 800.

Note that the phone must be in the idle state, otherwise you see the following message: `Phone busy, retry later`.

If DHCP is used in the network, the IP address may change. If the web browser loses contact with Konftel 800, check the IP address on the phone. For further information, see Viewing the IP address on page 20.

Use of a configuration file

You can create a configuration .xml file on Konftel 800. This file contains information about all the settings that were configured on the phone as of the moment of the file creation.

The configuration file can be used as a:

- Backup. This is applicable if the system has been reset to factory default.

- Configuration interface. Some settings are not configured through the web interface.
- Management tool. You can export, edit, and import settings to several phones instead of configuring the settings on each phone.
- Configuration file for **Device management**. For more information, see Device management on page 72.

The structure of the .xml file is as follows:

String	Description
<?xml_version>	To specify the number of the phone configuration version.
<Konftel800>	To specify the model of the conference phone.
<time>	To specify the time and region parameters.
<timezone type>	To specify the type of the timezone specified for the phone.
<ntp>	To specify whether NTP is applied.
<server type>	To specify the server which the phone uses to set the time.
<enable type>	To specify if NTP is enabled. The default setting is true.
<sip>	To specify SIP settings.
<transport_protocol type>	To specify the transport protocol which the phone must use.
<udp>	To specify that UDP is selected as the transport protocol. This is followed by the corresponding transport protocol settings.

Table continued…

<tcp>	To specify that TCP is selected as the transport protocol. This is followed by the corresponding transport protocol settings.
<sips>	To specify that SIPs is selected as the transport protocol. This is followed by the corresponding transport protocol settings.
<tls>	To specify that TLS is selected as the transport protocol. This is followed by the corresponding transport protocol settings.
<verify_server type>	To specify whether the phone must verify the server.
<verify_client type>	To specify whether the phone must verify the client.
<tls_password type>	To specify the password for the private key.
<tls_neg_timeout type>	To specify the TLS negotiation timeout in seconds for both outgoing and incoming connections. If zero, the phone uses no timeout.
<tls_method type>	To specify the TLS protocol method.
<require_client_cert type>	To specify whether the phone requires the client certificate.
<source_port type>	To specify the source port to listen to.
<primary_account>	To specify the primary account settings.
<user type>	To specify the user-defined name of the account.

Table continued…

<registrar type>	To specify the request URI for registration.
<reg_timeout type>	To specify the optional interval for registration in seconds. If zero, the phone uses the default interval. The default setting is 300.
<proxy type>	To specify the optional URI of the proxy to visit for all outgoing requests from the account.
<name type>	To specify the name of the account.
<keep_alive type>	To specify is the keep-alive transmission for the account is enabled.
<cred>	To specify the array of credentials. In case of registration, at least one credential must be available to successfully authenticate the service provider. If you want proxies to challenge the requests in the route set, you must specify more credentials.
<username type>	To specify an authentication name.
<realm type>	To specify the realm.
<password type>	To specify the password used for the account.
<secondary_account>	To specify the secondary account settings.
<user type>	To specify the user-defined name of the account.
<registrar type>	To specify the request URI for registration.

Table continued…

<reg_timeout type>	To specify the optional interval for registration in seconds. If zero, the phone uses the default interval. The default setting is `300`.
<proxy type>	To specify the optional URI of the proxy to visit for all outgoing requests from the account.
<name type>	To specify the name of the account.
<keep_alive type>	To specify is the keep-alive transmission for the account is enabled.
<cred>	To specify the array of credentials. In case of registration, at least one credential must be available to successfully authenticate the service provider. If you want proxies to challenge the requests in the route set, you must specify more credentials.
<username type>	To specify an authentication name.
<realm type>	To specify the realm.
<password type>	To specify the password used for the account.
<fallback_account>	To specify the fallback account settings.
<user type>	To specify the user-defined name of the account.
<registrar type>	To specify the request URI for registration.
<reg_timeout type>	To specify the optional interval for registration in seconds. If zero, the phone uses the default interval. The default setting is `300`.

Table continued…

<proxy type>	To specify the optional URI of the proxy to visit for all outgoing requests from the account.
<name type>	To specify the name of the account.
<keep_alive type>	To specify is the keep-alive transmission for the account is enabled.
<cred>	To specify the array of credentials. In case of registration, at least one credential must be available to successfully authenticate the service provider. If you want proxies to challenge the requests in the route set, you must specify more credentials.
<username type>	To specify an authentication name.
<realm type>	To specify the realm.
<password type>	To specify the password used for the account.
<dtmf>	To specify DTMF signalling settings.
<rfc4733_payload_type>	To specify the type of audio traffic.
<method type>	To specify the DTMF signalling method.
<codec>	To specify the codec settings.
<iLBC>	To specify the iLBC codec settings.

Table continued…

<prio type>	To specify the codec priority (0–6).
<PCMU>	To specify the PCMU codec settings.
<prio type>	To specify the codec priority (0–6).
<PCMA>	To specify the PCMA codec settings.
<prio type>	To specify the codec priority (0–6).
<OPUS>	To specify the OPUS codec settings.
<prio type>	To specify the codec priority (0–6).
<G729>	To specify the G729 codec settings.
<prio type>	To specify the codec priority (0–6).
<G722>	To specify the G722 codec settings.
<prio type>	To specify the codec priority (0–6).
<advanced>	To specify the configured advanced SIP settings.
<session_timers type>	To specify the chosen time-related mechanism to disconnect the sessions.
<session_expiration type>	To specify the session expiration time in seconds. The default setting is `1800` seconds.

Table continued…

<outbound_proxy type>	To specify the IP address of the outbound proxy.
<enable_sip_traces type>	To specify if the provision of key information for troubleshooting is enabled. The default setting is disabled.
<disable_rport type>	To specify if the remote port forwarding is enabled. The default setting is disabled.
<allow_contact_rewrite type>	To specify if storing the IP address from the response of the register request is enabled.
<nat_traversal>	To specify the configured NAT traversal settings.
<turn>	To specify if TURN is configured for the phone.
<user type>	To specify the user authentication name on the TURN server.
<server type>	To specify the IP address or the public name of the TURN server.
<password type>	To specify if the user authentication password on the TURN server is set.
<enable type>	To specify if TURN is enabled.
<stun>	To specify if STUN is configured for the phone.
<server type>	To specify the IP address or the public name of the STUN server.
<enable type>	To specify if STUN is enabled.

Table continued…

<ice>	To specify if ICE is configured for the phone.
<enable type>	To specify if ICE is enabled.
<phone>	To specify the configured basic settings of the phone.
<ringlevel type>	To specify the volume level configured.
<password type>	To specify the password used.
<name type>	To specify the name of the phone.
<language type>	To specify the language selected.
<is_daisy_chain_slave type>	To specify the mode of the phone in case of a daisy chain arrangement.
<network>	To specify the network parameters.
<vlanid type>	To specify the ID number that the phone uses for all IP telephony communication through VLAN.
<vlan type>	To specify if VLAN is enabled. The default setting is disabled.
<static_ip>	To specify the static IP settings.
<netmask type>	To specify the network mask for your phone.

Table continued…

<ip type>	To specify the IP address of the phone if DHCP is disabled.
<gateway type>	To specify the gateway for the phone.
<lldp>	To specify the LLDP settings.
<zip type>	To specify the ZIP-code of the phone location.
<unit type>	To specify the unit within the building where the phone is located.
<street type>	To specify the street of the building where the phone is located.
<room type>	To specify the room in the building where the phone is located.
<number type>	To specify the number of the building where the phone is located.
<name type>	To specify the name of the company that owns the phone.
<longitude type>	To specify the longitude of the location.
<latitude type>	To specify the latitude of the location.
<landmark type>	To specify the reference point for the location of the phone.
<floor type>	To specify the floor of the building for the location of the phone.
<enable type>	To specify if the LLDP settings are enabled. These settings are disabled by default.

Table continued…

<direction type>	To specify the direction of moving towards the location of the phone.
<county type>	To specify the country of the phone location.
<country_subdivision type>	To specify the region of the country of the phone location.
<city_division type>	To specify the city district or area of the phone location.
<city type>	To specify the city of the phone location.
<building type>	To specify the name or number of the building of the phone location.
<block type>	To specify the block within the city district.
<altitude type>	To specify the altitude of the location.
<additional type>	To specify any additional information related to the phone location.
<ieee_8021x>	To specify IEEE 802.1x parameters.
<username type>	To specify the phone username if IEEE 802.1x is enabled.
<enable type>	To specify whether IEEE 802.1x is enabled. It is disabled by default.
<eap_tls>	To specify whether the phone uses TLS EAP method.

Table continued…

<password type>	To specify the password for the TLS EAP method.
<enable type>	To specify whether TLS EAP method is enabled.
<eap_md5>	To specify whether the phone uses MD5 EAP method.
<password type>	To specify the password for MD5 EAP method.
<enable type>	To specify whether MD5 EAP method is enabled.
<hostname type>	To specify the hostname of the phone.
<domain type>	To specify the domain name of the phone.
<dns2 type>	To specify Domain Name Server (DNS) 2 of the phone. You can use maximum two DNS.
<dns1 type>	To specify DNS 1 of the phone.
<dhcp type>	To specify whether the phone uses DHCP to obtain network settings.
<media>	To specify the media settings.
<security>	To specify the means of encryption configured for the phone.
<srtp type>	To specify the SRTP parameters that the phone uses.
<srtcp type>	To specify whether SRTCP is enabled.

Table continued…

<capneg type>	To specify whether Capability Negotiation is enabled.
<device_management>	To specify the device management settings.
<update_max_wait type>	To specify the maximum time in seconds the phone waits for the update.
<server type>	To specify the device management server address if it is not provided by the DHCP option.
<lowest_tls_version type>	To specify the lowest TLS version for the phone.
<enable type>	To specify whether the Device Management is enabled.
<dhcp_option type>	To select the DHCP option used for the Device management server address.
<check_server_certificate type>	To specify whether the Check certificate is enabled.

ⓘ You can export and import a configuration file only through the web interface.

Exporting the configuration file

Use this procedure to export the configuration file from your Konftel 800.

Decide where the exported configuration file will be saved. By default, it is saved in the folder for downloaded files on your PC.

⇨ On the web interface, click **Provisioning**.

⇨ Go to the **Configuration** section.

⇨ Click the **Export configuration** button.

The web browser shows the configuration file.

⇨ Save the page in an .xml format in the dedicated folder.

⇨ Optional: Edit the .xml file in a suitable application.

Importing the configuration file

Use this procedure to import the previously saved configuration file to your Konftel 800.

⇨ On the web interface, click **Provisioning**.

⇨ Go to the **Configuration** section.

⇨ In the Import configuration, click the **Choose file** button.

⇨ Locate the configuration file in the folder where it is stored.

⇨ Select the file in an .xml format and open it.

You can see the name of the chosen file near the **Choose file** button.

⇨ Click the **Save** button.

The phone reboots or restarts to import the configuration if the configuration file application requires this reboot or restart.

Device management

Device management facilitates upgrading and configuration of multiple conference phones. For that, you must configure it. By default the device management is enabled.

The phone upgrades and sets configuration with the use of device management files. The appropriate files must be located on a server reachable from all the phones. This server is called a Device management server.

The configuration and firmware download are controlled with a configurable frequency. By default, it is set to every 30 minutes. You can edit this interval directly in the saved configuration file.

Configuration priorities

As the same configuration parameters can be entered in multiple locations, you must define the priorities. The local configuration file has the highest priority, and then the global configuration file. Configurations made directly on Konftel 800 or through the web interface are overridden the next time the configuration files are downloaded.

ⓘ There is only one exception to this rule: the phone language entered on the unit takes precedence.

Konftel Zero Touch Installation

Zero Touch Installation (ZTI) is an add-in for auto-provisioning that Konftel 800 supports. It provides for the remote configuration of the phone by using a data file

with settings. The phone downloads the file from a device management server. The user can apply ZTI when centrally upgrading the phone software.

Registration with the ZTI device management service

Use this procedure to register the phone with the device management service and receive the provisioning settings.

Connect the phone to the data network and start it.

⇨ In the web browser, enter https://www.konftel.com/zti-access.

⇨ Register the phone with Konftel ZTI by entering its MAC address and serial number.

The device management service provides the phone with the address of the provisioning server where the user can download the configuration file in .xml format.

⇨ Confirm your choice.

The phone restarts and goes to the appropriate server to download the configuration file.

Configuring device management settings on the phone

Use this procedure to configure the device management settings on the phone.

⇨ On the phone screen, tap **Settings** > **Device Management**.

⇨ Choose the parameter that you want to configure and proceed to the options available.

⇨ After the choices are made, return to the home screen. The phone reboots to apply the changes.

Configuring device management settings through the web interface

Use this procedure to configure the device management settings through the web interface.

⇨ On the web interface, click **Provisioning**.

⇨ Make the appropriate configurations.

⇨ Click **Save**.

The phone reboots to apply the changes.

Device management settings

The following are the device management settings of Konftel 800 available through the web interface in the **Provisioning** tab in the **Device management** section or on the phone in **Settings** > **Device Management**.

Name	Description
Enable	To enable or disable Device management. The options are: • **On**: Device Management is enabled. This is the default setting. • **Off**: Device management is disabled.
Maximum time to wait to update	To specify the maximum time in seconds the phone waits for the update. By default it is `1` second. ⓘ You can configure this parameter only through the web interface.
DHCP option	To select the DHCP option used for the Device management server address. The options are: • 43: Vendor specific. • 56: DHCP message. • 60: Class ID. • 61: Client ID. • 66: Server name. • 67: Bootfile name. • 242: the brand-specific option. • Off • Auto. This is the default setting.
File server	To specify the device management server address if it is not provided by the DHCP option.
TLS version	To specify the lowest TLS version for the phone. The options are: • TLS v1 • TLS v1.1 • TLS v1.2

Table continued…

Name	Description
DM check certificate	To enable or disable the verification of the authentication with a certificate. The options are: • **On**: Server certificates are checked. • **Off**: Server certificates are not checked. This is the default setting.
DM Certificate	To upload a certificate to the phone. This certificate is used for authentication in Device management.
DM root	To upload a root certificate. It contains a public key, which is used to verify other certificates when using Device management.
DM private key	To upload a private key. It is used for authentication when using Device management.

Files on the device management server
Global configuration file

The global configuration file contains the basic configuration, that is, all settings that are common for all conference phones in your location. The easiest way to create this file is to configure Konftel 800 and export the configuration file, or use the built-in configuration file creator.

The default name for this file is `kt800.xml`.

You can also create a name by using the **pagename** element in the configuration file. Instead of the .xml file, you can use cgi, php, asp, js, or jsp file formats, but this must be declared using the **type** element in the configuration file.

Konftel 800 searches for configuration files in the following order:

	Parameter value	Result
1	<nothing>	<pagename>.xml
2	cgi	<pagename>.cgi?phone_model=kt800>

Table continued…

3	%”%	<pagename>.php?phone_model=kt800>
4	asp	<pagename>.asp?phone_model=kt800>
5	E	<pagename>.js?phone_model=kt800>
6	E%	<pagename>.jsp?phone_model=kt800>
:	<any name>	<pagename>.<any name>?phone_model=kt800>
=	auto	The phone searches 1, 2, 3, 4, 5 and 6 in this order.

Creating the global configuration file

Use this procedure to create the global configuration file. This file contains the general information about the phone settings and must be created after you finalize all the basic configurations of Konftel 800.

Enable the **Device management** option and ensure that all the required server information is filled in.

⇨ On the web interface, select **Provisioning**.

⇨ In the **Configuration** subsection, click **Export configuration**.

The configuration file is created.

⇨ Optional: Edit the .xml file in a suitable editor.

⇨ Save the file as `kt800.xml` or with your custom name in the dedicated folder. The folder is located at the address specified in the **File server address** field.

Delete the local information from the global configuration file to avoid confusion in the future. Local information is information specific to the device, for example, account information.

Local configuration file

The local configuration file contains configuration parameters that are unique for every phone. The settings in this file have priority over the settings in the global configuration file.

The default name for this file is `kt800-<MAC>.xml`, where `<MAC>` is the MAC address of the specific phone.

ⓘ Write the MAC address without colons.

You can also create a name by using the **pagename** element in the configuration file. Instead of the .xml file, you can use cgi, php, asp, js, or jsp file formats, but this must be declared using the **type** element in the configuration file.

Konftel 800 searches for configuration files in the following order:

	Parameter value	Result
1	<nothing>	<pagename>-<MAC>.xml
2	cgi	<pagename>.cgi?phone_model=kt800&eth=<MAC>
3	%"%	<pagename>.php?phone_model=kt800&eth=<MAC>
4	asp	<pagename>.asp?phone_model=kt800&eth=<MAC>
5	E	<pagename>.js?phone_model=kt800&eth=<MAC>
6	E%	<pagename>.jsp?phone_model=kt800&eth=<MAC>
:	<any name>	<pagename>.<any name>? phone_model=kt800&eth=<MAC>
=	auto	The phone searches 1, 2, 3, 4, 5 and 6 in this order.

Creating the local configuration file

Use this procedure to create the local configuration files. They contain information about the unique settings of each Konftel 800.

Ensure you know the MAC addresses of all your Konftel 800 phones.

⇨ On the web interface, click **Provisioning**.

⇨ In the **Configuration** subsection, click **Export**.

The phone creates a configuration file.

⇨ Edit the .xml file in a suitable editor.

The file must contain only the elements that are unique for a specific phone.

⇨ Save the file as `kt800-<MAC>.xml` or with your custom name in the dedicated folder located at the address specified in the **File server address** field.

Firmware binary

This file contains the firmware binary that is downloaded and installed by Konftel 800 if the metadata file shows that it is newer than the currently installed version.

Firmware metadata file

This is a metadata file in .xml format with information of the firmware version in the binary file. The file is used to check whether the binary file must be downloaded to the phone.

The name of this file is set as `KT800_fw_version.xml`. The file contains the following elements in xml format: firmware version, filename, and checksum of the firmware binary. The following is the example of the firmware binary file:

```
<firmware_version>
   <version>2.3.9</version>
   <filename>KT800_v2.3.9.kt</filename>
   <checksum>XXXX</checksum>
</firmware_version>
```

Creating firmware binary and metadata files

Use this procedure to create the firmware binary and metadata files manually. Apply them to check whether there is a newer firmware version for your Konftel 800.

Collect the information about the version, file name, and checksum of the firmware binary for the phone.

⇨ Place the firmware binary file on the Device management server.

⇨ Create a firmware metadata file containing the version, file name, and checksum of the firmware binary.

⇨ Save the file as `<file name>.kt` in the dedicated folder located at the address specified in the **File server address** field.

⇨ Optional: Add the file type **.kt** to the MIME settings on the server after the files creation.

Upgrade in IP office

Konftel 800 supports the IP Office check-sync message with file ID 4 for firmware upgrades. You can find additional information about it in the IP Office documentation.

Fall back server support

Konftel 800 registers concurrently with the primary and secondary proxy servers. The phone also supports provisioning of a third-party fall back server when a connection with the primary or secondary server cannot be established. You can configure the third-party server details by using the web interface and the configuration file.

Factory reset

If for any reason, you must restore the factory settings on your Konftel 800, you can do it by means of the factory reset. In this case the phone removes all user-specific settings and returns to the factory settings. After the procedure is completed, you can repeatedly configure the settings.

Resetting to factory settings

Use this procedure to reset your Konftel 800 to factory settings. You can do the factory reset only on the phone.

⇨ Log in to the phone as the administrator.
⇨ On the phone screen, tap **Settings** > **Phone**.
⇨ Tap **Factory reset**.

The phone shows the following message: `Reset configuration to factory default. Press OK to confirm.`

⇨ Tap **Ok** to confirm the reset.
⇨ Optional: Tap **Cancel** to return to the **Phone** settings.

Web interface settings

The web server in Konftel 800supports secure connections using HTTPS. You can configure this parameter only through the web interface.

ⓘ The phone supports connection to the web interface only through `https`.

The following web interface settings can be configured for Konftel 800 in the **Provisioning** tab:

Name	Description
Secure HTTP	
Webapp HTTPs certificate	To upload a .PEM certificate to Konftel 800 to use HTTPS. ⓘ Konftel 800 supports certificates in the .PEM format only. You must convert the certificates and private keys to .PEM before using in the phone. For more information, see Converting the certificates to .PEM format on page 50

You can use the following command to generate a HTTPS web interface certificate:

```
openssl req –new –x509 –keyout https _ web _ certificate.pem –out
https _ web _ certificate.pem –day <number of days>-nodes
```

DEVICE STATUS VIEW

You can view the configured settings of your Konftel 800 through the web interface and get information about the device, logs, and licenses.

You can use this information for troubleshooting.

Device status

You can find the information about Konftel 800 status, including its current settings, through the web interface. This information can be useful for troubleshooting.

The following table describes the type of the information available in each of the status tab sections.

Section name	Description
General	To show the status information of Konftel 800, including the following: • Phone name • Product name • Build version • Hardware (HW) revision • Serial number • Smart Mic 1 firmware version • Smart Mic 2 firmware version
Network	To show the information about the network settings of the phone. You can see the following information: • IP address • MAC address • Bluetooth MAC address

Section name	Description
	• Hostname • Network mask • Domain • Gateway • Primary DNS • Secondary DNS
SIP	To show the information about the SIP settings of the phone. You can see the following information: • Primary account status • Secondary account status • Fallback account status
Time and region	To show the information about the time and region settings of the phone. You can see the following information: • Time • Date • Timezone

ⓘ You can not change settings in the **Status** tab.

Viewing the phone status

Use this procedure to view the status and settings of Konftel 800 through the web interface.

⇨ Log in to the web interface with the administrator's password.

⇨ Select the **Status** tab.

System logs

Information about log messages is available through the web interface in the **System logs** tab. These log types can be useful for troubleshooting.

You can select the following log types:

- All logs. This is the default setting.
- System logs

- PhoneApp logs
- Linux kernel logs
- Bluetooth stack logs
- PJSIP logs
- Device management
- SIP traces

You can also specify custom logs type in the **Custom logs type** field.

ⓘ You can not access logs through the phone user interface.

Viewing system logs

Use this procedure to choose and form the log messages through the web interface.

⇨ On the web interface, click **System logs**.

⇨ Under **Select log type**, select the log from a drop-down list.

⇨ Click the **Filter** button.

You can see the logs of the selected type in the field below.

⇨ Optional: You can do the following:

- Click the **Download all logs** button to download all the logs available. In this case the system downloads a `.zip` archive with the logs available.
- Click the **Download selected logs** button to download the logs of a selected type. In this case, the system downloads a `.txt` file with the logs of the selected type.
- Click the **Clear all logs** button to clear the list of available logs.

Network logs

You can get the traces of the phone's network activities through the web interface in the **Network logs** tab. The network logs can be useful for troubleshooting.

ⓘ You can get network logs only after the phone reboots into the Network logs mode.

Viewing network logs

Use this procedure to choose and form the network log messages through the web interface.

⇨ On the web interface, click **Network logs**.

⇨ You can do the following:

- Click the **Reboot into network log mode** button to reboot the phone into the network log mode.
- Click the **Download network logs** button to download the archive with the available network logs.

LICENSES

Some parts of the phone software are subject to open source license agreements. You can get the information about the use and redistribution conditions for the following:

- **BSD**. This is the Berkeley Software Distribution system for distribution of the source code to the operating system.
- **GPL v2.0**. This is the General Public License, version 2.0, which guarantees the end users the freedom to run, study, share and modify the software.
- **LGPL v2.1**. This is the Lesser General Public License, version 2.1, which is applicable to specially designated software packages of the Free Software Foundation and some other authors.
- **GFDL v1.2**. This is the GNU Free Documentation License, version 1.2, providing the freedom to copy and redistribute specific documentation.
- **GFDL v1.3**. This is the GNU Free Documentation License, version 1.3.
- **ISC**. This is the Internet Systems Consortium permissive free software license.
- **MIT**. This is the Massachusetts Institute of Technology permissive free software license.
- **OpenSSL**. This is the license to use OpenSSL being a software library for applications that secure network communications and help to identify the party at the other end.
- **PHP v3.0**. This is the license under which the PHP scripting language is released.
- **bzip2**. This is the license to a free and open-source file compression software that compresses single files.
- **socat**. This is the license to a relay for bidirectional data transfer between two independent data channels.
- **Libpng**. This is the license which defines the terms under which the libpng software library can be distributed.
- **Qt-Company-Commercial**. This is the license for development of proprietary software when the source code is not to be shared with third parties or there are other inconsistencies with the terms of the LGPL license.
- **TI-TSPA**. This is the Texas Instruments Incorporated license to publicly available technology and software.

- **Zlib**. This is the license which defines the terms under which the zlib software library can be distributed.

ⓘ You can get the license information only through the web interface.

Viewing licenses

Use this procedure to view the status and settings of Konftel 800 through the web interface.

⇨ Log in to the web interface.
⇨ Select the **Licenses** tab.
⇨ Select the license that you want to view from the list of licenses available.

Index

Konftel is a leading company within collaboration endpoint solutions. Since 1988, our mission has been to help people in businesses around the world to have meetings regardless of distance. Based on our success, we know that remote collaboration is a smooth way to save time, money and at the same time contribute to a more sustainable world. Crystal clear audio and a sharp video image are essential for efficient meetings, this is why we only focus on cutting-edge technology in our Collaboration Solutions. Our audio technology OmniSound® is built into all Konftel Conference phones and devices. The products are sold globally under the Konftel brand and our headquarter is based in Sweden. Read more about the company and our products at konftel.com.

Konftel AB, Box 268, SE-901 06 Umeå, Sweden
Tel: +46 90 70 64 89 **E-mail:** info@konftel.com