

Installation & Administration of Konftel 800

ENGLISH



NOTICES



Konftel AB hereby declares that this conference phone is in conformity with all the essential requirements and other relevant provisions of Radio Equipment Directive 2014/53/EU (RED). Please visit www.konftel.com to view the complete declaration of conformity.

 **WARNING:**

Do not expose Konftel 800 to water or moisture.

 **WARNING:**

Do not open the casing of Konftel 800.

Table of contents

Chapter 1: Introduction	6	Configuring Daylight Saving Time through the web interface.....	42
Purpose.....	6	Daylight Saving Time state.....	43
Change history.....	6	Minute offset.....	43
Chapter 2: Overview	10	Configuring the minute offset through the web interface.....	43
Phone overview.....	10	Configuring the minute offset using the configuration file.....	44
Safety guidelines.....	10	Time format.....	44
Physical layout.....	12	Configuring the time format using the configuration file.....	45
Connection layout.....	13	Provision of the NTP server address.....	45
Dimensions.....	14	Sleep mode.....	46
Icons.....	15	Enabling Sleep mode.....	46
Prerequisites.....	18	Network settings.....	47
Server configuration checklist.....	19	Configuring the network settings on the phone.....	47
Power supply connectivity.....	20	Configuring the Network settings through the web interface.....	48
Connection to other devices.....	20	Network settings description.....	48
Specifications.....	21	LLDP Data Units.....	55
Chapter 3: Initial setup and configuration	23	Media settings.....	58
Configuration of Konftel 800.....	23	Configuring the media settings on the phone.....	59
Centralized HTTP/HTTPS server.....	23	Configuring the media settings through the web interface.....	59
Setting the password for Konftel 800.....	24	Media settings description.....	59
Setting up a DHCP server.....	25	Voice quality monitoring.....	62
Connecting to a network with DHCP.....	25	Quality estimate metrics.....	64
Viewing the IP address.....	26	Analog parameters.....	65
Setting a static IP address.....	26	Configuring RTCP XR.....	65
Logging in to the web interface of Konftel 800.....	27	LDAP settings.....	66
Logging out from Konftel 800.....	28	Configuring the LDAP settings.....	67
Registering an account on the phone.....	28	LDAP settings description.....	67
Registering an account through the web interface.....	30	Configuring the LDAP number attributes through the web interface.....	72
Chapter 4: Settings configuration and management	31	SIP settings.....	73
Configuration of settings on Konftel 800.....	31	Configuring the SIP settings on the phone...	73
Input validation and data type restrictions....	31	Configuring the SIP settings through the web interface.....	73
Phone settings.....	32	SIP settings description.....	74
Configuring the phone settings on the phone.....	33	SIP account registration status.....	86
Configuring the phone settings through the web interface.....	33	Caller information presentation.....	87
Phone settings description.....	33		
Rebooting the phone.....	41		

Contents

Certificates application.....	88	Disabling Daisy Chain mode.....	111
Downloading the root certificate.....	88	Expansion microphone firmware upgrade... 111	
Installing the certificate.....	89	Upgrading expansion microphone firmware.....	112
Exporting the private key.....	89	Upgrading two expansion microphones.....	113
Converting the certificates to .PEM format... 90		Terminating expansion microphone upgrade.....	114
Standard encryption algorithms.....	90	Upgrading Smart Expansion Microphone manually.....	115
Standard encryption for 802.1x.....	91	Bluetooth® connection.....	115
Enabling EAP MD5 for 802.1x on the phone.....	92	Bluetooth® Classic profiles.....	116
Enabling EAP MD5 for 802.1x through the web interface.....	93	Pairing and connecting Bluetooth® devices.....	117
Standard encryption for media encryption with SRTP.....	93	Removing Bluetooth® pairing.....	118
Legacy encryption mode.....	94	Connection between paired Bluetooth® devices.....	118
Configuring Legacy encryption mode on the phone.....	94	Bluetooth® radio.....	119
Configuring Legacy encryption mode through the web interface.....	95	Disabling Bluetooth® radio.....	119
Configuring Legacy encryption mode using the configuration file.....	95	Chapter 6: Maintenance	121
FIPS mode.....	96	Provisioning on Konftel 800.....	121
FIPS mode for media encryption with SRTP.....	97	Firmware upgrade and downgrade.....	121
Configuring FIPS mode on the phone.....	97	Uploading a firmware file.....	121
Configuring FIPS mode through the web interface.....	98	Firmware upgrade using check-sync.....	122
Configuring FIPS mode using the configuration file.....	98	Firmware upgrade and downgrade using a USB mass storage device.....	123
USB only user mode.....	99	Upgrading firmware using a USB mass storage device without the administrator password.....	124
Time presentation in USB only user mode. 100		Upgrading the firmware using a USB mass storage device with the administrator password.....	125
USB only user mode icons.....	100	Configuration file.....	126
Chapter 5: Features and accessories	102	Configuration file structure.....	126
Konftel Unite.....	102	Exporting the configuration file.....	144
Pairing and connecting devices.....	102	Importing the configuration file.....	144
Disconnecting devices.....	103	Validation and migration of configuration... 145	
Deleting pairing.....	104	Device Management.....	146
Configuring the Konftel Unite settings.....	105	Registration with the ZTI device management service.....	147
Konftel Unite settings.....	105	Device Management settings.....	149
Expansion of the phone coverage.....	107	Files on the provisioning server.....	151
Functions of the Master and Slave devices 108		Global configuration file.....	151
Connection of the Slave devices to the Master phone.....	109	Creating the global configuration file.....	151
Arranging a daisy chain.....	109	Device-specific configuration file.....	152
Defining the mode of the phone.....	110	Creating the device-specific configuration file.....	152

Contents

Certificate configuration files.....	153
Certificate configuration file structure.....	154
SCEP support.....	158
Configuring SCEP settings through the web interface.....	160
Configuring SCEP using the configuration file.....	161
SCEP settings.....	161
Auto-renewal.....	163
Configuring SCEP renewal request.....	164
Firmware binary.....	164
Firmware metadata file.....	164
Creating firmware binary and metadata files.....	165
Upgrading multiple devices.....	165
Configuring multiple devices.....	166
Remote syslog server.....	167
Configuring remote syslog settings.....	167
Fall back server support.....	169
Factory reset.....	169
System recovery.....	169
Web interface settings.....	170
Protection against cross-site request forgery.....	171
Device status view.....	172
Device status.....	172
Viewing the phone status.....	173
System logs.....	173
Viewing system logs.....	174
PJSIP log levels.....	174
Setting PJSIP log level through the web interface.....	175
Setting PJSIP log level using the configuration file.....	175
Network logs.....	176
Viewing network logs.....	176
Licenses.....	177
Chapter 7: Appendix A.	
Encryption methods in	
Legacy encryption mode	178
Encryption methods in Legacy encryption mode.....	178
Index	182

INTRODUCTION

PURPOSE

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

CHANGE HISTORY

Issue	Date	Summary of changes
Release 1.0.6	September 2021	<ul style="list-style-type: none">• Updated Icons on page 15 with the Warning icon.• Added new section Rebooting the phone on page 41.• Added Input validation and data type restrictions on page 31.• Updated Phone settings description on page 33, Network settings description on page 48, Media settings description on page 59, LDAP settings description on page 67, and SIP settings description on page 74 with the requirements to a valid data input.• Added new section SIP account registration status on page 86.• Updated Configuration file structure on page 126 with new parameters.• Added new section SCEP support on page 158.

Table continued...

INTRODUCTION

Issue	Date	Summary of changes
Release 1.0.5	June 2021	<ul style="list-style-type: none">• Updated Icons on page 15 with the Clear call history button.• Updated Logging in to the web interface of Konftel 800 on page 27 with the information about lockout after incorrect login attempts.• Updated Phone settings description on page 33 with the default phone name and FIPS mode settings.• Updated Network settings description on page 48 with the information about IP address in the 802.1x slider section.• Updated SIP settings description on page 74 with the information about allow via header rewrite, use of static source ports, and USB only user mode.• Updated Standard encryption algorithms on page 90 with the information about FIPS mode.• Updated Legacy encryption mode on page 94 with the information about firmware upgrade.• Added new section FIPS mode on page 96.• Added new section USB only user mode on page 99.• Updated Expansion of the phone coverage on page 107 with the information about disabling the unused daisy chain ports during active calls.• Updated Bluetooth® connection on page 115 with the information about USB only user mode.• Added new section Firmware upgrade and downgrade using a USB mass storage device on page 123.• Updated Configuration file structure on page 126 with new parameters.• Added new section Protection against cross-site request forgery on page 171.• Added Appendix A with the information about the list of encryption methods enabled and disabled in Legacy encryption mode.

Table continued...

INTRODUCTION

Issue	Date	Summary of changes
Release 1.0.4	February 2021	<ul style="list-style-type: none">• Updated Phone settings description on page 33 with the Allow Legacy Encryption settings.• Added Provision of the NTP server address on page 45.• Updated Voice quality monitoring on page 62 with the quality estimate metrics and analog parameters.• Added Standard encryption algorithms on page 90.• Updated Konftel Unite on page 102 in line with the change in MD5 usage.• Added Expansion microphone firmware upgrade on page 111.• Updated Bluetooth® connection on page 115 with information on switching between the Bluetooth modes.• Updated Configuration file structure on page 126 with new parameters.
Release 1.0.3	October 2020	<ul style="list-style-type: none">• Updated Phone settings description on page 33 with the date, date format, time, time format, Daylight Saving Time (DST) mode, timezone and Custom DST settings.• Added Minute offset on page 43.• Added Time format on page 44.• Added Bluetooth® radio on page 119.• Added Firmware upgrade using check-sync on page 122.• Updated Configuration file structure on page 126 with new parameters.• Updated Certificate configuration files on page 153 with the information about the paths to the certificates, MD5 checksum, and certificate configuration file structure.

Table continued...

INTRODUCTION

Issue	Date	Summary of changes
Release 1.0.2	August 2020	<ul style="list-style-type: none">• Added Sleep mode on page 46.• Added Voice quality monitoring on page 62.• Added Bluetooth® connection on page 115.• Added LDAP settings on page 66.• Updated Configuration file structure on page 126 with new parameters.
Release 1.0.1	March 2020	<ul style="list-style-type: none">• Updated the Media settings description on page 59 with SRTP disablement.• Added Firmware upgrade and downgrade on page 121.• Added Validation and migration of configuration on page 145 to the Maintenance chapter.• Added Upgrading multiple devices on page 165.• Added Remote syslog server on page 167 to the Device Management section.

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 control 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 using, installing, configuring, and administering Konftel 800.

- Read, understand, and follow all the instructions.
- Do not drop, knock, or shake the device. 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 device 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 device. These openings are provided for ventilation, to protect the phone from overheating.
- Never push objects of any kind into this device 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.

OVERVIEW

- Do not use the device to report a gas leak in the vicinity of the leak.
 - Do not use the device near intensive care medical equipment or close to persons with pacemakers.
 - Do not place the device 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.

OVERVIEW

PHYSICAL LAYOUT



Figure 1: Front view of Konftel 800

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

Callout number	Description
1	Mute buttons
2	Volume down button

OVERVIEW

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

CONNECTION LAYOUT

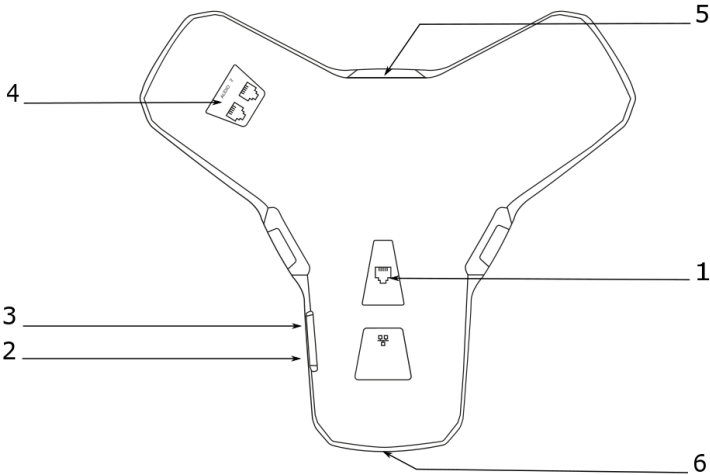


Figure 2: Connection layout of Konftel 800

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

OVERVIEW

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.

Parameter	Dimension
Width	326.41 mm
Length	369.87 mm
Height	74.7 mm


OVERVIEW

ICONS











Icons on the home screen of Konftel 800

Icon	Name	Description
	Recent	To check the call list. The phone provides the following information about the calls: <ul style="list-style-type: none">• Number. View the phone number of the contact.• Date. 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 the convenient time format.• Direction. View the incoming, outgoing and missed calls.
	Unite	To access the Konftel Unite settings.
	Call	To dial phone numbers and codes for telephone operations or Konftel Unite connection.
	Settings	To check and configure the settings from the phone. View the phone status and reach the menu.
	Warning	To notify that the SIP account registration failed. When you tap the Warning icon, the phone shows the following pop-up message: <code>No sip service registered (Wrong username/password or registrar?)</code> .
	Microphone Muted	To mute and unmute the phone.
	Volume Up	To increase the phone volume level.
	Volume Down	To decrease the phone volume level.













OVERVIEW

Icon	Name	Description
	NFC	To indicate the built-in NFC tag.










Other icons of Konftel 800

Icon	Name	Description
	Make Call or Answer	To indicate the phone off-hook status and answer an incoming call.
	Hang Up	To indicate the phone on-hook status and end a call.
	Incoming	To show an incoming call.
	Outgoing	To show an outgoing call.
	Missed	To indicate a missed call.
	Hold or On Hold	To put a call on hold or to indicate that a call is on hold.
	Conference	To arrange 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 arrange a private discussion with a participant of a conference call.

OVERVIEW

Icon	Name	Description
	Caps	To type in capital letters.
	Delete	To delete an unneeded number or letter.
	Visibility	To mark whether the characters must stay visible to the user, for example, when logging in with the password.
	Invisibility	To mark whether the characters must stay invisible to the user, for example, when logging 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.
	Arrow Left	To return to the previous page.

OVERVIEW

Icon	Name	Description
	Arrow Right	To move to subsections of a section.
	USB Connected	To indicate an active USB connection.
	Konftel Unite connected	To show the connection of the phone to Konftel Unite.
	Daisy Chain Mode	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.
	Contacts	To show that the LDAP external phone book is available.
	Bluetooth connection	To indicate an active Bluetooth® Classic connection.
	Call Transfer	To show that it is possible to transfer an ongoing call to another contact person.
	Clear call history	To clear all the call history in the call list.

PREREQUISITES

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

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

OVERVIEW

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.	Connect optional components and accessories to Konftel 800. Perform this task 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 Dynamic Host Configuration Protocol (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 table describes the tasks related to server configuration that you must perform for the initial installation of Konftel 800.

OVERVIEW

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 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, use the AC power adapter, which you can purchase 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:

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

OVERVIEW

SPECIFICATIONS

The following table lists the specifications that Konftel 800 supports:

Name	Description
Power	<ul style="list-style-type: none">• PoE 802.3af• PoE 802.3at• PoE injector available as an accessory
Connectivity	<ul style="list-style-type: none">• Ethernet RJ45 10/100 Mbps, PoE 802.3af, and PoE 802.3at• USB 3.0 device• Built-in Bluetooth® LE and NFC• Bluetooth® Classic (HFP, A2DP)• Daisy Chain (audio) ports (6-pin RJ-type)
Screen	Graphical touch screen with a resolution of approximately 480 x 800 and size of 4.3"
Acoustics	<ul style="list-style-type: none">• 3 symmetrically placed MEMS microphones• Full range speaker in the sealed enclosure
Music	<ul style="list-style-type: none">• PoE 802.3at: 91 dB and bass boost• PoE 802.3af: 87 dB• Daisy Chain: 91 dB
Speech	<ul style="list-style-type: none">• PoE 802.3at: 91 dB• PoE 802.3af: 87 dB• Daisy Chain: 91 dB
USB	<ul style="list-style-type: none">• Micro USB 3.0 device Type B• USB Type A
Bluetooth®	<ul style="list-style-type: none">• Bluetooth® LE• Bluetooth® Classic (HFP, A2DP)

OVERVIEW

Name	Description
Accessories	You can additionally purchase the following accessories: <ul style="list-style-type: none">• Konftel PoE kit• Konftel Smart Microphones• Konftel Daisy Chain kit
User interface	<ul style="list-style-type: none">• Simplified user interface• Functional keypad and dial pad• LED indicators for call and connectivity status
Mobile app	Konftel Unite. With the app, you can access your mobile phone contact book and calendar. The app is available for free at AppStore and Google Play
Device Configuration	<ul style="list-style-type: none">• Global .xml or MAC specific .xml configuration files• Web GUI administration

INITIAL SETUP AND CONFIGURATION

CONFIGURATION OF KONFTEL 800

Konftel 800 can use the following methods to obtain the required configuration parameters:

- Centralized HTTP/HTTPS server.
- Konftel 800 web interface when you log in as the administrator.
- Konftel 800 phone interface.

Centralized HTTP/HTTPS server

You can configure Konftel 800 to use DHCP to automatically obtain parameters from a DHCP server. You can use a DHCP Site Specific Option Number (SSON) to provide specific information for the Konftel 800 configuration. The following values are available: 43, 56, 60, 61, 66, 67, and 242. By default, the SSON value is 242.

Konftel 800 uses values of the following parameters from DHCP option specified by SSON:

- HTTPSRVR
- TLSSRV
- HTTPDIR
- L2QVLAN

DHCP Site Specific Option Number parameters

The following table describes the parameters that DHCP SSON contains:

Parameter	Description
HTTPSRVR	The IP Address or DNS name of an HTTP file server, which the device uses to obtain configuration, firmware, or certificates.
TLSSRV	The IP Address or DNS name of a file server, which the device uses to obtain configuration, firmware, or certificates. ⓘ The server authentication occurs by using the Transport Layer Security (TLS) protocol.

INITIAL SETUP AND CONFIGURATION

Parameter	Description
HTTPDIR	The path name to prepend to all file names that the device uses in HTTP and HTTPS GET operations during startup. The path is relative to the root of the TLS or HTTP file server. The path length is from 0 to 127 ASCII characters without spaces.
L2QVLAN	The VLAN ID of the voice Virtual Local Area Network (VLAN). The default value is 0.

Setting the password for Konftel 800

About this task

Use this procedure to set the password for your Konftel 800 when you first activate the phone or after a reset to the factory settings. By default, the administrator password is not set.

You must enter correct administrator password to change configuration of the phone. For that, you must always remember your password. If you forget the password, you can perform manual device recovery.

Before you begin

Connect the PoE cable to ensure the phone power supply.

Procedure

⇒ 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 administration mode, and you will be able to configure settings on the phone. However, you will not be able to access the web interface.

⇒ 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. As you enter the password, the phone informs if the password has acceptable length.

⇒ Type the password again to confirm it.

INITIAL SETUP AND CONFIGURATION

⇒ Tap the < icon three times to return to the home screen.

The phone reboots.

Related concepts

[Factory reset](#) on page 169

[System recovery](#) on page 169

Setting up a DHCP server

About this task

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

Before you begin

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

Procedure

- ⇒ Install the DHCP server software according to the server software vendor's instructions.
- ⇒ Configure the IP address for the phone.

Next steps

You must configure the required DHCP options to connect to the network with DHCP.

Related concepts

[Network settings description](#) on page 48

Connecting to a network with DHCP

About this task

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

Procedure

- To connect to the network with DHCP from Konftel 800, do the following:
 - Log in as the administrator.
 - Tap **Network**.
 - Enable **DHCP**.
 - Tap the < icon twice to return to the home screen.

INITIAL SETUP AND CONFIGURATION

The phone reboots.

- 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

About this task

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

Procedure

⇒ On the phone 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**
- **Smart Mic 1 Version**
- **Smart Mic 2 Version**

⇒ Tap the < icon twice to return to the home screen.

Setting a static IP address

About this task

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

Before you begin

Disable DHCP.

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

INITIAL SETUP AND CONFIGURATION

Procedure

- To set the static IP address from the phone, do the following:
Log in as the administrator and tap **Network**. If the administrator password is not set for the phone, on the phone screen, tap **Settings > Network**. Tap **Static IP**, and enter the following:
 - IP address
 - Netmask
 - GatewayReturn 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, click **Network**.
In the **Static IP** section, enter the following:
 - IP address
 - Network mask
 - GatewayClick **Save**.
The phone reboots.

Logging in to the web interface of Konftel 800

About this task

Use this procedure to log in to the web interface of your Konftel 800. You can access the web interface only if you set the administrator password for your phone.

After five incorrect login attempts, the web interface becomes blocked for 15 minutes. The web interface shows the following message: `Login has been suspended for 15 minutes due to too many invalid password entries`. If you enter the invalid password less than five times, then you have another five attempts after five minutes break.

📘 Konftel 800 officially supports only the Google Chrome browser.

The phone supports only HTTPS communication protocol.

Before you begin

Obtain the IP address and the administrator password for the phone.

Procedure

⇒ On the web browser, type the IP address of your phone in the following format:

INITIAL SETUP AND CONFIGURATION

`https://111.222.33.44/`

⇒ Enter the password in the **Password** field.

The password is the administrator password for your phone.

⇒ Click **Login** to log in to the webserver of your Konftel 800.

Logging out from Konftel 800

About this task

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

Before you begin

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

Procedure

On the web browser, click **Logout**.

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

Registering an account on the phone

About this task

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.

Before you begin

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

Procedure

⇒ Log in as the administrator and tap **SIP**. If the administrator is not set for the phone, tap **Settings > SIP**.

⇒ Tap **Primary Account**, and enter information in the following fields:

INITIAL SETUP AND CONFIGURATION

- **Account Name:** The name that the phone uses locally on the screen. You can set it based on your corporate standards.
- **User:** The SIP account name. The phone uses the content of this field to construct the user Universal Resource Identifier (URI). Do not include the @sipdomain.

This is a mandatory parameter.

- **Registrar Address:** The IP address or a fully qualified domain name (FQDN) of the SIP server where the account is registered. It can be in 10.10.1.100 format for a local SIP server or in the sip.company.net format for a public VoIP service provider or FQDN.

This is a mandatory parameter.

- **Proxy:** The proxy server the company uses for Internet communication. The address can be in 10.10.1.100:1234 format for a local proxy with the port specified or in the proxy.company.net:port format for FQDN.

The port value is optional. You can leave this field blank.

⇒ To ensure a persistent connection for the account, enable **Keep Alive**.

This will ensure a persistent connection for this account.

⇒ Tap **Credentials**, and enter information in the following fields:

- **Realm.** Realm identifies the SIP domain for Konftel 800 to accept incoming calls from. For example, company.net.

You can leave this field blank or put an asterisk (*) to accept all incoming call invites from any SIP domain.

- **Authentication Name.** If this parameter is not specified, the phone uses the content of the **User** field to authenticate and register the account.
- **Password.** The phone uses this password for the authentication with the Registrar. This is a mandatory parameter.

⇒ Tap the < icon to return to the account registration menu.

⇒ Optional: Enter **Registration Timeout** value 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 the < icon to return to the SIP menu.

Next steps

Repeat Steps above for the secondary and fallback accounts.

INITIAL SETUP AND CONFIGURATION

Registering an account through the web interface

About this task

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

Before you begin

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

Procedure

- ⇒ On the web interface, click **SIP**.
- ⇒ In the **Primary Account** section, enter information in the following fields:

- **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 above for the secondary and fallback accounts.
 - ⇒ Click **Save**.

The phone restarts the application to apply the changes.

SETTINGS CONFIGURATION AND MANAGEMENT

CONFIGURATION OF SETTINGS ON KONFTEL 800

You can configure almost all settings directly on your Konftel 800. For that you need to navigate through the menu and select the options you need. Using the web interface makes the settings configuration easier. This guide explains 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 log in as the Administrator.

INPUT VALIDATION AND DATA TYPE RESTRICTIONS

Positive input validation

Konftel 800 performs data input validation to ensure that the input contains only the permitted characters, values, and other data. The input type and length, and the data decoding, are also under control. The input validation protects the user against system malfunction and insertion of malicious codes.

The user's input validation takes place during the configuration of the settings on the phone, through the web interface, and by using the configuration file.

When the user tries to input invalid data on the phone or through the web interface, the phone does not accept or save the changed settings.

When the user tries to input invalid data during the configuration file import using the web interface or automatic provisioning of the phone, the server does not accept or save the invalid input. Konftel 800 does not accept configuration of the settings when:

- The user tries to import a file with invalid content for its type using the web interface or automatic provisioning.
- The user tries to import a large file using the web interface or automatic provisioning.

The maximum size of the files is the following:

- Certificates, public keys, and web certificates: 16KB
- Firmware: 200MB
- Configuration file: 100KB


SETTINGS CONFIGURATION AND MANAGEMENT

Input Data Type and Length Restrictions

Konftel 800 provides input data type and length validation. All validation rules take a stand on the existing requirements. For example, if the data input is a URL, validation rules are based on RFC for URLs.

When the user inputs data that do not meet the requirements, the system highlights the fields with the invalid data. The phone and the web server do not accept or process any data that does not meet the defined data type and length requirements.

If you input valid data, the phone reboots and applies the new configuration.

 When you type in values (text-based input), do not use the following characters:

! @ # \$ % ^ ? / \ - _

You can find the specific requirements and rules for valid data input in the settings description sections.

Related information

[Phone settings description](#) on page 33

[Network settings description](#) on page 48

[Media settings description](#) on page 59

[LDAP settings description](#) on page 67

[SIP settings description](#) on page 74

PHONE SETTINGS

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

- **Phone Name**
- **Phone Language**
- **Security**
- **Ringtone Level**
- **Key Tone**
- **Reboot Device**
- **Webapp Debug**
- **Daisy Chain Mode**
- **Factory Reset**
- **Admin Password**
- **Time and Region**

SETTINGS CONFIGURATION AND MANAGEMENT

- **Startup Sound**

Related concepts

[Phone settings description](#) on page 33

Configuring the phone settings on the phone

About this task

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

Procedure

- ⇒ On the phone screen, tap **Settings > Phone**.
- ⇒ 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, set time settings, choose Daisy Chain mode or reset the phone to factory settings.
- ⇒ After you made the choices, return to the home screen.

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

Configuring the phone settings through the web interface

About this task

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

Procedure

- ⇒ Log in to the web interface.
- ⇒ Click **Phone**.
- ⇒ Choose the parameter that you want to configure and proceed to the options available.
- ⇒ Click **Save**.

Phone settings description

The following table lists the basic settings of Konftel 800 available through the web interface in the **Phone** tab or on the phone in **Settings > Phone** and **Settings > Admin Login > Phone**.

SETTINGS CONFIGURATION AND MANAGEMENT


Name	Description
Phone	
Phone Name	<p>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. The default name is Konftel 800.</p> <p>Ensure that there is no empty space at the beginning or at the end of the string. The maximum input length is 28 characters.</p>
Phone Language	<p>To select the language. The options are:</p> <ul style="list-style-type: none">• English. This is the default setting.• Swedish• Danish• Norwegian• Finnish• Italian• German• French• Spanish• Portuguese• Dutch• Simplified Chinese <p>The characters on the Konftel 800 keyboard match the selected language for all languages except Simplified Chinese. For Simplified Chinese, Konftel 800 uses English keyboard layout.</p>
Security	
Allow Legacy Encryption	<p>To enable or disable legacy encryption for backward compatibility.</p> <p>By default, Legacy encryption mode is enabled.</p> <p> You can configure this parameter if you log in with the administrator password.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
FIPS Mode	<p>To enable or disable FIPS compliance.</p> <p>By default, FIPS mode is disabled.</p> <p> ⓘ You can configure this parameter if you log in with the administrator password.</p>
Admin Password	<p>To change the administrator password.</p> <p>Valid password is a single string that can have any characters in it except for the line break. The length of the password must not exceed 32 characters.</p> <p> ⓘ You can configure this parameter if you log in with the administrator password.</p> <p> ⓘ For security reasons, you can change the administrator password only on the phone.</p>
Ring Level	<p>To choose from six volume levels and Silent mode. The default setting is Level 4.</p> <p>If you select Silent mode, only the green LEDs on the phone flash when a call is received.</p>
Key Tone	<p>To enable or disable the key click sound as you tap the phone screen buttons.</p> <p>By default, the key tone is on.</p>
Reboot Device	<p>To reboot the phone when needed.</p> <p> ⓘ You can reboot the phone through the web interface and on the phone. You can initiate the reboot from the phone user interface only if you log in with the administrator password.</p>
Webapp Debug	<p>To enable or disable the debugging function for the web application. It activates the web application logging available in the System Logs tab. By default, Webapp Debug is off.</p> <p> ⓘ You can use this function only through the web interface.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
Daisy Chain	<p>To choose a mode, in which your Konftel 800 operates in case of a daisy chain arrangement. The options are:</p> <ul style="list-style-type: none">• Master. This is the default setting.• Slave <p> ⓘ You can configure this parameter on the phone if you log in with the administrator password. The administrator can also configure this parameter using the .xml configuration file.</p>
Factory Reset	<p>To reset the phone to its factory settings. By resetting the phone to its factory settings, you remove all the configurations set, imported and installed in course of the phone use.</p> <p> ⓘ You can do the factory reset only if you log in with the administrator password.</p>
Startup Sound	<p>To enable or disable the phone's branded startup sound. By default, the startup sound is on.</p> <p> ⓘ The change of this setting does not require a restart or reboot of the phone.</p>
Time and Region	
NTP Enable	<p>To enable or disable the Network Time Protocol (NTP). By default, NTP is enabled.</p> <p> ⓘ You can configure this parameter if you log in with the administrator password.</p>
NTP Server	<p>To specify the NTP server when NTP is enabled. By default the phone uses the following NTP server: <code>0.pool.ntp.org</code>.</p> <p> ⓘ You can configure this parameter if you log in with the administrator password.</p>


Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
Date	<p>To set the current date.</p> <p>ⓘ You can set the current date manually only if NTP is in disabled state.</p> <p>Specify the date by doing the following:</p> <ul style="list-style-type: none">• Manually enter the date in the field by clicking the day, month, and year to change the value.• Select a date from the date picker. <p>ⓘ You can use this function only through the web interface.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
Date Format	<p>To set the date format.</p> <p>The following date formats are available:</p> <ul style="list-style-type: none"> • dd M, D - Date, short name for the month and day of the week. For example, 10 Jan, Mon. • dd MM, DD - Date, full name for the month and day of the week. For example, 10 January, Monday. • M dd, D - Short name for the month, date, and short name for the day of the week. For example, Jan 10, Mon. • MM dd, DD - Full name for the month, date, and full name for the day of the week. For example, January 10, Monday. • D, dd M - Short name for the day of the week, date, and short name for the month. For example, Mon, 10 Jan. • DD, MM dd - Full name for the day of the week, full name for the month, and date. For example, Monday, January 10. • dd/mm/yy - Date/month/short numerical designation of the year. For example, 10/01/20. • dd/mm/yyyy - Date/month/full numerical designation of the year. For example, 01/10/2020. • mm/dd/yy - Month/date/short numerical designation of the year. For example, 01/10/2020. • mm/dd/yyyy - Month/date/full numerical designation of the year. For example, 01/10/2020. • yy/mm/dd - Short numerical designation of the year/month/date. For example, 20/01/10. • yyyy/mm/dd - Full numerical designation of the year/month/date. For example, 2020/01/10. <p>You can also leave the Default format of the date. In this case your Konftel 800 applies the date format that is standard for the selected language. For example, if your selected language is Finnish, the date format is <code>dd.mm.yyyy</code>.</p> <p> You can configure this parameter only through the web interface. The administrator can also configure this parameter using the <code>.xml</code> configuration file.</p>

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
Time	<p>To set the current time.</p> <p>i You can set the time manually only if NTP is in disabled state.</p> <p>See the time on the home screen of the phone.</p> <p>Set the time by doing the following:</p> <ul style="list-style-type: none">• Manually enter the time value in the field by clicking the hours, minutes, and seconds to change the value.• Select the time from the time picker. <p>i You can use this function only through the web interface.</p>
Time Format	<p>To set the time format.</p> <p>When you select the language, the time format automatically changes to the standard time format for the chosen language. You can manually change the convenient time format.</p> <p>The following time formats are available:</p> <ul style="list-style-type: none">• Default• 12 hours• 24 hours <p>i You can configure this parameter through the web interface. The administrator can also update settings with the .xml configuration file.</p>
Geo Timezone (auto DST)	<p>To enable or disable Daylight Saving Time (DST) mode based on the selected geographical timezone.</p> <p>By default, DST is disabled.</p> <p>i You can use this function only through the web interface.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
Timezone	<p>To specify a timezone and minute offset. The available timezone is based on Geo Timezone (auto DST) being enabled or disabled. With Geo Timezone (auto DST) disabled, the phone sets the time as a difference with the Coordinated Universal Time (UTC). You can specify the minute offset for the selected UTC time zone. The possible minute offset values are 0, 15, 30, and 45.</p> <p>With Geo Timezone (auto DST) enabled, the phone specifies the timezone based on the country and the city observing the DST.</p> <p>The default setting is UTC.</p> <ul style="list-style-type: none">① You can configure this parameter through the web interface. The administrator can also update settings with the .xml configuration file.
Daylight Saving Time	<p>To manually advance the clock during the specified period of time. Konftel 800 supports the Daylight Saving Time (DST) feature together with the UTC time zones.</p> <ul style="list-style-type: none">① You can configure this parameter through the web interface. The administrator can also update settings with the .xml configuration file.
Custom DST	<p>To enable or disable the custom DST mode.</p> <p>If Geo Timezone (auto DST) is enabled, Custom DST is automatically disabled.</p> <p>You can use the custom DST functions only with the enabled Custom DST.</p> <ul style="list-style-type: none">① You can configure this parameter through the web interface. The administrator can also update settings with the .xml configuration file.
Custom DST Settings	
Offset Hours	<p>To specify the time in hours between the standard time and the DST. The values are 1 and 2. The default setting is 1.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
Start Month	To select the month when to apply Offset Hours .
Start Day Mode	To select the day mode when to apply Offset Hours .
Start Day	To select the day when to apply Offset Hours . The value range is from 0 to 31.
Start Hour	To select the hour when to apply Offset Hours . The value range is from 0 to 23.
Stop Month	To select the month when to stop applying Offset Hours .
Stop Day Mode	To select the day mode when to stop applying Offset Hours .
Stop Day	To select the day when to stop applying Offset Hours . The value range is from 0 to 31.
Stop Hour	To select the hour when to stop applying Offset Hours . The value range is from 0 to 23.

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.

Rebooting the phone

About this task

Use this procedure to reboot your Konftel 800 using the user interface of the phone. Here you can reboot the phone without making additional power cycles.

You can reboot Konftel 800 from the user interface of the phone only if you log in as the administrator.

You can also reboot the phone from the web user interface.

Procedure

⇒ On the phone screen, tap **Settings > Admin Login > Phone**.

SETTINGS CONFIGURATION AND MANAGEMENT

⇒ Tap **Reboot**.

The phone shows the following pop-up message: `Reboot the phone. Press OK to confirm for 2 minutes and then hides it.`

⇒ To confirm the reboot, tap **Ok**.

The phone starts the reboot process and shows the following message: `Rebooting phone.`

⇒ Optional: To return to the **Phone** settings, tap **Cancel**.

Related concepts

[Phone settings description](#) on page 33

Configuring Daylight Saving Time through the web interface

About this task

Use this procedure to configure DST offset through the web interface.

- ① When you use the DST start parameters, enable the comparable DST stop parameters.

Procedure

- ⇒ Log in to the web interface.
- ⇒ Click **Phone**.
- ⇒ Enable **Custom DST**.
- ⇒ In the **Offset Hours** field, specify the time in hours between the standard time and the period when the DST parameter is active.

The values are 1 and 2. The default setting is **1**.

- ⇒ In the **Start Month** field, select the month to apply the DST offset.
- ⇒ In the **Start Day Mode** field, select the day mode to apply the DST offset.
- ⇒ In the **Start Day** field, specify the day to apply the DST offset.

The value range depends on the selected **Start Day Mode**. For example, if you select **Day of month** as the day mode, the value range is from 1 to 31. The value range for the weekday is from 0 to 7. Note that in this case, **0** and **7** mean Sunday.

When **Start Day Mode** is 0, the start day is a day of the month. In case of other values, the day is a day of the week: 1 is Monday, 5 is Friday. If **Start Day Mode** is 2 and **Start Day** is 5, you define the second Friday in the month.

The values -1 to -5 show a weekday in the month from the month end. If **Start Day Mode** is -1 and **Start Day** is 5, this is the last Friday in the month.

SETTINGS CONFIGURATION AND MANAGEMENT

- ⇒ In the **Start Hour** field, specify the hour to apply the DST offset.
- ⇒ In the **Stop Month** field, select the month to stop applying the DST offset.
- ⇒ In the **Stop Day Mode** field, select the day mode to stop applying the DST offset.
- ⇒ In the **Stop Day** field, specify the day to stop applying the DST offset.
The value range depends on the selected **Stop Day Mode**. For example, if you select **Day of month** as the day mode, the value range is from 1 to 31.
- ⇒ In the **Stop Hour** field, specify the hour to stop applying the DST offset.
- ⇒ Click **Save**.

Daylight Saving Time state

Check the Daylight Saving Time state on the status page. The following options are available:

- **On** shows that the DST is active. This happens when you configure a UTC timezone, enable **Custom DST**, and the current date is between the DST start day and DST stop day. In this case, you can add the offset to the current time.
- **Off** demonstrates that the DST is not active. This happens when you configure a UTC timezone with the **Custom DST** disabled, or the current date is not between the DST start day and DST stop day. In this case, you cannot add the offset to the current time.
- **Auto** means that there is a Geo timezone set, and the phone ignores the **Custom DST** settings. In this case, the DST settings are managed automatically.
- **Unknown** shows that the required information is currently unavailable. You must refresh the page and check it later.

Minute offset

Konftel 800 supports the minute offset of the specified UTC time zone. You can set the UTC time zone offset to 0, 15, 30, or 45 minutes.

Configuring the minute offset through the web interface

About this task

Use this procedure to configure the minute offset through the web interface.

Procedure

- ⇒ Log in to the web interface.
- ⇒ Click **Phone**.

SETTINGS CONFIGURATION AND MANAGEMENT

- ⇒ In the **Time and Region** section, disable **Geo Timezone (auto DST)**.
- ⇒ In the **Timezone** field, configure the following:
 - In the first drop-down list, select the UTC time zone.
 - In the second drop-down list, select the minute offset for the specified UTC time zone.
- ⇒ Click **Save**.

Configuring the minute offset using the configuration file

About this task

Use this procedure to configure the minute offset using the .xml configuration file.

Before you begin

Obtain the configuration .xml file for Konftel 800.

Procedure

- ⇒ In the configuration file, go to the `<time>` section.
- ⇒ Set the value in the `<timezone>` tag to your preferred UTC time zone:

```
<timezone>UTC+7</timezone>
```

- ⇒ To specify the minute offset, add the minute offset value to the specified `timezone`.

```
<timezone>UTC+7:15</timezone>
```

The UTC time zone offset is set to 15 minutes.

- ⇒ Save the configuration file.

Next steps

Upload the configuration file to the Device Management server or import the configuration file to the phone using the web interface.

Related concepts

[Configuration file](#) on page 126

Related tasks

[Importing the configuration file](#) on page 144

[Exporting the configuration file](#) on page 144

Time format

Konftel 800 supports various time formats so that the user get the convenient time presentation.

SETTINGS CONFIGURATION AND MANAGEMENT

The following values are available for the time format parameter:

- **hh:mm** - Konftel 800 shows time using the 24-hour clock approach.
- **hh:mm AP** - Konftel 800 shows time using the 12-hour clock approach.
- **Empty value** - Konftel 800 shows the standard time format for the selected language.

Configuring the time format using the configuration file

About this task

Configure the time format using the .xml configuration file.

Before you begin

Obtain the .xml configuration file for Konftel 800.

Procedure

- ⇒ In the configuration file, go to the `<time>` section.
- ⇒ Set the `<time_format>` parameter value.
- ⇒ Save the configuration file.

Next steps

Upload the configuration file to the Device Management server or import the configuration file to the phone using the web interface.

Related concepts

[Configuration file](#) on page 126

Related tasks

[Importing the configuration file](#) on page 144

[Exporting the configuration file](#) on page 144

Provision of the NTP server address

Use DHCP option 42 to provide NTP server address to Konftel 800 when using 802.1x certificates. In this case, you must have DHCP enabled on the phone to display the accurate time received from this NTP server address.

- ① Do not update the value in the configuration file while receiving the NTP address from the DHCP option 42.

If there is a configured NTP setting on the phone, and you set DHCP option 42 to provide NTP server address, then the address from DHCP option 42 overrides this setting in configuration. At that, Konftel 800 preserves the value in the configuration settings. The phone stores the NTP server address from DHCP

SETTINGS CONFIGURATION AND MANAGEMENT

option 42 separately in a volatile memory. So, when it reboots, the volatile memory becomes empty. If DHCP option 42 does not provide an NTP server address again, then the value from the configuration file becomes applicable.

Sleep mode

Konftel 800 supports Sleep mode feature, which saves power by turning the screen off after a specified period of inactivity. By default, Sleep mode is in disabled state. The phone administrator can enable Sleep mode and configure the time-out value.

The phone wakes up from Sleep mode when you do any of the following:

- Touch the screen
- Connect or disconnect the USB cable
- Connect or disconnect a daisy chain Slave device
- Connect or disconnect the Bluetooth® Classic

The phone also wakes up from Sleep mode during screen activity, such as an incoming call, Konftel Unite connection, or error prompts.

The phone cannot enter Sleep mode during an active call or when it is in music streaming mode.

Enabling Sleep mode

About this task

Enable Sleep mode and configure the time-out value using the .xml configuration file. The default value is 0, which means that the feature is disabled. To enable Sleep mode and to specify the time-out in minutes, set the value in the range from 1 to 500.

Before you begin

Obtain the .xml configuration file for Konftel 800.

Procedure

- ⇒ In the configuration file, go to the `<phone>` section.
- ⇒ Set the `<sleep_mode_timeout>` parameter to a value in the range from 1 to 500.
- ⇒ Save the configuration file.

SETTINGS CONFIGURATION AND MANAGEMENT

Next steps

Upload the configuration file to the Device Management server or import the configuration file to the phone using the web interface.

Related concepts

[Configuration file](#) on page 126

Related tasks

[Importing the configuration file](#) on page 144


[Exporting the configuration file](#) on page 144

NETWORK SETTINGS

The network settings of Konftel 800 include the following:

- DHCP
- Hostname
- Domain
- Static IP
- DNS1
- DNS2
- VLAN
- VLAN ID
- LLDP
- 802.1x
- SIP DiffServ
- Media DiffServ

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

 When you type in values (text-based input), do not use the following characters: !@#\$\$%^&?/\-_.

Related concepts

[Network settings description](#) on page 48

Configuring the network settings on the phone

About this task

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

SETTINGS CONFIGURATION AND MANAGEMENT

Before you begin

Log in as the administrator.

Procedure

- ⇒ In the **Settings** menu, tap **Network**.
- ⇒ Choose the parameter that you want to configure and proceed to the options available.
- ⇒ Tap the < icon twice to return to the home screen.
The phone reboots to apply the changes.

Configuring the Network settings through the web interface

About this task

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

Procedure

- ⇒ 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 description

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

Name	Description
Network	

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
DHCP	<p>To enable or disable Dynamic Host Configuration Protocol (DHCP) on your phone. Network devices use DHCP to obtain the parameters necessary for operation in the IP network. You must enable DHCP if no other specific information is given.</p> <p> ⓘ When the DHCP option is enabled, all other information on this page is set automatically.</p>
Hostname	<p>To specify the hostname of your phone in the network. By default, it is set to <code>konftel1800</code>. You can change it to another name.</p> <p>The accepted input is a string composed of digits or letters and a '-' character.</p> <p>For example, <code>Konftel1800-Room-2F17</code>.</p>
Domain	<p>To specify the domain where the device is located.</p> <p>The accepted input is a string composed of digits or letters and a '-' character.</p> <p>For example, <code>your-company1234.com</code>.</p> <p> ⓘ You can leave this field blank.</p>
Static IP	
IP	<p>To specify the IP address of the phone if DHCP is disabled. Here, the network administrator or the service provider provides the address.</p> <p>Input example: <code>127.0.0.1, 255.255.255.255</code>.</p> <p>The maximum accepted input value is 255.</p>
Netmask	<p>To specify the network mask for your phone. Usually, it is set to <code>255.255.255.0</code> to limit network traffic to the subnet.</p> <p> ⓘ The maximum accepted input value is 255.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT





Name	Description
Gateway	<p>To specify the gateway for your phone. The gateway is the address of the device or server used for Internet communication.</p> <p>Input example: 127.0.0.1, 255.255.255.255.</p> <p>The maximum accepted input value is 255.</p>
DNS 1	<p>To specify the address to the primary Domain Name System (DNS) server.</p> <p>Input example: 127.0.0.1, 255.255.255.255.</p> <p>The maximum accepted input value is 255.</p> <p> Leave the field blank for DHCP default settings.</p>
DNS 2	<p>To specify the address to an optional secondary DNS server.</p> <p>Input example: 127.0.0.1, 255.255.255.255.</p> <p>The maximum accepted input value is 255.</p> <p> Leave the field blank for DHCP default settings.</p>
VLAN	<p>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.</p> <p> The phone also uses this VLAN to communicate through the web interface.</p>
VLAN ID	<p>To specify the ID number to be used for all IP telephony communication through VLAN on your phone.</p> <p>The value range is from 0 to 4094.</p>
SIP DiffServ	<p>To specify a value from 0 to 63 to prioritize the SIP messages as a part of the quality of service (QoS) mechanism.</p> <p> You can configure this parameter through the web interface or the .xml configuration file.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT



Name	Description
Media DiffServ	<p>To specify a value from 0 to 63 to prioritize the media packets (voice) as a part of the quality of service (QoS) mechanism.</p> <p> You can configure this parameter through the web interface or the .xml configuration file.</p>
LLDP	<p>Enable</p> <p>To enable and disable specification of the phone location settings.</p> <p>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.</p> <p>By default, LLDP is enabled after the first boot, factory reset, and configuration reset.</p> <p> You can configure LLDP settings only through the web interface.</p>
Country Code	<p>To specify the country.</p> <p>The input data must consist of 2 or 3 uppercase letters or 3 digits.</p>
Country Subdivision	<p>To specify the part of the country.</p>
County	<p>To specify the county, parish, district, or other applicable administrative division.</p> <p>Do not use the following characters: ! @ # \$ % ^ * . - _ . The maximum input length is 50 characters.</p>
City	<p>To specify the city.</p> <p>Do not use the following characters: ! @ # \$ % ^ * . , . The maximum input length is 40 characters.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
City Division	<p>To specify the city district or area.</p> <p>Do not use the following characters: ! @ # \$ % ^ ? / \. The maximum input length is 40 characters.</p>
Block	<p>To specify the block within the city district.</p>
Street	<p>To specify the street.</p> <p>Do not use the following characters: ! @ # \$ % ^ ? / \. The maximum input length is 40 characters.</p>
Direction	<p>To specify the direction of moving along the street.</p> <p>Do not use the following characters: ^ ! @ # \$ % ^ * / \ _ 0-9.</p>
Trailing Street Suffix	<p>To specify the trailing street suffix.</p> <p>Both uppercase and lowercase of the input data is acceptable. Do not use the following characters: ! @ # \$ % ^ * / \ _ 0-9. The maximum input length is 10 characters.</p>
Street Suffix	<p>To specify the street suffix.</p> <p>Both uppercase and lowercase of the input data is acceptable. Do not use the following characters: ! @ # \$ % ^ * / \ _ or digits. The maximum input length is 15 characters.</p>
Number	<p>To specify the house number.</p> <p>The value range is from 0 to 65535.</p>
Number Suffix	<p>To specify the house number suffix.</p> <p>Do not use the following characters: ! @ # \$ % ^ *. The maximum input length is 20 characters.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
Landmark	To specify the reference point for the location. Do not use the following characters: ! @ # \$ % ^ \ / or digits. The maximum input length is 30 characters.
Additional	To specify additional reference points. Do not use the following characters: ! @ # \$ % ^ \ / or digits. The maximum input length is 30 characters.
Name	To specify the name of the company. By default, it is set to Konftel 800. The administrator can change it to another name. Do not use the following characters: ! @ # \$ % ^ ?. The maximum input length is 60 characters.
Zip	To specify the ZIP code of the location. Do not use the following characters: ! @ # \$ % ^ *. The maximum input length is 20 characters.
Building	To specify the name or number of the building. Do not use the following characters: ! @ # \$ % ^ ?. The maximum input length is 60 characters.
Unit	To specify the unit within the building. Do not use the following characters: ! @ # \$ % ^ ?. The maximum input length is 30 characters.
Floor	To specify the floor of the building. The range is from -5 to 250.
Room	To specify the room in the building. Do not use the following characters: ! @ # \$ % ^ ?. The maximum input length is 60 characters.

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
Place Type	<p>To specify the type of setting, for example, office.</p> <p>Do not use the following characters: ! @ # \$ % ^ ? / \. The maximum input length is 60 characters.</p>
Script	<p>To specify the script.</p> <p>Do not use the following characters: ! @ # \$ % ^ ? / \. The maximum input length is 60 characters.</p>
ELIN	<p>To specify Emergency Location Identification Number (ELIN).</p> <p>The maximum input length is 31 digits.</p>
802.1.x	
802.1x slider	<p>To enable or disable 802.1x. When enabled, the Konftel 800 asks an authentication server for permission when connected to the LAN.</p> <p>Konftel 800 requests a new IP address when 802.1x authentication succeeds for the first time. If you configure the phone to use DHCP, the phone does not request a new IP address until the current DHCP lease expires.</p>
Authentication Name	<p>To specify your name in the network.</p>
EAP MD5	<p>To enable or disable the Extensible Authentication Protocol (EAP) MD5 method.</p>
EAP TLS	<p>To enable or disable the EAP Transport Layer Security (TLS) method.</p>
EAP MD5	

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
EAP-MD5 Password	<p>To set EAP password.</p> <p>Valid password is a single string that can have any characters in it except for the line break. The length of the password must not exceed 32 characters.</p> <p> ⓘ This parameter is available in the web interface if you enable EAP-MD5 Password.</p>
EAP TLS	<p> ⓘ This section is available in the web interface if you enable EAP TLS.</p>
Certificate	<p>To specify the certificate for the phone to use for authentication if TLS is applied.</p>
CA Certificate	<p>To specify the public key in the root certificate which the phone uses to verify other certificates in case of TLS applied. The root certificate is also known as the Certificate Authority (CA) certificate.</p>
Private Key	<p>To specify the private key which the phone uses to verify other certificates in case of TLS applied.</p>
Private Key Password	<p>To specify the password for encryption of the private key when using TLS.</p> <p>Valid password is a single string that can have any characters in it except for the line break. The length of the password must not exceed 32 characters.</p>

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:

SETTINGS CONFIGURATION AND MANAGEMENT

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

SETTINGS CONFIGURATION AND MANAGEMENT

Category	TLV Name	String length	TLV String Value
ORGANIZATION SPECIFIC	IEEE 802.3 - LINK AGGREGATION	9	OUC = 00-12-0F; IEEE 802.3 SUBTYPE = LINK AGGREGATION 3; 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

SETTINGS CONFIGURATION AND MANAGEMENT

Category	TLV Name	String length	TLV String Value
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
TIA LLDP MED	INVENTORY - SOFTWARE REVISION	5–36	TIA OUC = 00-12-BB (HEX); SOFTWARE REVISION SUBTYPE = 7; SOFTWARE REVISION = VALUE
ORGANIZATION 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

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
- Voice Quality Monitor

Related concepts

[Media settings description](#) on page 59

SETTINGS CONFIGURATION AND MANAGEMENT

Configuring the media settings on the phone

About this task

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

Before you begin

Log in as the administrator.

Procedure

- ⇒ In the **Settings** menu, tap **Media**.
- ⇒ Choose the parameter that you want to configure and proceed to the options available.
- ⇒ Tap the < icon twice to return to the home screen.
The phone restarts the application to apply the changes.

Configuring the media settings through the web interface

About this task

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

Procedure

- ⇒ Log in to the web interface as the administrator.
- ⇒ Click **Media**.
- ⇒ Choose the parameter that you want to configure and proceed to the options available.
- ⇒ Click **Save**.

Media settings description

The following table lists the media settings of Konftel 800 available through the web interface in the **Media** tab or on the phone in **Settings > Admin Login > Media**.

- ① Starting from Release 1.0.1, the **SRTP**, **SRTCP**, and **Capability Negotiation** settings are not supported on Konftel 800 phones sold in Russia, Belarus, Kazakhstan, Kyrgyzstan, and Armenia to meet local restrictions on the use of encryption. On such phones, the settings related to **SRTP**, **SRTCP**, and **Capability Negotiation** are excluded both from the phone interface and the web interface, and you, as the administrator, cannot enable these settings.

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
Security	
SRTP	<p>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:</p> <ul style="list-style-type: none"> • 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 other devices do not support SRTP. <p>By default, SRTP is disabled.</p>
SRTCP	<p>To enable or disable the Secure Real Time Control Protocol (SRTCP). Enabled SRTCP means using the encrypted protocol.</p> <p>By default, SRTCP is disabled.</p>
Capability Negotiation	<p>To enable or disable the Session Description Protocol (SDP) capability negotiation. If Capability Negotiation is enabled, the phone can negotiate transport protocols and attributes.</p> <p>By default, Capability Negotiation is disabled.</p>
Codec	
Codec	<p>To set the priorities to your codec preferences, where 6 is high, 1 is low, and 0 disables the negotiation of the specific codec.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
ILBC Priority	<p>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.</p> <p>By default it is set to 0.</p>
OPUS Priority	<p>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. Opus provides an excellent Wideband and Narrowband performance versus bandwidth.</p> <p>By default it is set to 0.</p> <p>① Determine if your engineering VoIP environment can use OPUS.</p>
PCMU Priority	<p>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.</p> <p>By default it is set to 4.</p>
PCMA Priority	<p>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.</p> <p>By default it is set to 5.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
G722 Priority	<p>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.</p> <p>By default it is set to 6 (highest priority).</p> <p>① Consider OPUS to provide higher quality at a lower bandwidth.</p>
G729 Priority	<p>This is an ITU-T standard codec that operates at 8 kbit/s. It is mostly used in VoIP applications with low bandwidth requirement.</p> <p>By default it is set to 3.</p> <p>① Consider OPUS for a higher audio quality at a lower bandwidth. OPUS is also more resilient to transcoding.</p>
Voice Quality Monitor	
Enable RTCP XR	<p>To enable or disable the sending of the Real Time Control Protocol Extended Report (RTCP XR). If enabled, the quality parameters are sent as SIP PUBLISH messages to the specified report collector.</p> <p>By default, this option is disabled.</p>
RTCP XR Collector URI	To specify the report collector.

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

Voice quality monitoring

Configure Konftel 800 to generate quality metrics and evaluate the overall quality of the calls. You can use this information to troubleshoot various quality aspects of the phone calls.

Find the detailed description of the collected parameters in the following standards: RFC 6035 and RFC 3611.

SETTINGS CONFIGURATION AND MANAGEMENT

RTCP XR as voice quality monitoring report

If you enable the voice quality monitoring feature, the phone collects the metrics, generates Real-Time Control Protocol Extended Report (RTCP XR), and sends RTCP XR as a SIP PUBLISH message to the specified report collector. View the statistics of the established phone calls on a specific information collecting portal.

The phone collects the metrics in the following cases:

- One of the call parties ends the call.
- Call parameters, such as codec and far-end IP address or port, change.
- One of the call parties puts the call on hold or resumes it.

RTCP XR parameters

The following table lists parameters that the RTCP XR contains:

Parameter	Description
CallId	Party leg identifier
LocalId	Reporting device for the media session
RemoteId	Remote device of the media session
OrigID	Device that originated the session
LocalGroup	Identification for aggregation of the local phone
LocalAddr	Address information, including an IP address, a port number, and SSRC of the phone that receives the information
LocalMAC	The Media Access Control (MAC) address of the local phone
RemoteAddr	Address information, including an IP address, a port number, and SSRC of the phone that is the source of information.
Timestamps	Call start and call end in Coordinated Universal Time (UTC)
SessionDesc	A shortened version of the media session including codecs (ILBC, Opus, PCMU, PCMA, G722, or G729), silence suppression status (on or off), and number of packets per second

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Parameter	Description
JitterBuffer	Jitter Buffer metric definitions
PacketLoss	Packet loss percentage and Jitter buffer discard rate percentage
BurstGapLoss	Burst-to-Gap loss metric
Delay	Network delay between the call parties
Signal	Non-packet elements of the voice over IP system. Includes a Signal level (SL) metric, which typically has a negative value
QualityEst	Measures of the established call quality

Quality estimate metrics

The following table shows the direct measures of the quality of the established call or transmission. These metrics incorporate the effects of codec type, packet loss, discard, burstiness, and delay.

Metric	Description
RLQ	Listening Rating Factor (RLQ) metric based on burst packet loss and codec selection.
RCQ	Conversational Rating Factor (RCQ) metric measures voice quality based on transmission delay, burst packet loss, and burst loss recency.
MOSLQ	A mean opinion score for listening quality (MOSLQ). The scale of speech quality is one (bad) through five (excellent).
MOSCQ	A mean opinion score for conversational quality (MOSCQ). Includes recency and delay effects, which affect conversational quality.
QoEEstAlg	A text description of the algorithm, which estimates all voice quality metrics.

SETTINGS CONFIGURATION AND MANAGEMENT

Analog parameters

The following table lists the analog parameters that the RTCP XR does not provide, but they influence the call quality statistics:

Name	Description
NoiseLevel	The average silence period noise level (expressed in dBm), reported by the speech processor.
LocalRERL	The average local residual echo return loss (RERL) level (expressed in dB), reported by the echo canceller.
NewLocalLoopEPDelay	The local loop echo path delay (expressed in ms), calculated by the local echo canceller.

The analog parameter data are updated every second. The phone regularly collects the analog parameter data and sends them to generate the RTCP XR report.

Configuring RTCP XR

About this task

By default, the voice quality monitoring feature on Konftel 800 is disabled. To use this feature, enable it and specify the Uniform Resource Identifier (URI) of the RTCP XR collector. You can do this on the phone, through the phone web interface, or using the configuration .xml file.

The acceptable formats for the collector URI are as follows:

- hostname
- hostname:port
- user@hostname
- user@hostname:port

Before you begin

Obtain the RTCP XR collector URI from your service provider.

Procedure

- To configure RTCP XR from the phone interface, do the following:
Log in as the administrator.

SETTINGS CONFIGURATION AND MANAGEMENT

Navigate to **Media > Voice Quality Monitor** and move the **Enable RTCP XR** slider to the right to activate RTCP XR.

In the **RTCP XR Collector URI** field, specify the RTCP XR collector URI.

For example, `rtcpxr@rtcpxr.ringcentral.com`.

Tap the < icon three times to return to the home screen.

The phone restarts the application to apply the changes.

- To configure RTCP XR from the web interface, do the following:

Log in to the phone web interface.

On the **Media** tab, in the **Voice Quality Monitor** section, move the **Enable RTCP XR** slider to the right to activate RTCP XR.

In the **RTCP XR Collector URI** field, specify the RTCP XR collector URI.

For example, `rtcpxr@rtcpxr.ringcentral.com`.

Click **Save**.

The phone restarts the application to apply the changes.

- To configure the RTCP XR using the configuration file, do the following:

Obtain the configuration .xml file.

Find the RTCP XR settings under the `<voice_quality_monitor>` section.

In the `<enable_rtcp_xr>` tag, specify `true` to enable RTCP XR.

In the `<rtcp_xr_collector_uri>` tag, specify the collector URI.

For example, `rtcpxr@rtcpxr.ringcentral.com`.

Save the configuration file.

Import the configuration file to the phone through the web interface or to the provisioning server to configure several phones simultaneously.

Related concepts

[Device Management](#) on page 146

Related tasks

[Exporting the configuration file](#) on page 144

LDAP SETTINGS

Konftel 800 supports connection to an external phone book using the Lightweight Directory Access Protocol (LDAP). When the LDAP feature is in the enabled state, you can browse and use the contact information stored in a remote company directory. The LDAP phone book is available in the **Dialpad** view of the phone interface.

SETTINGS CONFIGURATION AND MANAGEMENT

An LDAP database can contain thousands of contacts. To facilitate the search through the directory server, Konftel 800 has a built-in search function, which filters the content from the LDAP database, based on the search parameters that you enter.

To make the LDAP phone book available, you must activate the LDAP feature by specifying the LDAP server to connect to and the search parameters. You can configure the LDAP settings during or after the installation of Konftel 800.

Configuring the LDAP settings

About this task

Configure the LDAP settings through the web interface of your Konftel 800.

Procedure

- ⇒ Log in to the web interface.
- ⇒ Navigate to the **LDAP** tab.
- ⇒ Choose the parameter that you want to configure and proceed to the options available.
- ⇒ Click **Save**.

The phone restarts the application to apply the changes.

LDAP settings description

The following table lists the LDAP settings of Konftel 800 available through the web interface in the **LDAP** tab.

Parameter	Description
Connection	
Enable	To specify if the LDAP feature is enabled. By default it is disabled.
URL	To specify the URL of the LDAP server host. The phone supports LDAP and LDAP over SSL (LDAPS). URL also can contain the port that the phone connects to.

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Parameter	Description
Certificate	To upload a certificate to the phone. This certificate is used for authentication on the LDAP server.
CA Certificate	To upload a root certificate. It contains a public key, which is used to verify other certificates when using LDAP.
Private Key	To upload a private key. It is used for authentication when using LDAP.
Username	To specify the username if the LDAP server requires one. Leave this field blank if the LDAP server does not require a username.
Password	To specify the password if the LDAP server requires one. Valid password is a single string that can have any characters in it except for the line break. The length of the password must not exceed 32 characters. Leave this field blank if the LDAP server does not require a password.
Search options	
Search base	To specify the distinguished name (DN) of the search base. Example: dc=domain, dc=com. ⓘ Do not use the following characters: (), !, , &, *, -.
Name filter	To define how the phone applies the entered search characters. The filter complies with the string representation of LDAP search filters described in RFC2254. The search character entered by the user replaces % in the filter string. Example: ((sn=%*) (cn=%*)) : the phone displays to the user all entries with the search characters in the beginning of the sn or cn attribute.

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Parameter	Description
Display name	<p>To specify how the phone displays the search hits.</p> <p>Example: %cn shows the cn attribute.</p> <p>%givenName %sn shows the givenName attribute and the sn attribute with a space in between.</p>
Sort results	<p>To specify if the phone sorts the search hits based on the Display name.</p> <p>By default, this setting is enabled.</p>
Max hits	<p>To specify the maximum number of hits to return for each LDAP search.</p> <p>The value range is from 0 to 1000. The default value is 20.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Parameter	Description
Number attributes	<p data-bbox="348 264 919 344">To define the attributes that the phone displays for a selected search hit. The phone receives the displayed information from the LDAP server.</p> <p data-bbox="348 368 986 424">The number of the Number attribute tags inside the Number attributes tag may be 0 – 30.</p> <p data-bbox="348 440 986 647">Each Number attribute consists of an identifier <code><id></code> and its value <code><value></code>. The identifier is the number attribute in the form in which the LDAP directory stores it. The <code><id></code> tag cannot be empty. The value is the short description or the label that the user sees on the phone screen for a specific number attribute. You can use the same label for several ids.</p> <p data-bbox="348 663 975 719">There are default and custom labels. The default labels are the following:</p> <ul data-bbox="348 735 544 895" style="list-style-type: none">• Phone number• Mobile• Home• Work• Other <p data-bbox="348 911 919 935">The <code>Custom</code> label are the labels that the user defines.</p> <p data-bbox="348 959 975 1046">The phone translates each label from the default list to the language specified for the device. The phone does not translate the custom labels and displays them as user sets.</p> <p data-bbox="348 1062 986 1150">A custom label can be empty. In this case the phone gives it a default <code>PHONENUMBER</code> label and translates to the device language.</p> <p data-bbox="348 1166 958 1254">Example: the identifier <code>mobile2</code> with the value <code>MOBILE</code> shows the second mobile phone number and the label on separate rows for the selected contact.</p> <p data-bbox="348 1270 953 1326">There are maximum 30 labels of the Number attributes in the web UI.</p>
Dial options	

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Parameter	Description
Country code	<p>To specify the country code where the phone is located. In case the country code in any phone number attribute is identical to that code, the phone ignores it.</p> <p>The maximum input length is 3 digits. You can also use the + symbol.</p> <p>Example: +999, +23, 831, 12.</p>
Area code	<p>To specify the area code where the phone is located. In case the area code in any phone number attribute is identical to that code, the phone ignores it.</p> <p>The maximum input length is 10 digits.</p>
External prefix	<p>To specify a special prefix for dialing external numbers.</p> <p>Example: 0 to get a dialing tone in some cases.</p>
Min length for external prefix	<p>To restrict the external prefix that the phone adds only if the phone number is longer than the minimum length. This allows to use short internal numbers.</p> <p>The value range is from 0 to 32. The default setting is 0.</p>
Exact length for no external prefix	<p>To specify that the phone must not add the external prefix if the phone number is exactly of the entered length.</p> <p>The default setting is 0.</p>
Number prefix for no external prefix	<p>To specify the initial number for the phone numbers in case of using which the phone adds no external prefix. All numbers that start with this number will not have the external prefix added. You can use this option if all internal numbers start with a certain number.</p> <p>The default setting is 0.</p>

① If complete information is unavailable, you can configure only the known parameters.

SETTINGS CONFIGURATION AND MANAGEMENT

Configuring the LDAP number attributes through the web interface

About this task

Configure the LDAP number attributes through the web interface of your Konftel 800.

You can also configure the LDAP number attributes using a configuration file. For that you must define the corresponding parameter and then import the configuration file.

Procedure

- ⇒ Log in to the web interface.
- ⇒ Navigate to the **LDAP** tab.
- ⇒ Scroll down to the **Number attributes** section.
- ⇒ Add the number attribute label.
- ⇒ Fill in the title for a number attribute in the **Attribute** field.
- ⇒ Choose the description label from the **Localized labels** dropdown list.

Note that if the label stays empty, it uses the localized default label.

- ⇒ Optional: Enable the **Custom** control element to edit the label.

The **Custom** control element is in the enabled state automatically if the attribute is not in the list of the approved attributes.

- ⇒ Optional: You can also do one of the following:
 - Add a number attribute entity by clicking the **Add attribute label** button. The default ID of the number attribute entity is `telephoneNumber` and the value is `PHONENUMBER`.

Note that there can be maximum 30 number attribute labels in the web UI.

- Delete a number attribute entity by clicking the **Delete** button next to the respective number attribute.

- ⇒ Click **Save**.

The phone restarts the application to apply the changes.

The order of the configured number attributes depends on the order of attributes defined on the LDAP server.

Related concepts

[Configuration file](#) on page 126

Related tasks

[Importing the configuration file](#) on page 144

SETTINGS CONFIGURATION AND MANAGEMENT

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.

- ① If you do not configure the SIP account for Konftel 800, the phone operates in USB only user mode.

Configuring the SIP settings on the phone

About this task

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

Before you begin

Log in as the administrator.

Procedure

- ⇒ In the **Settings** menu, tap **SIP**.
- ⇒ Choose the parameter that you want to configure and proceed to the options available.
- ⇒ Tap the < icon to return to the home screen.

The phone restarts the application to apply the changes.

Configuring the SIP settings through the web interface

About this task

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

SETTINGS CONFIGURATION AND MANAGEMENT

Procedure

- ⇒ Log in to the web interface as the administrator.
- ⇒ Click **SIP**.
- ⇒ Choose the parameter that you want to configure and proceed to the options available.
- ⇒ Click **Save**.

The phone restarts the application to apply the changes.

SIP settings description

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

Name	Description
Transport	
Transport Protocol	To choose one of the following protocols: <ul style="list-style-type: none">• UDP. This is the default setting.• TCP• TLS• SIPS <p>① Even if you choose TLS, the Konftel 800 still accepts incoming UDP or TCP signaling.</p>
Source port	To optionally specify the local port Konftel 800 will use for SIP signaling. The value range is from 0 to 65535.
TLS	
① This section is available in the web interface if you choose TLS or SIPS transport protocol.	

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
TLS Method	<p>To choose the security methods to be applied. The options are:</p> <ul style="list-style-type: none">• TLSv1• TLSv1_1• TLSv1_2. This is the default setting.
Verify Client	<p>To enable or disable Verify Client. The options are:</p> <ul style="list-style-type: none">• Yes: The phone activates peer verification for incoming secure SIP connections.• No. This is the default setting.
Verify Server	<p>To enable or disable Verify Server. The options are:</p> <ul style="list-style-type: none">• 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 ends the connection for a non-valid server certificate.• No. This is the default setting.
Require Client Certificate	<p>To enable or disable client certificate verification. The options are:</p> <ul style="list-style-type: none">• Yes: The phone rejects incoming secure SIP connections if the client does not have a valid certificate.• No. This is the default setting.
Negotiation Timeout	<p>To specify the time-out 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 stops the negotiation. To disable the time-out, enter 0.</p> <p>The value range is from 0 to 7200. The default setting is 0 seconds.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
Certificate	<p>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, 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.</p> <p> ⓘ This setting is available only through the web interface in the SIP section.</p>
CA Certificate	<p>To upload a certificate for TLS or SIPS communication received from a Certificate Authority (CA). Use it to verify other certificates. You need the CA certificate if you have Verify Server or Verify Client enabled.</p> <p> ⓘ This setting is available only through the web interface in the SIP section.</p>
Private Key	<p>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.</p> <p> ⓘ This setting is available only through the web interface in the SIP section.</p>
Password	<p>To specify the password used for encryption of the private key if it is encrypted.</p> <p>Valid password is a single string that can have any characters in it except for the line break. The length of the password must not exceed 32 characters.</p>
Primary Account	

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
Account Name	<p>To set the name for the primary account displayed locally on the screen according to the existing corporate standards.</p> <p>❗ In USB only user mode the phone does not display the account name on the home screen in Idle mode.</p>
User	<p>To set the account or customer name for the primary account.</p> <p>Do not use the following characters: #%@.</p>
Registrar	<p>To specify the IP address or the FQDN of the SIP server where the primary account is registered. For example, use the 10.10.1.100 format for a local SIP server or the sip.company.net format for a public VoIP service provider.</p> <p>The value range for port number is from 0 to 65535.</p>
Proxy	<p>To specify the Universal Resource Identifier (URI) of the proxy server used by the primary account.</p>
Keep Alive	<p>To make the phone maintain an active connection to the network. The options are:</p> <ul style="list-style-type: none"> • Yes: If you select this, the phone renews the connection of the phone primary account to the network. • No. This is the default setting.
Realm	<p>To specify the SIP 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.</p> <p>Your input strings must be in one of the following formats:</p> <ul style="list-style-type: none"> • * (except for the following characters: # %). This can be any SIP host for authorization. • <hostname> • <sip_user>@<hostname>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT


Name	Description
Authentication Name	To specify the SIP name to use in authentication.
Password	<p>To define the password for the Realm or domain authentication in the primary account.</p> <p> You can configure this parameter if you log in with the administrator password.</p> <p>On the phone, the password can be configured in Settings > SIP > Primary Account > Credentials.</p> <p>Valid password is a single string that can have any characters in it except for the line break. The length of the password must not exceed 32 characters.</p>
Registration Timeout	<p>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.</p> <p>The value range is from 1 to 7200. The default value is 300 seconds.</p>
Secondary Account	
Account Name	To set the name for the secondary account displayed locally on the screen according to the existing corporate standards.
User	<p>To set the account or customer name for the secondary account.</p> <p>Do not use the following characters: #%@.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT


Name	Description
Registrar	<p>To specify the IP address or the FQDN of the SIP server where the secondary account is registered.</p> <p>The accepted input is a string composed of digits or letters, and a '-' character. Digits after the : symbol specify port number. The port number value range is from 0 to 65535.</p> <p>Example: 0-mht.be-1.a-1s-o45.t-ha-t4:65535</p>
Proxy	<p>To specify the URI of the proxy server used by the secondary account.</p>
Keep Alive	<p>To make the phone maintain an active connection to the network with the secondary account.</p>
Realm	<p>To specify the SIP domain where the SIP authentication of the secondary account with the name and password is valid.</p> <p>Your input strings must be in one of the following formats:</p> <ul style="list-style-type: none"> • * (except for the following characters: # %). This can be any SIP host for authorization. • <hostname> • <sip_user>@<hostname>
Authentication Name	<p>To specify the number that is assigned to the user in the secondary account.</p>
Password	<p>To define the password for the Realm or domain authentication in the secondary account.</p> <p> You can configure this parameter if you log in with the administrator password.</p> <p>On the phone, the password can be configured in Settings > SIP > Secondary Account > Credentials.</p> <p>Valid password is a single string that can have any characters in it except for the line break. The length of the password must not exceed 32 characters.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
Registration Timeout	<p>To specify the time when the registration of the secondary account expires and the SIP server is sent a corresponding request.</p> <p>The value range is from 1 to 7200. The default value is 300 seconds.</p>
Fallback Account	
Account Name	<p>To set the name for the fallback account displayed locally on the screen according to the existing corporate standards.</p>
User	<p>To set the account or customer name for the fallback account.</p> <p>Do not use the following characters: # % @.</p>
Registrar	<p>To specify the IP address or the FQDN of the SIP server where the fallback account is registered.</p> <p>The accepted input is a string composed of digits or letters, and a '-' character. Digits after the : symbol specify port number. The port number value range is from 0 to 65535.</p> <p>Example: 0-mht.be-1.a-1s-o45.t-ha-t4:65535</p>
Proxy	<p>To specify the URI of the proxy server used by the fallback account.</p>
Keep Alive	<p>To make the phone maintain an active connection to the network with the fallback account.</p>
Realm	<p>To specify the SIP domain where the SIP authentication of the fallback account with the name and password is valid.</p> <p>Your input strings must be in one of the following formats:</p> <ul style="list-style-type: none"> • * (except for the following characters: # %). This can be any SIP host for authorization. • <hostname> • <sip_user>@<hostname>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
Authentication Name	To specify the number that is assigned to the user in the fallback account.
Password	<p>To define the password for the Realm or domain authentication in the fallback account.</p> <p> ⓘ You can configure this parameter if you log in with the administrator password.</p> <p>On the phone, the password can be configured in Settings > SIP > Fallback Account > Credentials.</p> <p>Valid password is a single string that can have any characters in it except for the line break. The length of the password must not exceed 32 characters.</p>
Registration Timeout	<p>To specify the time when the registration of the fallback account expires and the SIP server is sent a corresponding request.</p> <p>The value range is from 1 to 7200. The default value is 300 seconds.</p>
DTMF	

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
DTMF Method	<p>To define the Dual-tone multi-frequency (DTMF) signaling method. The options are:</p> <ul style="list-style-type: none"> • RFC 4733. With this method, DTMF signals are carried in RTP packets by using a separate RTP payload format. It is set by default. • SIP Info. With this method, the DTMF signals are sent as SIP requests. The SIP switch creates the tones if the call is transferred to the PSTN. • In-band. With this method, the phone generates the tones and sends them in the voice frequency band. <p>ⓘ Use RFC 4733 or SIP Info as the preferred methods because they are more consistent with other tones available. Switch to In-band only when your SIP server does not support other DTMF signaling methods.</p> <p>ⓘ When RFC 4733 is configured as the DTMF method on Konftel 800, but the other party does not accept such method during SIP negotiation, the phone falls back into using the In-band method.</p>
RFC 4733 Payload Type	<p>To specify the type of audio traffic. The range is from 96 to 127. By default, it is payload type 101.</p>
Advanced	
Disable 'rport'	<p>To enable or disable remote port forwarding. By default, the setting is disabled.</p>
Session Timers	<p>To set a time-related mechanism to disconnect the sessions that the phone establishes. The options are:</p> <ul style="list-style-type: none"> • Disabled. This is the default setting. • Optional • Mandatory
Session Expiration	<p>To specify the session expiration time in seconds.</p> <p>The value range is from 0 to 2147483647. The default setting is 1800 seconds.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
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. By default, the setting is disabled.
Allow Contact Rewrite	To enable or disable storing the IP address from the response of the register request. If there is a change detected, the phone unregisters the available SIP URI (contact) and updates it with the new address. By default, the setting is enabled.
Allow Via Rewrite	To enable or disable rewriting of the VIA header in the SIP REGISTER requests. If there is a change detected, the phone overwrites the VIA header with the new data. By default, the setting is enabled.
Enable SIP Replaces	To enable or disable the SIP <code>Replaces</code> header.

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT


Name	Description
Use Static Source Port	<p>To enable or disable using static source ports for the SIP signaling. When Konftel 800 has a configured SIP account, it can handle firewalls differently. The options are:</p> <ul style="list-style-type: none">• Use static port number for outgoing TCP and TLS packets. The configuration parameter <code><use_static_source_port></code> is set to <code>true</code> in the configuration file. You must configure the <code><source_port></code> parameter to specify the source ports of TCP and TLS packets. By default, the source ports are the following:<ul style="list-style-type: none">• UDP/TCP: 5060.• TLS: 5061.• Use ephemeral source ports for outgoing TCP and TLS packets. Here the configuration parameter <code><use_static_source_port></code> is set to <code>false</code> in the configuration file. <p>By default, the setting is disabled.</p> <p> To configure this parameter, only use the configuration file.</p>
NAT Traversal	<p>Enable ICE</p> <p>To enable or disable the Interactive Connectivity Establishment (ICE). ICE provides various techniques to allow SIP-based VoIP devices to successfully traverse the variety of firewalls that might exist between the devices. The protocol provides a mechanism for the endpoints to identify the most optimal path for the media traffic to follow.</p> <p>By default, the setting is disabled.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT



Name	Description
Enable STUN	<p>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 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.</p> <p>By default, the setting is disabled.</p> <p> Another definition of STUN is the Session Traversal Utilities for NAT.</p>
STUN Server	<p>To enter the IP address or the public name of the STUN server.</p> <p>The accepted input is a string composed of digits or letters and a '-' character.</p> <p>For example, <code>0-mht.be-1.a-1s-o45.t-ha-t4</code>.</p>
Enable TURN	<p>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 has 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.</p> <p>By default, the setting is disabled.</p> <p> To enable TURN, you must enable ICE.</p>

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Name	Description
TURN Server	<p>To enter the IP address or the public name of the TURN server.</p> <p>The accepted input is a string composed of digits or letters, and a '-' character. Digits after the : symbol specify port number. The port number value range is from 0 to 65535.</p> <p>For example, 0-mht.be-1.a-1s-o45.t-ha-t4:65535.</p>
User	<p>To specify the user authentication name on the TURN server.</p>
Password	<p>To enter the user authentication password on the TURN server.</p> <p>Valid password is a single string that can have any characters in it except for the line break. The length of the password must not exceed 32 characters.</p>

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

SIP account registration status

SIP account is a specifically configured set of credentials that provides access to SIP telephony and allows users to make calls from the phone. The SIP settings on Konftel 800 provide for configuring the primary account, the secondary account, and the fallback account.

If the phone has several configured SIP accounts, but there is only one registered account, the phone displays the name of the registered account on its idle home screen.

You can tell if the phone has a configured and registered SIP account or problems with the SIP account registration by looking at its home screen. The following options are available:

- The phone has no SIP account configured. Konftel 800 displays the phone name, the **Bluetooth** and **Settings** buttons on its idle home screen. The phone does not display the account name.
- The phone has the SIP account configured but not registered. For example, this can be due to invalid credentials of the SIP account or network problems. Konftel 800 displays the **Warning** icon, the account name, the **Recent**, **Call**, **Unite**, and **Settings** buttons on its idle home screen. When you tap the account

SETTINGS CONFIGURATION AND MANAGEMENT

name or the **Warning** icon, the phone displays the following pop-up message: No sip service registered (Wrong username/password or registrar?). It disappears automatically after a certain timeout, or you can tap **Ok** to return to the home screen.

- The phone has the SIP account configured and registered. The phone displays the phone name, the account name, the **Recent**, **Call**, **Unite**, and **Settings** buttons on the idle home screen.

You can use Konftel 800 regardless of the SIP account registration status. When the phone has no SIP account configured or registered, it acts as a speakerphone that you can use to conduct virtual meetings and listen to audio files.

Related information

[Phone settings description](#) on page 33

Caller information presentation

Konftel 800 displays the calling person information to show who is calling or display that the caller ID is unknown. This data is available on the **Incoming Call**, **Active Call**, and **Recent Call List** screens.

The phone shows the information that it receives from the caller's SIP invite message. It includes the following:

- CNAM: Usually specifies the contact name.
- CID: Usually specifies the caller's phone number.

For example, when Konftel 800 receives the SIP invite message `From: "John Doe" <sip:1234@192.168.1.4>`, John Doe is the CNAM and 1234 is the CID.

The following table lists the screen information, which Konftel 800 displays, depending on the parameters the server provides:

Screen	Description
Incoming Call	Konftel 800 displays the CNAM and the CID. If the server does not provide the CID, the phone displays the CNAM. If the server does not provide the CNAM or the CID, the phone displays Unknown.

Table continued...

SETTINGS CONFIGURATION AND MANAGEMENT

Screen	Description
Active Call	Konftel 800 displays the CNAM. If the server does not provide the CNAM, the phone displays the CID. If the server does not provide the CNAM or the CID, the phone displays <i>Unknown</i> .
Recent Call List	Konftel 800 displays the CID. If the server does not provide the CID, the phone displays <i>Unknown</i> .

CERTIFICATES APPLICATION

Use certificates to authenticate Konftel 800 using TLS. You can apply certificates manually when configuring the advanced settings of your phone, or the phone can automatically download the certificates from the provisioning server if you enabled Device Management.

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

Related concepts

[Provisioning on Konftel 800](#) on page 121

Downloading the root certificate

About this task

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

Before you begin

Connect to Microsoft Server Certification Authority.

SETTINGS CONFIGURATION AND MANAGEMENT

Procedure

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

Installing the certificate

About this task

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. The following is the procedure for Google Chrome. For information about other web browser applications, see the instructions provided by the software manufacturers.

Before you begin

Open your web browser.

Procedure

- ⇒ Click **Settings > Advanced > Privacy and security > Manage certificates**.
- ⇒ In the **Certificates** window, click **Import**.
- ⇒ In the **Certificate Export Wizard** window, click **Next** to proceed.
- ⇒ Specify the file you want to import and click **Next**.
- ⇒ Choose the key store for the certificate and click **Next**.
- ⇒ Click **Finish**.

Exporting the private key

About this task

Use this procedure to export the private key that the phone will apply for authentication using TLS/SIPS and EAP-TLS. You can use your regular web browser. The following is the procedure for Google Chrome. For information about other web browser applications, see the instructions provided by the software manufacturers.

Before you begin

Open your web browser.

Procedure

- ⇒ Click **Settings > Advanced > Privacy and security > Manage certificates**.
- ⇒ In the **Certificates** window, select the certificate to export and click **Export**.

SETTINGS CONFIGURATION AND MANAGEMENT

- ⇒ In the **Certificate Export Wizard** window, click **Next** to proceed.
- ⇒ Click **Yes** to export the private key.
- ⇒ Select the format in which you want to export the private key file and click **Next**.
- ⇒ Specify the file name, choose the location to export the certificate, and click **Next**.
- ⇒ Click **Finish**.

Converting the certificates to .PEM format

About this task

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

Procedure

- ⇒ Use the following Openssl commands to convert the files:

From .DER to .PEM:

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

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.

STANDARD ENCRYPTION ALGORITHMS

Konftel 800 uses encryption algorithms that comply with the current industry standards. Currently, the phone supports the data integrity algorithms with no publicly known vulnerabilities and are the US National Institute of Standards and Technology approved.

Standard encryption algorithms for the external connections to the system (for example, TLS) include the following:

- Symmetric Encryption:
 - AES 256 (required)
 - AES 192 and AES 128 (optional)
- Asymmetric Encryption:
 - RSA: 2048 (required) and 4096 (optional)

SETTINGS CONFIGURATION AND MANAGEMENT

- DH: 2048 (required) and 4096 (optional)
- ECC: secp384r1 and secp256r1 (required)
- Hash Algorithms
 - SHA2 (required)
 - SHA3 (optional)
- Hashed Message Authentication Code:
 - HMAC-SHA2 (required)
 - HMAC-SHA1 (used for integrity and routing)

Konftel 800 provides support to specific FIPS-related encryption algorithms, which makes it ready for operation in FIPS mode.

When you need legacy or non-standard encryption algorithms for the external connections, you can use Legacy encryption mode. In this case the phone works with the encryption algorithms applied before R.1.0.4.

Standard encryption application areas:

- Web pages for administration
- SIP with TLS
- Device management to HTTPS server
- LDAP with TLS
- Media encryption with SRTP
- 802.1x

Related information

[Encryption methods in Legacy encryption mode](#) on page 178

Standard encryption for 802.1x

You can configure Konftel 800 to allow 802.1x authentication to use EAP MD5 method.

If you need to use EAP MD5 method for 802.1x, ensure that you set the **Allow Legacy Encryption** option to true and **FIPS Mode** to false. When you try to enable **EAP MD5** while **Allow Legacy Encryption** is disabled, the phone warns you with the following message: `EAP MD5 requires Allow Legacy Encryption to be enabled.` When you try to enable **Allow Legacy Encryption** while **FIPS Mode** is enabled, the phone warns you with the following message: `Allow Legacy Encryption cannot be enabled while FIPS mode is enabled.`

You can configure Konftel 800 to allow 802.1x authentication to use EAP MD5 method on the phone, through the web interface, or using a configuration file.

SETTINGS CONFIGURATION AND MANAGEMENT

When you upgrade the phone from a version without the legacy encryption option and enable EAP MD5 method, the phone automatically enables the **Allow Legacy Encryption** option.

- ① When you import a configuration file, the phone settings update in line with the imported configuration file. If the value of `<eap_md5>` is set to `true`, you must also set the value of `<allow_legacy_encryption>` to `true`.

Related tasks

[Importing the configuration file](#) on page 144

Related information

[Configuration file structure](#) on page 126

[Network settings description](#) on page 48

Enabling EAP MD5 for 802.1x on the phone

About this task

Use this procedure to configure 802.1x and EAP MD5 method for 802.1x on the phone.

Before you begin

- Disable **FIPS Mode**.

You cannot enable **EAP MD5 Enable** if **FIPS Mode** is enabled. If you try to enable it, the phone shows the following warning message: `EAP MD5 requires FIPS mode to be disabled.`

- Enable **Allow Legacy Encryption**.

You cannot enable **EAP MD5 Enable** if **Allow Legacy Encryption** is disabled. If you try to enable it, the phone shows the following warning message: `EAP MD5 requires Allow Legacy Encryption to be enabled.`

Procedure

- ⇒ Log in as the administrator.
- ⇒ Navigate to **Network > 802.1x**, and move the **802.1x** slider to the right to enable 802.1x.
- ⇒ In the **Authentication Name** field, enter the authentication name.
- ⇒ Activate **EAP MD5 Enable**.
- ⇒ In the **EAP-MD5 Password** field, enter the password for EAP MD5.
- ⇒ Tap the `<` icon three times to return to the home screen.

The phone reboots to apply the changes.

SETTINGS CONFIGURATION AND MANAGEMENT

Related tasks

[Configuring Legacy encryption mode on the phone](#) on page 94

Enabling EAP MD5 for 802.1x through the web interface

About this task

Use this procedure to configure 802.1x and EAP MD5 method for 802.1x through the web interface.

Before you begin

- Disable **FIPS Mode**.

You cannot enable **EAP MD5** if **FIPS Mode** is enabled. If you try to do it, the phone shows the following warning message: `EAP MD5 requires FIPS mode to be disabled.`

- Enable **Allow Legacy Encryption**.

You cannot enable **EAP MD5** if **Allow Legacy Encryption** is disabled. If you try to do it, the phone shows the following warning message: `EAP MD5 requires Allow Legacy Encryption to be enabled.`

Procedure

- ⇒ Log in as the administrator.
- ⇒ Choose the **Network** tab.
- ⇒ In the **802.1x** section, enable **Enable 802.1x**.
- ⇒ In the **Username** field, enter the user name.
- ⇒ To activate EAP MD5 method for 802.1x, enable **EAP MD5 Enable**.

The **EAP MD5** section becomes visible.

- ⇒ In the **Password** field, enter the password for EAP MD5.
- ⇒ Click **Save**.

The phone reboots to apply the changes.

Related tasks

[Configuring Legacy encryption mode through the web interface](#) on page 95

Standard encryption for media encryption with SRTP

When the key exchange for media encryption with SRTP occurs, Konftel 800 supports the `AES_256_CM_HMAC_SHA1_80` mandatory crypto.

SETTINGS CONFIGURATION AND MANAGEMENT

Some servers do not support this mandatory crypto. In this case you must enable the **Allow Legacy Encryption** option to make an SRTP call. By default, it is disabled.

In this case, with Legacy encryption mode enabled, the phone offers AES_CM_128_HMAC_SHA1_80 crypto only.

Legacy encryption mode

Konftel 800 also supports specific legacy encryption algorithms. If you enable Legacy encryption mode, the phone offers all the previously supported ciphers for the SSL negotiation and cryptos for SRTP. You can check the offered ciphers using a specialized network protocol analyzer. At that, the phone supports the legacy encryption algorithms only for backward compatibility.

By default, this feature is enabled.

Firmware upgrade

When you upgrade Konftel 800 from a version without the legacy encryption option, the phone automatically enables the **Allow Legacy Encryption** option. When you reset Konftel 800 to the factory default state, the phone also enables the **Allow Legacy Encryption** option.

When upgrading, the phone automatically enables the **Allow Legacy Encryption** option, if **802.1x** with **EAP MD5** is enabled.

Related information

[Encryption methods in Legacy encryption mode](#) on page 178

Configuring Legacy encryption mode on the phone

About this task

Use this procedure to configure Legacy encryption mode of your Konftel 800 on the phone.

If you configure the phone to allow 802.1x authentication to use EAP MD5 method, you cannot disable legacy encryption. The phone warns you with a message: Allow Legacy Encryption cannot be turned off while 802.1x with EAP MD5 is enabled.

If you configure the phone to enable FIPS mode, you cannot enable Legacy encryption mode. The phone warns you with a message: Allow Legacy Encryption cannot be enabled while FIPS Mode is enabled.

SETTINGS CONFIGURATION AND MANAGEMENT

Before you begin

Log in as the administrator.

Procedure

- ⇒ In the **Settings** menu, tap **Phone > Security**.
- ⇒ Enable **Allow Legacy Encryption**.
- ⇒ Tap the < icon three times to return to the home screen.

The phone reboots to apply the changes.

Configuring Legacy encryption mode through the web interface

About this task

Use this procedure to configure Legacy encryption mode of your Konftel 800 through the web interface.

If you configure the phone to allow 802.1x authentication to use EAP MD5 method, you cannot disable legacy encryption. The phone warns you with a message: `Allow Legacy Encryption cannot be turned off while 802.1x with EAP MD5 is enabled.`

If you configure the phone to enable FIPS mode, you cannot enable Legacy encryption mode. The phone warns you with a message: `Allow Legacy Encryption cannot be enabled while FIPS mode is enabled.`

Before you begin

Log in to the web interface as the administrator.

Procedure

- ⇒ Click **Phone**.
- ⇒ In the **Advanced** section, enable **Allow Legacy Encryption**.
- ⇒ Click **Save**.

The phone reboots to apply the changes.

Configuring Legacy encryption mode using the configuration file

About this task

Use this procedure to configure Legacy encryption mode of your Konftel 800 using the .xml configuration file. When you boot the phone after successful provisioning, the setting file changes, depending on the configuration of the standard encryption use.

SETTINGS CONFIGURATION AND MANAGEMENT

Before you begin

Get the configuration .xml file for Konftel 800.

Procedure

- ⇒ Open the configuration file.
- ⇒ In the <phone> section, locate <allow_legacy_encryption> tag and set the value to true.
- ⇒ Save the configuration file.

Next steps

Upload the configuration file to the Device Management server or import the configuration file to the phone using the web interface.

Related tasks

[Importing the configuration file](#) on page 144

Related information

[Configuration file structure](#) on page 126

FIPS MODE

Konftel 800 supports a specific FIPS mode to make the encryption and cryptographic functions compliant with Federal Information Processing Standards (FIPS). When you enable FIPS mode, the phone employs approved key exchange algorithms, cryptographic algorithms and authentication techniques to meet the FIPS 140-2 requirements.

When Konftel 800 needs cryptographically secure numbers, it uses random number generator functions from FIPS 140-x compliant cryptographic libraries. A specific FIPS approved random number generator renders cryptographic number initialization vectors.

With FIPS mode enabled, the device management with HTTPS server occurs using the SSL encryption method.

By default, FIPS mode is disabled.

- ❗ If you configure the phone to allow legacy encryption, you cannot enable FIPS mode. You will see a popup message: `FIPS mode cannot be enabled while Allow Legacy Encryption is enabled.`

If you configure the phone to use 802.1x with EAP MD5, you cannot enable FIPS mode. The phone warns you with a message: `FIPS mode cannot be enabled while 802.1x with EAP MD5 is enabled.`

SETTINGS CONFIGURATION AND MANAGEMENT

Related concepts

[Standard encryption for 802.1x](#) on page 91

[Legacy encryption mode](#) on page 94

FIPS mode for media encryption with SRTP

When the key exchange for media encryption with SRTP occurs with FIPS mode enabled, Konftel 800 supports only one mandatory crypto

AES_256_CM_HMAC_SHA1_80.

The conference phone supports only the same mandatory crypto

AES_256_CM_HMAC_SHA1_80 when both **FIPS Mode** and **Allow Legacy**

Encryption are disabled.

When the administrator disables **FIPS Mode** and enables **Allow Legacy**

Encryption, Konftel 800 supports only AES_CM_128_HMAC_SHA1_80 for media encryption with SRTP.

Configuring FIPS mode on the phone

About this task

Use this procedure to configure FIPS mode of your Konftel 800 on the phone.

Before you begin

- Log in as the administrator.
- Disable **Allow Legacy Encryption** and EAP MD5 method for 802.1x.

Procedure

- ⇒ In the **Settings** menu, tap **Phone > Security**.
- ⇒ Enable **FIPS Mode**.
- ⇒ Tap the < icon three times to return to the home screen.

The phone reboots to apply the changes.

Related concepts

[Legacy encryption mode](#) on page 94

[Standard encryption for 802.1x](#) on page 91

SETTINGS CONFIGURATION AND MANAGEMENT

Configuring FIPS mode through the web interface

About this task

Use this procedure to configure FIPS mode of your Konftel 800 through the web interface.

Before you begin

- Log in as the administrator.
- Disable **Allow Legacy Encryption** and EAP MD5 method for 802.1x.

Procedure

- ⇒ Click **Phone**.
- ⇒ In the **Advanced** section, enable **FIPS Mode**.
- ⇒ Click **Save**.

The phone reboots to apply the changes.

Related concepts

[Legacy encryption mode](#) on page 94

[Standard encryption for 802.1x](#) on page 91

Configuring FIPS mode using the configuration file

About this task

Use this procedure to configure FIPS mode of your Konftel 800 using the .xml configuration file. When you boot the phone after successful provisioning, the setting file changes, depending on the configuration of the standard encryption use.

Before you begin

Get the configuration .xml file for Konftel 800.

Procedure

- ⇒ Open the configuration file.
- ⇒ In the `<phone>` section, locate `<fips_mode>` tag and set the value to true.

By default, the value is false.

- ⇒ Save the configuration file.

The phone reboots, if the FIPS mode value differs from the previously configured value.

SETTINGS CONFIGURATION AND MANAGEMENT

Next steps

Upload the configuration file to the Device Management server or import the configuration file to the phone using the web interface.

Related tasks

[Importing the configuration file](#) on page 144

Related information

[Configuration file structure](#) on page 126

USB ONLY USER MODE

Konftel 800 supports USB only user mode. With this feature, the conference phone can operate with no SIP account and SIP register configured. In USB only user mode Konftel 800 acts as a speakerphone that the user can use to conduct virtual meetings and listen to audio files.

USB and Bluetooth® connection

In USB only user mode, the phone operates as a USB device connected to a USB host.

In this mode, the phone supports connection to Bluetooth® devices using Bluetooth® Classic.

- ① The administrator can use the configuration file to disable Bluetooth®. The **Bluetooth** button becomes inactive, and if the user taps it, the phone shows the following message: `Bluetooth is disabled by the administrator.`

When idle, Konftel 800 does not display **Account Name** on the home screen in USB only user mode. The user can see the phone name and the connection option as follows:

- When the user connects the phone using USB, Konftel 800 indicates `USB audio` on the home screen.
- When the user uses Bluetooth® to connect the phone, Konftel 800 indicates `Bluetooth® audio` on the home screen.
- When the user uses both Bluetooth® and USB for connection, Konftel 800 indicates `Bluetooth® audio` on the home screen.

Time presentation in USB only user mode

When the phone has NTP server settings enabled but it cannot connect to the NTP server in USB only user mode, Konftel 800 does not display time on the home screen and in the settings menu.

SETTINGS CONFIGURATION AND MANAGEMENT

When the phone has NTP server settings disabled, the user can set the time manually. Then the options of the time presentation are the following:

- On the home screen when there is no active Bluetooth® or USB connection.
- On the status bar when the user connects to Konftel 800 using Bluetooth® or USB.

Related concepts

[Provision of the NTP server address](#) on page 45

[Firmware upgrade and downgrade](#) on page 121

Time presentation in USB only user mode


When the phone has NTP server settings enabled but it cannot connect to the NTP server in USB only user mode, Konftel 800 does not display time on the home screen and in the settings menu.

When the phone has NTP server settings disabled, the user can set the time manually. Then the options of the time presentation are the following:



- On the home screen when there is no active Bluetooth® or USB connection.
- On the status bar when the user connects to Konftel 800 using Bluetooth® or USB.

USB only user mode icons

The following table shows the icons on the home screen of Konftel 800 in USB only user mode:

Icon	Name	Description
	USB Connected	To indicate an active USB connection. The phone displays the USB Connected icon and shows <code>USB audio</code> on the idle home screen.

SETTINGS CONFIGURATION AND MANAGEMENT

Icon	Name	Description
	Bluetooth connection	<p>To configure Bluetooth® Classic settings and to indicate an active Bluetooth® Classic connection.</p> <p>The phone shows the Bluetooth connection icon and Bluetooth® audio indication on the idle home screen.</p> <p>ⓘ If the administrator uses the .xml configuration file to disable Bluetooth®, then the Bluetooth connection icon is inactive.</p>
	Settings	<p>To check and configure the settings from the phone. View the phone status and reach the menu.</p> <p>The following settings are available in USB only user mode:</p> <ul style="list-style-type: none"> • Status • Phone • Konftel Unite • Bluetooth • Admin Login

- ⓘ When Konftel 800 shows either the **USB Connected** or the **Bluetooth connection** icon on the idle home screen, the phone displays time on the status bar.

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. Download and install Konftel Unite free from App Store and Google Play like any other application. 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. For example, answer and hang up the call, mute and unmute the microphone, dial a number, adjust the volume level, and hold and resume the call.

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.

Starting from R 1.0.4, Konftel 800 uses SHA256 method for challenge-response authentication to connect to Konftel Unite.

- ① If your conference phone fails to connect to Konftel Unite, you must download a newer version of the application from App Store or Google Play. It works both with R 1.0.4 and earlier released firmware.

Configure Konftel Unite parameters on the phone and from the mobile device with the application installed.

Pairing and connecting devices

About this task

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.

- ① You can pair up to 100 mobile phones or tablets with your Konftel 800. But only one user connection is active at a time.

FEATURES AND ACCESSORIES

Before you begin

Install Konftel Unite on your mobile device.

Procedure

⇒ 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 for about 30 seconds.

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

⇒ Tap **Enter** on the conference phone to start pairing.

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

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

- ⓘ You cannot connect Konftel 800 to a Bluetooth® device for call handling or audio streaming while the Konftel Unite connection is active.

Disconnecting devices

About this task

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

Before you begin

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

Procedure

- To disconnect from the mobile device, do the following:
In Konftel Unite, tap the connection symbol in the upper left corner of the screen.

FEATURES AND ACCESSORIES

Optional: Under **Change device**, select another conference phone to connect to.

You can do it if there are other conference phones available nearby.

The application starts connecting to the selected conference phone.

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 Konftel 800, do one of the following:
 - Tap **Konftel Unite > Disconnect Device**.
 - Tap **Settings > Konftel Unite > Disconnect Device**.

The phone displays the following question: `Disconnect device <Device Name>?`

To confirm, tap **Ok**.

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

Deleting pairing

About this task

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

Before you begin

Pair Konftel 800 with a mobile device with Konftel Unite.

Procedure

- ⇒ To delete the pairing from the conference phone, on the home screen, do one of the following:
 - Tap **Konftel Unite**.
 - Tap **Settings > Konftel Unite**.
- ⇒ Tap **Remove Bonding Information**.
- ⇒ Tap **Ok** to confirm removal of all bonding information from the device.

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.

FEATURES AND ACCESSORIES

Configuring the Konftel Unite settings

About this task

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

Procedure

- ⇒ 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

The following table lists the parameters for Konftel 800, which you can set from the Konftel Unite interface:

Name	Description
Connection	To enable or disable the connection to Konftel 800. The options are: <ul style="list-style-type: none">• 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.
Moderator code	To join the scheduled conference calls as a moderator. You must enter respective codes in the following fields: <ul style="list-style-type: none">• 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.

Table continued...

FEATURES AND ACCESSORIES

Name	Description
My bridge	<p>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.</p> <p>The My bridge button appears in the calendar view.</p>
Meeting notification	<p>To set a reminder about a call. The options are:</p> <ul style="list-style-type: none">• 5 minutes before• 10 minutes before• 15 minutes before• Never
Calendars to show	<p>To select the calendars in the mobile phone from which you want Konftel Unite to take the information.</p>
Tell a colleague	<p>To share information about Konftel Unite with a person that you want. You can do it by using an email application.</p> <p>After you confirm that Konftel Unite can access 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.</p>
Read more about Konftel Unite	<p>To get additional information about Konftel Unite. The application forwards you to the web site with the corresponding information.</p>
Feedback and support	<p>To share your experience of using the application and request for support. The options are:</p> <ul style="list-style-type: none">• A messenger, for example, Viber, WhatsApp, Telegram, and so on.• An email application.• Connection by Bluetooth®.

Table continued...

FEATURES AND ACCESSORIES

Name	Description
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

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. 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

Arrange 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
- Expansion microphone — Master phone — Slave phone

FEATURES AND ACCESSORIES

Functions of the Master and Slave devices

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 **Microphone Muted**.
- Send information to the master device when you adjust the volume on it.

① You cannot make calls between the Master and the Slave devices.

In a daisy chain, the Slave device follows the signal from the Master device to enter Sleep mode or Active mode.

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 5 W.

Connection of the Slave devices to the Master phone

In a daisy chain, Konftel 800 disables all unused daisy chain ports during active calls to provide for the best possible audio experience. That means, that the time, when a Slave device activates, is dependent on the Master phone status as follows:

- The Master phone is in the Idle state. When the user connects an expansion microphone or a Slave phone to the Master phone, Konftel 800 immediately detects it, and the connected device becomes directly available for operation.
- The Master phone has an active call. When the user connects an expansion microphone or a Slave phone to the Master phone, the connected device becomes available for operation only after the call ends.

The same approach is applicable when the user disconnects and reconnects an expansion microphone or a Slave phone to the Master phone during an active call. In this case, the connected device also becomes available for operation only after the call ends.

Functions of the Master and Slave devices

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:

FEATURES AND ACCESSORIES

- 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 **Microphone Muted**.
- Send information to the master device when you adjust the volume on it.

❗ You cannot make calls between the Master and the Slave devices.

In a daisy chain, the Slave device follows the signal from the Master device to enter Sleep mode or Active mode.

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 5 W.

Connection of the Slave devices to the Master phone

In a daisy chain, Konftel 800 disables all unused daisy chain ports during active calls to provide for the best possible audio experience. That means, that the time, when a Slave device activates, is dependent on the Master phone status as follows:

- The Master phone is in the Idle state. When the user connects an expansion microphone or a Slave phone to the Master phone, Konftel 800 immediately detects it, and the connected device becomes directly available for operation.
- The Master phone has an active call. When the user connects an expansion microphone or a Slave phone to the Master phone, the connected device becomes available for operation only after the call ends.

The same approach is applicable when the user disconnects and reconnects an expansion microphone or a Slave phone to the Master phone during an active call. In this case, the connected device also becomes available for operation only after the call ends.

Arranging a daisy chain

About this task

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

Before you begin

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 long. You can purchase the Daisy Chain kit as an accessory.

FEATURES AND ACCESSORIES

The cable of the Smart Mic is 3 m long.

Procedure

⇒ 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

About this task

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

Procedure

- To define the mode of your Konftel 800 on the phone, do the following:

Log in as the administrator.

In the **Settings** menu, tap **Phone > Daisy Chain**.

Select the required mode.

The options are:

- **Master**
- **Slave**

Tap the < icon three times to return to the home screen.

The phone restarts the application to apply the changes.

- To define the mode of your Konftel 800 through the web interface, do the following:

On the web interface, click **Phone**.

In **Daisy Chain Mode**, select the required mode from the drop-down list.

The options are:

- **Master**. This is the default mode.
- **Slave**

Click **Save**.

The slave unit displays the **Daisy Chain Mode** icon and the following message: *Daisy Chain*. This message remains for the period when the phone is in Slave mode within the daisy chain arrangement.

FEATURES AND ACCESSORIES

Disabling Daisy Chain mode

About this task

Use this procedure to disable Daisy Chain mode through the web interface or from the phone.

Before you begin

Ensure that the phone displays the **Daisy Chain** icon.

Procedure

- To disable Daisy Chain mode from the web interface, do the following:
 - On the web interface, click **Phone**.
 - In **Daisy Chain Mode**, select **Master**.
 - Click **Save**.
- To disable Daisy Chain mode from the phone, do the following:
 - Touch the phone screen and enter the administrator password.
 - Tap **Phone > Daisy Chain**.
 - Select **Master** mode.
 - Tap the < icon three times to return to the home screen.

Application restarts and restores the Master status.

EXPANSION MICROPHONE FIRMWARE UPGRADE

You can upgrade the expansion microphone firmware to the Konftel 800 firmware version when your Smart Mic has an older firmware installed. Regularly updating the expansion microphone firmware to match the phone firmware ensures the best possible audio performance.

The phone suggests an automatic upgrade of the expansion microphone firmware when you connect your Smart Mic to Konftel 800. You can connect one or two Smart Mics simultaneously.

You can also initiate the expansion microphone firmware upgrade manually.

If you connect the expansion microphone to Konftel 800 during an active call, the upgrade does not start until the call ends.

During the upgrade, the phone rejects all incoming and outgoing calls and does not activate the **Call Transfer** feature. At that Konftel 800 indicates that it is **Busy**.

FEATURES AND ACCESSORIES

Upgrading expansion microphone firmware

About this task

Use this procedure to upgrade the expansion microphone firmware when the Smart Mic and your device have different firmware installed.

Before you begin

Make sure Konftel 800 is in Idle Mode.

Procedure

- ⇒ Connect the expansion microphone to your conference phone using the available audio expansion port.

The expansion microphone LEDs flash red once.

A pop-up dialog window shows the following message: `A connected microphone needs firmware upgrade. Upgrade now?`

- ⇒ On the pop-up dialog window, tap **Yes** to start the upgrade.

The LEDs on the phone turn red to indicate that it is busy with the microphone upgrade. The expansion microphone LEDs start flashing green.

The phone displays the `Upgrade in progress` message and shows the upgrade progress in percentage (0%-100%).

When you connect one Smart Mic to Konftel 800, the phone shows the upgrade status for Smart Mic 2 as `N/A`.

Smart Mic 1: 10%

Smart Mic 2: N/A

- ⇒ Optional: To cancel the upgrade, tap **No**.

In this case, you postpone the upgrade until the phone reboots.

Result

If the upgrade is complete, the microphone LEDs turn off, and Konftel 800 displays the following message:

`Upgrade in progress`

`Smart Mic 1: Done`

`Smart Mic 2: N/A`

In 10 seconds, the pop-up dialog window hides, and the phone enters Idle mode.

FEATURES AND ACCESSORIES

If the Smart Mic firmware upgrade fails, the microphone LEDs turn off, and the phone displays the `Smart Mic 1: Failed` message.

Upgrading two expansion microphones

About this task

Use this procedure to upgrade two expansion microphones connected to your device simultaneously.

Before you begin

Connect Smart Mic 1 to the first audio expansion port of your conference phone.

Procedure

- ⇒ Connect Smart Mic 2 to your conference phone using the second audio expansion port.

The LEDs on the phone turn red to indicate that it is busy with the microphone upgrade. The Smart Mic 2 LEDs start flashing green.

A pop-up dialog window provides the expansion microphones upgrade status in the following format:

```
Smart Mic 1: 20%  
Smart Mic 2: 10%
```

- ⇒ Optional: Terminate Smart Mic 2 upgrade by detaching the expansion microphone from the phone.

In this case, you postpone the upgrade until you connect Smart Mic 2 again.

Result

When the upgrade is complete for Smart Mic 1 and Smart Mic 2 is still upgrading, the LED turns off on Smart Mic 1, and Konftel 800 displays the following message:

```
Upgrade in progress  
Smart Mic 1: Done  
Smart Mic 2: 86%
```

When the upgrade is complete for both microphones, their LEDs turn off, and Konftel 800 displays the following message:

```
Upgrade in progress  
Smart Mic 1: Done  
Smart Mic 2: Done
```

FEATURES AND ACCESSORIES

In 10 seconds, the pop-up dialog window hides, and the phone enters Idle mode.

If the firmware upgrade for any of the expansion microphones fails, the microphone LEDs turn off, and the phone displays the message stating the `Failed` status of the corresponding Smart Mic.

Terminating expansion microphone upgrade

About this task

Use this procedure to terminate the expansion microphone upgrade.

You can do it in the following cases:

- The phone has one Smart Mic 1 connected; or
- The phone has both Smart Mic 1 and Smart Mic 2 connected simultaneously.

Before you begin

Connect Smart Mic 1 and Smart Mic 2 to the phone and start the upgrade process for both expansion microphones.

Procedure

⇒ Detach Smart Mic 2 from the phone.

Smart Mic 1 continues upgrading with the value for the upgrade progress being updated.

Smart Mic 2 upgrade dialog indicates an error and aborts the mic upgrade. Konftel 800 displays the following message:

```
Upgrade in progress
Smart Mic 1: 50%
Smart Mic 2: Failed
```

When Smart Mic 1 upgrade is complete, its LED turns off, and Konftel 800 displays the following message:

```
Upgrade in progress
Smart Mic 1: Done
Smart Mic 2: Failed
```

This message disappears in 10 seconds.

⇒ Optional: To upgrade Smart Mic 2, connect it to the conference phone and proceed with the upgrade.

FEATURES AND ACCESSORIES

Upgrading Smart Expansion Microphone manually

About this task

Upgrade your expansion microphone manually when it is convenient to you.

Procedure

⇒ Hold the **Microphone Muted** button on the Smart Mic while you connect the microphone cable, and keep holding the button for 5 seconds after you inserted the cable.

When you release the button, it flashes red one time and then starts flashing green to indicate that the upgrade process has started. The LEDs on the phone turn red to indicate that it is busy with the microphone upgrade. The upgrade process takes about 7 minutes. When the upgrade is completed, the microphone LEDs turn off.



⇒ Check the microphone version by doing one of the following:

- On the phone screen, tap **Settings > Status**.
- On the web interface, go to the **Status** tab.

BLUETOOTH® CONNECTION

Konftel 800 can establish wireless communication over Bluetooth® with devices equipped with Bluetooth® connectivity, such as mobile phones, tablets, or computers. With Bluetooth®, you can use the phone as a speakerphone for call handling, or as an audio receiver for audio streaming.

The following table lists the Bluetooth® technologies that Konftel 800 supports:

Bluetooth® technology	Konftel 800 icon	Functionality
Bluetooth® LE		To connect to a mobile device with Konftel Unite application installed on it. For more information, see Konftel Unite on page 102. This is the default mode.
Bluetooth® Classic		To connect to Bluetooth® devices, such as mobile phones, tablets, and personal computers, for call handling or audio streaming.

FEATURES AND ACCESSORIES

Konftel 800 has a modified Pulse-code modulation (PCM) bus installed. This provides for a better audio transmission compared to the previous releases of the phone.

- ① You cannot use Bluetooth® LE and Bluetooth® Classic connection simultaneously.

If you connect Konftel 800 to a Bluetooth® device, you cannot connect it to a mobile device with the Konftel Unite application until you end the connection to the Bluetooth® device.

If you connect Konftel 800 to a mobile device using the Konftel Unite application, you cannot connect it to another Bluetooth® device until you end the connection to Konftel Unite.

In USB only user mode, the phone supports connection to Bluetooth® devices using Bluetooth® Classic.

Switching between the Bluetooth® modes

The default mode is Bluetooth® LE. To switch to Bluetooth® Classic, you must pair and connect Konftel 800 to a Bluetooth® device. When you select Bluetooth® Classic mode, the phone turns off Bluetooth® LE. If there is no Bluetooth® Classic connection, the phone switches back to Bluetooth® LE after a timeout.

In case of a successful Bluetooth® Classic connection, Konftel 800 restores Bluetooth® LE mode when you end the Bluetooth® Classic connection.

Bluetooth® Classic profiles

The following table describes the Bluetooth® Classic profiles that Konftel 800 supports:

Bluetooth® profile	Konftel 800 role	Functionality description
Hands-Free Profile (HFP)	Speakerphone	When Konftel 800 is paired with a Bluetooth® device, and the two devices are connected, the phone acts as a speakerphone. You can use the phone to handle Bluetooth® calls. Konftel 800 synchronizes the volume level with the volume level of the Bluetooth® device, and you can control the volume from both devices.

FEATURES AND ACCESSORIES

Bluetooth® profile	Konftel 800 role	Functionality description
Advanced Audio Distribution Profile (A2DP)	Audio receiver	<p>When Konftel 800 is paired with a Bluetooth® device, and the two devices are connected, Konftel 800 acts as an audio receiver. You can use the phone to stream multimedia audio from the Bluetooth® device.</p> <p>ⓘ You cannot activate A2DP during SIP or USB calls.</p>

ⓘ To use the Bluetooth® Classic functionality on Konftel 800, your Bluetooth® device must support HFP or A2DP or both.

Pairing and connecting Bluetooth® devices

About this task

To enable Bluetooth® communication between Konftel 800 and another Bluetooth® device, you must pair the two devices and ensure that they are in a connected state. The devices stay in a paired state until you remove the pairing.

ⓘ You can connect only one device supporting Bluetooth® at a time.

Procedure

⇒ On the Konftel 800 screen, tap **Settings > Bluetooth > Pair with device**.

The LEDs start flashing blue, and the phone displays the following message:
This phone is now discoverable as "<Phone Name>".

The time-out value for discoverable mode is 120 seconds.

ⓘ Tap **Cancel** to cancel pairing, for example, if you do not want to make the phone discoverable. In this case, you return to the **Bluetooth** menu.

⇒ On your Bluetooth® device, find Konftel 800 in the list of devices available for Bluetooth® connection and tap the phone name.

Konftel 800 establishes the connection with the Bluetooth® device and displays the Bluetooth® icon and one of the following messages:

- If Konftel 800 retrieves the device name from your Bluetooth® device, it displays **Connected to <your Bluetooth device name>**. For example, **Connected to My Smartphone**.

FEATURES AND ACCESSORIES

- If Konftel 800 does not retrieve the device name from your Bluetooth® device, it displays `Connected to <your device Bluetooth address>`. For example, `Connected to 00:11:22:33:FF:EE`.
- ① Konftel 800 is not visible in the Konftel Unite application while the conference phone and the Bluetooth® device are in the connected state.

Related concepts

[Phone settings description](#) on page 33

Removing Bluetooth® pairing

About this task

Use this procedure to remove the pairing between Konftel 800 and your other Bluetooth® device to delete unwanted pairings.

also deletes the Bluetooth® pairing information when you reset the phone to factory settings or perform system recovery.

- ① Removing Bluetooth® pairing as described below does not affect Konftel Unite pairing information.

Before you begin

Ensure that Konftel 800 and the Bluetooth® device are in the paired state.

Procedure

- ⇒ Tap **Settings > Bluetooth > Remove pairing**.

The phone displays the following question: `Do you want to remove all Bluetooth pairing information from the phone?`

- ⇒ To confirm that you want to delete the Bluetooth® pairing information, tap **Ok**.

The phone restarts the application to apply the changes.

Related tasks

[Logging in to the web interface of Konftel 800](#) on page 27

[Setting the password for Konftel 800](#) on page 24

Connection between paired Bluetooth® devices

Connection

After you pair Konftel 800 and your Bluetooth® device, the two devices establish the connection.

FEATURES AND ACCESSORIES

Disconnection

The connection ends if you manually disconnect Konftel 800 from the Bluetooth® device or if the distance between the devices does not allow to maintain the communication.

When the Bluetooth® device ends the connection, Konftel 800 displays the following message: `Disconnected` and then stops displaying the Bluetooth® icon.

Reconnection

You can reconnect your Bluetooth® device to Konftel 800 if the two devices are in a paired state. You can reconnect Konftel 800 to the paired Bluetooth® device only from the paired Bluetooth® device.

Bluetooth® radio

Konftel 800 supports the Bluetooth® radio feature, which makes the device visible to other Bluetooth® devices. By default, the Bluetooth® radio is in the enabled state. The administrator can disable the Bluetooth® radio. When disabled, Bluetooth® LE and Bluetooth® Classic connection are not available on Konftel 800.

Related concepts

[Bluetooth® connection](#) on page 115

Disabling Bluetooth® radio

About this task

Use this procedure to disable Bluetooth® radio using the `.xml` configuration file. The default value is `true`, which means that the feature is enabled.

Before you begin

Obtain the `.xml` configuration file for Konftel 800.

Procedure

⇒ In the configuration file, go to the `<bluetooth>` section.

⇒ Set the `<enable>` parameter to `false`.

```
<bluetooth>
  <enable type = "bool">false</enable>
</bluetooth>
```

⇒ Save and import the configuration file.

FEATURES AND ACCESSORIES

The phone restarts the application.

Related concepts

[Configuration file](#) on page 126

Related tasks

[Importing the configuration file](#) on page 144

MAINTENANCE

PROVISIONING ON KONFTEL 800

To ensure effective operation of your Konftel 800, you can upload to the phone the latest firmware version with the software update packages and configuration file with the necessary settings. You can upgrade and configure a single phone or multiple phones simultaneously.

Provisioning option	Upgrade and configuration description
Single phone	Use the phone web interface to upload a firmware file as well as to export and import a configuration file to Konftel 800.
Multiple phones	Use the Device Management feature to upgrade and configure multiple Konftel 800 phones simultaneously over a provisioning server. The Device Management settings are available both on the phone and through the web interface.

Firmware upgrade and downgrade

Starting from Release 1.0.1, you can both upgrade and downgrade the firmware of Konftel 800 using the Device Management. The phone application installs the firmware whenever the firmware version found in the firmware file downloaded from the provisioning server differs from the version of the currently running firmware.

When the upgrade or downgrade process starts, Konftel 800 performs the firmware upgrade file validation to ensure that no file data is corrupted.

- ⓘ The downgrade causes a factory reset and sets all user settings, configurations, and data to factory default.

Uploading a firmware file

About this task

Upgrade or downgrade your Konftel 800 using a firmware file stored on the local hard disk. When the phone starts to install the firmware file you uploaded, it

MAINTENANCE

identifies the firmware version and follows the upgrade or downgrade scenario based on the firmware version.

Before you begin

Download the appropriate firmware file and save it in a specified location on your personal computer.

Procedure

- ⇒ On the web interface, click **Provisioning**.
- ⇒ In the **Firmware** section, click the **Choose file** button.
- ⇒ Locate and select the downloaded firmware file.

The name of the chosen file is near the **Choose file** button.

- ⇒ Click **Save**.

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

Note that the phone must be in the idle state. If the phone is not in the idle state, you see the following message on the web interface: Phone is currently in "Busy" state, please retry later.

Next steps

If DHCP is used in the network, the IP address might change. If the web browser loses contact with Konftel 800, check the IP address on the phone.

Related tasks

[Viewing the IP address](#) on page 26

Firmware upgrade using check-sync

Konftel 800 automatically starts the firmware upgrade procedure when it receives a check-sync event from your SIP server. To use this feature, you must enable Device Management on your phone.

- ① The phone checks the firmware and starts the firmware upgrade only if the new firmware differs from the firmware installed.

If Konftel 800 receives a check-sync NOTIFY event in Idle Mode, it automatically starts the Device Management procedure, which includes downloading the firmware file. The phone is in Idle Mode when there are no active calls, it is not streaming music over USB or Bluetooth®, and the idle screen is active. If the phone receives the check-sync NOTIFY event during an active call, it waits till the call ends and then immediately starts downloading the provisioning data.

MAINTENANCE

Konftel 800 checks the check-sync message for the reboot parameter value:

Event: check-sync;reboot=true

or

Event: check-sync;reboot=false

If the reboot value is **true**, Konftel 800 reboots regardless of any available firmware upgrades or new configuration files. The phone applies the new configuration of firmware before the forced reboot. If the reboot value is **false** or not defined, the phone restarts the application, reboots, or does nothing depending on the requirements of the firmware upgrade or new configuration parameters in the configuration file.

Firmware upgrade and downgrade using a USB mass storage device

Konftel 800 uses the USB mass storage device to support firmware upgrade and downgrade without the web interface. When you connect the USB mass storage device to Konftel 800, the phone starts auto-mounting and finds the firmware file stored on the USB mass storage device. The auto-mounting and parsing process takes up to 30 seconds depending on your flash drive.

Before performing upgrade or downgrade, the phone does not compare the firmware version on the USB mass storage device and the currently used firmware version.

If the firmware file is invalid, the phone shows the following message: `Invalid upgrade file.`

- ① The phone starts the upgrade or downgrade procedure immediately if it is in Idle Mode. Otherwise, Konftel 800 ends an active operation and then starts the upgrade process.

It is impossible to make calls or enter any menu on the phone during the upgrade.

Konftel 800 blocks the upgrade procedure using the USB mass storage device, if the phone already starts the upgrading procedure using the Device Management provisioning server.

The phone supports several USB flash drive file systems including FAT32 and NTFS.

- ① Konftel 800 supports only one partition USB flash drives for the upgrade.

MAINTENANCE

If you set **Admin Password** in **Settings > Phone**, enter a valid administrator password before the phone starts the upgrade procedure.

- ① You can upgrade or downgrade the out-of-the-box Konftel 800 during the initial boot if you connect the USB mass storage device to the phone and follow the upgrade procedure.

Upgrading firmware using a USB mass storage device without the administrator password

About this task

Use this procedure to upgrade or downgrade your Konftel 800 using a USB mass storage device if you have no administrator password set.

Before you begin

- Download the appropriate firmware file and save it in a specified location on your personal computer.
- Upload the firmware file from your personal computer to the USB mass storage device root folder. The file name must be `upgrade.kt`.
- Make sure Konftel 800 is in Idle Mode.

Procedure

⇒ Connect the USB mass storage device to Konftel 800 USB port.

When checking for the appropriate firmware upgrade file, the phone shows the following message: `Checking upgrade file`. Then the phone displays the following message: `Firmware version x.x.x.x.x found on USB. Upgrade now?`, where `x.x.x.x.x` is the version of the valid firmware file.

⇒ Tap **Yes** to proceed with the upgrade.

The phone starts the upgrade procedure, showing the following message: `Upgrade in progress, please wait`. When the upgrade procedure ends, the phone reboots to apply the changes.

⇒ Optional: Tap **No** to discontinue the upgrade.

If you tap **No** accidentally, to restart the procedure, reconnect a USB mass storage device to Konftel 800 USB port.

Related tasks

[Uploading a firmware file](#) on page 121

MAINTENANCE

Upgrading the firmware using a USB mass storage device with the administrator password

About this task

Use this procedure to upgrade or downgrade your Konftel 800 using a USB mass storage device if you have an administrator password set.

Before you begin

- Download the appropriate firmware file and save it in a specified location on your personal computer.
- Upload the firmware file from your personal computer to the USB mass storage device root folder. The file name must be `upgrade.kt`.
- Make sure Konftel 800 is in Idle Mode.

Procedure

⇒ Connect a USB mass storage device to Konftel 800 USB port.

While checking for the appropriate firmware upgrade file, the phone shows the following message: `Checking upgrade file`. Then the phone displays the following message: `Firmware version x.x.x.x.x found on USB. Upgrade now?`, where `x.x.x.x.x` is the version of the valid firmware file.

⇒ Tap **Yes** to proceed with the upgrade.

The phone displays the **Admin Password** popup.

⇒ In the **Admin Password** field, type the administrator password.

⇒ Optional: If you enter an incorrect administrator password, the phone displays the following message: `Invalid password`. Do the following:

Tap **Ok**.

Type the correct administrator password.

⇒ Tap **Upgrade**.

The phone starts the upgrade procedure, showing the following message: `Upgrade in progress, please wait`. When the upgrade procedure ends, the phone reboots to apply the changes.

⇒ Optional: Tap **Cancel** to discontinue.

If you tap **Cancel** accidentally, to restart the procedure, reconnect a USB mass storage device to Konftel 800 USB port.

Related tasks

[Uploading a firmware file](#) on page 121

MAINTENANCE

Configuration file

Create an .xml configuration 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:

- 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. Export, edit, and import settings to several phones instead of configuring the settings on each phone.
- Configuration file for Device Management.

① You can export and import a configuration file only through the web interface.

Related concepts

[Device Management](#) on page 146

Configuration file structure

The following table shows the default structure of the .xml file:

String	Description
<xml>	To specify the number of the phone configuration version and encoding.
<KT800>	To specify the model of the conference phone.
<time>	To specify the time and region parameters.
<timezone>	To specify the type of the time zone set for the phone. If you set the string value to the name of a time zone, for example, to <i>Europe/Amsterdam</i> , it automatically enables the Geo Timezone (auto DST) parameter on the phone web UI.
<time_format>	To specify the time format for the phone.

Table continued...

MAINTENANCE

String	Description
<ntp>	To specify whether NTP is applied.
<server>	To specify the server which the phone uses to set the time.
<enable>	To specify whether NTP is enabled. The default setting is true.
<date_format>	To specify the date format for the phone.
<custom_dst>	To specify the Daylight Saving Time parameters.
<enable>	To specify whether the Daylight Saving Time is enabled. The default setting is false.
<offset_hours>	To specify the time in hours between the standard time and daylight saving time. The values are 1 and 2. The default setting is 1.
<dst_start>	To specify when to apply the offset for daylight saving time.
<month>	To specify the month when to apply the offset.
<day>	To specify the day when to apply the offset.
<day_mode>	To specify the day mode when to apply the offset. The value range is from -5 to 5.
<hour>	To specify the hour when to apply the offset
<dst_stop>	To specify when to stop the offset for daylight saving time.
<month>	To specify the month when to stop the offset.

Table continued...

MAINTENANCE

String	Description
<day>	To specify the day when to stop the offset.
<day_mode>	To specify the day mode when to stop the offset.
<hour>	To specify the hour when to stop the offset.
<media>	To specify the media settings.
<security>	To specify the means of encryption configured for the phone.
<srtp>	To specify the SRTP parameters that the phone uses.
<srtcp>	To specify whether SRTCP is enabled.
<capneg>	To specify whether Capability Negotiation is enabled.
<codec>	To specify the codec settings.
<iLBC>	To specify the internet Low Bitrate Codec (iLBC) codec settings.
<prio>	To specify the codec priority (0–6).
<mode>	To specify the frame length in ms.
<OPUS>	To specify the OPUS codec settings.
<prio>	To specify the codec priority (0–6).
<PCMU>	To specify the PCMU codec settings.
<prio>	To specify the codec priority (0–6).
<PCMA>	To specify the PCMA codec settings.

Table continued...

MAINTENANCE

String	Description
<prio>	To specify the codec priority (0–6).
<G722>	To specify the G722 codec settings.
<prio>	To specify the codec priority (0–6).
<G729>	To specify the G729 codec settings.
<prio>	To specify the codec priority (0–6).
<rtp_pt_98_ilbc>	To specify that the server gets iLBC packets as payload type 98. By default it is set to 104. You can also set the value to 98 to ensure interoperability with specific systems.
<voice_quality_monitor>	To specify the Voice Quality Monitor settings.
<enable_rtcp_xr>	To specify whether the sending of RTCP XR is enabled.
<rtcp_xr_collector_uri>	To specify the Uniform Resource Identifier (URI) of the RTCP XR collector.
<sip>	To specify SIP settings.
<primary_account>	To specify the primary account settings.
<name>	To specify the name of the account.
<user>	To specify the user-defined name of the account.
<registrar>	To specify the request URI for registration.
<proxy>	To specify the optional URI of the proxy to visit for all outgoing requests from the account.

Table continued...

MAINTENANCE

String	Description
<keep_alive>	To specify whether 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.
<realm>	To specify the realm.
<username>	To specify an authentication name.
<password>	To specify the password used for the account.
<reg_timeout>	To specify the optional interval for registration in seconds. If zero, the phone uses the default interval. The default setting is 300.
<secondary_account>	To specify the secondary account settings.
<name>	To specify the name of the account.
<user>	To specify the user-defined name of the account.
<registrar>	To specify the request URI for registration.
<proxy>	To specify the optional URI of the proxy to visit for all outgoing requests from the account.
<keep_alive>	To specify whether the keep-alive transmission for the account is enabled.

Table continued...

MAINTENANCE

String	Description
<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.
<realm>	To specify the realm.
<username>	To specify an authentication name.
<password>	To specify the password used for the account.
<reg_timeout>	To specify the optional interval for registration in seconds. If zero, the phone uses the default interval. The default setting is 300.
<fallback_account>	To specify the fallback account settings.
<name>	To specify the name of the account.
<user>	To specify the user-defined name of the account.
<registrar>	To specify the request URI for registration.
<proxy>	To specify the optional URI of the proxy to visit for all outgoing requests from the account.
<keep_alive>	To specify whether the keep-alive transmission for the account is enabled.

Table continued...

MAINTENANCE

String	Description
<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.
<realm>	To specify the realm.
<username>	To specify an authentication name.
<password>	To specify the password used for the account.
<reg_timeout>	To specify the optional interval for registration in seconds. If zero, the phone uses the default interval. The default setting is 300.
<source_port>	To specify the source port to listen to. The value range is from 0 to 65535.
<transport_protocol>	To specify the transport protocol which the phone must use.
<tls>	To specify that TLS is selected as the transport protocol. This is followed by the corresponding transport protocol settings.
<tls_method>	To specify the TLS protocol method.
<tls_neg_timeout>	To specify the TLS negotiation time-out in seconds for both outgoing and incoming connections. If zero, the phone uses no time-out.
<tls_password>	To specify the password for the private key.

Table continued...

MAINTENANCE

String	Description
<verify_client>	To specify whether the phone must verify the client.
<verify_server>	To specify whether the phone must verify the server.
<require_client_cert>	To specify whether the phone requires the client certificate.
<advanced>	To specify the configured advanced SIP settings.
<disable_rport>	To specify whether the remote port forwarding is enabled. The default setting is disabled.
<session_timers>	To specify the chosen time-related mechanism to disconnect the sessions.
<session_expiration_minimum>	To specify the minimum session expiration value in seconds. The default value is 90 seconds.
<session_expiration>	To specify the session expiration value in seconds. The default setting is 1800 seconds.
<outbound_proxy>	To specify the IP address of the outbound proxy.
<enable_sip_traces>	To specify whether the provision of key information for troubleshooting is enabled. The default setting is disabled.
<allow_contact_rewrite>	To specify whether the storing of the IP address from the response of the register request is enabled.

Table continued...

MAINTENANCE

String	Description
<allow_via_rewrite>	To specify whether rewriting of the VIA header in the SIP stack is enabled.
<enable_sip_replaces>	To specify whether the SIP Replaces header must be used.
<contact_use_src_port_even_with_dns>	To specify whether the SIP stack should continue to retrieve the local ephemeral port even if the stack is configured with DNS.
<enable_lock_codec>	To specify whether the lock codec feature is enabled.
<use_static_source_port>	To specify whether the use of static source port feature is enabled.
<dtmf>	To specify DTMF signaling settings.
<method>	To specify the DTMF signaling method.
<rfc4733_payload_type>	To specify the type of audio traffic. The value range is from 96 to 127.
<nat_traversal>	To specify the configured NAT traversal settings.
<ice>	To specify whether ICE is configured for the phone.
<enable>	To specify whether ICE is enabled.
<stun>	To specify whether STUN is configured for the phone.
<enable>	To specify whether STUN is enabled.
<server>	To specify the IP address or the public name of the STUN server.

Table continued...

MAINTENANCE

String	Description
<turn>	To specify whether TURN is configured for the phone.
<enable>	To specify whether TURN is enabled.
<server>	To specify the IP address or the public name of the TURN server.
<user>	To specify the user authentication name on the TURN server.
<password>	To specify whether the user authentication password on the TURN server is set.
<phone>	To specify the configured basic settings of the phone.
<name>	To specify the name of the phone. The maximum input length is 28 characters.
<language>	To specify the language selected.
<allow_legacy_encryption>	To specify whether Legacy encryption mode is enabled. The default setting is true.
<password>	To specify the password used. The maximum input length is 32 characters.
<ringlevel>	To specify the volume level configured. The range is from 0 to 6.
<key_tone>	To specify whether the key tone is enabled.
<is_daisy_chain_slave>	To specify the mode of the phone in case of a daisy chain arrangement.
<fips_mode>	To specify whether FIPS mode is enabled. The default setting is false.

Table continued...

MAINTENANCE

String	Description
<phone_status_api>	To specify whether the phone status API feature is enabled.
<sleep_mode_timeout>	To specify the time-out value in minutes. Two values are available: 0 and 500.
<enable_startup_sound>	To specify whether the start-up sound is enabled. The default setting is true.
<bluetooth>	To specify the Bluetooth parameters.
<enable>	To specify whether Bluetooth is enabled. The default setting is true.
<network>	To specify the network parameters.
<dhcp>	To specify whether the phone uses DHCP to obtain network settings.
<hostname>	To specify the hostname of the phone.
<domain>	To specify the domain name of the phone.
<dns1>	To specify Domain Name Server (DNS) 1 of the phone.
<dns2>	To specify DNS 2 of the phone. You can use maximum two DNS.
<static_ip>	To specify the static IP settings.
<ip>	To specify the IP address of the phone if DHCP is disabled.
<netmask>	To specify the network mask for your phone.
<gateway>	To specify the gateway for the phone.

Table continued...

MAINTENANCE

String	Description
<vlan>	To specify whether VLAN is enabled. The default setting is disabled.
<vlanid>	To specify the ID number that the phone uses for all IP telephony communication through VLAN. The value range is from 0 to 4096.
<ieee_8021x>	To specify IEEE 802.1x parameters.
<enable>	To specify whether IEEE 802.1x is enabled. It is disabled by default.
<username>	To specify the phone username if IEEE 802.1x is enabled.
<eap_md5>	To specify whether the phone uses MD5 EAP method.
<enable>	To specify whether MD5 EAP method is enabled.
<password>	To specify the password for MD5 EAP method.
<eap_tls>	To specify whether the phone uses TLS EAP method.
<enable>	To specify whether TLS EAP method is enabled.
<password>	To specify the password for the TLS EAP method.
<lldp>	To specify the LLDP settings.

Table continued...

MAINTENANCE

String	Description
<enable>	To specify whether the LLDP settings are enabled. These settings are disabled by default.
<country>	To specify the country of the phone location.
<country_subdivision>	To specify the region of the country of the phone location.
<county>	To specify the county, parish, district, or other applicable administrative division. The maximum input length is 50 characters.
<city>	To specify the city of the phone location. The maximum input length is 40 characters.
<city_division>	To specify the city district or area of the phone location. The maximum input length is 60 characters.
<block>	To specify the block within the city district.
<street>	To specify the street of the building where the phone is located.
<direction>	To specify the direction of moving towards the location of the phone.
<trailing_street_suffix>	To specify the trailing street suffix. The maximum input length is 10 characters.
<street_suffix>	To specify the street suffix. The maximum input length is 15 characters.
<number>	To specify the number of the building where the phone is located.

Table continued...

MAINTENANCE

String	Description
<number_suffix>	To specify the building number suffix. The maximum input length is 20 characters.
<landmark>	To specify the reference point for the location of the phone. The maximum input length is 30 characters.
<additional>	To specify any additional information related to the phone location. The maximum input length is 30 characters.
<name>	To specify the name of the company that owns the phone. The maximum input length is 60 characters.
<zip>	To specify the ZIP-code of the phone location. The maximum input length is 20 characters.
<building>	To specify the name or number of the building of the phone location. The maximum input length is 60 characters.
<unit>	To specify the unit within the building where the phone is located. The maximum input length is 30 characters.
<floor>	To specify the floor of the building for the location of the phone.
<room>	To specify the room in the building where the phone is located. The maximum input length is 60 characters.
<place_type>	To specify the type of setting, for example, office. The maximum input length is 60 characters.

Table continued...

MAINTENANCE

String	Description
<script>	To specify the script. The maximum input length is 60 characters.
<elin>	To specify Emergency Location Identification Number (ELIN). The maximum input length is 31 characters.
<qos>	To specify the quality of service (QoS) parameters.
<dscp_sip>	To specify a value in the range from 0 to 63 to prioritize the SIP messages.
<dscp_media>	To specify a value in the range from 0 to 63 to prioritize the media packets.
<device_management>	To specify the Device Management settings.
<enable>	To specify whether Device Management is enabled.
<update_interval>	To specify the update interval in the range from 1 minute to 21,000 minutes. The default setting is 60 minutes.
<update_max_wait>	To specify the maximum time in seconds the phone waits for the update.
<server>	To specify the Device Management server address if it is not provided by the DHCP option.
<check_server_certificate>	To specify whether the Check certificate is enabled.
<lowest_tls_version>	To specify the lowest TLS version for the phone.

Table continued...

MAINTENANCE

String	Description
<dhcp_option>	To select the DHCP option used for the Device Management server address.
<SCEP>	To specify the SCEP settings.
<SCEP_ENTITY_CLASS>	To identify the entity class for which identity the SCEP server generates the identity certificates.
<PASSWORD>	To specify the SCEP password.
<MYCERTURL>	To specify the URL of the SCEP server from which the phone obtains an identity certificate.
<MYCERTRENEW>	To specify the percentage of the identity certificate's validity interval after which the renewal procedures begin. The value range is from 1 to 99. The default value is 90.
<MYCERTKEYLEN>	To specify the length of the public and private keys. The default value is 1024.
<MYCERTDN>	To specify the subject of a SCEP certificate request.
<MYCERTCN>	To specify the Common Name (CN) of a SCEP certificate request.
<MECERTCAID>	To specify an identifier for the CA certificate to sign the SCEP certificate request, in case the server hosts multiple Certificate Authorities.
<SCEPENCALG>	To specify SCEP Encryption Algorithm.
<logging>	To specify the syslog settings.

Table continued...

MAINTENANCE

String	Description
<remote_syslog_enable>	To specify whether the remote syslog feature is enabled.
<remote_syslog_host>	To specify the IP address or the host of the remote syslog server.
<pjsip_log_level>	To set the PJSIP log level. The value range is from 0 to 5.
<ldap>	To configure the LDAP options.
<enable>	To enable the LDAP feature. By default it is disabled.
<name_filter>	To define how the phone applies the entered search characters.
<server_url>	To specify the URL of the LDAP server host. It includes the protocol (LDAP/LDAPS) and the port number.
<search_base>	To specify the distinguished name of the search base.
<user_name>	To specify the username for the LDAP server.
<password>	To specify the password for the LDAP server.
<max_hits>	To specify the maximum number of hits to return for each LDAP search. The value range is from 0 to 1000.
<country_code>	To specify the country code of the phone location.

Table continued...

MAINTENANCE

String	Description
<area_code>	To specify the area code of the phone location. The maximum input length is 10 digits.
<external_prefix>	To specify a special prefix for dialing external numbers.
<min_length_for_ext_prefix>	To restrict the external prefix that the phone adds only if the phone number is longer than the minimum length. The value range is from 0 to 32.
<number_prefix_for_no_ext_prefix>	To specify the initial number for the phone numbers in case of using which the phone adds no external prefix.
<exact_length_for_no_ext_prefix>	To specify the exact length for the phone numbers if the phone adds no external prefix.
<number_attributes>	To specify if there are configured number attributes.
<number_attribute>	To define the attributes that the phone displays if it receives them from the server.
<id>	To define the identifier of the number attribute in the form in which the LDAP directory stores it.
<value>	To define the label that the user sees on the phone screen for a specific number attribute.
<display_name>	To specify how the phone displays the name it searched for.
<sort_results>	To specify if the phone sorts the search hits based on the Display name.

Table continued...

MAINTENANCE

String	Description
<use_dm_certificates_for_ldaps>	To specify if the phone uses any device management certificates for LDAPS.
<httpd>	To configure the web server options.
<min_allowed_tls_version>	To specify the minimum allowed TLS version. The default setting is 1.2. To enable support of TLS v.1.0 and TLS v.1.1, set the value to <code>all</code> .

Exporting the configuration file

About this task

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

Before you begin

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

Procedure

- ⇒ On the web interface, click **Provisioning**.
- ⇒ In the **Configuration** section, click **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

About this task

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

Procedure

- ⇒ On the web interface, click **Provisioning**.
- ⇒ Go to the **Configuration** section.
- ⇒ In **Import Configuration**, click the **Choose file** button.

MAINTENANCE

- ⇒ Locate the configuration file in the folder where it is stored.
- ⇒ Select the file in an .xml format and open it.

The name of the chosen file is near the **Choose file** button.

- ⇒ Click **Save**.

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

Validation and migration of configuration

Starting from Release 1.0.1, Konftel 800 validates and migrates the phone configuration to ensure consistency of the configuration file with the firmware version. With this feature, the phone provides reliable automatic migration of the configuration file to match the newer firmware version if necessary.

Configuration validation

Konftel 800 validates compatibility of the configuration with the firmware against an xml schema file based on the configuration file version.

Starting from Release 1.0.1, a configuration file has a version number attribute. The phone application compares the configuration file version to the firmware version running on the phone to determine the migration steps required to make the configuration file consistent with the firmware.

All the configuration files that Konftel 800 generated before Release 1.0.1 acquire the `<KT800 version="0">` attribute in the xml root element. The configuration files generated with Release 1.0.1 acquire the `<KT800 version="1">` attribute. With each new release, the configuration service increases the configuration file version number by one leaving the incompatible configuration changes attributed to previous file versions.

❗ The phone does not support downgrade of a configuration file.



To avoid failure of the configuration file import or automatic provisioning, ensure that you do not change the version number in a configuration file manually.

Configuration migration

The migration feature ensures seamless import of the configuration data in the following cases:

- During the phone boot
- During the configuration file import using the web interface
- During automatic provisioning of the phone using Device Management

MAINTENANCE

Configuration import can fail if the configuration file does not match the xml schema file. In this case, you see the following message on the phone web interface: Failed to migrate configuration file.

Device Management

The Device Management feature facilitates upgrade and configuration of multiple conference phones. To use this feature, you must configure it. By default, Device Management is enabled.

Konftel 800 upgrades and sets configuration by using the Device Management files. The necessary files must be available on a server reachable from all the phones. This server is called the provisioning server. The service provider is in charge of uploading the necessary files to the provisioning server.

When the phone sends a request for firmware during Device Management, the server provides an HTTP redirection response. It includes a path to the server hosting the firmware. Konftel 800 follows the redirection to obtain the firmware.

The device controls the configuration and firmware download with a frequency of 1 hour.

Files on the provisioning server

The following files must be available on the provisioning server:

- Firmware file
- Firmware metadata file
- Global configuration file
- Device-specific configuration file (optional)
- Global certificate configuration file
- Device-specific certificate configuration file (optional)

Configuration priorities

The following table describes the priorities for files downloaded to the phone during the Device Management configuration upgrade:

MAINTENANCE

File type	Description
Configuration file	<p>The global configuration file has the highest priority.</p> <p>If the device-specific configuration file is present on the provisioning server, the phone downloads it after the global configuration file.</p> <p>If the new configuration file contains the same parameters as already configured by the user, all user configurations are overridden during the Device Management update.</p>
Certificate configuration file	<p>The device-specific certificate configuration file has the highest priority.</p> <p>The phone downloads the global configuration file only after it tried to download the device-specific configuration file.</p> <p>The certificates the phone downloads from the provisioning server overwrite any certificates you downloaded manually using the phone web interface.</p>

Konftel Zero Touch Installation

Zero Touch Installation (ZTI) is an add-in for automatic 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.

Related concepts

[Certificate configuration files](#) on page 153

[Configuration file](#) on page 126

Registration with the ZTI device management service

About this task

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

Before you begin

Connect the phone to the data network and start it.

Procedure

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

MAINTENANCE

- ⇒ 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

About this task

Use this procedure to configure the Device Management settings on the phone.

Procedure

- ⇒ Log in as the administrator.
- ⇒ On the phone screen, tap **Settings > Device Management**.
- ⇒ Choose the parameter that you want to configure and proceed to the options available.
- ⇒ After you made the choices, return to the home screen.

The phone reboots to apply the changes.

Configuring Device Management settings through the web interface

About this task

Use this procedure to configure the Device Management settings through the web interface.

Procedure

- ⇒ Log in as the administrator.
- ⇒ On the web interface, click **Provisioning**.
- ⇒ Make the appropriate configurations.
- ⇒ Click **Save**.

The phone reboots to apply the changes.

MAINTENANCE

Device Management settings

The following table lists 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	<p>To enable or disable Device Management. The options are:</p> <ul style="list-style-type: none">• On: Device Management is enabled. This is the default setting.• Off: Device Management is disabled.
Update interval	<p>To specify the update interval in minutes the phone waits to re-sync with the provisioning server. The default value is 60 minutes.</p> <p>The phone accepts values in the range from 1 to 21,000.</p> <p> You can configure this parameter through the web interface or through the .xml configuration file.</p>
Maximum time to wait to update	<p>To specify the maximum time in seconds the phone waits for the update. By default, it is 1 minute.</p> <p>This time-out is not used during the first start of Device Management. Device Management starts for the first time as soon as the network is configured. After that, Device Management starts at the intervals you specified using the Update interval parameter and uses the Maximum time to wait to update value.</p> <p> You can configure this parameter through the web interface or through the .xml configuration file.</p>
Provisioning Server	<p>To specify the Device Management server address if it is not provided by the DHCP option.</p>

Table continued...

MAINTENANCE

Name	Description
Check Server Certificate	<p>To enable or disable the verification of the authentication with a certificate. The options are:</p> <ul style="list-style-type: none">• On: Server certificates are checked.• Off: Server certificates are not checked. This is the default setting.
Lowest TLS Version	<p>To specify the lowest TLS version for the phone. The options are:</p> <ul style="list-style-type: none">• 1• 1.1• 1.2
DHCP Option	<p>To select the DHCP option used for the Device Management server address.</p> <p>With all DHCP options, the phone obtains the URL and directory of the server where the configuration file is located. The Device Management server then looks for <code>kt800.xml</code> as a global configuration file, and <code>kt800-<MAC>.xml</code> for a device-specific file.</p> <p>The DHCP options are:</p> <ul style="list-style-type: none">• 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.
Certificate	<p>To upload a certificate to the phone. This certificate is used for authentication in Device Management.</p>
CA Certificate	<p>To upload a root certificate. It contains a public key, which is used to verify other certificates when using Device Management.</p>

Table continued...

MAINTENANCE

Name	Description
Private Key	To upload a private key. It is used for authentication when using Device Management.

Files on the provisioning server

The following files must be available on the provisioning server:

- Firmware file
- Firmware metadata file
- Global configuration file
- Device-specific configuration file (optional)
- Global certificate configuration file
- Device-specific certificate configuration file (optional)

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`.

Instead of the `.xml` file format, you can also use `cgi`, `php`, `asp`, `js`, or `jsp` file formats. Konftel 800 first searches for the configuration file in `.xml` format. If the phone fails to find the `.xml` file on the provisioning server, it searches for the configuration file in other formats specified above.

Creating the global configuration file

About this task

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 set all the basic configurations of Konftel 800.

Before you begin

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

MAINTENANCE

Procedure

- ⇒ On the web interface, click **Provisioning**.
- ⇒ In the **Configuration** section, click **Export Configuration**.

The configuration file is created.
- ⇒ Optional: Edit the .xml file in a suitable editor.
- ⇒ Save the file as `kt800.xml` in the dedicated folder. The folder is located at the address specified in the **Provisioning Server** field.
 - ⓘ Do not use a custom name for this file because the file name `kt800` is hardcoded in Device Management configuration and it will not search for files with a different name.

Next steps

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.

Device-specific configuration file

The device-specific 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.

Instead of the .xml file format, you can also use `cgi`, `php`, `asp`, `js`, or `jsp` file formats. Konftel 800 first searches for the configuration file in .xml format. If the phone cannot find the .xml file on the provisioning server, it searches for the configuration file in the other formats.

Creating the device-specific configuration file

About this task

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

Before you begin

Obtain MAC addresses of all your Konftel 800 phones. Ensure that you write the MAC address without colons.

MAINTENANCE

Procedure

- ⇒ On the web interface, click **Provisioning**.
- ⇒ In the **Configuration** section, click **Export Configuration**.

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` in the dedicated folder located at the address specified in the **Provisioning Server** field.

- ⓘ Do not use a custom name for this file because the file name `kt800-<MAC>` is hardcoded in Device Management configuration and it will not search for files with a different name.

Certificate configuration files

Certificate configuration files stored on the provisioning server allow you to automatically download certificate files to Konftel 800. These files are required for the server validation by the phone and TLS authentication by the server.

The service provider can upload a global certificate configuration file and a device-specific certificate configuration file.

The default name for the global configuration file is `kt800_certcfg.xml`. The default name for the global configuration file is `kt800_certcfg-<MAC>.xml`, where `<MAC>` is the MAC address of the specific phone.

Instead of the .xml file format, the service provider can also use cgi, php, asp, js, or jsp file formats. Konftel 800 first searches for the configuration file in .xml format. If the phone fails to find the .xml file on the provisioning server, it searches for the configuration file in other formats specified above.

The typical certificate configuration file consists of four sections:

- 802.1x: specifies the 802.1x certification arrangements of the phone.
- SIP: contains the Session Initiation Protocol (SIP) certification arrangements of the phone.
- Provisioning: runs through the provisioning server certification arrangements of the phone.
- LDAP: specifies the LDAP server certificate arrangements of the phone.

- ⓘ In some cases, the certificate configuration file can lack some sections. This happens if the relevant certificates are not available for the phone.

Each section includes the following certificate files:

MAINTENANCE

- CA certificate
- Device certificate
- Device private key.

Each section contains the path details for the CA certificate, Device certificate, and Device private key.

① The path to the certificate can be a relative path or a complete URI. For example, a relative path can look like `<ca_uri>ca.crt</ca_uri>` or `<ca_uri>certs/ca.crt</ca_uri>`. In the first case, the phone looks for the `ca.crt` file in the same catalog as the configuration file. In the second case, the phone looks for the `ca.crt` file in the `certs` catalog relative to the configuration file.

The file can have the path to the certificate in the form of a complete URI, like `<ca_uri>https://hostname.io/path/ca.crt</ca_uri>`. In this case, the phone uses a specific URI to download the certification file.

The section also specifies a SHA256 or an MD5 checksum for each element in it. This checksum (also called SHA256 hash algorithm or MD5 hash algorithm) is a type of digests of the specified certificates.

① Konftel 800 uses MD5 checksum only when **Allow Legacy Encryption** is enabled. In this case, both SHA256 and MD5 hash algorithms are supported. When **Allow Legacy Encryption** is disabled, Konftel 800 supports only SHA256 hash algorithm. Then the phone does not use MD5 as the checksum for certificates if it downloads and stores them during provisioning.

The phone starts downloading the certificate if the hash algorithm value is different from the one of the certificate file that Konftel 800 stores. That means that the phone downloads one certificate file only once and subsequently checks that the certificate file is still the same.

Related concepts

[Legacy encryption mode](#) on page 94

Certificate configuration file structure

The following table shows the format of the certificate file:

String	Description
<code><certificates></code>	To specify the certificates that the phone applies.

Table continued...

MAINTENANCE

String	Description
<ether_8021x>	To specify the 802.1x certification arrangements of the phone.
<ca_uri>	To specify the 802.1x path to check the CA certificate.
<ca_hash algo="md5">	To specify the MD5 hash algorithm that the phone uses to verify the 802.1x CA certificate.
<cert_uri>	To specify the 802.1x path to get the device certificate.
<cert_hash algo="md5">	To specify the MD5 hash algorithm that the phone uses to verify the 802.1x device certificate.
<privkey_uri>	To specify the 802.1x path to get the private key.
<privkey_hash algo="md5">	To specify the MD5 hash algorithm that the phone uses to verify the 802.1x private key.
<sip>	To specify the SIP certification arrangements of the phone.
<ether_8021x>	To specify the path to get the CA certificate for the SIP connection.
<ca_uri>	To specify the MD5 hash algorithm that the phone uses to verify the CA certificate for the SIP connection.

Table continued...

MAINTENANCE

String	Description
<ca_hash algo="md5">	To specify the path to get the device certificate for the SIP connection.
<cert_uri>	To specify the MD5 hash algorithm that the phone uses to verify the device certificate for the SIP connection.
<cert_hash algo="md5">	To specify the path to get the private key for the SIP connection.
<privkey_uri>	To specify the MD5 hash algorithm that the phone uses to verify the private key for the SIP connection.
<provisioning>	To specify the provisioning server certification arrangements of the phone.
<ether_8021x>	To specify the path to get the CA certificate for connection to the provisioning server.
<ca_uri>	To specify the MD5 hash algorithm that the phone uses to verify the CA certificate for connection to the provisioning server.
<ca_hash algo="md5">	To specify the path to get the device certificate for connection to the provisioning server.

Table continued...

MAINTENANCE

String	Description
<cert_uri>	To specify the MD5 hash algorithm that the phone uses to verify the device certificate for connection to the provisioning server.
<cert_hash algo="md5">	To specify the path to get the private key for connection to the provisioning server.
<privkey_uri>	To specify the MD5 hash algorithm that the phone uses to verify the private key for connection to the provisioning server.
<ldap>	To specify the LDAP server certificate arrangements of the phone.
<ether_8021x>	To specify the path to get the CA certificate for connection to the LDAP server.
<ca_uri>	To specify the MD5 hash algorithm that the phone uses to verify the CA certificate for connection to the LDAP server.
<ca_hash algo="md5">	To specify the path to get the device certificate for connection to the LDAP server.
<cert_uri>	To specify the MD5 hash algorithm that the phone uses to verify the device certificate for connection to the LDAP server.

Table continued...

MAINTENANCE

String	Description
<code><cert_hash algo="md5"></code>	To specify the path to get the private key for connection to the LDAP server.
<code><privkey_uri></code>	To specify the MD5 hash algorithm that the phone uses to verify the private key for connection to the LDAP server.

The following is an example of the certificate configuration file for Konftel 800. Note that it contains only 2 out of 4 sections.

```
<certificates>
  <ether_8021x>
    <ca_uri>8021x_ca.crt</ca_uri>
    <ca_hash algo="md5">c49d8fd0cbb6bfc26ef752296d6d17f7</ca_hash>
    <cert_uri>8021x_dev.crt</cert_uri>
    <cert_hash algo="md5">ca059972d02b2853a92704a7a7640f3f</
cert_hash>
    <privkey_uri>8021x_priv.key</privkey_uri>
    <privkey_hash algo="md5">f4728d6356204c6fccc91989ef733553</
privkey_hash>
  </ether_8021x>
  <provisioning>
    <ca_uri>prov_ca.crt</ca_uri>
    <ca_hash algo="md5">e5116932d3685ea18ead10a55b825145</ca_hash>
  </provisioning>
</certificates>
```

- ① If you enable **Allow Legacy Encryption**, the certificate configuration file can contain both MD5 and SHA256 hash algorithms. If you disable **Allow Legacy Encryption**, then only the SHA256 hash algorithm is supported.

Related concepts

[Legacy encryption mode](#) on page 94

SCEP support

Konftel 800 supports Simple Certificate Enrollment Protocol (SCEP) required for managing digital certificate obtainment. SCEP is used to contact a SCEP server to get an Identity certificate. The device uses this certificate for all TLS connections if

MAINTENANCE

they do not have manually configured certificates (SIP TLS, 802.1x EAP-TLS, Provisioning via TLS, LDAP). You can also obtain a CA certificate if the SCEP server has corresponding configurations.

SCEP enrollment

You can configure SCEP through the web interface and importing the configuration file with the specific SCEP settings. After Konftel 800 reboots, it attempts to connect the specified SCEP server. If the server is reachable, it provides the certificates with the settings matching the server configuration. If the received certificate is valid and the SCEP enrollment is successful, the phone saves the configuration and reboots.

When the device requests an SCEP server to get or renew a certificate, the request must be approved. The following types of request approval are available:

- Manual approval. The SCEP server receives your request, and then the SCEP server administrator must approve it. The next request of the device results in the certificate provision.
- Automatic approval. The SCEP server checks your request for validity, then if the parameters are accurate, approves the request and sends you the certificate.

The enrollment fails if the settings configuration on the phone and the server do not match. Here, Konftel 800 triggers the next enrollment in 24 hours.

If you upload a certificate to the phone through the web interface or using automatic provisioning only for one connection, for example, for the LDAP connection, that connection continues to use the configured certificate. Other connections use the SCEP Identity certificate received from the SCEP server.

Mandatory SCEP parameters

Successful enrollment is only possible if you configure the relevant SCEP server and valid SCEP settings. When you enter the URL of the dedicated SCEP server, you must specify the following parameters:

- Common Name
- CA Identifier
- Initiate renewal on % of Validity interval
- Key Length
- Password

① There is no check of mandatory parameters in automatic provisioning and configuration file import. You must always provide valid data.

MAINTENANCE

Background polling

If you configure SCEP with the valid data, the phone attempts to connect to the SCEP server. If the server is reachable, it immediately starts processing the enrollment or renewal request. If the connection fails, Konftel 800 attempts to contact the SCEP server in the background.

For manual approval of a certificate, the phone sends the first request after the reboot and repeats it 20 times within 300 seconds. If the request stays unapproved, the phone tries to connect again in 24 hours.

Related information

[SCEP settings](#) on page 161

Configuring SCEP settings through the web interface

About this task

Use this procedure to configure SCEP settings of your Konftel 800 through the web interface. If you input invalid data to a setting field, the web interface highlights the field when you click the **Save** button.

Before you begin

Log in to the web interface as the administrator.

Procedure

- ⇒ On the web interface, click **Provisioning**.
- ⇒ Proceed to the **SCEP** section.
- ⇒ Specify the URL of the relevant SCEP server in the **SCEP Server** field.
- ⇒ Configure the mandatory and optional SCEP parameters.
- ⇒ Click **Save**.

The phone reboots to apply the changes.

The web interface shows *Save Succeeded* pop-up message.

Related concepts

[SCEP support](#) on page 158

Related information

[SCEP settings](#) on page 161

MAINTENANCE

Configuring SCEP using the configuration file

About this task

Use this procedure to configure SCEP settings of your Konftel 800 through the web interface in the **Provisioning** tab using the configuration file import. For successful certificate enrollment, you must provide valid data.

Before you begin

Get the configuration .xml file for Konftel 800.

Procedure

- ⇒ Open the configuration file.
- ⇒ In the <SCEP> section, configure the required parameters.
- ⇒ Save the configuration file.

Next steps

Upload the configuration file to the Device Management server or import the configuration file to the phone using the web interface.

Related tasks

[Importing the configuration file](#) on page 144

SCEP settings

The following table lists the SCEP settings of Konftel 800 available through the web interface in the **Provisioning** tab in the **SCEP** section.

Name	Description
SCEP server	To specify the URL of the SCEP server to obtain an identity certificate if it does not have one from that server.
Common Name	To specify the Common Name (CN) used in the Subject of a SCEP certificate request. The input length is from 8 to 255 characters. The default value is the serial number of the phone, for example: E3A0330077. This is a mandatory parameter.

MAINTENANCE

Name	Description
Subject	<p>To specify the SUBJECT part of a SCEP certificate request that is common for all phones.</p> <p>The format is /C=US/ST=NJ/L=MyTown/O=MyCompany.</p>
CA Identifier	<p>To specify an identifier for the CA certificate to sign the SCEP certificate request if the server hosts multiple Certificate Authorities. The input length is from 0 to 255 ASCII characters.</p> <p>The default value is CAIdentifier.</p> <p>This is a mandatory parameter.</p>
Initiate renewal on % of Validity Interval	<p>To specify the percentage of the identity certificate Validity interval after which the renewal procedures initiation occurs.</p> <p>The format is whole numbers from 1 to 99. The default value is 90.</p> <p>This is a mandatory parameter.</p>
Key Length	<p>To specify the bit length of the public and private keys generated for the SCEP certificate request. You can choose the key length from the following list:</p> <ul style="list-style-type: none">• 1024• 2048 <p>The default value is 1024.</p> <p>This is a mandatory parameter.</p>
Entity Class	<p>To identify the entity class to generate identity certificates using SCEP.</p>

MAINTENANCE

Name	Description
Password	<p>To specify the password to include in the challenge Password attribute of an SCEP certificate request. The password can contain up to 4000 ASCII characters.</p> <p>The default value is the serial number of the phone, for example: E3A0330077.</p> <p>This is a mandatory parameter.</p>
Encryption Algorithm	<p>To specify the SCEP encryption algorithm.</p> <p>You can choose the encryption algorithm from the following list:</p> <ul style="list-style-type: none">• DES• AES-256 <p>The default value is DES.</p>

① All the configured SCEP settings return to the default values after factory reset.

Auto-renewal

The SCEP server provides a device certificate with a specified validity period, meaning that the device certificate expires in a pre-set amount of days. After it expires, you must get a new device certificate from the SCEP server. You can configure the date and time to send the renewal request for the certificate. You must specify the renewal date and time in percent of the expired validity period of the valid certificate. For example, you can configure to send the renewal request when the current certificate validity period expires by 95%. You must enter 95 in the **Initiate renewal on % of Validity Interval** field.

When the auto-renewal of the certificates is complete, the phone reboots as soon as it enters Idle mode. After the reboot, Konftel 800 starts using the new device certificate.

① The phone can also boot up with an expired certificate. If you have the renewal request parameter configured, the phone sends the renewal request after the phone boots up.

MAINTENANCE

Configuring SCEP renewal request

About this task

When Konftel 800 receives a device certificate from a SCEP server, the certificate has a specified validity period, after which the certificate expires. Use this procedure to configure a SCEP renewal request through the web interface.

Before you begin

Log in to the web interface as the administrator.

Procedure

- ⇒ On the web interface, click **Provisioning**.
- ⇒ In the **SCEP** section, enter the value in **Initiate renewal on % of Validity Interval**.

The value range is from 1 to 99. The default value is 90.

- ⇒ Click **Save**.

The phone reboots to apply the changes.

The web interface shows *Save Succeeded* pop-up message.

Related concepts

[SCEP support](#) on page 158

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

Firmware metadata file is 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.

- Firmware version
- Filename
- Checksum of the firmware binary

The following is the example of the firmware binary file:

MAINTENANCE

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>
```

- ❗ If the firmware binary file which is specified in the firmware metadata file is not uploaded to the provisioning server, the phone fails to upgrade and shows the following error message after reboot: `Upgrade failed.`

Creating firmware binary and metadata files

About this task

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

Before you begin

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

Procedure

- ⇒ 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 **Provisioning Server** field.
- ⇒ Optional: Add the file type `.kt` to the MIME settings on the server after the files creation.

Upgrading multiple devices

About this task

You can upgrade firmware on multiple Konftel 800 devices using Device Management instead of upgrading each phone individually. For this purpose, Device Management must be enabled for the devices, the provisioning server must be specified for the devices, and the firmware binary file and the firmware metadata file must be available on the provisioning server.

MAINTENANCE

Before you begin

Ensure that the firmware filename matches the `<filename>` value in the metadata file, and that the firmware version in both files is the same.

Procedure

- ⇒ Check if Device Management is enabled on the phones you want to upgrade and enable if necessary.

You can do this on the phone by logging in as an administrator and navigating to **Settings > Device Management** or through the web interface on the **Provisioning** tab in the **Device Management** section.

- ⇒ Check if the provisioning server is configured for the phones you want to upgrade and configure if necessary.

You can do this on the phone by logging in as an administrator and navigating to **Settings > Device Management** or through the web interface on the **Provisioning** tab in the **Device Management** section.

- ⇒ Upload the binary file and the firmware metadata file to the provisioning server.

When the phones contact the provisioning server, the upgrade process starts.

Next steps

You can check the firmware version from the phone by navigating to **Settings > Status** or through the web interface in the **Status** tab.

Related concepts

[Device Management settings](#) on page 149

[Firmware metadata file](#) on page 164

[Firmware binary](#) on page 164

Configuring multiple devices

About this task

You can configure multiple Konftel 800 devices using the configuration file as a management tool instead of configuring the settings on each phone individually. For this purpose, you need to export the configuration file, edit the settings as necessary, and then place the configuration file to the provisioning server.

Before you begin

Ensure that you or the service provider have configured the provisioning server for your phones.

MAINTENANCE

Procedure

- ⇒ Log in to the web interface.
- ⇒ Export the configuration file by clicking **Export Configuration** on the **Provisioning** tab.

The phone generates the global configuration `kt800.xml` file.

- ⇒ Optional: Edit the configuration file using a suitable application.
 - ⓘ The settings file might not contain some settings if they represent a default value. To include such settings in the configuration file, you need to change them to a non-default value using the phone interface or the web interface.
- ⇒ Upload the file to the provisioning server.

During the next Device Management configuration upgrade, the system applies the configuration file to the phones. After the phones reboot, they all have the same settings specified in the configuration file.

Related concepts

[Configuration file](#) on page 126

[Device Management](#) on page 146

Related tasks

[Creating the global configuration file](#) on page 151

Remote syslog server

Konftel 800 supports syslog protocol to allow centralized log management. You can configure the phone so that it logs to a remote server and sends the syslog messages to your own system or a third-party system.

With the remote syslog feature enabled, the phone sends the syslog messages to the syslog server and also logs them in the local log.

By default, the remote logging feature on Konftel 800 is in the disabled state.

Configuring remote syslog settings

About this task

To use the remote syslog feature, you need to do the following:

- Enable your phone to deliver syslog messages to the syslog server.
- Configure the destination server which receives the syslog events.

MAINTENANCE

You can do this using the configuration file stored on the Device Management server. You can find the syslog settings under the `<logging>` section of the configuration file.

① The default syslog port is 514, and you cannot change this setting.

The `<remote_syslog_host>` tag can be missing in the `<logging>` section if you use a configuration file exported from the phone application. This can happen because the `<remote_syslog_host>` default value is blank, and the phone application does not export blank tags.

Before you begin

Obtain the configuration .xml file for Konftel 800.

Procedure

⇒ In the configuration file, go to the `<logging>` section.

⇒ Set the value in the `<remote_syslog_enable>` tag to `true` as shown in the following example:

```
<remote_syslog_enable>true</remote_syslog_enable>
```

⇒ Specify the host URL in the `<remote_syslog_host>` tag as shown in the following example:

```
<remote_syslog_host>1.2.3.4</remote_syslog_host>
```

Replace the 1.2.3.4 with the IP address or hostname of your remote syslog server.

⇒ Save the configuration file.

Next steps

Upload the configuration file to the Device Management server or import the configuration file to the phone using the web interface.

The phone sends syslog messages to the syslog server after the next reboot. The phone continues sending syslog messages until you set the `<remote_syslog_enable>` parameter in the configuration file to `false`.

Related concepts

[Configuration file](#) on page 126

Related tasks

[Importing the configuration file](#) on page 144

[Exporting the configuration file](#) on page 144

MAINTENANCE

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.

Performing factory reset

About this task

You can reset your Konftel 800 to factory default. You can do the factory reset only on the phone after you log in as the administrator.

If you need to perform the factory reset without logging in as the administrator, follow the procedure described in [Performing system recovery](#) on page 170.

Procedure

- ⇒ 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.

System recovery

As an administrator, you can perform system recovery on Konftel 800 to return the phone to operable state, for example, after a faulty upgrade or when the phone application fails. System recovery replaces the current firmware with the previously installed operable firmware version.

You can also perform system recovery to reset the administrator password.

- ① System recovery erases all settings including the account information.

MAINTENANCE

Performing system recovery


Before you begin

Ensure that you save the configuration file from your Konftel 800. System recovery erases all settings.

Procedure

- ⇒ Power cycle the phone to start the boot process.
- ⇒ When the LEDs turn green, start tapping the **Microphone Muted** button on the phone and continue tapping until the LEDs turn off.
- ⇒ Tap the **Microphone Muted** button once again.
- ⇒ When the LEDs turn red, tap the **Volume up** button once to confirm the system recovery.

The LEDs turn off. The phone starts regular boot. After the boot up, the phone displays the following message: Upgrade the phone to complete recovery.

 If you want to cancel the system recovery, do not tap **Volume up** button on the phone when the LEDs turn red.

- ⇒ After the phone boots up, set the administrator password.
- ⇒ Upgrade the phone to complete system recovery.

Next steps

Upload the configuration file with necessary settings.

Related concepts


[Provisioning on Konftel 800](#) on page 121

Related tasks

[Setting the password for Konftel 800](#) on page 24

Web interface settings

The web server in Konftel 800 supports 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 table shows the web interface settings that you can configure for Konftel 800 in the **Provisioning** tab:

MAINTENANCE

Name	Description
Secure HTTP	
Webapp HTTPs Certificate	To upload a .PEM certificate to Konftel 800 to use HTTPS. ① 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 90

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
```

Protection against cross-site request forgery

When the user logs in to the web interface of Konftel 800 with the administrator password, the web application of the phone uses specific tokens to protect against Cross-Site Request Forgery (CSRF) attacks.

CSRF is an attack that tricks the user into submitting a malicious request. The attacker takes the identity and privileges of the user to make undesired actions on the user's behalf. CSRF attacks target functionality that causes a state change, for example changing the user's password. If the user stays authenticated to the website during the attack, the website can not distinguish between forged and legitimate requests.

Konftel 800 generates a new CSRF token on each request. Each link or parameter change in the web interface needs to have a CSRF token as a request parameter. The web application checks if the token in the request is the correct one. For example, if the attacker copies an existing link from the open web interface of Konftel 800, the server responds with the following error code: HTTP status code 403, forbidden.

- ① You are recommended to administer the settings in the web UI only from one computer and one browser simultaneously. This way you can minimize the risk of getting the error code message due to incorrect token use.

MAINTENANCE

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: <ul style="list-style-type: none">• Phone Name• Product Name• Build Version• HW Revision• Serial Number• Smart Microphone 1 Version• Smart Microphone 2 Version
Network	To show the information about the network settings of the phone. You can see the following information: <ul style="list-style-type: none">• IP Address• MAC Address• Bluetooth MAC Address• Hostname• Network Mask• Domain• Gateway• Primary DNS• Secondary DNS

MAINTENANCE

Section name	Description
SIP	To show the information about the SIP settings of the phone. You can see the following information: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• NTP Status• Time• Date• Timezone• Daylight Saving Time

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

Viewing the phone status

About this task

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

Procedure

- ⇒ Log in to the web interface.
- ⇒ 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**

MAINTENANCE

- **Bluetooth Stack Logs**
- **PJSIP logs**
- **Device Management**
- **SIP traces**
- **Device Management Debug**

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

① You can not access logs through the phone user interface.

Viewing system logs

About this task

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

Procedure

- ⇒ On the web interface, click **System logs**.
- ⇒ Under **Select Logs Type**, select the log from the 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. Here, the system downloads a .zip archive with the logs available.
 - Click the **Download Selected Logs** button to download the logs of a selected type. Here, 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.

PJSIP log levels

Konftel 800 uses the PJSIP library in its real-time media communication. PJSIP is a free and open-source multimedia communication library working with standard-based protocols such as SIP, STUN, and TURN. This library also combines three main components of real-time multimedia communication: signaling, media features, and NAT traversal.

You can use PJSIP logs for information and troubleshooting.

Konftel 800 provides the following PJSIP log levels:

- **Fatal**. This is the least detailed printout. You can see those events that are fatal for the operation.

MAINTENANCE

- **Error.** You can see the list of error events.
- **Warning.** You can see the list of warnings relevant to the device operation.
- **Info.** You can see information about the actions of the device. This is the default option.
- **Debug.** You can get information about specific actions of the device and use it for debugging.
- **Trace.** This is the most detailed printout. You can see all the actions made by the device.

You can set the PJSIP log level through the web interface or using a configuration .xml file.

Setting PJSIP log level through the web interface

About this task

Use this procedure to manually set the PJSIP log level to generate a log message printout with the required details. For example, when you enable a higher log level, you receive useful information for troubleshooting.

Before you begin

Log in to the web interface.

Procedure

- ⇒ On the web interface, click the **System logs** tab.
- ⇒ Choose the required value from the **PJSIP Log Level** list.

The value depends on the level of printout details provision you need.

- ⇒ Click **Save**.

The phone restarts the application to apply the changes.

Next steps

Check the PJSIP printout information.

Setting PJSIP log level using the configuration file

About this task

Set PJSIP log level using the .xml configuration file to generate a detailed log message printout. For example, when you set a higher log level, you receive useful information for troubleshooting. When you boot the phone after provisioning, the setting file is changed depending on the configuration of the standard encryption use.

MAINTENANCE

Before you begin

Obtain the configuration .xml file for Konftel 800.

Procedure

- ⇒ Open the configuration file.
- ⇒ In the <logging> section, locate the <pjsip_log_level> tag and set the necessary value.

The value range is from 0 to 5. The values correspond to the following five levels with different printout detalization:

- 0: Fatal
- 1: Error
- 2: Warning
- 3: Info
- 4: Debug
- 5: Trace. This is the most detailed printout.

- ⇒ Save the configuration file.

The phone reboots if the PJSIP log level value differs from the previously configured value.

On the web interface, the **PJSIP Log Level** value changes to reflect the value from the configuration file.

Next steps

Upload the configuration file to the Device Management server or import the configuration file to the phone using the web interface.

Related information

[Configuration file structure](#) on page 126

Network logs

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

- ① You can get network logs only after the phone reboots into Network logs mode.

Viewing network logs

About this task

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

MAINTENANCE

Procedure

- ⇒ 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 Network log mode.
 - Click the **Download Network Logs** button to download the archive with the available network logs.

LICENSES

On the **Licenses** web page, you can get the general information about the use and other conditions for the third party components. This web page also contains a copyright URL by using which you can find and download the document with a complete list of the third party components and licenses.

- ① You can get the license information only through the web interface.

APPENDIX A. ENCRYPTION METHODS IN LEGACY ENCRYPTION MODE

ENCRYPTION METHODS IN LEGACY ENCRYPTION MODE

The following table lists the encryption methods enabled and disabled in Legacy encryption mode:

Cipher	802.1X	LDAP	SIP TLS	HTTPS	Legacy Cipher
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA256	Y	Y			Y
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	Y	Y			Y
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Y	Y	Y	Y	N
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Y	Y	Y	Y	N
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	Y	Y	Y	Y	N
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	Y	Y	Y	Y	N
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	Y	Y	Y	Y	N
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	Y	Y	Y	Y	N
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Y	Y	Y	Y	N

Table continued...

APPENDIX A. ENCRYPTION METHODS IN LEGACY ENCRYPTION MODE

Cipher	802.1X	LDAP	SIP TLS	HTTPS	Legacy Cipher
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Y	Y	Y	Y	N
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Y	Y	Y	Y	N
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Y	Y	Y	Y	N
TLS_RSA_WITH_AES_128_GCM_SHA256	Y	Y	Y	Y	N
TLS_RSA_WITH_AES_256_GCM_SHA384	Y	Y	Y	Y	N
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	Y	Y		Y	Y
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	Y	Y	Y	Y	Y
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	Y	Y	Y	Y	Y
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	Y	Y	Y	Y	Y
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	Y	Y	Y	Y	Y
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	Y	Y		Y	Y
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	Y	Y	Y	Y	Y

Table continued...

APPENDIX A. ENCRYPTION METHODS IN LEGACY ENCRYPTION MODE

Cipher	802.1X	LDAP	SIP TLS	HTTPS	Legacy Cipher
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	Y	Y	Y	Y	Y
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	Y	Y	Y	Y	Y
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	Y	Y	Y	Y	Y
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	Y	Y		Y	Y
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	Y	Y	Y	Y	Y
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	Y	Y	Y	Y	Y
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	Y	Y	Y	Y	Y
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	Y	Y	Y	Y	Y
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	Y	Y		Y	Y
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Y	Y	Y	Y	Y
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	Y	Y	Y	Y	Y
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	Y	Y	Y	Y	Y

Table continued...

APPENDIX A. ENCRYPTION METHODS IN LEGACY ENCRYPTION MODE

Cipher	802.1X	LDAP	SIP TLS	HTTPS	Legacy Cipher
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	Y	Y	Y	Y	Y
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	Y	Y		Y	Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Y	Y	Y	Y	Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	Y	Y	Y	Y	Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Y	Y	Y	Y	Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	Y	Y	Y	Y	Y
TLS_RSA_WITH_3DES_EDE_CBC_SHA	Y	Y		Y	Y
TLS_RSA_WITH_AES_128_CBC_SHA	Y	Y	Y	Y	Y
TLS_RSA_WITH_AES_128_CBC_SHA256	Y	Y	Y	Y	Y
TLS_RSA_WITH_AES_256_CBC_SHA	Y	Y	Y	Y	Y
TLS_RSA_WITH_AES_256_CBC_SHA256	Y	Y	Y	Y	Y
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA				Y	Y
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256				Y	Y

Index

Numerics

802.1x

standard encryption 91

A

analog parameters

RTCP XR 65

application to manage the phone

102

B

basic settings 33

Bluetooth

audio streaming 115

deleting pairing 118

paired devices connection 118

paired devices reconnection

118

pairing 117

reconnection 118

Bluetooth Classic 115

profiles 116

Bluetooth LE 115

Bluetooth radio 119

disabling 119

buttons 12

C

CA certificate 153

Caller ID 87

caller information 87

Caller name 87

certificate application 89

converting the certificates

to .PEM format 90

downloading the root certificate

88

exporting the private key 89

certificate configuration file

structure 154

certificate configuration files 153

certificates application 88

changing password 33

check-sync NOTIFY event 122

codecs 73

conference phone 10

configuration

advance settings 170

centralized http/https server 23

Device Management settings

148

HTTP/HTTPS server 23

media settings 59

methods 23

migration 145

multiple devices 166

network settings 47, 48

phone interface 23

phone settings 32

SIP settings 73

web interface 23

web interface settings 170

configuration checklist 19

configuration file 126

export 144

import 144

structure 126

configuring the phone 31

connecting to a network with DHCP

25

connection

using Bluetooth 115

connection layout 13

cross-site request forgery 171

D

daisy chain

arranging 109

cascading 107

defining mode 110

disabling mode 111

expansion microphones 107

master phone 107–109

slave phone 107–109

daisy chain mode 33

INDEX

- data input
 - data type [31](#)
 - length restriction [31](#)
 - validation [31](#)
- daylight saving time [33](#)
- Daylight Saving Time
 - configuring through web interface [42](#)
 - state [43](#)
- Device certificate [153](#)
- device information [172](#)
- Device Management [146](#)
 - files on server [151](#)
- Device Management Server [146](#)
- Device Management settings
 - configuring on the phone [148](#)
 - through the web interface [148](#)
- device-specific configuration file
 - [152](#)
 - creating [152](#)
- DHCP [45, 47](#)
- DHCP SSON [23](#)
- dimensions [12, 14](#)
- document changes [6](#)
- downgrade [121](#)
- E**
- encryption methods
 - legacy encryption mode [178](#)
- expansion microphone
 - firmware upgrade [112, 113](#)
 - automatic [111](#)
 - manual [111, 115](#)
 - termination [114](#)
- expansion microphones [107](#)
- external phone book [66](#)
- F**
- factory reset [169](#)
- fall back server [169](#)
- fallback account [73](#)
- FIPS [96](#)
- FIPS mode [96](#)
 - configuring
 - on the phone [97](#)
- FIPS mode (*continued*)
 - configuring (*continued*)
 - through the web interface [98](#)
 - using configuration file [98](#)
 - media encryption with SRTP [97](#)
- firmware
 - downgrading [121](#)
 - upgrade
 - using mass storage device
 - with administrator password [125](#)
 - without administrator password [124](#)
 - upgrading [121](#)
- firmware binary [164](#)
- firmware binary, creation [165](#)
- firmware downgrade [121](#)
- firmware metadata file [164](#)
- firmware rollback [121](#)
- firmware upgrade
 - multiple devices [165](#)
 - using check-sync [122](#)
 - using the downloaded file [121](#)
 - using USB mass storage device [123](#)
- G**
- global configuration file [151](#)
 - creation [151](#)
- I**
- icons [12, 15](#)
 - usb only user mode [100](#)
- installing the certificate [89](#)
- intended audience [6](#)
- L**
- language [33](#)
- LDAP [66](#)
 - configuring number attributes [72](#)
 - settings [67](#)
- legacy encryption [94](#)

INDEX

- legacy encryption mode [90, 94](#)
 - configuring
 - through the web interface [95](#)
 - using configuration file [95](#)
 - configuring on the phone [94](#)
 - encryption methods [178](#)
- licenses [177](#)
- LLDP Data Units [55](#)
- logging in [27](#)
- logs [172](#)
- M**
- media encryption with SRTP
 - FIPS mode [97](#)
 - standard encryption [93](#)
- media settings [58, 59](#)
 - configuring on the phone [59](#)
 - configuring through the web interface [59](#)
- metadata file, creation [165](#)
- minute offset [43](#)
 - configuring
 - through the web interface [43](#)
 - using the configuration file [44](#)
- N**
- network logs [176](#)
- network settings [47, 48](#)
 - configuring on the phone [47](#)
 - through the web interface [48](#)
- NTP server address [45](#)
- O**
- overview [10](#)
- P**
- password
 - reset [169](#)
 - setting [24](#)
- phone management application
 - configuring settings from the mobile device [105](#)
 - deleting pairing [104](#)
 - phone management application (*continued*)
 - disconnecting devices [103](#)
 - pairing and connecting devices [102](#)
 - settings [105](#)
 - phone name [33](#)
 - phone reboot
 - from the phone's user interface [41](#)
 - phone settings configuration
 - on the phone [33](#)
 - through the web interface [33](#)
 - physical layout [12](#)
 - PJSIP log level [174](#)
 - setting through web interface [175](#)
 - setting using configuration file [175](#)
 - PJSIP logs [174](#)
 - power supply [20](#)
 - power-saving mode [46](#)
 - prerequisites [18](#)
 - primary account [73](#)
 - protection against CSRF [171](#)
 - provisioning [121](#)
 - files on server [151](#)
 - purpose [6](#)
- R**
- reboot device [33](#)
- rebooting the phone
 - from the phone's user interface [41](#)
- registering
 - accounts [28, 30](#)
 - fallback account [28, 30](#)
 - on the phone [28](#)
 - primary account [28, 30](#)
 - secondary account [28, 30](#)
 - through the web interface [30](#)
- registration with the ZTI device management service [147](#)
- remote syslog
 - configuring [167](#)
- remote syslog server [167](#)

INDEX

- reset
 - to factory default [169](#)
 - to previous firmware version [169](#)
- reset to factory settings [169](#)
- ringtone level [33](#)
- rollback [121](#)
- RTCP XR [65](#)
 - collector URI [65](#)
 - enabling [65](#)
 - parameters [62](#)
 - quality estimate metrics [64](#)
- S**
- safety guidelines [10](#)
- safety instructions [10](#)
- SCEP
 - auto-renewal [163](#)
 - background polling [158](#)
 - certificate management [158](#)
 - configuring renewal request [164](#)
 - configuring through web interface [160](#)
 - configuring using the configuration file [161](#)
 - enrollment [158](#)
 - settings [161](#)
- secondary account [73](#)
- setting PJSIP log level
 - through web interface [175](#)
 - using configuration file [175](#)
- setting static IP address
 - from the phone [26](#)
 - through the web interface [26](#)
- setting up, DHCP server [25](#)
- settings
 - Device Management [149](#)
- SIP account
 - registration status [86](#)
- SIP invite [87](#)
- SIP NOTIFY [122](#)
- SIP settings [73](#), [74](#)
 - configuring settings on the phone [73](#)
- Site Specific Option Number [23](#)
- sleep mode [46](#)
 - enabling [46](#)
- Smart Mic [107](#)
 - upgrade [112](#), [113](#)
 - automatic [111](#)
 - manual [111](#), [115](#)
 - termination [114](#)
- source port [73](#)
- specifications [21](#)
- standard encryption [90](#)
 - 802.1x [91](#)
 - media encryption with SRTP [93](#)
- standard encryption for 802.1x
 - configuring
 - on the phone [92](#)
 - through the web interface [93](#)
- start up sound [33](#)
- static IP [47](#)
- status [172](#)
 - viewing [173](#)
- syslog [167](#)
- system logs [173](#)
- system recovery [169](#)
 - procedure [170](#)
- T**
- through the web interface [73](#)
- time and region settings [33](#)
- time format [44](#)
 - configuring
 - using the configuration file [45](#)
- TLS [73](#)
- transport protocol [73](#)
- U**
- usb only user mode [99](#)
 - icons [100](#)
 - time presentation [100](#)
- V**
- valid input [31](#)
- viewing

INDEX

viewing (*continued*)

- firmware version [26](#)

- IP address [26](#)

- MAC address [26](#)

- network logs [176](#)

- system logs [174](#)

voice quality monitoring [62](#)

- quality estimate metrics [64](#)

W

- web interface [27](#), [72](#)

- logging out [28](#)

- webapp debug [33](#)

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. We know that remote collaboration is an effective way to save time, money and contribute to a more sustainable world. We are Climate Neutral Certified, offering customers an option to purchase video conferencing equipment while keeping a clear climate conscience. 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 headquarters are 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

