Alcatel·Lucent

Installation and Administration of OmniTouch 4135 IP

ENGLISH

Rev 3C

ABOUT THIS DOCUMENT

This document only includes setup, registration of accounts and configuration. The use of the conference phone is described in the *Quick reference guide* and the *User guide*. The latest version of all documentation can be downloaded from www.alcatel-lucent.com.

CONTENT

Description **2**

Display information and web interface **3**
Display screen 3
Navigation and selection in menus 4
Using the web interface 6

Installation **7**
Connecting 7
Obtaining a network address 8
Login 8
Basic settings 9
Registering an account 11

Settings **13**
Login 13
Basic 13
SIP 16
Network 22
Media 25
LDAP 28
Web interface 30
Time & Region 31
Management 32
System 33

Headset and PA installation and settings **34**
Connecting a wireless headset 34
Connecting a PA interface box 35
PA settings 36

Hard system recovery **38**

Management – upgrade and configuration **39**
Firmware upgrade 39
Using a configuration file 40
Using a provisioning server 48

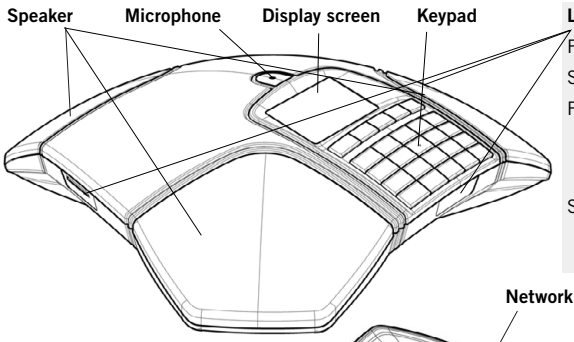
Managing phone book and conference guide **52**
Importing and exporting contacts 52
Importing and exporting conference groups 53

Checking status and logs **54**
Device 54
Network 54
Time & Region 55
SIP 55
Media 56
Log 57
Licenses 58

Technical data **59**

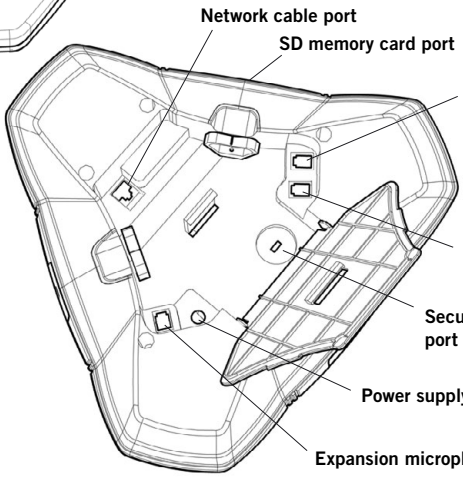
Appendix **61**

DESCRIPTION



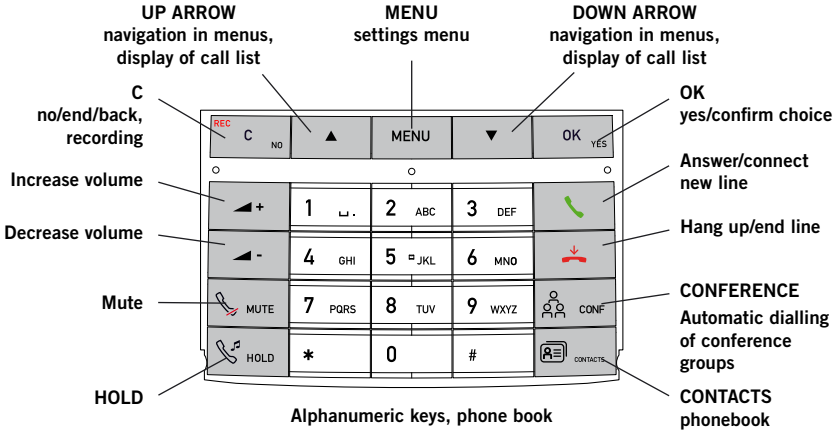
LEDs

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



Maintenance

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

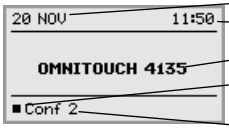


Some OmniTouch 4135 IP have a different keypad with other symbols. This does not affect the functions of the buttons

DISPLAY SCREEN

On Hook

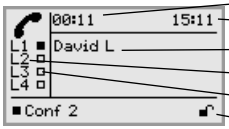
Press ↓ to display this screen.



Date
Time
Display text (can be changed)
■ **Registered**
□ **Not registered**
Account name (can be changed)

Off Hook

Press ↓ to display this screen.



Call duration
Time
Information text (see below)
Phone lines (L1–L4)
Line status (see below)
Secure connection (see page 10)

Line status:

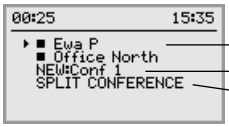
- □ Line free (Before account name – telephone not registered)
- ■ Line connected (Before account name – telephone registered)
- ■ Line on hold ("HOLD" displayed on the screen – all calls on hold)
- ✕ Line (called party) busy
- Own line put on hold by other party
- ● Recording call
- Secure connection

Information text displays one of the following:

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

Line menu

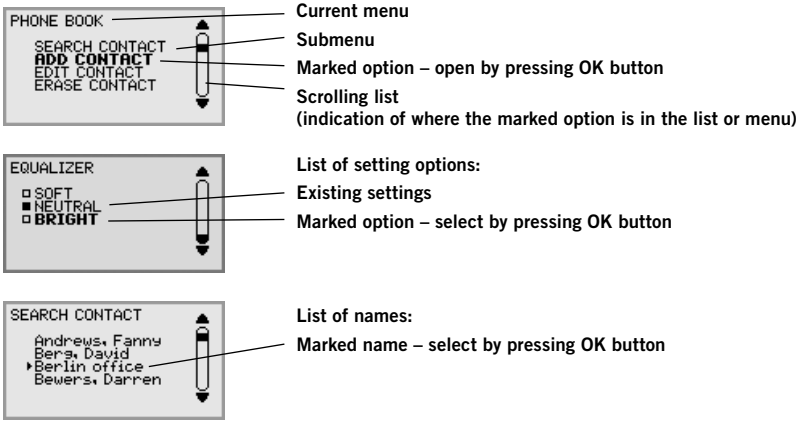
The line menu makes it possible to affect individual lines; put a call on hold, connect a call on hold or cut the line. The ⁂ (**Conference**) button toggles between the off hook screen and line menu during a call. The line menu may also be reached by pressing **MENU** > **LINE MODE** during a call.



Line/number/name
New line
Option for creating or splitting conference calls

Menu

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



NAVIGATION AND SELECTION IN MENUS

⇨ Press **MENU**.

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

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

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

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

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

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

Writing style in instructions

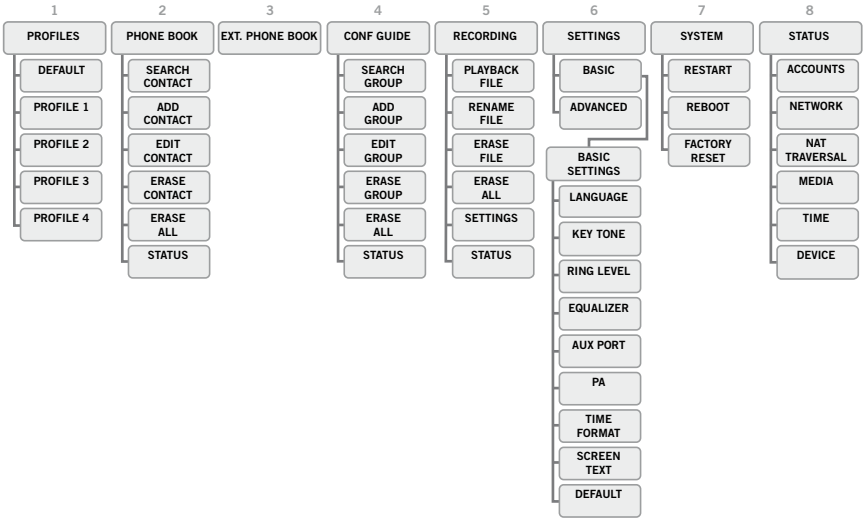
In the instructions, **MENU** > **SETTINGS** (6) means you should:

⇨ Press **MENU**.

⇨ Mark the **SETTINGS** option using the arrow buttons and confirm by pressing **OK** to open the menu (or press button number **6**).

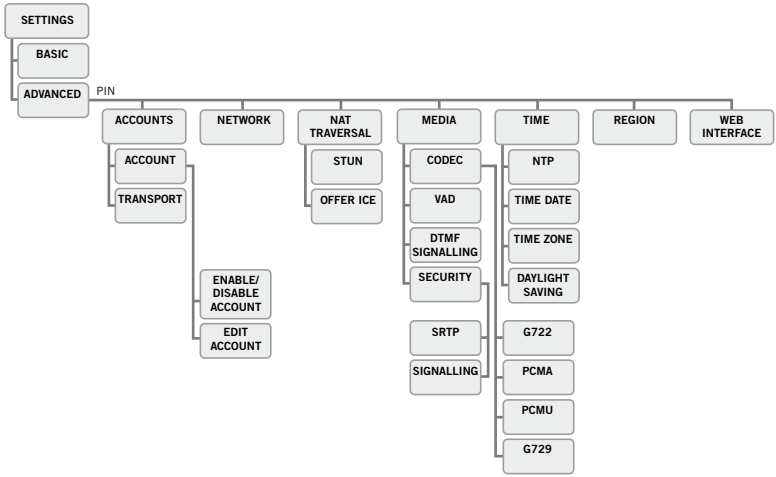
Correspondingly, **Phone book** > **Conference Guide** in the web interface means you should select Menu Phone book and the Conference Guide tab.

Menu tree



Menu tree, advanced settings

The advanced settings are protected by administrator's PIN code. The default value is **1234**.



The simplest way to make settings and edit contacts is using a PC and the OmniTouch 4135 IP web interface.

USING THE WEB INTERFACE

You can use the web browser of a PC connected to the same network to manage contacts, conference groups and settings in the OmniTouch 4135 IP.

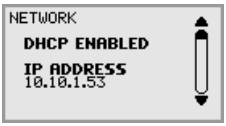
For security reasons, recordings can only be managed directly on the OmniTouch 4135 IP. All other settings that can be made directly on the OmniTouch 4135 IP can also be made via the web interface. It is also possible to import and export contacts and conference groups, name user profiles and change PIN codes, which can only be done via the web interface. The administrator can also view logs, update software and create a configuration file.

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

Checking IP address

⇨ Press **MENU** and select the sub menu **STATUS** > **NETWORK** (8,2).

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

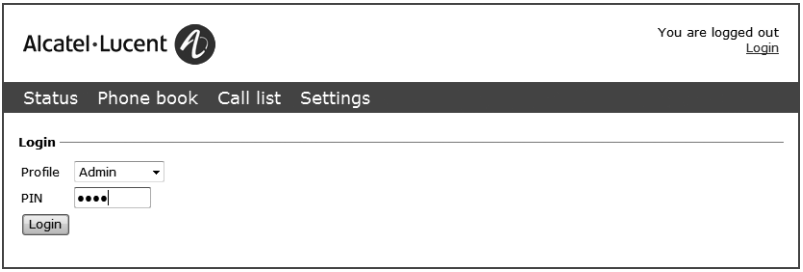


ⓘ Use this address to log into the web server in the conference phone.

Login

⇨ Log into the web server in OmniTouch 4135 IP by entering the phone's network address in your computer's web browser.

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

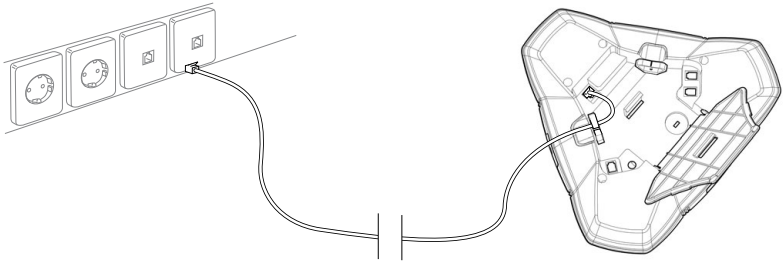


The printed Installation Guide provides brief and simplified installation instructions. The guide includes the basic settings for a quick start and works in most cases.

CONNECTING

⇨ Connect the OmniTouch 4135 IP to the network with the provided cable as illustrated below.

ⓘ The OmniTouch 4135 IP is operated directly from the network (Power over Ethernet). If the network does not supports this, a power adapter may be purchased as accessory.



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

The OmniTouch 4135 IP must obtain a network address and be registered in a SIP PBX before it can be used. The easiest way to register an account and make the settings in the OmniTouch 4135 IP is using a computer connected to the same network and via the integrated web server.

OBTAINING A NETWORK ADDRESS

Connecting to a network with DHCP

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

Connecting to a network with static IP addresses

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

⇨ Press **MENU** and select **SETTINGS** > **ADVANCED** (6,2).

⇨ Enter the PIN code.

ⓘ The default code is **1234**.

⇨ Select **NETWORK** (2)

⇨ Select **STATIC IP**.

⇨ Enter values for the IP ADDRESS.

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

⇨ Enter HOST NAME
Default is kt300ip.

⇨ Enter DOMAIN

⇨ Enter NETMASK

⇨ Enter GATEWAY

⇨ Enter DNS 1

⇨ Enter DNS 2
The display shows DONE.

LOGIN

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

BASIC SETTINGS

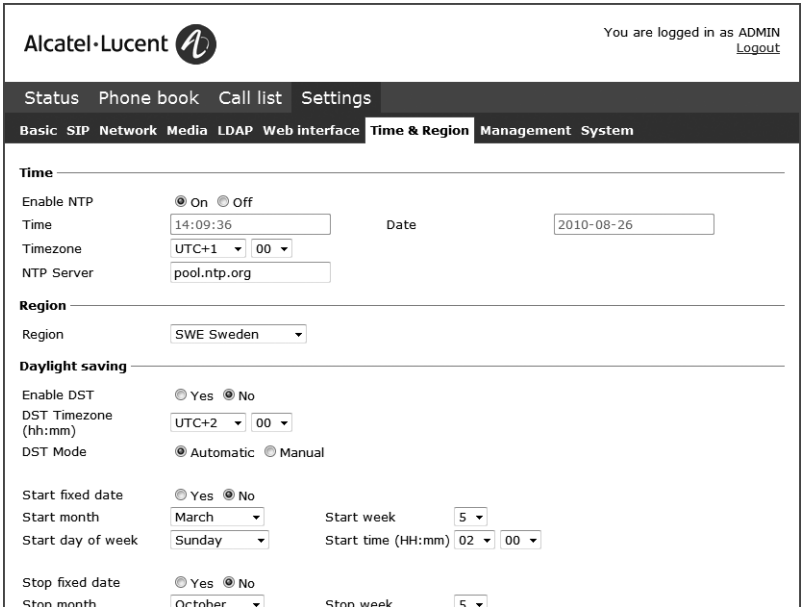
The following settings should be done during installation.

ⓘ See page 47 about Provisioning if you are responsible for installing or upgrading many phones.

Note that all settings on the Basic tab also affect the user profile Default. Other user profiles can be changed individually. The settings on the Basic tab, except the name and PIN for Admin, can be modified by any user. Other settings require a login as Admin.

Setting time and region

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



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

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

⇨ Select the region where you are.

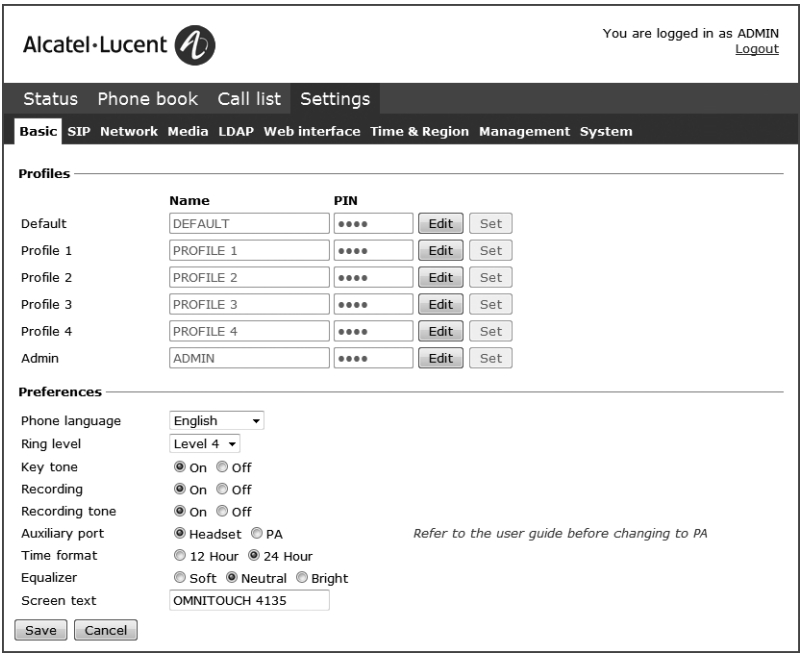
ⓘ This setting affects the signalling.

⇨ Save the setting.

The OmniTouch 4135 IP reboots with the new settings.

Changing the language

⇨ Select **Settings** > **Basic**.



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

Changing the PIN

We recommend that you change the PIN code for Admin from the default setting to protect the settings. Make a note of the new PIN code and keep it in a safe place. The administrator's PIN code can only be reset by a full factory reset!

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

⇨ Enter a new PIN.

ⓘ The PIN code may consist of 8 digits.

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

REGISTERING AN ACCOUNT

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

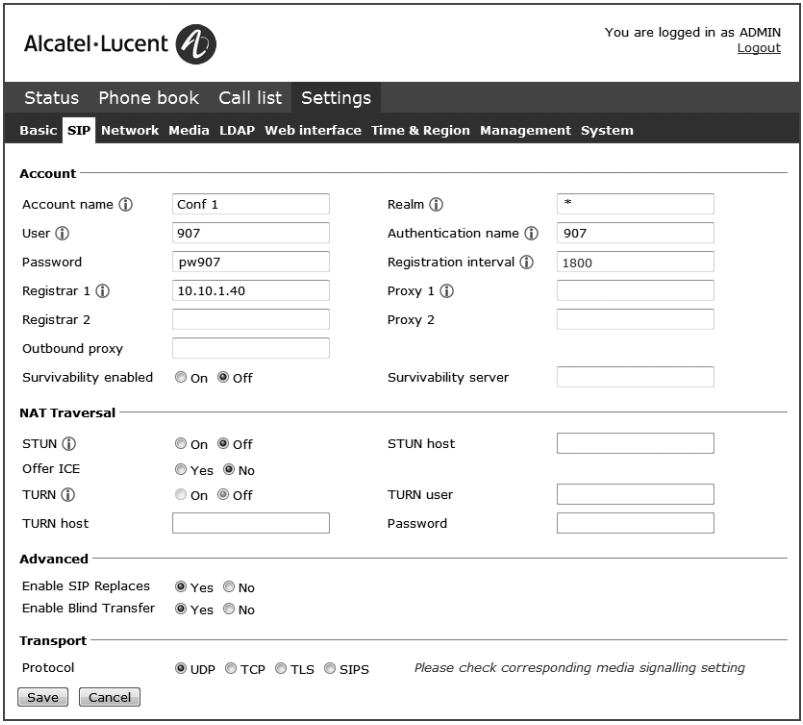
See the heading “SIP” on page 16 for a detailed description of all settings.

⇨ Select **Settings** > **SIP**.

⇨ Enter the account information you have received.

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

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

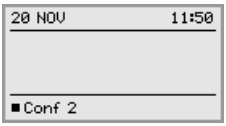


⇨ Select a method of NAT traversal if you have received this information.

⇨ Select a different transport protocol if you have received this information. See page 19 about using a secure transport protocol.

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

The OmniTouch 4135 IP responds by showing REGISTERING. If registration is successful, your selected account name will appear at the bottom of the display screen next to a shaded square.



Make media settings

⇨ Select a different codec priority, if you do not accept the default settings. See page 25.

⇨ Select a SRTP option if you need a secure media protocol. See page 26. Note that this also requires a corresponding transport setting on the SIP tab.

Almost all settings can be done directly on The OmniTouch 4135 IP. See “NAVIGATION AND SELECTION IN MENUS” on page 4 for using the menu system. We explain how to make settings using the web interface as this is the easiest method.

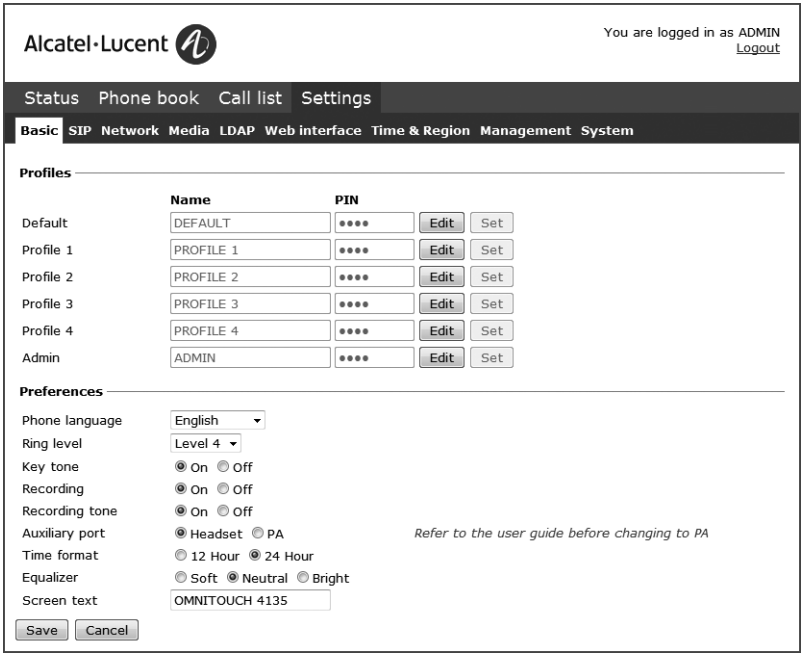
For safety reasons, recordings can only be managed directly on the OmniTouch 4135 IP. All other settings can be changed via the web interface. The web interface also allows you to import and export contacts and conference groups, rename user profiles and change PIN codes. As an administrator, you can also study logs, upgrade the software and create an XML based configuration file for easier management of a set of phones.

LOGIN

See “USING THE WEB INTERFACE” on page 6 for a description of how to log in to the web server in The OmniTouch 4135 IP.

BASIC

⇨ Select **Settings** > **Basic**.



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

Profiles – edit name and PIN

We recommend that you change the PIN code from the default setting to protect the settings.

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

⇨ Enter a new PIN code.

ⓘ The PIN code may consist of 8 digits.

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

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

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

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

Language

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

On phone: **MENU** > **SETTINGS** > **BASIC** > **LANGUAGE** (6,1,1).

Ring level

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

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

On phone: **MENU** > **SETTINGS** > **BASIC** > **RING LEVEL** (6,1,3).

Key tone

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

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

On phone: **MENU** > **SETTINGS** > **BASIC** > **KEY TONE** (6,1,2).

Recording

It is possible to turn off the recording feature. This setting can only be done by the administrator and affects all profiles.

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

Recording tone

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

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

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

Settings when connecting external equipment (Aux)

The OmniTouch 4135 IP can be connected to a wireless headset or an external PA system. An optional PA interface box is required for PA system connection.

⇨ Select the **PA** option to activate features for external microphone mixer and PA system.

ⓘ Do not select the PA option unless a PA system is connected. This option turns off the internal microphone and internal speakers as default. The HEADSET option may be selected whether or not a headset is connected.

Time format

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

On phone: **MENU** > **SETTINGS** > **BASIC** > **TIME FORMAT** (6,1,7).

Equalizer

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

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

On phone: **MENU** > **SETTINGS** > **BASIC** > **EQUALIZER** (6,1,4).

Screen text

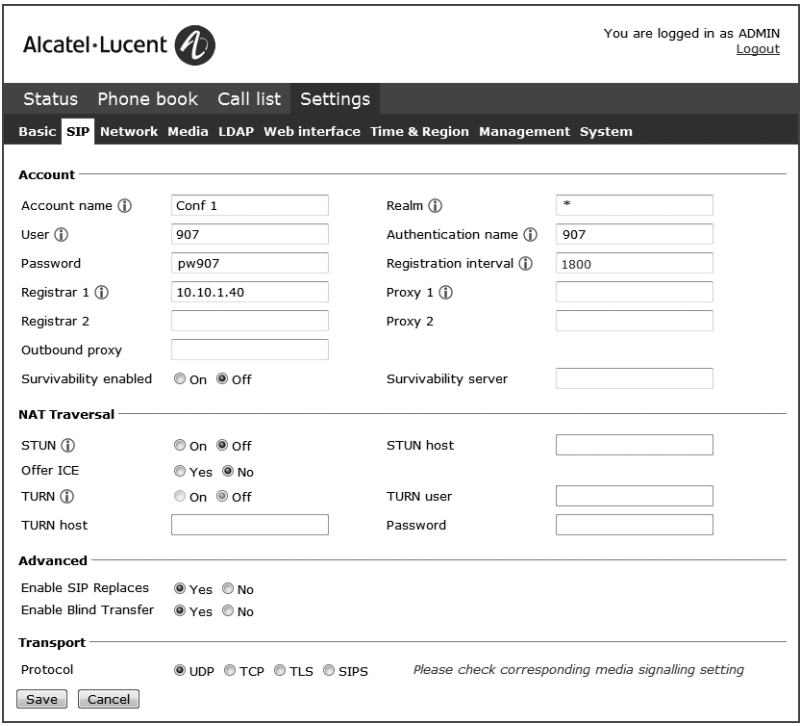
The text on the display screen is shown when The OmniTouch 4135 IP is in stand-by mode (on hook).

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

On phone: **MENU** > **SETTINGS** > **BASIC** > **SCREEN TEXT** (6,1,8).

SIP

⇨ Select **Settings** > **SIP**



Account

Account name	This is the name displayed on the screen. It can be set according to company standards.
User	The account (customer) name.
Password	The password used for the Realm authentication.
Registrar 1	Shall contain the IP address or the public name of the SIP server where the account is registered (e.g. 10.10.1.100 for a local SIP server or sip.company.net for a public VoIP service provider)
Registrar 2	Alternative registrar for SIP redundancy
Realm	The protection domain where the SIP authentication (name and password) is valid. This is usually the same as the registrar. If

	left blank, or marked with a "*", the information is taken from the Registrar field.
Authentication name	The name used for the Realm authentication. This may be the same as the user name, but must be filled in.
Registration Interval	This is a request to the SIP server for when the registration should expire. OmniTouch 4135 IP automatically renews the registration within the time interval if the phone is still on and connected to the server. The default value is 1800 seconds.
Proxy 1	Shall contain the proxy server used for Internet communication, if any. Can be left blank.
Proxy 2	
Outbound proxy	
Survivability enabled	
Survivability server	

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **ACCOUNTS** (6,2,1).

Nat traversal

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

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

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

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

STUN	STUN (*Simple Traversal of UDP through NATs*) is a protocol 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 a NAT to

	discover the presence and specific type of NAT and obtain the mapped (public) IP address (NAT address) and port number that the NAT has allocated for the application's *User Datagram Protocol* (UDP) connections to remote hosts. The protocol requires assistance from a 3rd-party network server (STUN server). STUN should be activated if an external SIP server cannot connect to the OmniTouch 4135 IP behind a firewall NAT function and the SIP server supports STUN. A suitable STUN server is usually provided by the VoIP service provider. Note: STUN might also be referred to as *Session Traversal Utilities for NAT*.
STUN host	The IP address or public name of the STUN server.
Offer ICE	ICE (*Interactive Connectivity Establishment*), is a STUN addition that provides various techniques to allow SIP-based VoIP devices to successfully traverse the variety of firewalls that may exist between the devices. The protocol provides a mechanism for both endpoints to identify the most optimal path for the media traffic to follow.
TURN	TURN (*Traversal Using Relay NAT*) TURN is an extension of the STUN protocol that enables NAT traversal when both endpoints are behind symmetric NAT. With TURN, media traffic for the session will have to go to a relay server. Since relaying is expensive, in terms of bandwidth that must be provided by the provider, and additional delay for the media traffic, TURN is normally used as a last resort when endpoints cannot communicate directly.
TURN User	User authentication name on the TURN server.
TURN host	The IP address or public name of the TURN server.
Password	User authentication password on the TURN server.

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **NAT TRAVERSAL** (6,2,3).

Advanced

Enable SIP Replaces	Default is **Yes**. Setting this option to **No**, will instruct the PBX not to use the *SIP replace* header. Some PBXes try to take over the bridging functionality from OmniTouch 4135 IP using this command, which causes the calls to interrupt.
Enable Blind Transfer	Default is **No**. Setting this option to **Yes**, will enable the transfer function (**MENU** > **TRANSFER**) during a call if the PBX supports blind transfer.

Transport

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

Note that if you choose to use a secure connection, both units must support it. Otherwise they cannot negotiate a connection. If an incoming call demands a secure TLS or SIPS connection, the OmniTouch 4135 IP uses the appropriate protocol even if you have set the phone to use UDP.

Protocol

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

UDP is the default protocol for SIP.

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

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

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

ⓘ Even if Transport is set to TLS or SIPS, the OmniTouch 4135 IP still accepts incoming UDP or TCP signalling.

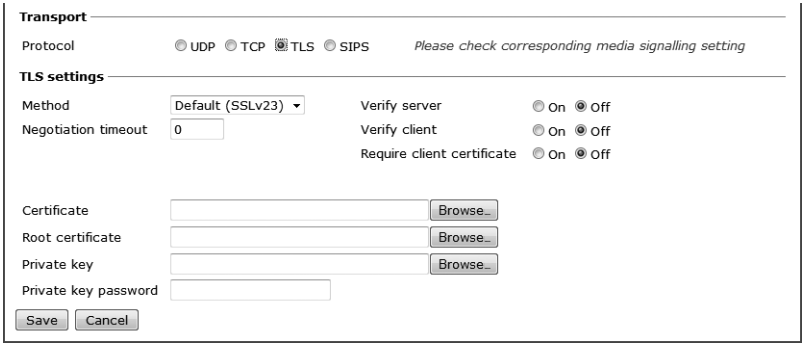
On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **ACCOUNTS** > **TRANSPORT** (6,2,1,3).

TLS Settings

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

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

Youcan further increase security by requiring verification of the server, or the client when the OmniTouch 4135 IP acts as a server for incoming calls.

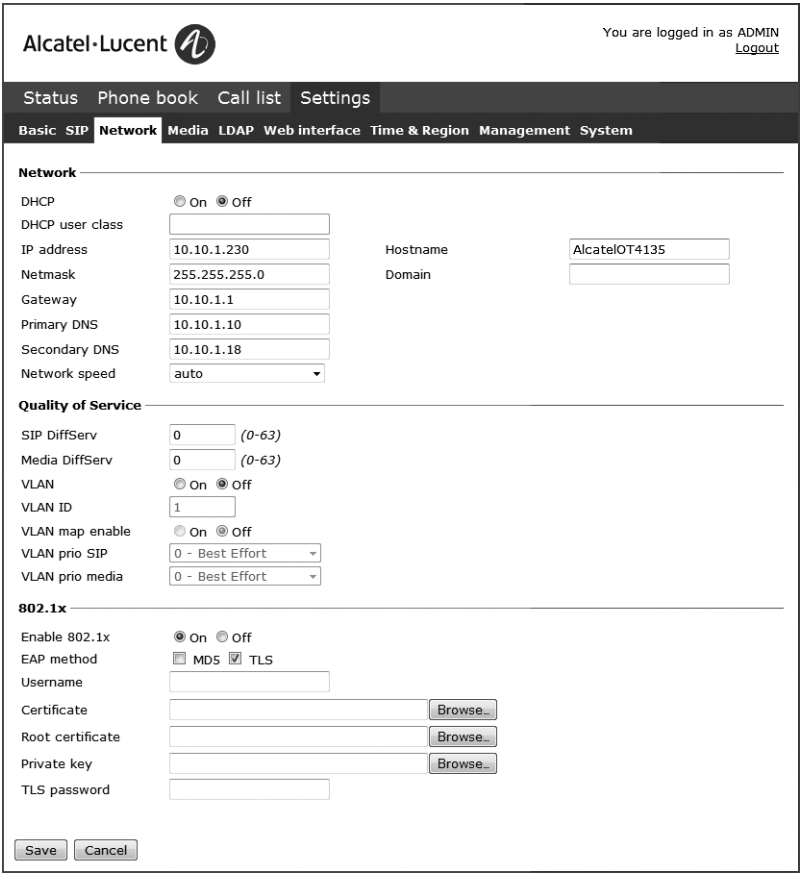


Method	The TLS includes a variety of security measures. The methods are defined in the versions of the standard (SSL, SSL v2, SSL v3, TLS v1, TLS v2). The default method is SSLv23, which accepts both SSL v2 and v3.
Negotiation timeout	The TLS settings are negotiated during a call setup (both incoming and outgoing). If this negotiation does not succeed within the specified time (seconds) the negotiation is aborted. Timeout is disabled with 0 (zero).
Verify client	When set to On, the OmniTouch 4135 IP will activate peer verification for incoming secure SIP connections (TLS or SIPS).
Require client certificate	When set to On, the OmniTouch 4135 IP rejects incoming secure SIP connections (TLS or SIPS) if the client does not have a valid certificate.
Verify server	When the OmniTouch 4135 IP is acting as a client (outgoing connections) using secure SIP (TLS or SIPS) it will always receive a certificate from the peer. If Verify server is set to On, the OmniTouch 4135 IP closes the connection if the server certificate is not valid.

Certificate	Here you can upload a certificate to the OmniTouch 4135 IP to be used for TLS or SIPS communication. A certificate is a file that combines a *public key* with information about the *owner* of the public key, all signed by a trusted third party. If you trust the third party, then you can be sure that the public key belongs to the person/organization named in that file. You can also be sure that everything you decrypt with that public key is encrypted by the person/organization named in the certificate.
Root certificate	The public key in the root certificate is used to verify other certificates. A root certificate is only needed if you have selected client or server verification. A root certificate is signed by the same public key that is in the certificate, a so-called "self-signed" certificate. A typical root certificate is one received from a *Certificate Authority*.
Private key	Here you can upload a private key to the OmniTouch 4135 IP to be used for TLS or SIPS communication. A private key is one of the keys in a key-pair used in *asymmetric cryptography*. Messages encrypted using the public key can only be decrypted using the private key.
Private key password	The password used for encryption of the private key, if it is encrypted.

NETWORK

⇨ Select **Settings** > **Network**.



DHCP — *Dynamic Host Configuration Protocol* is used by network devices (clients) to obtain the parameters necessary for operation in the IP network. This protocol reduces system administration workload, allowing devices to be added to the network with little or no manual configuration.

DHCP should be set to On if no other information is given. When set to On, all information on this page will be set automatically.

DHCP user class — Leave blank if this option is not required by the DHCP server.

IP address — IP address of the device (OmniTouch 4135 IP). The address

	is provided by the network administrator or service provider if DHCP is not in use.
Hostname	Set to ALCATELOT4135 as default. Can be changed to suitable name.
Netmask	Usually set to 255.255.255.0 to limit network traffic to the subnet.
Domain	The domain where the device is located. May be left blank.
Gateway	The device or server used for Internet communication.
Primary DNS	The address to the primary DNS (*Domain Name System*) server - a program or computer that maps a human-recognisable name to its computer-recognisable identifier (IP address).
Secondary DNS	The address of an optional secondary DNS server.
Network speed	Auto or locked at 100 Mbit/s full duplex. Only lock the speed if the network does not support auto negotiation.

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

Quality of Service

Quality of service is used in IP networks to provide different priority to different applications, users, or to guarantee a certain level of performance to a critical data flow such as voice or video. *Differentiated Services* or *DiffServ* is a networking architecture that specifies a simple mechanism for classifying network traffic using a 6-bit field in the header of the IP packets. *VLAN* (*Virtual LAN*) is a technology to logically divide a physical network into several logical nets and thus to differentiate traffic.

SIP DiffServ	Enter a value between 0 and 63 to prioritize the SIP messages.
Media DiffServ	Enter a value between 0 and 63 to prioritize the media packets (voice).
VLAN	By enabling this option, all communication to and from OmniTouch 4135 IP is done via the VLAN specified under VLAN ID. Note that this VLAN also must be used to communicate with OmniTouch 4135 IP via the web interface.
VLAN ID	The ID number to be used for the IP telephony VLAN.
VLAN map enable	Enabling VLAN priority mapping from the DiffServ setting.
VLAN prio SIP	Set a value between 0 and 7 to prioritize the SIP messages in the VLAN.
VLAN prio media	Set a value between 0 and 7 to prioritize the media packets in the VLAN.

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **NETWORK** > **ETHERNET** > **VLAN** (6,2,2,2,1).

802.1x

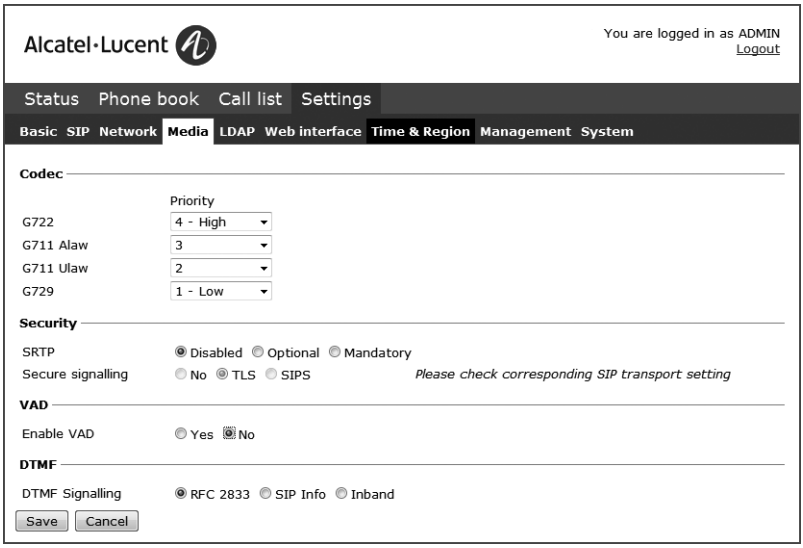
IEEE 802.1X is an IEEE Standard for port-based Network Access Control and is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

Enable 802.1x	By enabling this option, OmniTouch 4135 IP asks an authentication server for permission when connected to the LAN.
EAP method	Select which EAP (*Extensible Authentication Protocol*) method to use: MD5 or TLS.
Username	The device identity in the network.
MD5 password	Password for the device identity when using MD5.
Certificate	Here you can upload a certificate to the OmniTouch 4135 IP to be used for authentication when using TLS.
Root certificate	The public key in the root certificate is used to verify other certificates when using TLS.
Private key	Here you can upload a private key to the OmniTouch 4135 IP to be used for authentication when using TLS.
TLS password	The password used for encryption of the private key when using TLS.

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **NETWORK** > **ETHERNET** > **802.1X AUTH** (6,2,2,2,2).

MEDIA

⇨ Select **Settings** > **Media**.



The media settings determine how audio is sent between the devices. The devices negotiate via SIP before a call is connected. All devices must support the same media types, codecs and security settings.

Codec

Codecs are used to convert an analogue voice signal to a digitally encoded version and vice versa. Codecs vary in the sound quality they deliver and the bandwidth required. The OmniTouch 4135 IP supports the most common codecs and each codec can be given a precedence depending on your requirements for high quality audio or low bandwidth use.

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

G722 — G.722 is an *ITU-T* standard codec that provides 7 kHz wideband audio at a data rate within 64 kbit/s. It offers greatly improved speech quality compared with older narrowband codecs such as G.711, but requires a high quality network connection between the devices.

G711 Alaw	G.711 is an ITU-T standard codec that uses audio companding. Companding algorithms reduce the dynamic range of an audio signal. In analogue systems, this can increase the signal-to-noise ratio achieved during transmission and, in the digital domain, can reduce the quantization error. Two main compression algorithms are defined in the standard, the μ-law algorithm (used in North America and Japan) and A-law algorithm (used in Europe and the rest of the world).
G711 Ulaw	See G711 μ-law above.
G729	G.729 is an ITU-T standard codec that operates at 8 kbit/s. It is mostly used in VoIP applications with low bandwidth requirement.

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **MEDIA** > **CODEC** (6,2,4,1).

Security

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

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

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

SRTP	If set to disabled, the media is sent using RTP. Note that despite this setting, the OmniTouch 4135 IP will still use a secure channel if the opposite device demands it. If set to optional or mandatory, a padlock will be shown in the bottom right-hand corner of the screen. If the other devices support SRTP, the padlock will be locked. Otherwise, an open padlock will be displayed. If set to mandatory, the call will not be connected if the other devices do not support SRTP.
Secure signalling	The SIP messages (signalling) and the SRTP cipher key are sent on a different channel than the media and are not affected by the RTP/SRTP setting. To ensure a secure connection, the signalling must be secured using **TLS** or **SIPS**, see page 20. Note that the SIP transport setting must be set accordingly.

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **MEDIA** > **SECURITY** (6,2,4,4).

VAD

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

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

DTMF

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

If the device itself generates the tones and they are sent in the voice-frequency band, the method is called **Inband**. This is not the best method when using VoIP. Low bit rate codecs may corrupt the signalling tones and make it difficult for the switch to identify them.

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

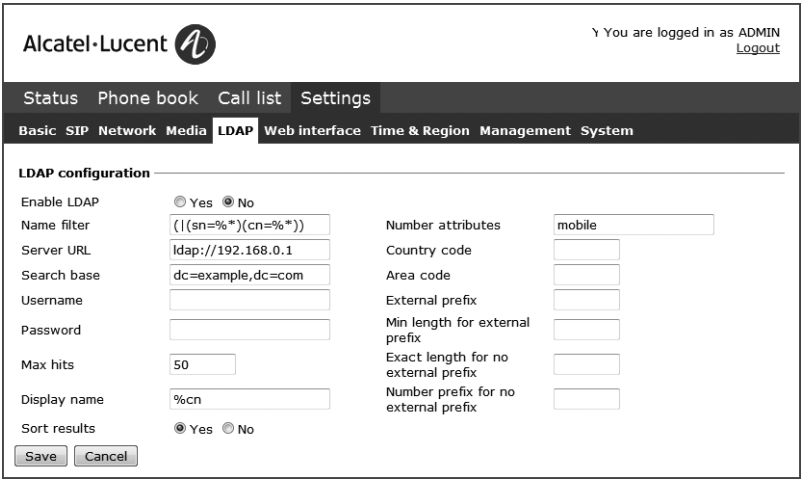
With **SIP Info** the DTMF signals are sent as SIP requests. The SIP switch creates the tones if the call is transferred to the PSTN.

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

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **MEDIA** > **DTMF SIGNALLING** (6,2,4,3).

LDAP

⇨ Select **Settings** > **LDAP**.



OmniTouch 4135 IP has support for an external phone book, which means it can communicate with a directory server using LDAP (*Lightweight Directory Access Protocol*). The built in search function dynamically filters the content from the LDAP database, based on the search characters the user enter.

To make the LDAP phone book available, the administrator has to activate and configure the LDAP feature.

ⓘ When enabled, it replaces the internal phonebook when the button (**Contacts**) is pressed. The internal phonebook can still be reached via **MENU** > **PHONEBOOK**.

Enable LDAP	The LDAP feature is disabled by default because it has to be configured.
Name filter	Defines how the entered search characters are used. The filter is designed conforming to the string representation of LDAP search filters described in *RFC2254*. The character % in the filter string will be replaced with the search character entered by the user. Example: **(|(sn=%*)(cn=%*))** - All entries with the search characters in the beginning of the **sn** OR **cn** attribute are presented to the user.
Server URL	The IP address of the LDAP server host. Supports *ldap* and *ldaps*.

Search base	The DN (*distinguished name*) of the search base Example: **dc=domain, dc=com**.
Username	Leave this field blank if the LDAP server does not require a username.
Password	Leave this field blank if the LDAP server does not require username and password.
Max hits	The maximum number of hits to return for each LDAP search.
Display name	Specifies how the search hits shall be presented on the display in OmniTouch 4135 IP. Example: **%cn** - shows the **cn** attribute. **%givenName %sn** - shows the **givenName** attribute and the **sn** attribute with a space in between.
Sort results	Sorts the search hits based on the Display name.
Number attributes	Here you define the attributes that shall be displayed for a selected search hit. Example: **mobile telephoneNumber** - shows the mobile phone number and office phone number on separate rows for the selected Display name.
Country code	By entering the country code where the phone is located, the country code in any phone number attribute is ignored, if it is identical.
Area code	By entering the area code where the phone is located, the area code in any phone number attribute is ignored, if it is identical.
External prefix	If a special prefix is needed to dial external numbers, it should be added here.
Min length for external prefix	Restricts the external prefix to be added only if the phone number is longer than the min length. This makes it possible to use short internal numbers.
Exact length for no external prefix	The external prefix in not added if the phone number has exactly the entered length.
Number prefix for no external prefix	All numbers that starts with this number will not have the external prefix added. Useful if you know that all internal numbers start with a certain number.

WEB INTERFACE

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

The web server in the OmniTouch 4135 IP supports secure connections using HTTPS.

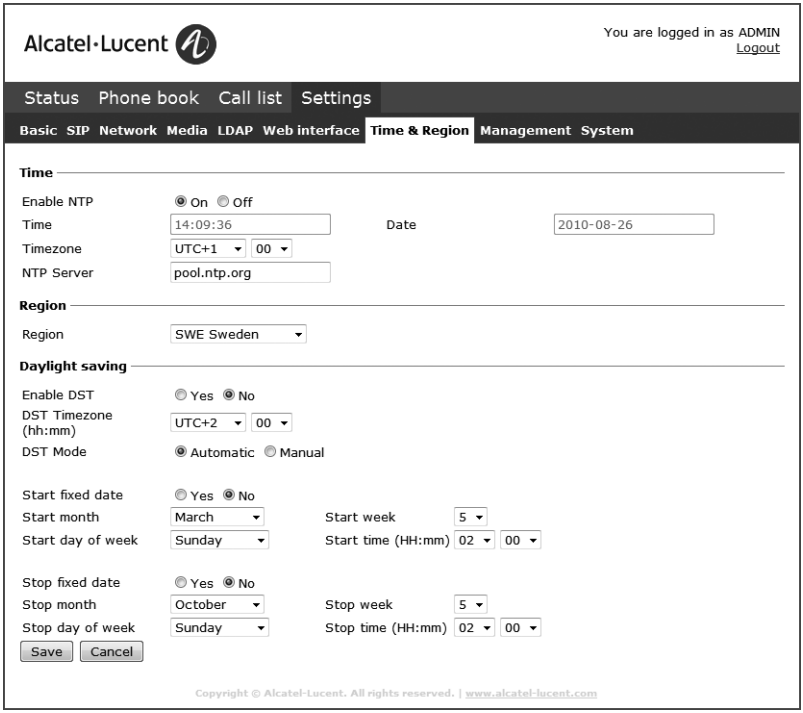
Enable HTTPS — Set *Enable HTTPS* to On if you need a secure communication between the PC used for setup and the phone.

Certificate — To use HTTPS you need to upload a certificate to the phone.

On phone: **MENU** > **SETTINGS** > **ADVANCED** > (PIN) > **WEB INTERFACE** (6,2,7).

TIME & REGION

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



Time

Enable NTP	NTP (*Network Time Protocol*) is a protocol for distributing the *Coordinated Universal Time* (UTC) by means of synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.
Time	This field shows the actual time if NTP is enabled. Otherwise enter the correct time (hh:mm:ss) and save the setting.
Date	This field shows the actual date if NTP is enabled. Otherwise enter the correct date (yyyy-mm-dd) and save the setting.
Timezone	Select the UTC time zone in your country.

NTP Server	The *NTP pool* is a dynamic collection of networked computers that volunteer to provide highly accurate time via NTP to clients worldwide. These computers are part of the pool.ntp.org domain and part of several subdomains divided by geographical zones. They are distributed to NTP clients via round robin DNS.

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

Region

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

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

Daylight saving

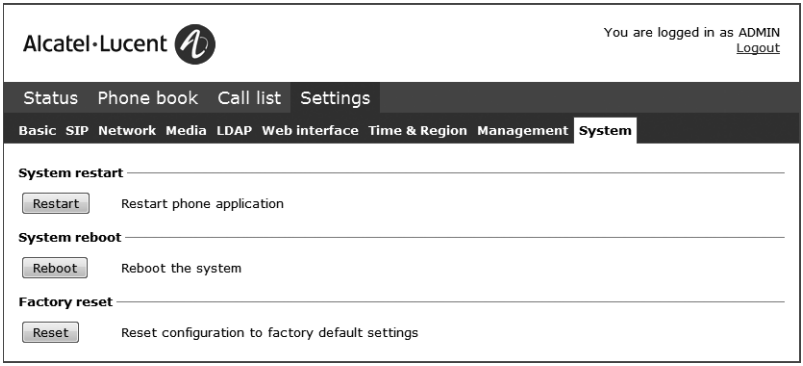
Enable DST	Select the Yes radio button if DST (*Daylight Saving Time* or *Summer Time*) is used in your country.
DST Timezone	Select the offset from UTC time when daylight saving is in use.
DST Mode	When set to Automatic, OmniTouch 4135 IP uses dates stored in the phone to adjust for DST. When set to Manual, you need to manually set the offset two times a year.
Start/Stop fixed date	Set to Yes if DST changes the same date every year in your country. Then select the time and date it changes. Set to No if DST changes a specific week and day each eyar. (For instance third sunday in March.) Then select the month, week and time it changes.

MANAGEMENT

See “MANAGEMENT – UPGRADE AND CONFIGURATION” on page 39.

SYSTEM

⇨ Select **Settings** > **System**.



Application restart

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

On phone: **MENU** > **SYSTEM** > **RESTART** (7,1).

System reboot

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

On phone: **MENU** > **SYSTEM** > **REBOOT** (7,2).

Factory reset

The **Reset** button resets the OmniTouch 4135 IP to factory default settings. All personal settings, including account information, are erased.

On phone: **MENU** > **SYSTEM** > **FACTORY RESET** (7,3).

Hard reset to factory settings

See page 38 about resetting the phone if you have forgotten the Admin PIN code.

CONNECTING A WIRELESS HEADSET

⇨ Connect the headset to the Aux port on OmniTouch 4135 IP.

The microphones from the OmniTouch 4135 IP and the wireless headset will work simultaneously and transmit the call to other participants in the phone conference.

Please refer to the headset manual for further information.

Turning off the internal speakers when using a headset

The internal speakers can be turned off temporarily if you wish to use the OmniTouch 4135 IP as a personal telephone with a headset.

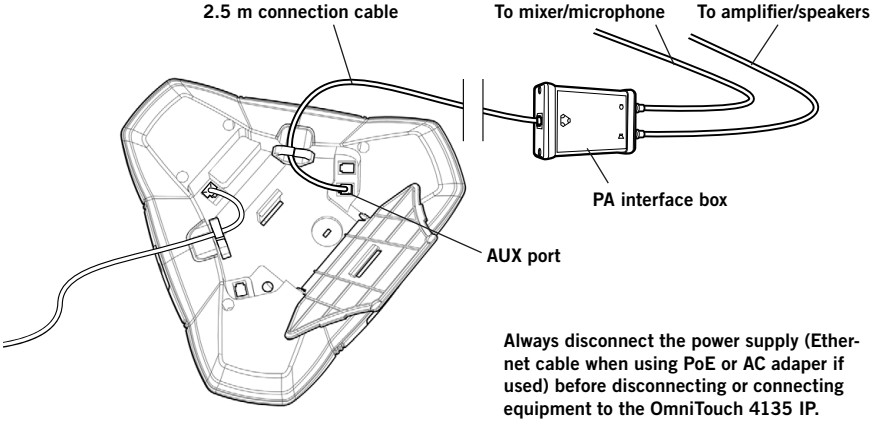
⇨ During a call, select **MENU** > **HEADSET**.

⇨ Select YES when asked “SPEAKER OFF?”.

ⓘ The speakers come on automatically when the call is ended.

CONNECTING A PA INTERFACE BOX

The OmniTouch 4135 IP can be connected to an external PA system using a PA interface box.



Always disconnect the power supply (Ethernet cable when using PoE or AC adaper if used) before disconnecting or connecting equipment to the OmniTouch 4135 IP.

⇨ Connect the PA-box to the AUX port on OmniTouch 4135 IP with the included cable.

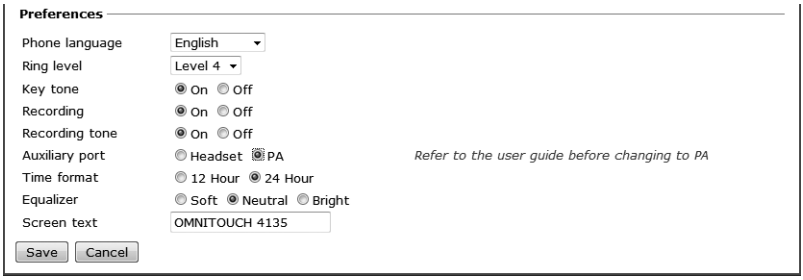
⇨ Connect the external amplifier to the RCA connector marked with a speaker.

⇨ Connect the microphone mixer to the RCA connector marked with a microphone.

Changing the auxilary port setting

⇨ Select **Settings** > **Basic**.

⇨ Select **PA** under the heading **Auxilary port** to aktivate the functions for external microphones and speaker system.



⇨ Click on **Save**.

ⓘ Do not select the PA option unless a PA system is connected. This option turns off the internal microphone and internal speakers as default.

On phone: **MENU** > **SETTINGS** > **BASIC** > **AUX PORT** (6,1,5).

PA SETTINGS

To match several types of situations and equipment, there are some settings available in the OmniTouch 4135 IP menu.

Activating internal microphone and speakers

ⓘ These settings are not available via the web interface.

⇨ Select **MENU** > **SETTINGS** > **BASIC** > **PA** (6,1,6).

⇨ Select INTERNAL MIC and press **OK** to switch between on (shaded box) and off.

ⓘ To ensure maximum audio quality, do not use the internal microphone and external microphones connected via the PA box at the same time.

ⓘ Only the internal microphone is turned off. Any external microphones connected to the OmniTouch 4135 IP are still turned on.

⇨ Select INTERNAL SPKR and press **OK** to switch between on (shaded box) and off.

ⓘ To ensure maximum audio quality, do not use the internal speakers and external speakers connected via the PA box at the same time.

Adjusting microphone volume from PA

⇨ During a call, select **MENU** > **PA** > **PA MONITOR**.

⇨ Adjust the microphone volume from the mixer so that the level on the display screen is around 10–12 when speaking in a normal tone.

Adjusting PA calibration manually

It is possible to calibrate the duplex performance of the conference phone when it is connected to a PA system. The calibration level can be set automatically by the OmniTouch 4135 IP or adjusted manually to any value between 0 and 5 (0 being full duplex).

- Increase the calibration if the other party experiences disturbing echo.
- Decrease the calibration if the other party experiences low duplex, i.e. your voice is muted or clipped when the other party is speaking.

ⓘ The position of the PA system's microphones and speakers and the amplifier's settings may affect full duplex performance.

⇨ Select **MENU** > **PA** > **CALIBRATION**.

ⓘ AUTO is the default setting and is recommended in most cases. The figure shown in brackets is the measured calibration value.

⇨ Select different levels and compare the audio quality to achieve your preferred setting.

ⓘ NB. You must ask the person you are calling to assess the effect of the adjustments you make.

Reset configuration

If you have forgotten the Admin PIN code, the only way to reset it to default is to do a hard factory reset. This is the same as the Factory reset in the system menu (**MENU** > **SYSTEM** > **FACTORY RESET**).

ⓘ This erases all settings including account information and contacts!

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

⇨ Press and hold the **MENU** button while you connect the cable again (i.e. starts the OmniTouch 4135 IP). Hold the button pressed until the SYSTEM RECOVERY menu is shown on the display.

ⓘ You can press any other button than **1**, **2**, or **3** to start the phone without resetting.

⇨ Press **1** to select **Reset configuration** and confirm with **OK**.

⇨ Upgrade to the latest version of the software when the phone has started and redo the setup of account and other settings (see page 9).

Restore firmware

This replaces the current software with the one supplied with the phone. All settings are erased.

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

⇨ Press and hold the **MENU** button while you connect the cable again (i.e. starts the OmniTouch 4135 IP). Hold the button pressed until the SYSTEM RECOVERY menu is shown on the display.

ⓘ You can press any other button than **1**, **2**, or **3** to start the phone without restoring the firmware.

⇨ Press **3** to select **Restore firmware** and confirm with **OK**.

All content in the phone's memory is erased and the firmware supplied with the phone is written to the memory.

⇨ Upgrade to the latest version of the software when the phone has started and redo the setup of account and other settings (see page 9).

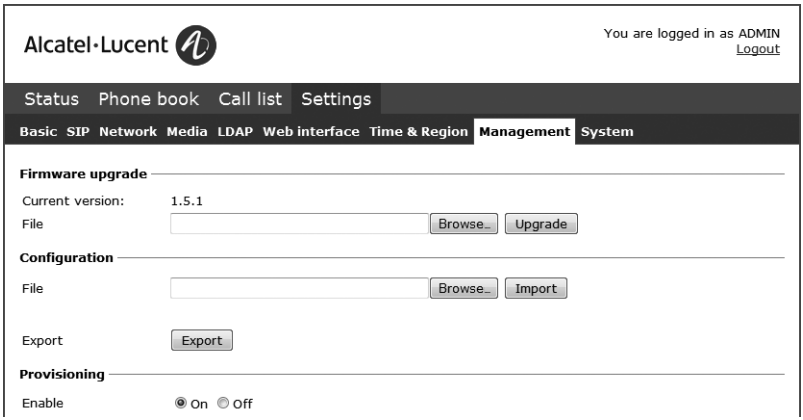
FIRMWARE UPGRADE

t is possible to download the latest firmware version, via the website (**www.businesspartner.alcatel-lucent.com**). The OmniTouch 4135 IP can then be upgraded via a computer connected to the same network or using a SD card.

The OmniTouch 4135 IP can also be upgraded and configured using a provisioning server (see page 47).

Using the web interface

I⇨ Select **Settings** > **Management**.



Upgrading from downloaded file

⇨ Download the firmware file from **www.businesspartner.alcatel-lucent.com**.

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

⇨ Click on the **Upgrade** button.
The browser window and the OmniTouch 4135 IP display shows that the upgrading has begun.

ⓘ The download and installation can take several minutes. Do not interrupt the upgrade and do not disconnect plugs to the OmniTouch 4135 IP during the upgrade. Interrupting the upgrade may render the conference phone inoperable.

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

Upgrading from SD card

Upgrading from SD card may be suitable if you have many phones to upgrade. The phones do not have to be connected to the network.

⇨ Download the latest firmware as above and save it on a SD card.

⇨ Put the SD card in the phone you want to upgrade.

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

⇨ Press and hold the **MENU** button while you connect the cable again (i.e. starts the OmniTouch 4135 IP). Hold the button pressed until the SYSTEM RECOVERY menu is shown on the display.

ⓘ You can press any other button than **1**, **2**, or **3** to start the phone without any change.

⇨ Press **2** to select **SD-card upgrade**.

The OmniTouch 4135 IP is upgraded with the firmware file on the SD card and starts when the upgrade is done.

After upgrading

If DHCP is used in the network, the IP address may have been changed. If the web browser loses contact with OmniTouch 4135 IP, check the IP address on the conference phone (see “USING THE WEB INTERFACE” on page 6).

USING A CONFIGURATION FILE

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

- Backup (i.e. if the system has been reset to factory default)
- Configuration interface (there are some settings that are not configurable via the web interface)
- Management tool (export, edit and import settings to a set of phones instead of doing the settings on each phone)
- Use with a Provisioning server, see page 47.

The structure of the xml file is as follows:

Tag	Default	Description
<config_version>		
<locale>		
<region>	SWE	
<default_language>	eng	The language used in the MMI if no language has been set for the profile used. Valid is: dan, tur, spa, dut, eng, ger, por, fin, ita, swe, gre, fra, nor, pol, rus
<default_timeformat>	12	Default time format used in the MMI if no time format has been set for the profile used. Valid values are: 12 or 24.
<recording>		
<enable>	true	
<logging>		
<level>	3	The phone application logs messages to log facility LOCAL0. Log level 1–5 (equivalent to Fatal–Trace)
<log_sip>	true	Log SIP messages to log facility LOCAL1. Default is true.
<remote_log>	false	Log messages to a remote log server. Default is false.
<remote_host>		Remote log server.
<network>		
<net>		
<dhcp>	true	Specify if DHCP should be used to obtain network settings. If so, the other network settings (except dhcp_userclass) won't be used.
<dhcp_userclass>		Specify if this option is used by the DHCP server.
<ip>		Specify the IP address.
<netmask>		The netmask of the IP address.
<gateway>		Specify the default gateway to be used.
<dns1>		Specify at most two Domain Name Servers to be used.
<dns2>		
<hostname>	AlcatelOT4135	Specify host name.
<domain>		Specify domain name.
<vlan>		Virtual LAN enabled if set to true
<enable>	false	
<id> VLAN ID.	1	
<std_prio_map>	false	
<sip_priority>	0	
<media_priority>	0	
<ether_8021x>		
<enable>	false	
<username>		

```
            <eap_md5>
                <enable>        false
                <password>
            <eap_tls>
                <enable>        false
                <password>
    <qos>
        <dscp_sip>              0
        <dscp_media>            0
    <time>
        <ntp>                   true
        <timezone>              UTC+01:00
        <ntps>                  pool.ntp.org
        <dst_save>              false
        <dst_auto>              true
        <dst_offset>            UTC+2:00
        <dst_start_fixed>       false
        <dst_start_month>       3
        <dst_start_week>        5
        <dst_start_day>         0
        <dst_start_time>        02:00
        <dst_stop_fixed>        false
        <dst_stop_month>        10
        <dst_stop_week>         5
        <dst_stop_day>          0
        <dst_stop_time>         02:00
```

<sip>

<udp_transport>	true	Specify if UDP shall be used as transport.
<udp_port>	5060	Specify the UDP port to listen to.
<tcp_transport>	false	Specify if TCP shall be used as transport.
<tcp_port>	5060	Specify the TCP port to listen to.
<tls_transport>	false	Specify if TLS shall be used as transport.
<tls_port>	5061	Specify the TLS port to listen to.
<sips_transport>	false	Specify if SIPS shall be used as transport.
<rtp_port>	4000	Specify the start port for RTP traffic.
<outbound_proxy>		Specify the URL of outbound proxies to visit for all outgoing requests. The outbound proxies will be used for all accounts and will be used to build the route set for outgoing requests. The final route set for outgoing requests will consist of the outbound proxies and the proxy configured in the account.
<use_stun>	false	Use Simple Traversal of UDP through NATs (STUN) for NAT traversal. Default is no.
<stun_domain>		Specify domain name to be resolved with DNS SRV resolution to get the address of the STUN servers. Alternatively application may specify stun_host and stun_relay_host instead.
<stun_host>		Specify STUN server to be used in "HOST[:PORT]" format. If port is not specified, default port 3478 will be used.

<use_turn>	false	Use Traversal Using Relay NAT (TURN) for NAT traversal. Default is no.
<turn_host>		Specify TURN relay server to be used.
<turn_tcp>	false	Use TCP connection to TURN server. Default is false.
<turn_user>		TURN username.
<turn_passwd>		TURN password.
<nat_type_in_sdp>	1	Support for adding and parsing NAT type in the SDP to assist troubleshooting. The valid values are: 0: no information will be added in SDP and parsing is disabled 1: only the NAT type number is added 2: add both NAT type number and name
<require_100rel>	false	Specify whether support for reliable provisional response (100rel and PRACK) should be required by default. Note that this setting can be further customized in account configuration.
<use_srtp>	0	Specify default value of secure media transport usage. Note that this setting can be further customized in account configuration. 0: SRTP will be disabled, and the transport will reject RTP/SAVP offer. 1: SRTP will be advertised as optional and incoming SRTP offer will be accepted. 2: The transport will require that RTP/SAVP media shall be used.
<srtp_secure_signaling>	1	Specify whether SRTP requires secure signalling. This option is only used when use_srtp option above is non-zero. Note that this setting can be further customized in account configuration. 0: SRTP does not require secure signalling 1: SRTP requires secure transport such as TLS 2: SRTP requires secure end-to-end transport (SIPS)
<codec1>		
<type>	G722	Codec type
<name>	G722	Codec name
<prio>	4	Codec priority (0-4)
<codec2>		
<type>	PCMA	Codec type
<name>	PCMA	Codec name
<prio>	3	Codec priority (0-4)
<codec3>		
<type>	PCMU	Codec type
<name>	PCMU	Codec name
<prio>	2	Codec priority (0-4)
<codec4>		
<type>	G729	Codec type
<name>	G729	Codec name
<prio>	1	Codec priority (0-4)
<dtmf>	2	DTMF signalling. Default is 2.

		0: In-band 1: SIP message 2: RTP message
<no_vad>	true	Disable VAD? Default is VAD enabled.
<ec_tail>	0	Echo canceller tail length, in milliseconds.
<enable_ice>	false	Enable ICE?
<enable_relay>	false	Enable ICE relay?
<enable_presence>	false	Enable the use of presence signalling.
<enable_sip_replaces>	true	
<enable_blind_transfer>	false	

<tls>

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

<account1>

<valid>	true	Shall always be set to true.
<name>		User defined name of the account
<id>		The full SIP URL for the account.
<registrar>		This is the URL to be put in the request URI for the registration.
<registrar2>		Used for redundancy
<publish_enabled>	false	If this flag is set, the presence information of this account will be published to the server where the account belongs.
<initial_auth>	false	If this flag is set, the authentication client framework will send an empty Authorization header in each initial request.
<initial_algo>		Specify the algorithm to use when empty Authorization header is to be sent for each initial request (see above).
<pidf_tuple_id>		Optional PIDF tuple ID for outgoing PUBLISH and NOTIFY. If this value is not specified, a random string will be used.
<force_contact>		Optional URI to be put as Contact for this account. It is recommended that this field is left empty, so that the value will be calculated automatically based on the transport address.
<require_100rel>	false	Specify whether support for reliable provisional response (100rel and PRACK) should be required for all sessions of this account.

<proxy_uri>		Optional URI of the proxies to be visited for all outgoing requests that are using this account (REGISTER, INVITE, etc).
<proxy_uri2>		Optional URI of the proxies (for redundancy) to be visited for all outgoing requests that are using this account.
<reg_timeout>	1800	Optional interval for registration, in seconds. If the value is zero, default interval will be used.
<cred>		Array of credentials. Normally, if registration is required, at least one credential should be specified to successfully authenticate the service provider. More credentials can be specified, for example when it is expected that requests will be challenged by the proxies in the route set.
<realm>	*	Realm. Use "*" to make a credential that can be used to authenticate any challenges.
<scheme>		Scheme (e.g. "digest").
<username>		Authentication name
<cred_data_type>	0	Type of data (0 for plaintext password).
<cred_data>		The data, which can be a plaintext password or a hashed digest.
<auto_update_nat>	true	This option is useful for keeping the UDP transport address up to date with the NAT public mapped address. When this option is enabled and STUN is configured, the library will keep track of the public IP address from the response of REGISTER request. Once it detects that the address has changed, it will unregister current Contact, update the UDP transport address and register a new Contact to the registrar.
<ka_interval>	15	Set the interval for periodic keep-alive transmission for this account. If this value is zero, keep-alive will be disabled for this account. The keep-alive transmission will be sent to the registrar's address after successful registration.
<ka_data>		Specify the data to be transmitted as keep-alive packets. Default: CR-LF.
<use_srtp>	0	Specify whether secure media transport should be used for this account. 0: SRTP will be disabled and the transport will reject RTP/SAVP offer. 1: SRTP will be advertised as optional and incoming SRTP offer will be accepted. 2: The transport will require that RTP/SAVP media is used.
<srtp_secure_signaling>	1	Specify whether SRTP requires secure signalling. This option is only used when use_srtp option above is non-zero. 0: SRTP does not require secure signalling 1: SRTP requires secure transport such as TLS 2: SRTP requires secure end-to-end transport (SIPS)

<sip_redundancy>		
<options_interval>	30	
<enable_pcs>	false	
<pcs_address>		

<provisioning>

<dev_mgnt>		
<enable>	true	
<use_dhcp_option>	true	
<dhcp_option>	43	
<file_server_address>		URL to DM server if DHCP not used
<pagename>		Base name of the configuration files to download. If setting is missing, it will be interpreted as ot4135
<firmware_upgrade_override_uri>		Use if the firmware upgrade files is located at a different address than the configuration files
<type>		Not used
<update_interval>	*/30 * * * *	DM update interval in crontab format
<https_check_srv_cert>	true	Verify server certificate.
<https_protocol>	auto	HTTPS protocol to use, mainly for old servers where opsnSSL can't detect the version automatically

<www>

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

<pa>

<enable_pa>	false	PA enabled, true or false
<enable_internal_mic>	false	Internal mic enabled when PA set to true.
<enable_internal_spkr>	false	Internal speakers enabled when PA set to true.
<calibration>	0	Calibration value. Note that 0 is auto, 1 is calibration value 1, 2 is calibration value 1, etc.

<ldap>

<enable>	false	
<name_filter>	(l(sn=%*)(cn=%*))	Name filter according to RFC2254.
<server_url>		URL of the LDAP server.
<search_base>	dc=example,dc=com	Search DN
<username>		Username. Leave blank if server accepts queries without a bind.
<password>		Password. Leave blank if server accepts queries without a bind.
<max_hits>	20	Max hits to return for each LDAP search.
<number_attributes>	mobile	Attributes from were the phone numbers should be read.
<country_code>		Country code which the phone resides in.
<area_code>		Area code which the phone resides in.
<external_prefix>		External prefix to prepend to external LDAP numbers.

<min_length_for_ext_prefix>		Minimum length (before conversion) when external prefix should be added.
<exact_length_for_no_ext_prefix>		Exact length (before conversion) were no external prefix should be added.
<number_prefix_for_no_ext_prefix>		Number prefix (before conversion) when no external prefix should be added.
<display_name>	%cn	Attribute that should be shown in the LDAP phone book.
<sort_results>	true	Sort LDAP search results.

Export configuration

⇨ Select **Settings** > **Management**.

⇨ Click on the **Export** button under **Configuration**.

The configuration file is shown in the web browser.

⇨ Choose to save the page as an xml file.

The xml file is as default saved in your folder for downloaded files. The default name is "ot4135-<MAC>.xml" (the MAC address of the unit).

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

Import configuration

⇨ Click on the **Browse...** button under **Configuration**.

⇨ Select the xml file and choose to open it.

⇨ Click on the **Import** button.

USING A PROVISIONING SERVER

Using *Provisioning* facilitates the upgrading and configuration of multiple conference phones. To use this feature, the Provisioning needs to be enabled and configured and the appropriate files must be located on a server reachable from all phones, here called a *Provisioning server*.

The configuration and firmware download are controlled with a configurable frequency. The default value is once every 30 minutes. (Note: The interval can only be edited directly in the configuration file.)

Configuration priorities

Because the same configuration parameters can be entered in multiple locations, there is a need for priorities. The local configuration files have the highest priority followed by the global configuration file. Configuration entered on the unit itself, via the web interface or directly on the phone, is overridden the next time the configuration files are downloaded.

ⓘ Note one exception. Phone language entered on the unit will take precedence.

ⓘ Note also that the server files (global and local configuration files) do not have to include all elements in the terminal configuration file. For example, by excluding the SIP account password, it is possible to set this on the terminal it without being overwritten by the server.

Files on the provisioning server

Global configuration file

The global configuration file contains the basic configuration – all settings that are common for all conference phones on your location. One easy way to create this file is simply to configure one phone and export the configuration file.

The default name for this file is *ot4135.xml*, but it is possible to create a custom name by using the *pagename* element in the configuration file.

Local configuration file

The local configuration file contains configuration parameters that are unique for every conference phone. The settings in this file takes precedence over the settings in the global configuration file.

The default name for this file is *ot4135-<MAC>.xml*, where <MAC> is the MAC address of the specific conference phone.

It is possible to create a custom name by using the *pagename* element in the configuration file.

Firmware binary

Contains the firmware binary that will be downloaded and installed by OmniTouch 4135 IP if the metadata file shows that this is a newer version than the present installed. The binary file can be downloaded from **www.businesspartner.alcatel-lucent.com**.

Firmware metadata file

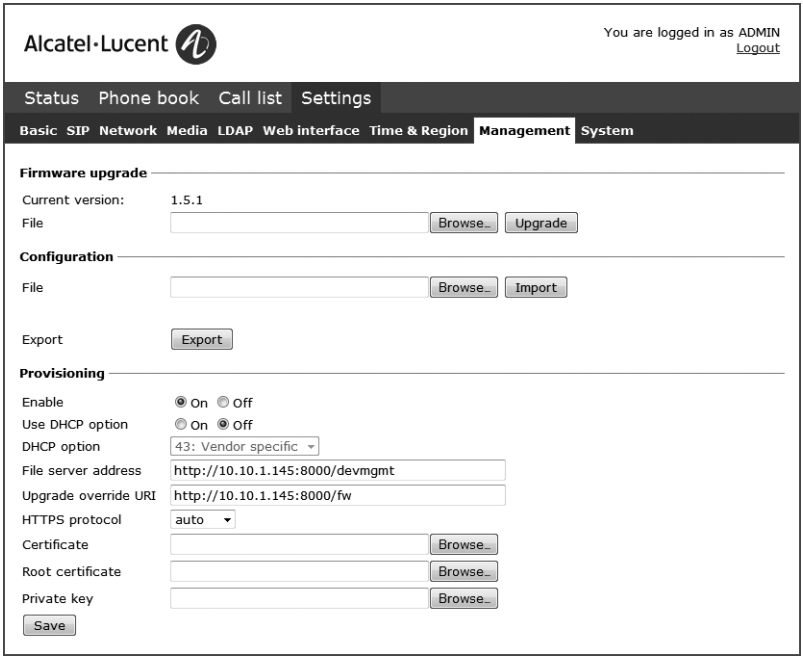
A metadata file in xml format with information of the firmware version in the binary file. The file is used to check if the binary file should be downloaded to the phone or not.

The name of this file shall be *ot4135_fw_version.xml*. The file shall contain the following elements in xml format.

<firmware_version>
<version>X.X.X </version> Eg. 1.5.1
<filename>xxxx </filename> Eg. ot4135_v1.5.1.kt
</firmware_version>

Provisioning configuration in OmniTouch 4135 IP

⇨ Select **Settings** > **Management**.



Provisioning

Enable	On enables Provisioning.
Use DHCP option	Set to on if you want to use DHCP option for DM server address.
DHCP option	Specifies which DHCP option to use.
File server address	DM server address if not provided by DHCP option.
Upgrade override URI	Use if the firmware upgrade files is located at a different address than the configuration files.
HTTPS protocol	Default is auto, but can be set to SSLv2 or SSLv3 if open-ssl auto detection fails.
Certificate	Here you can upload a certificate to the OmniTouch 4135 IP to be used for authentication when using Provisioning.
Root certificate	The public key in the root certificate is used to verify other certificates when using Provisioning.
Private key	Here you can upload a private key to the OmniTouch 4135 IP to be used for authentication when using Provisioning.

ⓘ Read more about certificates on page 21.

Setting up a Provisioning server

This is a description of a manual method to create the configuration files. This procedure can be simplified using a Device management system.

⇨ Select **Settings** > **Management**.

⇨ Enable Provisioning and enter the server information.

Creating a global configuration file

⇨ Configure one phone with the basic configuration.

⇨ Click on **Export** to create a configuratuion file.

⇨ Edit the xml file in a suitable editor.

⇨ Delete all elements that shall be set by the local configuration file or shall be set on the terminal.

ⓘ Update frequency and pagename can't be entered via the web interface.

⇨ Save the file with the name **ot4135.xml** on the *File server address* specified above.

Creating local configuration files

⇨ Save a copy of the configuration file for each conference phone on your location.

⇨ Delete all elements that are set by the global configuration file or shall be set on the terminal.

The default name for each file is *ot4135-<MAC>.xml*, where <MAC> is the MAC

address of the specific conference phone.

⇨ Place the configuration files on the Provisioning server.

Firmware binary

⇨ Place the firmware binary file on the Provisioning server.

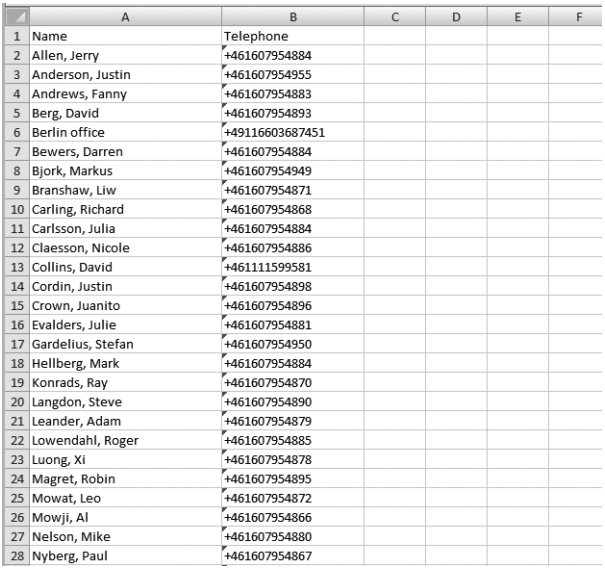
⇨ Create a Firmware metadata file according to page 49 and place it on the Provisioning server.

ⓘ Depending on the server used, and the security settings, there might be necessary to add the file type *.kt* to the MIME settings on the server. This is easily checked by trying to download the kt file from a web browser.

IMPORTING AND EXPORTING CONTACTS

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

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



	A	B	C	D	E	F
1	Name	Telephone				
2	Allen, Jerry	+461607954884				
3	Anderson, Justin	+461607954955				
4	Andrews, Fanny	+461607954883				
5	Berg, David	+461607954893				
6	Berlin office	+49116603687451				
7	Bewers, Darren	+461607954884				
8	Bjork, Markus	+461607954949				
9	Branshaw, Liw	+461607954871				
10	Carling, Richard	+461607954868				
11	Carlsson, Julia	+461607954884				
12	Claesson, Nicole	+461607954886				
13	Collins, David	+461111599581				
14	Cordin, Justin	+461607954898				
15	Crown, Juanito	+461607954896				
16	Evalders, Julie	+461607954881				
17	Gardelius, Stefan	+461607954950				
18	Hellberg, Mark	+461607954884				
19	Konrads, Ray	+461607954870				
20	Langdon, Steve	+461607954890				
21	Leander, Adam	+461607954879				
22	Lowendahl, Roger	+461607954885				
23	Luong, Xi	+461607954878				
24	Magret, Robin	+461607954895				
25	Mowat, Leo	+461607954872				
26	Mowji, Al	+461607954866				
27	Nelson, Mike	+461607954880				
28	Nyberg, Paul	+461607954867				

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

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

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

Importing contacts

⇨ Select **Phone Book**.

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

⇨ Open your CSV file.

⇨ Click on **Import**.

ⓘ The name is limited to 15 characters, since the OmniTouch 4135 IP screen cannot display more than 15 characters.

Exporting contacts

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

⇨ Click on **Export**.

⇨ Save the document.

IMPORTING AND EXPORTING CONFERENCE GROUPS

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

	A	B	C	D	E	F	G
1	Group	Name	Number				
2	Sales	Carlsson, Julia	+4616017954884				
3	Sales	Berg, David	+4616017954893				
4	Sales	Berlin office	+4966023687451				
5	Sales	UK office	+4416057953687				
6	Development	Bjork, Markus	+4616017954949				
7	Development	Branshaw, Liw	+4616017954871				
8	Development	Luong, Xi	+4616017954878				
9	Development	Lowendahl, Roger	+4616017954885				
10							
11							
12							
13							
14							
15							

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

DEVICE

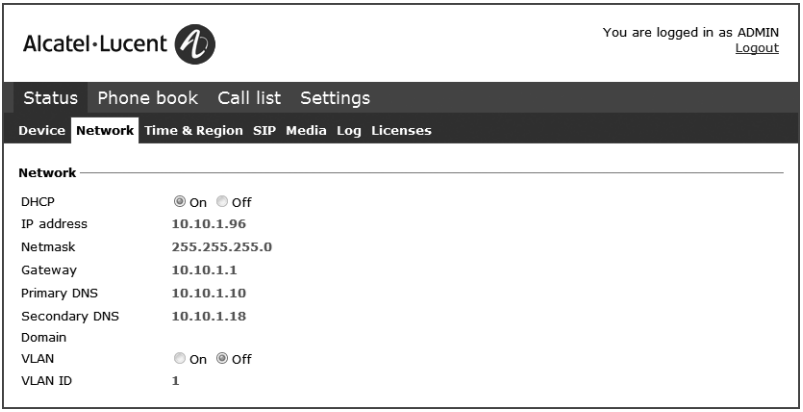
⇨ Select **Status** > **Device**.

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

On phone: **MENU** > **STATUS** > **DEVICE** (8,6).

NETWORK

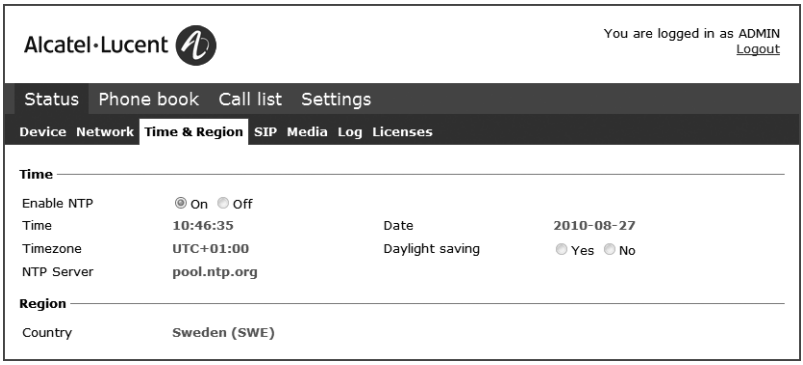
⇨ Select **Status** > **Network**.



On phone: **MENU** > **STATUS** > **NETWORK** (8,2).

TIME & REGION

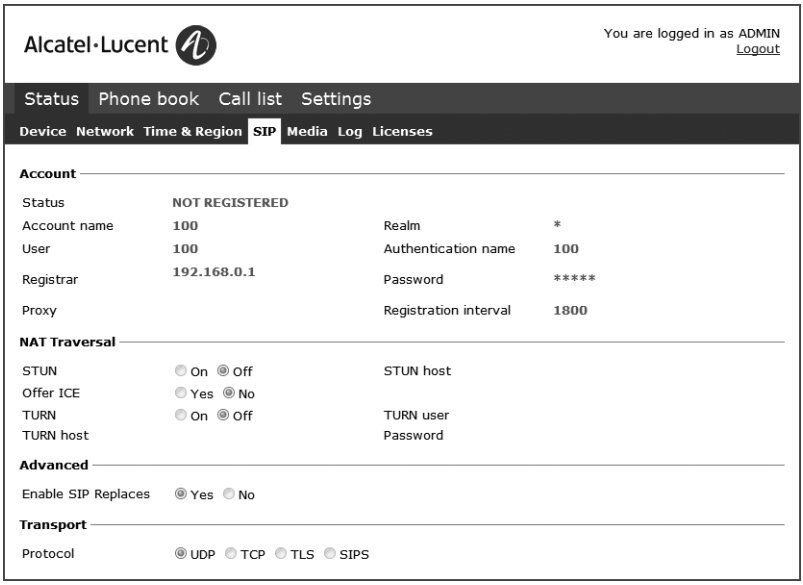
⇨ Select **Status** > **Time & Region**.



On phone: **MENU** > **STATUS** > **TIME** (8,5).

SIP

⇨ Select **Status** > **SIP**.



Account

On phone: **MENU** > **STATUS** > **ACCOUNT** (8,1,1).

NAT traversal

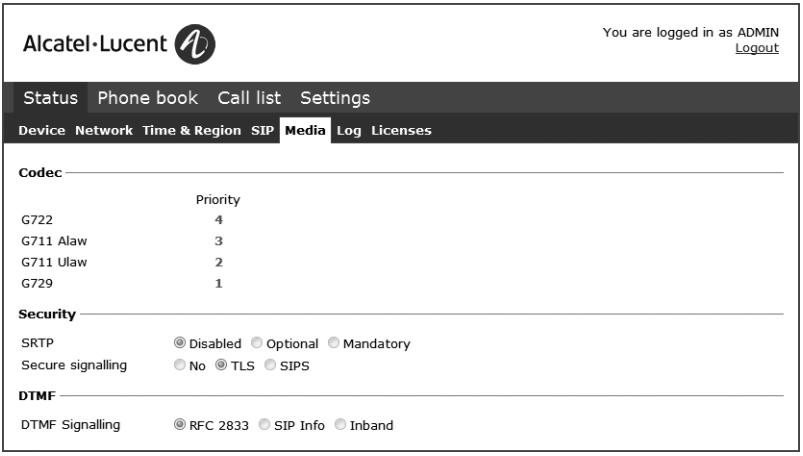
On phone: **MENU** > **STATUS** > **NAT TRAVERSAL** (8,3).

Transport

On phone: **MENU** > **STATUS** > **ACCOUNTS**> **TRANSPORT** (8,1,2).

MEDIA

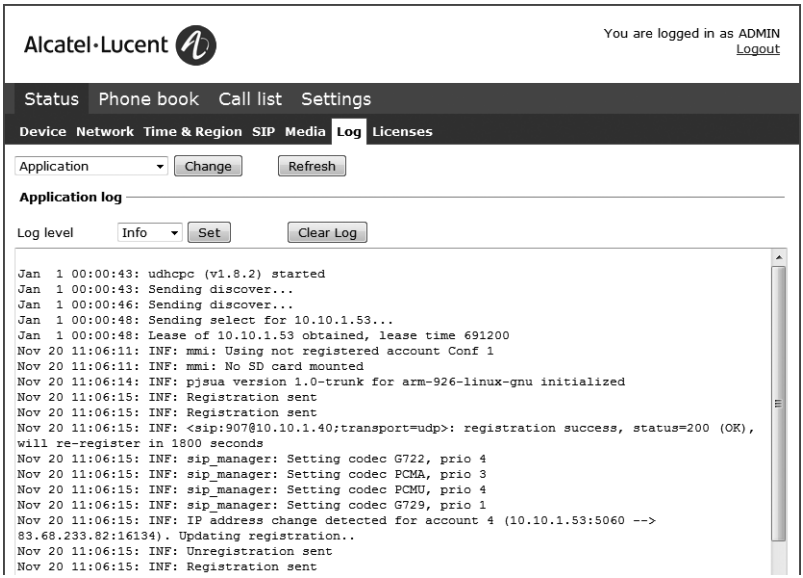
⇨ Select **Status** > **Media**.



On phone: **MENU** > **STATUS** > **MEDIA** (8,4).

LOG

⇨ Select **Status** > **Log**.



The Log tab contains five types of log messages and can be useful for trouble shooting.

⇨ Select the log you want to review and click on the **Change** button.

ⓘ The **Refresh** button adds all new messages sent since the present log was chosen.

Application log

This shows the phone application messages. The log can be filtered from “Fatal” (only the fatal error messages) to “Trace” (all messages).

The application log can for example be used for troubleshooting LDAP issues. (See the administrator’s guide at **www.openldap.org** for information about common error codes.)

The **Clear log** button erases all content in the log.

SIP Trace

The SIP Trace logs the communication between the phone and the SIP PBX.

The **Clear log** button erases all content in the log.

It is possible to disable the SIP trace log

⇨ Select SIP logging **Off** and click on the **Set** button.

System log

Shows the phone system messages.

Device management log

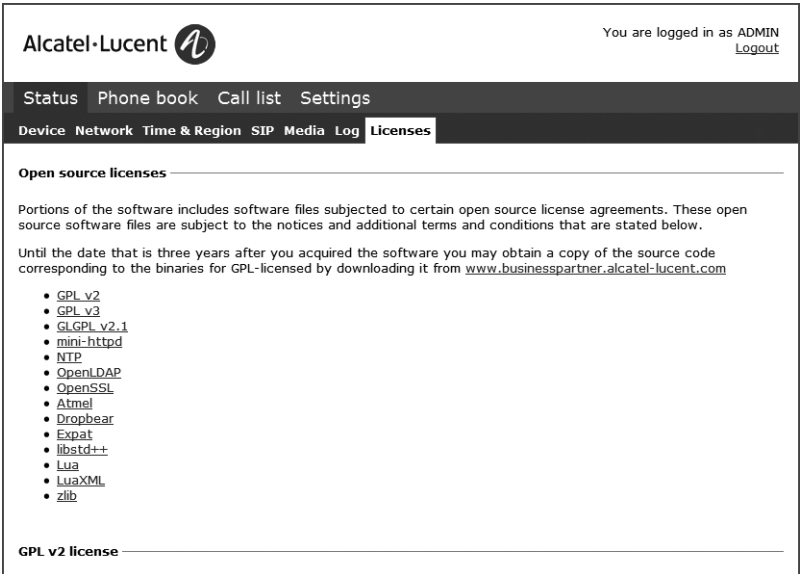
Logs the provisioning activities.

Upgrade log

Logs the upgrade procedure.

LICENSES

⇨ Select **Status** > **Licenses**.



The Licenses tab contains information of open source licenses.

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

Connectivity

Network connection	RJ45, Ethernet 10/100 Base T
Power supply	Transformer 100–240 V AC/13.5 V DC IEEE 802.3af Power over Ethernet class 3.
Extra microphones	x2 modular 4/4
Auxiliary	Modular 4/4 for wireless headset

Network and communication

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

Sound

Technology	OmniSound™® 2.0 Wideband
Microphone	Omni-directional
Reception area	Up to 30 metres^2, >10 people
Speaker	Frequency band 200–7000 Hz,
Volume	90 dB SPL 0.5 m
Equalizer	Three pitches: soft, neutral, bright

Environment

Temperature:	5°–40°C
Relative humidity:	20-80% condensation free
Recommended acoustic conditions:	
	Reverberation period: 0.5 S Rt 60
	Background noise: 45 dBA

Approvals

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

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City,
California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.