IP DECT 6000 System

INSTALLATION & CONFIGURATION GUIDE

VINGTOR

TECHNICAL MANUAL

A100K10652

Zenitel Norway AS and its subsidiaries assume no responsibilities for any errors that may appear in this publication, or for damages arising from the information in it. No information in this publication should be regarded as a warranty made by Zenitel Norway AS.

The information in this publication may be revised or changed without notice. Product names mentioned in this publication may be trademarks of others and are used only for identification.

Contents

Figures

Tables

1 About this Document

This document is intended for qualified technicians who will install, configure and maintain the IP DECT 6000 System. The document also provides information on the web browser-based user interface of the Server 6000 and base station as well as the configuration of the IP DECT handsets in the AlphaCom/ACM exchange so that they can be used as mobile intercom stations.

The IP DECT 6000 System comprises the following:

Product	Part Number
IP DECT Server 6000	2211000100
IP DECT Base Station	2211000600
Repeater Wall / Repeater Ceiling	2211050100 / 2211050110
IP DECT Handsets	2211100501, 2211100502, 2211100505, 2211100506
IP DECT Alarm Server	2210020000, 2210020002

☞ *The configuration of the Alarm Server is described in the corresponding manual as listed under Related Documentation below.*

1.1 Before You Begin

This document assumes the following:

- You have a working knowledge of AlphaCom/ACM exchange operations and the exchange is installed and initialized and is working properly.
- You have a working knowledge of deployment in general.
- A site survey has been conducted and the installer has access to these plans. The site survey should determine the number of handsets and RF channels that are needed.

1.2 Publication Log

Rev.	Date	Author	Comments
1.0	02-11-2009	HKL	Published
1.5	28-1-2011	HKL	handsets
1.6	12-3-2012	HKL	Rough handsets Subscription

1.3 Related Documentation

For further information about the IP DECT 6000 System not covered by this manual, refer to the following documentation:

Doc. no.	Subject	Documentation
A100K10676	IP DECT Planning & Deployment	IP DECT Deployment Guide on Ships
A100K10677	IP DECT Alarm Server	IP DECT Alarm Server Configuration Guide
A100K10777	IP DECT Configuration	IP DECT Quick Configuration Guide
	IP DECT Handset Operation	IP DECT Handset User Guides

2 The IP DECT 6000 System

This section provides a description of the IP DECT 6000 System.

The IP DECT Server 6000 communicates with the AlphaCom/ACM exchange over a LAN (Local Area Network).

A typical IP DECT 6000 System comprises the following components:

- IP DECT Server 6000
- Base Stations
- Repeaters
- Administrative Computer
- Handsets and accessories
- Alarm Server

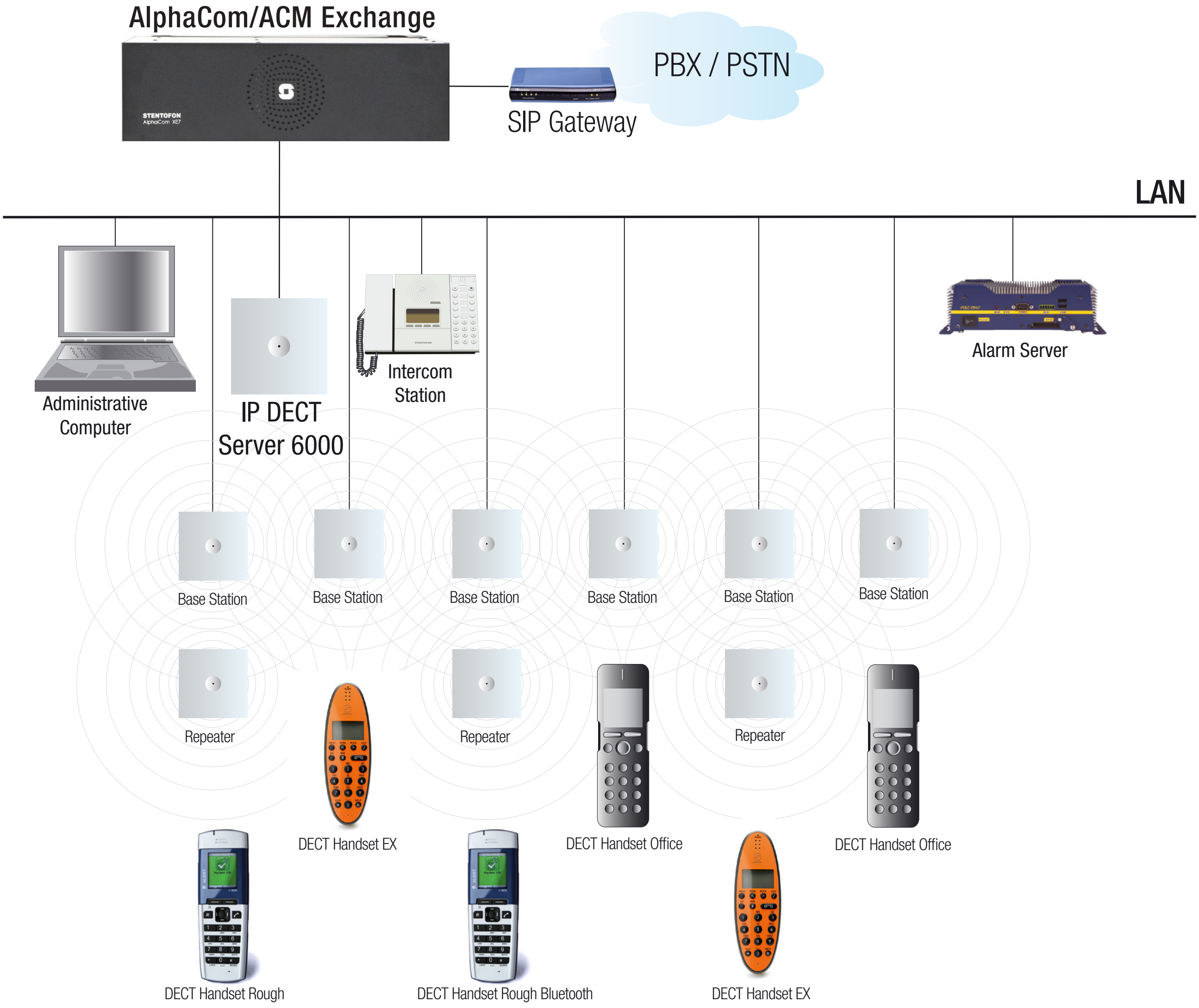


Figure 1 IP DECT 6000 System Configuration

2.1 IP DECT Server 6000

Below is an overview of the system capacity of the IP DECT Server 6000.

Table 1 Overview of System Capacity

Description	Capacity
Max. number of base stations Note: A minimum of 1 base station is required as the Server 6000 does not have a built-in radio.	255
Max. number of simultaneous calls on each base station	11
Max. number of repeaters on each base station	6
Max. number of simultaneous calls on an IP DECT Server 6000 (G.711)	30
Max. number of registered handsets	500

The Server 6000 controls the wireless infrastructure of the IP DECT system. It manages base stations, repeaters and the IP interface to the AlphaCom/ACM exchange.

SIP (Session Initiation Protocol) is the protocol used for controlling communication sessions between the Server 6000 and the AlphaCom/ ACM exchange.

A Server 6000 is installed directly on the Local Area Network (LAN) and must be managed as part of the corporate network.

2.2 Wireless Bands

The wireless solution supports two wireless bands, allowing operation in various countries and regions. Supported wireless bands are:

- ETSI DECT (1880-1900 MHz), referred to as DECT
- USA DECT (1920-1930 MHz), referred to as 1G9

The wireless band used by an IP DECT 6000 System is determined by the base stations and handsets delivered with the solution.

☞ *This document only describes equipment in the ETSI DECT band.*

2.3 Base Station

The base stations are positioned in the area to send and receive calls, i.e. between the wireless server and the handset. The base station contains internal antennas and handles 11 speech channels simultaneously. A base station is able to synchronize with other base stations. When the base station is synchronized with other base stations, a person speaking on a handset can move between base stations (i.e. handover) without any interference.

The transmission length is up to 100 meters/329 feet according to IEEE 802.3u on a twisted pair cable, e.g. cat.5e. The base station is a class 1 PoE device (802.3af) and must be powered accordingly (maximum power supply consumption is 3.0W according to PoE 802.3af). The radius coverage of the base station is up to 90 meters/295 feet indoors and up to 300 meters/984 feet outdoors with a handset in line-of-sight (coverage area onboard ship is 50 meters indoors and 150 meters outdoors).

Coverage area decreases depending on the type of building materials and obstructive elements. To ensure proper coverage in the areas required, it is necessary to either conduct a site survey or base the deployment plan on the deployment guidelines.

2.4 Repeater

The repeater can be used to extend the coverage area in a wireless radio synchronization solution, where it serves as a receiver and transmitter in relaying radio signals. Depending on the repeater type, it can be mounted either on the wall or on the ceiling. The wireless repeater is used in areas with limited voice traffic, where cabling is difficult. The repeater does not increase the number of traffic channels, but increases the coverage area established with the base station. Up to three repeaters can be placed in cascade formation directing coverage in a certain direction. If the radio environment is difficult, one should avoid installing repeaters.

Each base station can support up to 6 repeaters.

2.4.1 Programming Software

The application software for programming the repeater and software downloads to the repeater is called ServiceTool.

☞ *ServiceTool is not used for adjusting the Rough/Office Handset.*

The ServiceTool software is available as a download from the STENTOFON AlphaWiki website.

2.5 Handset

The handset is a lightweight, ergonomically designed wireless unit that includes an LCD display and keypad.

2.5.1 Handover

Handover refers to the ability to move between the coverage areas of different radio units on the same system while talking, without interruptions in the conversation.

2.6 Administrative Computer

An administrative computer is required for configuration and maintenance of the Server 6000 and base station. This computer may be temporarily connected directly to the device or to the network. A dedicated computer is not required.

2.7 Requirements for the IP DECT 6000 System

This section provides information about the environmental, electrical, and software requirements for the IP DECT 6000 System.

2.7.1 IP DECT Server 6000

2.7.1.1 Environmental Requirements

The installation area must be:

- clean, free of traffic and excess dust, dry, and well ventilated
- within the temperature range of 10°C/50°F and 40°C/104°F

- between 20% and 80% non-condensing relative humidity

☞ *The installation area must be of sufficient height from the floor to prevent water damage.*

2.7.1.2 Electrical Requirements

The following electrical requirements must be met:

- Power consumption: 8V/500 mA
- Typical power consumption: 5W per unit
- The supplied power for the AC adaptor power supply must be 110 to 240 ac nominal, 50/60 Hz.

2.7.2 Base Stations and Repeaters

2.7.2.1 Environmental Requirements

- Avoid installing base stations and repeaters on large concrete or marble columns because they affect radio coverage. If possible, place the base station a minimum of one meter/3.3 feet from these types of columns.
- Avoid installing a base station or repeater with the antenna housing near metal objects. Be careful not to damage existing wiring or panels.
  - On ships, the radiating cable solution is used instead.
- If possible, keep the base station and repeater away from steel constructions.
  - On ships, the radiating cable solution is used instead.
- Only position base stations and repeaters where the signal is needed.
- The installation area must be clean, free of traffic and excess dust, dry, and well ventilated.
- The installation area must be within the temperature range of 10°C/50°F and 40°C/104°F.
- The installation area must be between 20% and 80% non-condensing relative humidity.
- The minimum distance between two base stations varies depending on the material and construction of buildings, but there must always be synchronization chains and radio coverage overlap between the two base stations or handover between radio units.
- The time it takes a person to cross the common coverage area (of at least 2 base stations) must be 10 seconds or more, as the handset needs time to scan for an alternative base station.

2.7.2.2 Electrical Requirements for Base Station

The following electrical requirements must be met:

- The base station operates on standard twisted pair Ethernet cable - e.g. minimum Cat.5e - to prevent disturbances from other equipment.
- Maximum power supply consumption is 3.0W (IEEE 802.3af class 1 device).
- The maximum average radiated output power for the antenna is 10mW – peak radiation is 250 mW (over a time period of 0.4 ms) EIRP/channel.

2.7.2.3 Electrical Requirements for Repeater

- The power supply for the repeater must be 110 V to 120 V ac nominal or 220 V to 230 V ac nominal, 50/60 Hz.

2.7.3 Handsets

2.7.3.1 Environmental Requirements

- The area where the handset is used must be within the temperature range of 0°C/32°F and 40°C/104°F.
- For correct battery charging, the room temperature must be between 0°C/32°F and 25°C/77°F. Therefore, the handset must not be placed in direct sunlight. The battery has a built-in heat sensor which will stop battery charging if the temperature is too high.
- The area where the handset is used must be between 20% and 80% non-condensing relative humidity.

2.7.3.2 Electrical Requirements

The following electrical requirement must be met:

- The power supply for the charger must be 110 V to 120 V ac nominal or 220 V to 230 V ac nominal, 50/60 Hz.

2.7.4 Maintenance Software

This section describes the computer requirements to run the installation and maintenance tools of the handset and repeater.

2.7.4.1 Software Requirements

- Operating System: Windows 2000 (SP4), Windows XP (SP2), Windows Vista
- CPU: Minimum 400MHz (2000/XP), 1GHz (Vista)
- RAM: Minimum 256 MB (2000/XP), 1 GB (Vista)
- GPU/Display: XGA (1024x768)
- Harddisk: Minimum recommended harddisk size by OS and other installed applications + 25 MB free space for the application.

☞ *Depending on other applications running on the system, CPU, RAM and harddisk values may vary.*

2.8 Installation Prerequisites

☞ *Ensure that a deployment plan has been conducted and that the installer has access to these plans before proceeding any further. For more information about deployment, see “Deploying the IP DECT Server 6000”*

Before you start the installation you need to find the following information and perform the following tasks:

- ARI codes (serial numbers) for the Server 6000 (see label on the rear of the package unit)
- Serial numbers for handsets. Refer to “Retrieving the Serial Number of the Handset”.
- AC (Authentication Codes)

  - The AC is a customer-defined optional subscription PIN code of a maximum of eight digits for the individual handset. The AC can be used when connecting the handset to the Server 6000. The AC does not need to be configured for the handsets to function.

- Repeaters:
  - Mark each repeater with the number of the related base station. This way you can easily configure the system on site.
- Handsets:
  - To use the handsets, you must first install the radio infrastructure, e.g. base stations and repeaters to transmit and receive radio signals to and from the handsets. There are no direct connections between the handset and the system. For more information about base station and repeater installation, refer to “Installing Base Station” and “Installing the Repeater”.
- Charging battery
  - When charging the handset battery for the first time, leave the handset in the charger for 14 - 16 hours to ensure that the battery is fully charged and the handset ready for use. Refer to “Charging Handsets”.

3 Deploying the IP DECT Server 6000

Before you install the IP DECT Server 6000 solution, it is necessary to carry out a complete site design – at the minimum on the basis of environmental drawings (like GA for ships, or floor plans for buildings) - to determine the exact location of the Server 6000, base stations, repeaters and the number of handsets required.

☞ *For deployment on ships, see Zenitel's **IP DECT Deployment on Ships**.*

☞ *Due to the unexpected nature of RF propagation in an indoor environment, an actual on-site test may need to be carried out before the installation is complete.*

While an extensive guide to effective RF coverage planning is beyond the scope of this manual, the following points should be taken into consideration when planning the site, prior to base station and repeater installation:

- The base station/repeater provides typical RF coverage of up to 50 meters/164 feet in a typical indoor office environment and up to 300 meters/984 feet in an open area (line-of-sight), extending in all directions from the base station/repeater. The exact coverage range depends on the building architecture, wall material and surroundings.
- The wireless solution can support a maximum of 500 handsets and 255 base stations. (See Table 1 in section 2.1).
- Handset handover: handsets can move between coverage areas of base stations and repeaters while receiving continuous service and maintaining conversations in progress. However, for steel container-like rooms (such as ship cargo rooms) it is not to be expected that the standard radio antenna base stations will be able to support handover.
  - For deployment on ships, the radiating cable solution may be used.
- For efficient handover of conversations between base stations, deploy base stations with wide overlap between them (i.e. plan for some areas to be covered by more than one base station). Overlaps are necessary to maintain seamless handover and to establish synchronization chains. A good example may be a cafeteria during lunch hour where temporary concentrations of handsets may occur. The overlap carries the excess call load to adjacent base stations to provide uninterrupted services to subscribers.
- Typically, installations such as office buildings, hotels and hospitals should be equipped with base stations/repeaters on several floors to create uniform and complete RF coverage.
- Open areas can be covered with a sparse network of base stations. In such applications, the base stations/repeaters cover an extended range due to the extended line-of-sight RF propagation capability.
- Ensure that there is no residential DECT system (home DECT) on the site.

3.1 Recommendations for Base Station / Repeater Placement

- In large halls, the base station/repeater (wall) should be installed vertically in the middle of the space below the drop ceiling.
- In corridors, the base station/repeater (wall) should be installed vertically, preferably at corridor intersections where propagation patterns follow the corridor patterns. The base station/repeater should point towards the corridor and preferably at mid-height between the floor and the actual ceiling. In cases where there are tall objects in the area, the base station/repeater should be installed

above those objects but still kept distant from the ceiling.

- In multi-story buildings, base stations/repeaters may be installed on opposite sides of the floors to take advantage of the floor-to-floor coverage. The coverage design cannot rely entirely on floor-to-floor propagation; due to variations in local attenuation patterns, each case must be verified.
- If the building contains a central open space with windows to the other areas, base stations/repeaters may be installed in this open space to provide a good coverage for the rooms in the inner circle on all floors (e.g. hotels).
- If a base station/repeater (wall) hangs vertically on a wall, the RF coverage in front of it is twice as large as the coverage at the rear. When a base station/repeater is installed on the outside of an outer wall, the RF coverage behind it is strongly attenuated by the wall.
- Base stations/repeaters should preferably not be installed near large metallic objects.
- Reinforced concrete structures have a high attenuation factor inside a building. Consequently, a higher number of base stations/repeaters have to be installed in the building as these structures decrease their coverage range. Lighter types of construction require fewer base stations since attenuation figures are considerably lower.

3.2 Deployment of a Server 6000 Multi-Cell System

3.2.1 Sync over Air

As a user moves from one base station radio coverage area to another, the call must be handed over to the next radio unit. To create handover between radio units, it is necessary to establish synchronization chains. If the synchronization between radio units is lost, then handover is not possible and ongoing calls will be terminated.

☞ *Each base station must be placed within the radio coverage area of at least one other base station or repeater (radio units).*

3.2.2 Examples of Synchronization Chains

Certain rules must be taken into consideration when establishing synchronization chains:

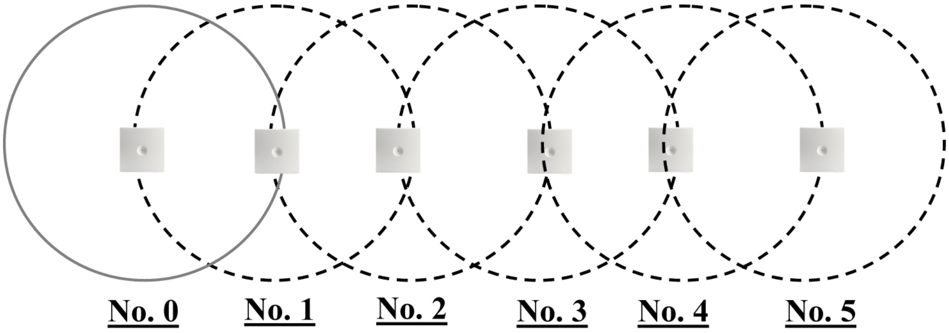
- The distance over which synchronization can take place is limited to a distance similar to a loss not exceeding 25 dB. If signal loss exceeds 25 dB, it is not certain that synchronization will be stable.
  - For example, the signal measured next to the base station is 100 dB. The handset with test display active is moved away from the base station until the reading in the display shows 75 dB. This is the spot where the next base station should be installed.
- It is recommended that a base station synchronizes with at least two other radio units, and that a secondary sync way is defined to ensure system redundancy. If the primary sync way is not working, then the secondary sync way takes over and the synchronization chain is not broken.
- Synchronization chains for the Server 6000 Solution can be made with base stations and repeaters.
- As you can only configure a repeater to synchronize on one radio ID, it is not possible to define secondary sync ways for repeaters.

As the Server 6000 uses the DECT interface to synchronize on, one base station is configured as the Sync Master. It is recommended to place the Sync Master in the middle of the building or on the deck that is mid-way between the decks of a ship.

☞ *It is recommended to make a site plan. Every base station must be numbered with Radio ID, Primary sync Radio ID, and Secondary sync Radio ID.*

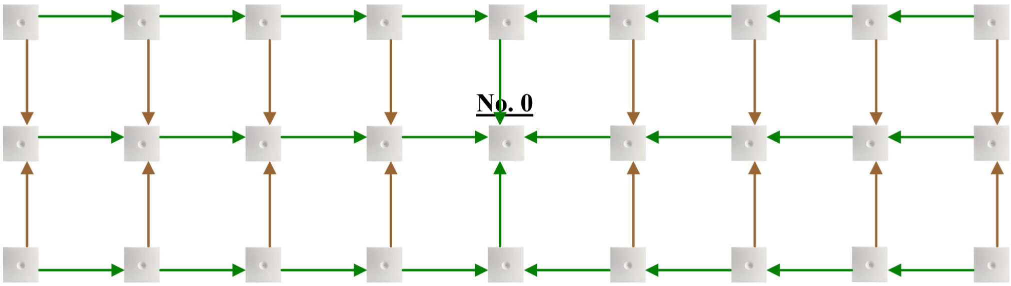
3.2.2.1 Sync Chain With One Sync Master (Primary Sync Ways)

Figure 2 Synchronization Chain



- The synchronization chain must always overlap with the base station to sync on.
- No. 0 is the Sync Master (can be numbered 0 to 255).
- Other radio units are connected to the Sync Master through the synchronization chain.
- If one of the radio units in the synchronization chain is not working, then all radio units behind are also not working.

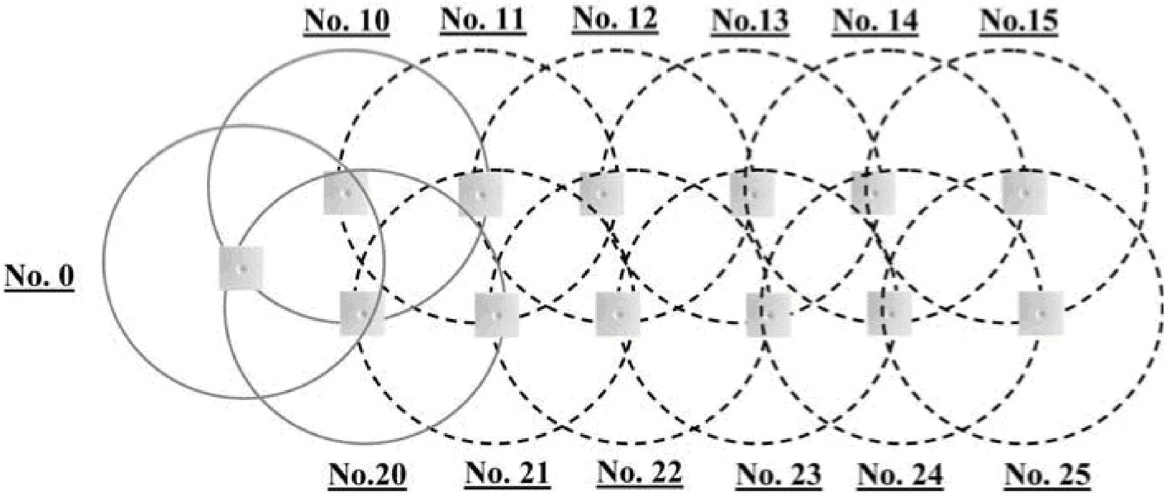
Figure 3 Synchronization Chain Layout without Secondary Sync Ways



- **No. 0** is the Sync Master (can be numbered 0 to 255).
- Green line: Shows the primary sync ways.
- Brown line: Only handover overlap is needed.

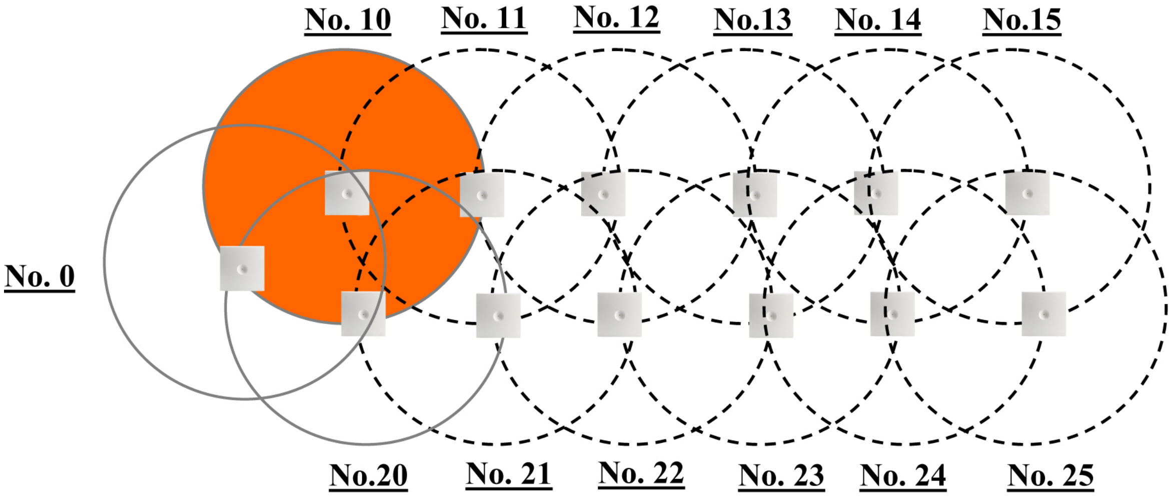
3.2.2.2 Synchronization Chain With Secondary Sync Ways

Figure 4 Synchronization Chain with Secondary Sync Ways



- No. 0 is the Sync Master (may be numbered 0 to 255).
- No. 10 and No. 20: Primary and secondary sync on No. 0.
- No. 11: Primary sync on No. 10 and secondary sync on No. 21.

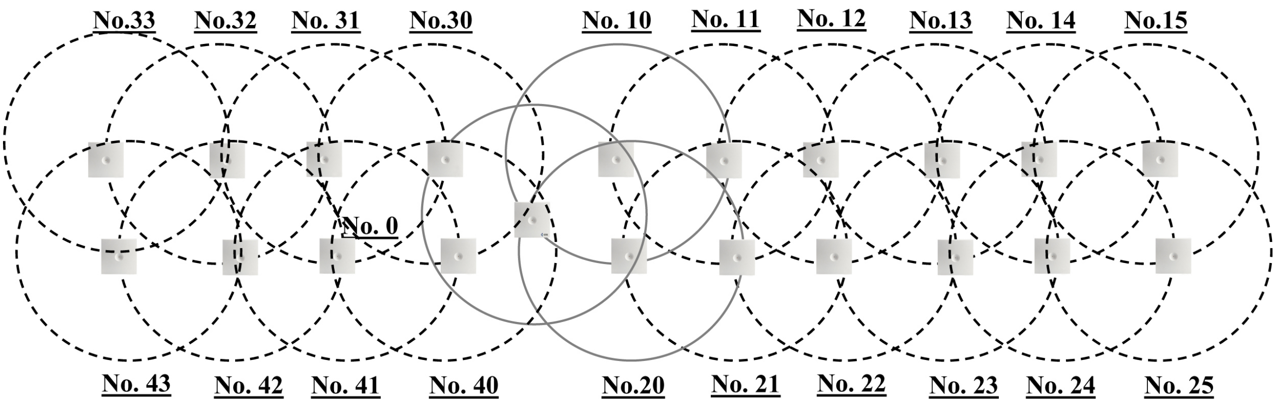
Figure 5 Synchronization Chain with Secondary Sync Ways



- No. 0 is the Sync Master (may be numbered 0 to 255).
- No. 10 and No. 20: Primary and secondary sync on No. 0.
- No. 11: Primary sync on No. 10 and secondary sync on No. 21.

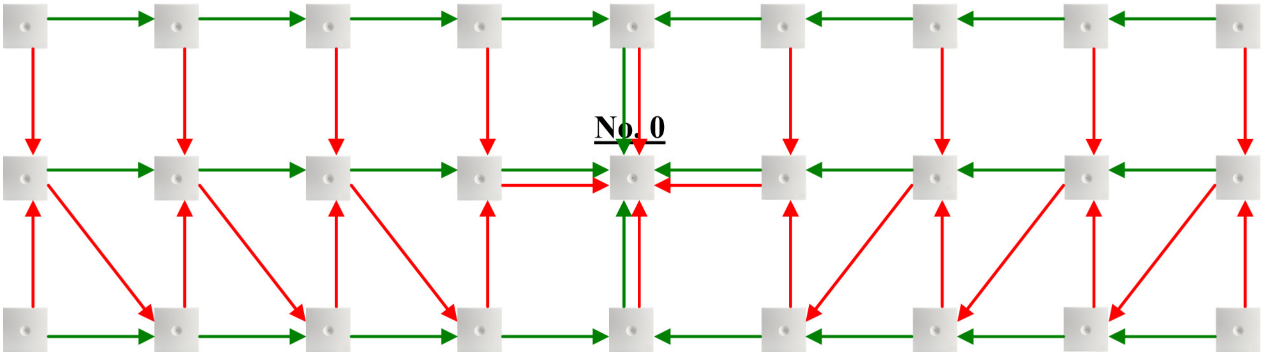
In the example above, base station No. 10 is down. As a consequence, base station No. 11 must use the secondary sync way on base station No. 21.

Figure 6 Synchronization Chain with Secondary Sync Ways



- No. 0 is the Sync Master (may be numbered 0 to 255).
- No. 10, No. 20, No. 30, and No. 40: Primary and secondary sync on No. 0.
- No. 11: Primary sync on No. 10 and secondary sync on No. 21.
- No. 21: Primary sync on No. 20 and secondary sync on No. 11.
- No. 31: Primary sync on No. 30 and secondary sync on No. 41.
- No. 41: Primary sync on No. 40 and secondary sync on No. 31.

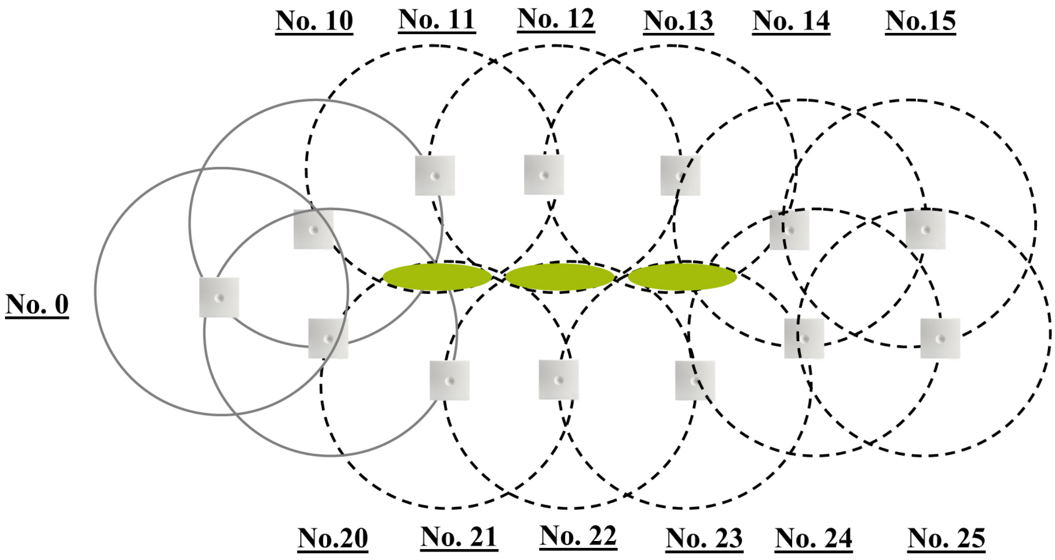
Figure 7 Synchronization Chain Layout with Secondary Sync Ways



- **No. 0** is the Sync Master (may be numbered 0 to 255).
- Green line: Shows the primary sync ways.
- Red line: Shows the secondary sync ways.

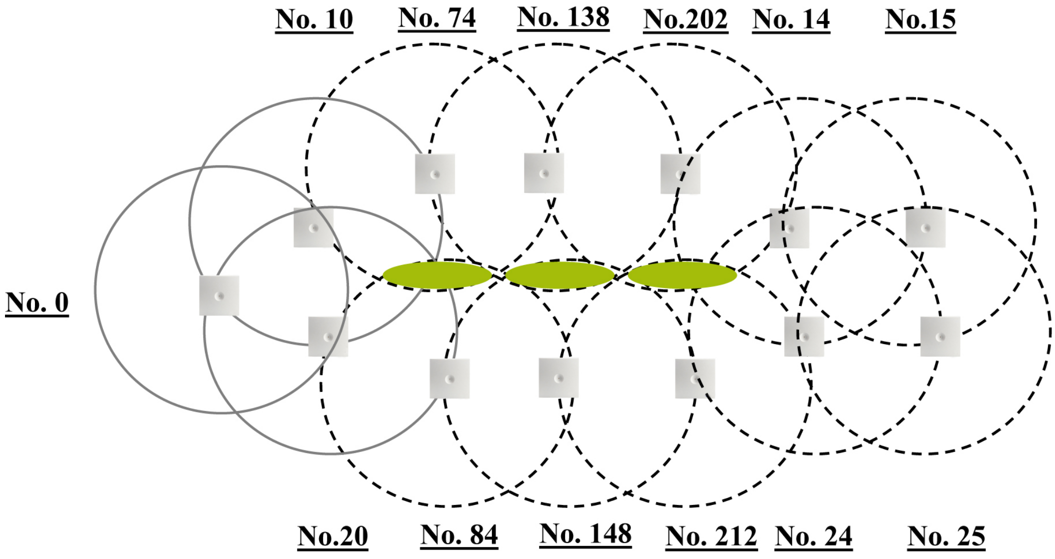
3.2.2.3 Sync Chain With and Without Secondary Sync Ways

Figure 8 Sync Chain With and Without Secondary Sync Ways



- No. 0 is the Sync Master (may be numbered 0 to 255).
- No. 10 and No. 20: Primary and secondary sync on No. 0.
- No. 11, No. 12, and No. 13: Only primary sync.
- No. 14 and No. 15: Primary sync and secondary sync.
- No. 21, No. 22, and No. 23: Only primary sync.
- No. 25: Primary sync on No. 24 and secondary sync on No. 15.
- No. 11 and No. 21: Only handover overlap (Marked in green).

Figure 9 Synchronization Chain With Repeaters



- No. 0 is the Sync Master (may be numbered 0 to 255).
- No. 10 and No. 20: Primary and secondary sync on No. 0.
- No. 74, No. 138, and No. 202: Repeaters - no secondary sync possible.
- No. 14 and No. 15: Primary sync and secondary sync on repeater.
- No. 84, No. 148, and No. 212: Repeaters - no secondary sync possible.
- No. 24 and No. 25: Primary sync and secondary sync.
- No. 74 and No. 84: Only handover overlap (Marked in green).

4 Installing the IP DECT Server 6000

This section provides a general description of the IP DECT Server 6000 as well as information about resetting the hardware using the Reset button on the faceplate. Before you install the equipment, ensure that a site plan has been prepared that defines the location of the Server 6000.

4.1 Description of the Server 6000

4.1.1 Type and Part Number

The Server 6000 contains RF circuitry that comply with the local band standards ETSI DECT and USA DECT 6.0.

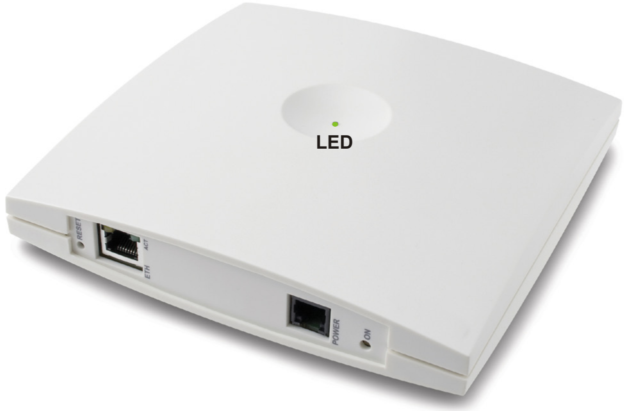
Model type: IP DECT Server 6000 1.8/1.9 GHz with SIP Protocol

Part Number: 221 100 0100

4.1.2 Server 6000 Appearance and Components

The Server 6000 front cover has a LED located in the middle that indicates the operating status of the unit.

Figure 10 Server 6000 - Front view



4.1.3 Server 6000 LED Indicators

4.1.3.1 Front Cover

The Server 6000 front cover has one LED indicator showing the faults and failures of the device. The indicator is off when the Server 6000 is not powered. The LED flashes when the Server 6000 initializes. The indicator is on when the Server 6000 is operating.

Table 2 LED Indicator Description - Front Cover

LED Indicator	Meaning
Steady green	OK and idle
Slow green flashing	OK and active voice call
Fast green flashing	Active, in operation with maximum active connections (busy)
Slow red flashing	Missing base station
Fast red flashing	Error
Steady red	Reset/shutdown in progress
Steady red for 5 seconds followed by fast red flashing	Reset to factory settings

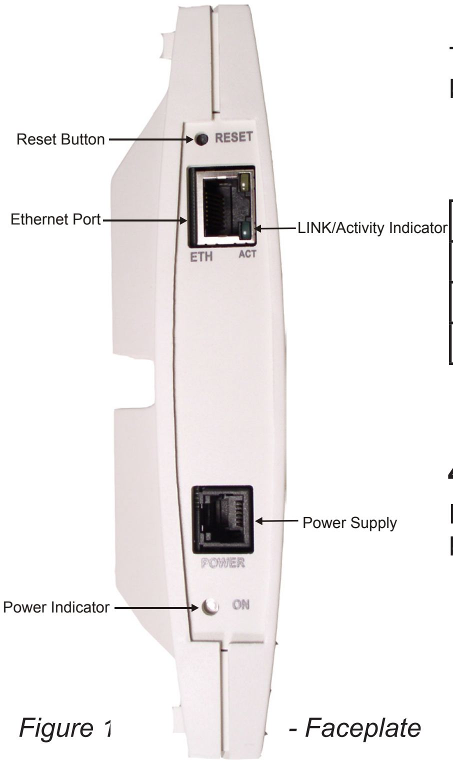


Figure 1 - Faceplate

4.1.3.2 Faceplate

The various stages of the LED indicator on the faceplate are described below.

Table 3 LED Indicator Description - Faceplate

LED Indicator	Meaning
LINK/Activity Indicator - green	Link layer SW has established connection
LINK/Activity Indicator - green flashing	Activity
Power Indicator - green	Server 6000 is connected to power

4.1.4 Server 6000 Reset Button

It is possible to restart or reset the Server 6000 by pressing the Reset button on the faceplate.

4.1.4.1 Resetting the Server 6000 Hardware

This section contains a description of the different actions that occur when the Reset button is pressed.

Table 4 Reset Button Description

Button Press	Action
Short press (2 to 5 sec.)	System restarts when button is released.
Long press (5 to 9 sec.) until front LED flashes red, then release button.	Resets the system to factory default settings (original IP settings and empty user data base) and restarts the system. Firmware version is not affected.

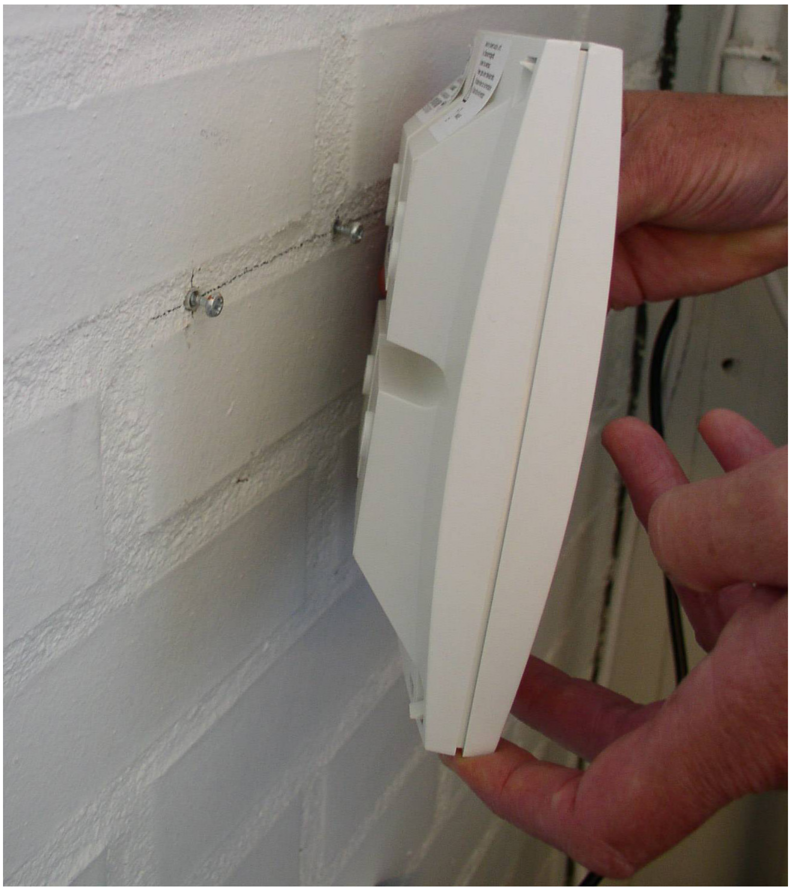
4.2 Mounting/Connecting the Server 6000

The Server 6000 is suitable for mounting indoors on a wall. The procedure is as follows:

1. Mount the Server 6000 on the wall, using the anchors and screws provided.
2. Connect the power supply cable into the RJ45 plug on the Server 6000.

✋ ***When you place the Server 6000 on the screws, ensure that the screws do not touch the printed circuit board.***

Figure 12 Server 6000 Wall Mounting



5 Installing the Base Station

This section provides information about the base station and how to install it.

Before you install the equipment, ensure that a site plan has already defined the location of the base stations.

This section includes information about:

“Base Station Description”

“Installing the Base Station”

“Recording the Installation Information”

5.1 Base Station Description

5.1.1 Base Station provides RF Channels to Handsets

The base station is a compact device that contains RF circuitry and transmit/receive antennas. The main function of the base station is to provide audio and data communication between the handsets and the Server 6000. The base station supports 11 RF channels for DECT or USA DECT bands.

☞ *The base station is also termed the RFP (Radio Fixed Part) by some manufacturers.*

The RF communication is provided according to the band standard at the site:

- DECT Base station provides 11 RF channels of 1.8 GHz, DECT standard, used in Europe, Australia and South America.
- USA DECT Base station provides 11 RF channels of 1.9 GHz, USA DECT standard, used in North America (please ask your Zenitel distributor for order information about this equipment).

5.1.2 Base Station Type and Part Number

The base station contains RF circuitry that comply with the local band standards: UPCS, DECT, or ETSI DECT.

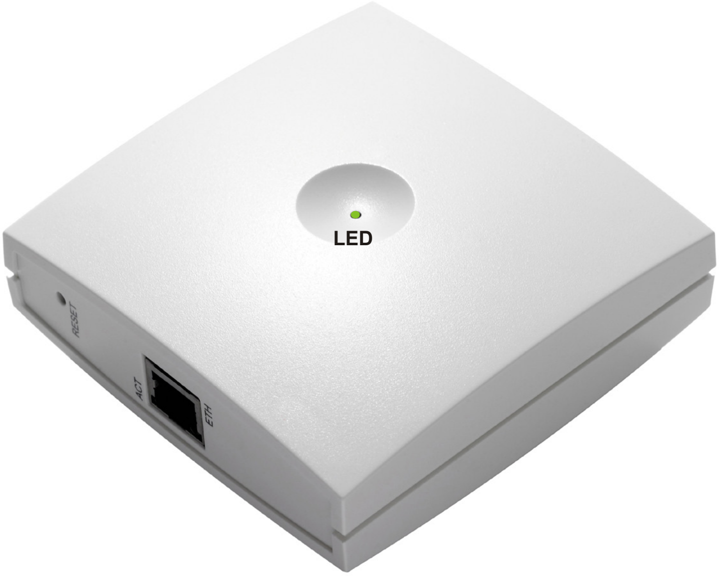
Model type: IP DECT Base for Server 6000

Part Number: 221 100 0600

5.1.3 Base Station Appearance and Components

The base station front cover has a LED that indicates the operating status of the unit

Figure 13 Base Station - Front view



The base station faceplate includes a Reset Button, a LINK/Activity Indicator, and an Ethernet Port (Power supply through PoE).

For more information on the Reset button, refer to “Resetting the Base Station Hardware”.

5.1.4 Base Station LED Indicators

5.1.4.1 Front Cover

The base station front cover has one indicator describing the base station faults and failures. The indicator is off when the base station is not powered. The LED flashes when the base station initializes. The indicator is on when the base station is operating.

Table 5 LED Indicator Description - Front Cover

LED Indicator	Meaning
Steady green	OK and idle
Slow green flashing	OK and active voice call
Fast green flashing	Active, in operation with max. active connections (busy)
Fast red flashing	Error
Steady red	Reset/shutdown in progress
Steady red for 5 seconds followed by fast red flashing	Reset to factory settings

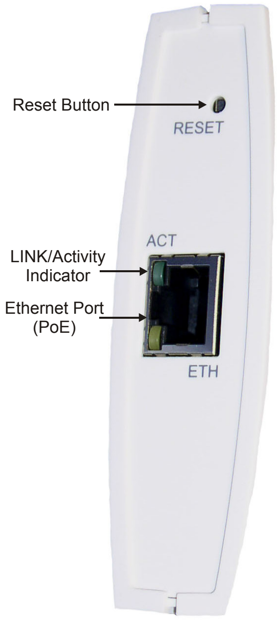


Figure 14 Base Station - Faceplate

5.1.4.2 Faceplate

Table 6 LED Indicator Description - Faceplate

LED Indicator	Meaning
LINK/Activity Indicator - green	Link layer SW has established connection
LINK/Activity Indicator - green flashing	Activity
Power Indicator - green	Base is connected to Power

5.1.5 Base Station Reset Button

It is possible to restart or reset the base station by pressing the Reset button on the faceplate of the base station.

5.1.5.1 Resetting the Base Station

The table below shows the different processes that are put into motion when the Reset button is pressed.

Table 7 Reset Button Description

Press button	Action
Short press (2 to 5 sec.)	System restarts when button is released.
Long press (5 to 9 sec.) until front LED flashes red, then release button.	Resets the system to factory default settings (original IP settings and empty user database) and restarts the system. Firmware version is not affected.

5.2 Mounting/Connecting the Base Station

The base station is suitable for mounting indoors on a wall.

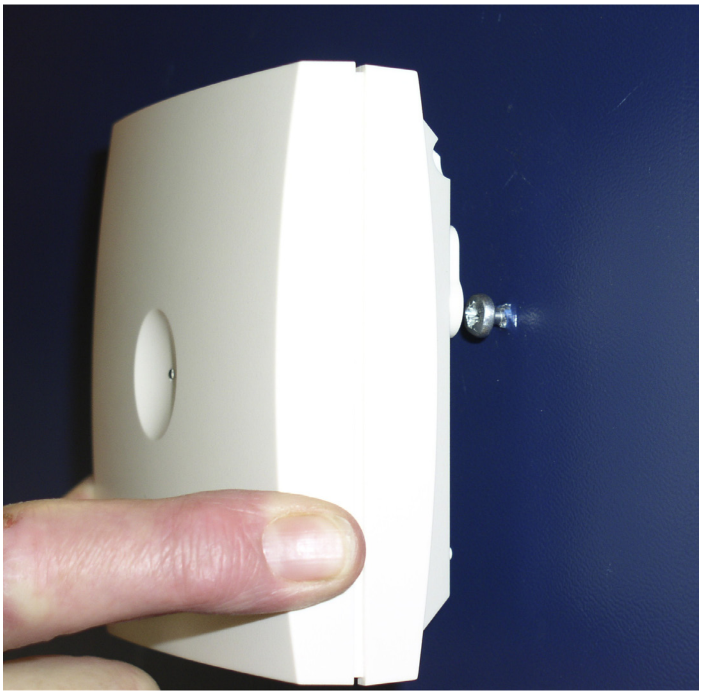
☞ *Before beginning the installation, determine the position of the base station for best coverage. The coverage depends on the construction of the building, architecture, and the choice of building materials. Refer to “Environmental Requirements” for more information about the environmental requirements for base stations.*

5.2.1 Wall Mounted (Vertical) Installation RF Coverage

For best RF coverage, the base station must be mounted vertically on walls. The antennas must always be kept perpendicular to the floor.

✋ ***Caution: The base station must not be installed at any angle other than vertical. If the base station is placed upside-down, the coverage area of the base station is decreased by 40% - 50% and it might not transmit or receive effectively. If possible, avoid mounting the base station on soft-surfaced walls such as those covered with canvas, metal or sponge-like materials.***

Figure 15 Base Station - Wall Mounting

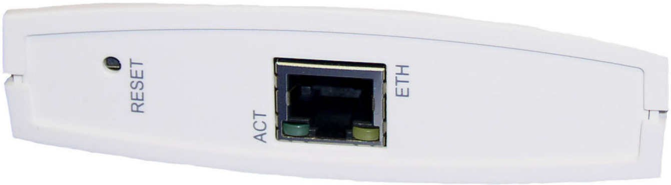


To mount and connect the base station, do the following:

1. Mount the base station on the wall using the anchors and screws accompanying the product.
2. Insert the RJ45 plug into the Ethernet connector at the bottom of the base station.

✋ ***When you place the base station on the screws, ensure that the screws do not touch the printed circuit board.***

Figure 16 Base Station - Ethernet Connector



5.3 Recording the Installation Information

After completing the installation of the base stations, record the location of each base station and add a descriptive text in the web interface of the Server 6000 under **Administration > Base stations**.

6 Installing the Repeater

This section provides information about the repeater and how to unpack and install it. The are two parts to installing the repeater, i.e. a software installation and a hardware installation.

Before you install the equipment, ensure that a site planner has defined the location of the repeaters.

This section includes information about:

- "Repeater Description"
- "Installing the Repeater"
- "Recording the Installation Information"
- "Checking Indicators"
- "Powering the Repeater"
- "Programming a Repeater with the Programming Kit"

6.1 Repeater Description

6.1.1 Repeater provides RF Channels to Handsets

The repeater is a building block used to extend the coverage area in a system. The repeater does not increase the number of traffic channels. However, it provides a larger physical spreading of the traffic channels and thereby increases the coverage area established with the base stations. The repeaters are mainly used in areas with limited traffic. The repeater is available with 4 voice channels. It is wireless and does not need a physical connection to the wireless server, making it very easy to install. The repeaters can be supplied with an external antenna making it possible to create radio coverage in a remote area without cabling to the rest of the installation.

☞ *The repeater is also termed WRFP (Wireless Radio Fixed Part) by some manufacturers.*

6.1.2 Repeater Type and Part Number

The repeater contains RF circuitry that is compliant with the local band standards: UPCS, DECT, or ETSI DECT. The wall-mounted repeater is available as a full slot repeater. A full slot repeater covers four simultaneous speech channels. These channels are borrowed from the attached base station, and are not additional channels to the total number of channels on the system.

Type	Part Number
Repeater Wall	221 105 0100
Repeater Ceiling	221 105 0110

6.1.3 Repeater Appearance and Components

The repeater connection panel includes the following:

- Power supply connection (also connection for programming the repeater).
  - The power supply for the repeater is ordered separately.
- Antenna connector for repeaters supplied with external antenna connection.
  - The external antenna including antenna cable is ordered separately.
- LED that indicates whether or not the unit is functioning.

6.1.4 Repeater LED Indicator

The repeater has one LED indicator describing the repeater operations. The LED is off when the repeater is not powered. When the LED flashes after the repeater has been powered, sync has still not been established. As soon as sync has been established, the LED is on. Each time a handset connects to the repeater, the LED flashes briefly. Each time a handset makes a handover to a repeater, the LED flashes briefly.

6.2 Installing the Repeater

Before beginning the installation, determine the position for best coverage of the repeater. The coverage depends on the construction of the building, architecture, and the type of building materials.

6.2.1 Environmental requirements

- Avoid installing repeaters on large concrete or marble columns because these columns affect radio coverage. If possible, place the repeater a minimum of 1 meter or 3.3 feet from these types of columns.
- Avoid installing a repeater with the antenna housings near metal objects. Be careful not to damage existing wiring or panels.
- Avoid positioning repeaters in ducts, plenums or hollow spaces used to transport environmental air except where the duct, plenum or hollow space is created by a suspended ceiling having lay-in panels.
- Avoid positioning repeaters directly on metallic surfaces. If possible, place the repeater a minimum of 1 meter or 3.3 feet from these types of surfaces.
- Avoid positioning repeaters behind furniture.
- Only position repeaters where the signal is needed.
- The installation area must be clean, free of traffic and excess dust, dry, and well ventilated.
- The installation area must be within the temperature ranges of 10°C/50°F and 40°C/104°F.
- The installation area must have non-condensing relative humidity between 20% and 80% .

☞ *The repeater does not add channels, it only adds additional coverage area.*

The repeater can be registered on the system:

- when placed within the coverage area of a base station
- when placed within the coverage area of an already-installed repeater

For best RF coverage, the repeater must be mounted vertically on walls.

✋ ***The repeater must not be installed at any angle other than vertical. If the repeater is placed upside-down, the coverage area of the repeater is decreased by 40% - 50% and it may not transmit or receive effectively.***

To install and mount the repeater:

1. Connect the power supply cable into the RJ11 connector at the bottom of the repeater.
2. Mount the repeater onto the wall using the screws accompanying the repeater.

6.3 Recording the Installation Information

After completing the installation of the repeaters, record the location of each repeater.

6.4 Checking Indicators

Verify that the repeater LED indicator is steadily on, indicating that the repeater is functioning.

6.5 Powering the Repeater

6.5.1 Power Options

The power supply for the repeater is 9VDC, 300mA.

6.6 Programming a Repeater with the Programming Kit

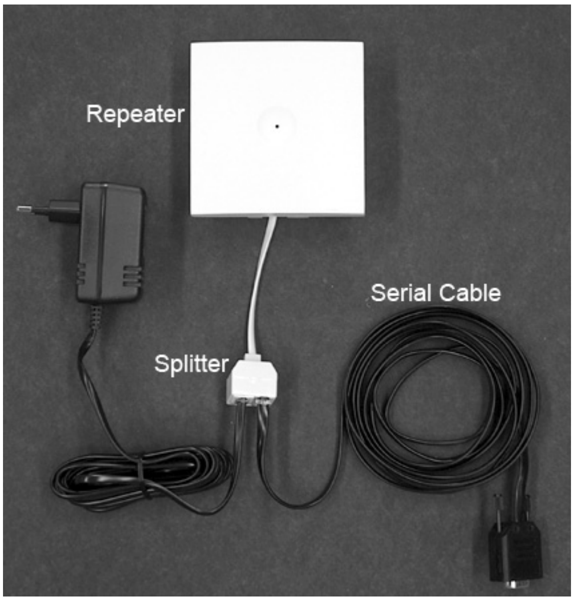
6.6.1 Contents of the Repeater Programming Kit

The Repeater Programming Kit (part no. 2211050130) comprises:

- splitter
- serial cable

☞ *For programming the repeater you also need the ServiceTool programming software and the power supply for the repeater. ServiceTool is not part of the Repeater Programming Kit and is available as a download from the STENTOFON AlphaWiki website. The power supply for the repeater is ordered separately (part no. 2211050200).*

Figure 17 Repeater Programming Kit



6.6.2 Setting up the Hardware for Repeater Programming

1. Unplug the repeater power supply and insert the splitter.
2. Connect the repeater power supply to the splitter and the mains. The LED should start to flash.
3. Ensure that you have the appropriate power supply for the local requirements.
4. Connect the serial cable to the splitter and COM port of your computer. The repeater is now ready for programming via ServiceTool.

☞ *The order sequence (steps 1, 2 and 3) of the setup should be followed.*

6.6.3 Programming the Repeater with ServiceTool

ServiceTool is the application software installed on your computer that you use for repeater programming and software downloading to the repeater.

ServiceTool identifies the type of repeater, and with this software it is possible to program the repeater to connect to the DECT Radio Infrastructure solutions.

Before you start programming the repeater, ensure that the repeater is connected to the computer and the mains.

In a single cell solution, the numbers assigned to the repeaters must be between 2 and 7. The number of the base station is set to 1 by default.

In a multi-cell solution, the numbering of the base stations and repeaters has to follow the numbering in the table below.

Table 8 Repeater Numbering in a Multi-Cell Solution

Base Station	Repeater 1	Repeater 2	Repeater 3
0	64	128	192
1	65	129	193
2	66	130	194
3	67	131	195
4	68	132	196
5	69	133	197
6	70	134	198
7	71	135	199
8	72	136	200
9	73	137	201
10	74	138	202
11	75	139	203
12	76	140	204
13	77	141	205
14	78	142	206
15	79	143	207
16	80	144	208

17	81	145	209
18	82	146	210
19	83	147	211
20	84	148	212
21	85	149	213
22	86	150	214
23	87	151	215
24	88	152	216
25	89	153	217
26	90	154	218
27	91	155	219
28	92	156	220
29	93	157	221
30	94	158	222
31	95	159	223
32	96	160	224
33	97	161	225
34	98	162	226
35	99	163	227
36	100	164	228
37	101	165	229
38	102	166	230
39	103	167	231
40	104	168	232
41	105	169	233
42	106	170	234
43	107	171	235
44	108	172	236
45	109	173	237
46	110	174	238
47	111	175	239
48	112	176	240
49	113	177	241
50	114	178	242
51	115	179	243
52	116	180	244
53	117	181	245
54	118	182	246
55	119	183	247
56	120	184	248
57	121	185	249
58	122	186	250
59	123	187	251
60	124	188	252
61	125	189	253
62	126	190	254
63	127	191	255
64	128	192	0
65	129	193	1
66	130	194	2

67	131	195	3
68	132	196	4
69	133	197	5
70	134	198	6
71	135	199	7
72	136	200	8
73	137	201	9
74	138	202	10
75	139	203	11
76	140	204	12
77	141	205	13
78	142	206	14
79	143	207	15
80	144	208	16
81	145	209	17
82	146	210	18
83	147	211	19
84	148	212	20
85	149	213	21
86	150	214	22
87	151	215	23
88	152	216	24
89	153	217	25
90	154	218	26
91	155	219	27
92	156	220	28
93	157	221	29
94	158	222	30
95	159	223	31
96	160	224	32
97	161	225	33
98	162	226	34
99	163	227	35
100	164	228	36
101	165	229	37
102	166	230	38
103	167	231	39
104	168	232	40
105	169	233	41
106	170	234	42
107	171	235	43
108	172	236	44
109	173	237	45
110	174	238	46
111	175	239	47
112	176	240	48
113	177	241	49
114	178	242	50
115	179	243	51
116	180	244	52

117	181	245	53
118	182	246	54
119	183	247	55
120	184	248	56
121	185	249	57
122	186	250	58
123	187	251	59
124	188	252	60
125	189	253	61
126	190	254	62
127	191	255	63
128	192	0	64
129	193	1	65
130	194	2	66
131	195	3	67
132	196	4	68
133	197	5	69
134	198	6	70
135	199	7	71
136	200	8	72
137	201	9	73
138	202	10	74
139	203	11	75
140	204	12	76
141	205	13	77
142	206	14	78
143	207	15	79
144	208	16	80
145	209	17	81
146	210	18	82
147	211	19	83
148	212	20	84
149	213	21	85
150	214	22	86
151	215	23	87
152	216	24	88
153	217	25	89
154	218	26	90
155	219	27	91
156	220	28	92
157	221	29	93
158	222	30	94
159	223	31	95
160	224	32	96
161	225	33	97
162	226	34	98
163	227	35	99
164	228	36	100
165	229	37	101
166	230	38	102

167	231	39	103
168	232	40	104
169	233	41	105
170	234	42	106
171	235	43	107
172	236	44	108
173	237	45	109
174	238	46	110
175	239	47	111
176	240	48	112
177	241	49	113
178	242	50	114
179	243	51	115
180	244	52	116
181	245	53	117
182	246	54	118
183	247	55	119
184	248	56	120
185	249	57	121
186	250	58	122
187	251	59	123
188	252	60	124
189	253	61	125
190	254	62	126
191	255	63	127
192	0	64	128
193	1	65	129
194	2	66	130
195	3	67	131
196	4	68	132
197	5	69	133
198	6	70	134
199	7	71	135
200	8	72	136
201	9	73	137
202	10	74	138
203	11	75	139
204	12	76	140
205	13	77	141
206	14	78	142
207	15	79	143
208	16	80	144
209	17	81	145
210	18	82	146
211	19	83	147
212	20	84	148
213	21	85	149
214	22	86	150
215	23	87	151
216	24	88	152

217	25	89	153
218	26	90	154
219	27	91	155
220	28	92	156
221	29	93	157
222	30	94	158
223	31	95	159
224	32	96	160
225	33	97	161
226	34	98	162
227	35	99	163
228	36	100	164
229	37	101	165
230	38	102	166
231	39	103	167
232	40	104	168
233	41	105	169
234	42	106	170
235	43	107	171
236	44	108	172
237	45	109	173
238	46	110	174
239	47	111	175
240	48	112	176
241	49	113	177
242	50	114	178
243	51	115	179
244	52	116	180
245	53	117	181
246	54	118	182
247	55	119	183
248	56	120	184
249	57	121	185
250	58	122	186
251	59	123	187
252	60	124	188
253	61	125	189
254	62	126	190
255	63	127	191

✋ ***Repeaters and base stations cannot have the same number. Neither can the repeater have a number identical to another base station or another repeater in a situation where common overlap is present between the actual units (Numbers in red indicate where numbering could be identical between different units). If this occurs, handover between the different units is not possible.***

Table 9 Example of a Normal Base Station/Repeater Configuration

Numbering of base stations and repeaters in a normal configuration	
First repeater	Base station number + 64 Base to synchronize on: base station number
Second repeater	Base station number + 128 Base to synchronize on: base station number
Third repeater	Base station number + 192 Base to synchronize on: base station number

Table 10 Example of Repeater Jump Configuration

Numbering of repeaters in a repeater jump configuration	
First repeater in chain	Base station number + 64 Base to synchronize on: base station number
Second repeater in chain	Base station number + 128 Base to synchronize on: Number of previous repeater
Third repeater in chain	Base station number + 192 Base to synchronize on: Number of previous repeater

For more information on programming the repeater with ServiceTool, refer to the **Help File** in ServiceTool. The ServiceTool software is available as a download from the STENTOFON AlphaWiki website.

7 Preparing the Handset for Use

This section provides information on how to prepare the handset for use, install and charge the battery, and retrieve the serial numbers on the different handsets.

This section includes information about:

- “Handset Description”
- “Installing Battery”
- “Charging Handsets”
- “Retrieving the Serial Number of the Handset”

For more information on the different handsets, refer to the Handset User Guides.

The charger and the power supply for the charger are ordered separately (refer to the sections below on “Charger Types and Part Numbers” and “Power Supply Types and Part Numbers” for information on part numbers).

7.1 Handset Description

The handset is a lightweight, ergonomically designed wireless unit that includes an LCD display and keyboard.

7.1.1 Handset Types and Item Numbers

Table 11 Handset Types

Type	Item number
Handset Rough w/ beltclip	2211100505
Handset Rough w/ Bluetooth & beltclip	2211100506
Handset Rough	2211100103
Handset Rough w/ Bluetooth	2211100104
Handset Office	2211100502
Handset EX	2211100501

7.1.2 Charger Types and Item Numbers

Table 12 Charger Types

Type	Item number
Handset EX Charger	2211100556
Handset Office Charger	2211100220
Handset Rough Charger	2211100560

7.2 Installing the Battery

✋ ***Take the following precautions before you handle the batteries:***

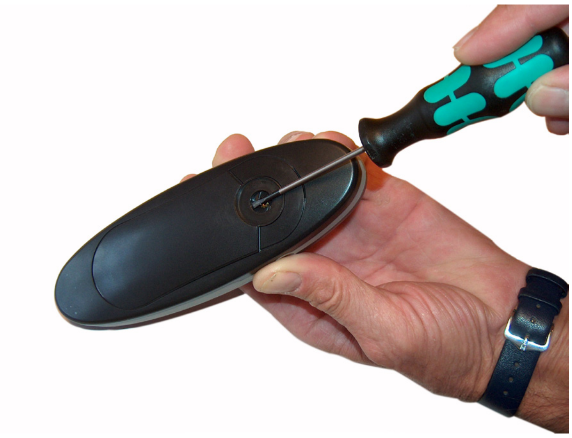
- Do not replace the batteries in potentially explosive environments such as rooms where flammable liquids or gases are present.
- Do not dispose of the battery in a fire as it will explode.
- Only use the proper batteries and the approved charger to charge the batteries.
- Only use battery with part no. 84743411 in the EX Handset. Do not use these batteries with other products. These batteries were designed specifically for use with the EX Handset and the charger ONLY. Improper use of the batteries may cause them to become a fire hazard.
- Only use battery with part no. 84743418 (ICP73048) in the Rough/ Office Handset. Do not use this battery with other products. This battery was designed specifically for use with the Rough/Office Handset and the charger ONLY. Improper use of the battery may cause them to become a fire hazard.
- Do not do anything that would cause the battery to short circuit.
- Do not let the battery or the charger come into contact with conductive metal objects.

7.2.1 Installing the Battery on EX Handset

To change the battery:

5. Unscrew the plate on the rear of the handset to access the battery compartment. Use a normal screw driver.
6. Insert the screwdriver into the small crack behind the back cover and lift to remove it.
7. Place the battery plug in the slot in the battery box.
8. Insert battery with its label showing.
9. Replace the back cover.

Figure 18 Removing Back Cover from EX Handset

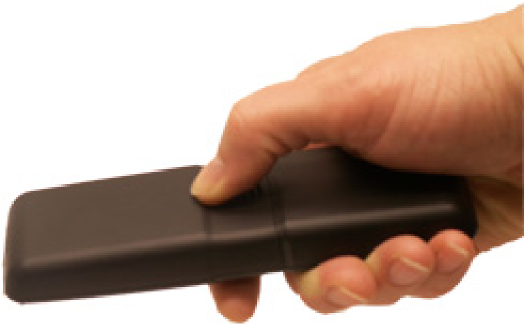


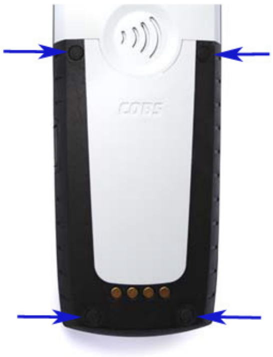
7.2.2 Installing Battery on Office Handset

To install the battery:

1. Press down the back cover and slide it towards the bottom of the handset.
2. Lift off the back cover.
3. Insert the battery with its label showing.
4. Replace the back cover by pressing it back into the locked position (when you hear a click, the back cover is in position).

Figure 19 Removing Back Cover from Office Handset





7.2.3 Installing Battery on Rough Handset

To install the battery:

1. Remove the battery cover by unfastening the four screws at the back-bottom part of the handset.
2. Carefully remove the battery cover.
3. Insert the battery with its label showing.
4. Replace the battery cover by refastening the four screws.

7.3 Charging Handsets

7.3.1 Using the Charger

Each handset is charged using a handset charger, which is a compact desktop unit designed to charge and automatically maintain the correct battery charge levels and voltage.

The charger for the EX Handset is powered by an AC (115VAC or 230VAC) adapter that supplies the 9VDC at 230mA charger requirement.

The charger for the Rough/Office Handset is powered by an AC (110VAC to 240VAC) adapter that supplies the 8VDC at 350mA charger requirement.

Figure 20 Single Charger for EX Handset

7.3.2 Charging the Battery

7.3.2.1 EX Handset

When charging the battery for the first time, it is necessary to leave the handset in the charger for 14 - 16 hours for the battery to be fully charged and the handset ready for use.

☞ *Normally, it takes approximately 3½ hours to charge the handset to its full capacity starting from being completely discharged.*

To charge the battery:

- Place the handset in the charger.

For correct charging, ensure that the room temperature is between 0°C/32°F and 25°C/77°F. Do not place the handset in direct sunlight. The battery has a built-in heat sensor which will stop charging if the battery temperature is too high.

If the handset is turned off when placed in the charger, only the LED indicates charging. When the handset is turned off, the LED flashes at a low frequency while charging and lights steadily when the charging is finished. There will be no reaction for incoming calls.

If the handset is turned on when charging, the display shows the charging status. It will not vibrate and B-answer is inactive. The handset reacts normally for incoming calls. The display goes back to normal mode when fully charged.

It is necessary to recharge the battery when the display shows “BATTERY LOW” or if the handset cannot be turned on. When the battery is fully discharged, up to 10 minutes may pass before charging begins (display lights up). When the charger begins the charging, the status is shown on the display if the handset is turned on.

The handset displays a progress indicator bar that shows how fully charged the battery is.

The handset LED has the following indication:

- LED steadily on = handset is fully charged
- LED flashing = handset is charging

7.3.2.2 Rough/Office Handset

When charging the battery for the first time, it is necessary to leave the handset in the charger for 14 - 16 hours for the battery to be fully charged and the handset ready for use.

☞ *During normal operation, it takes approximately 4 hours to charge the handset from being fully discharged to its full capacity.*

To charge the battery:

- Place the handset in the charger.

For correct charging, ensure that the room temperature is between 0°C/32°F and 40°C/104°F. Do not place the handset in direct sunlight. The battery has a built-in heat sensor which will stop charging if the battery temperature is too high.

If the handset is turned off when placed in the charger, there is nothing to indicate that it is charging. There will be no reaction for incoming calls.

If the handset is turned on when charging, the display shows a blue charging icon. The charging icon turns green when fully charged (when the handset is removed from the charger, the charging icon disappears). It will not vibrate. B-answer is inactive. The handset reacts normally for incoming calls.

It is necessary to recharge the battery when the handset display shows the ‘battery low’ icon, or if the handset cannot be turned on.

After charging, a green icon will be displayed to indicate that the battery is fully charged.

7.4 Retrieving the Serial Number of the Handset

To enable service to the handset, the serial number must be programmed into the system database via the web-based user interface of the IP DECT Server 6000. (For more information, refer to “Registering Handsets”).

The serial number (IPEI number) of each handset is found either on a label, which is placed behind the battery, or on the packaging label.

7.4.1 Retrieving Serial Number on EX Handset

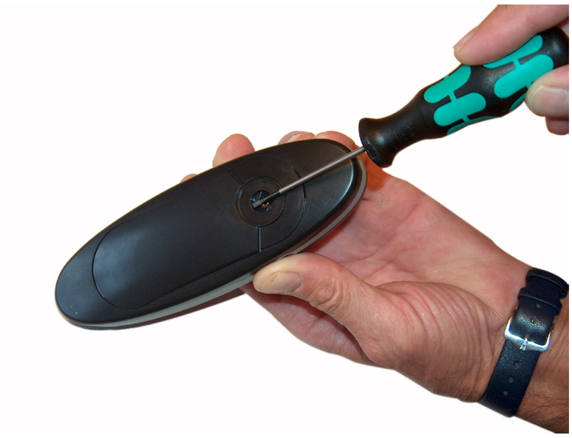
To show the serial number on the handset display for an EX Handset:

1. Enter ***99984***
2. Press ✓
   - the serial number will appear on the handset display.
3. Press **<** for 5 seconds to exit the menu.

To retrieve the serial number on an EX Handset:

1. Use a screwdriver to unscrew the plate on the rear of the handset to access the battery compartment.
2. The plate on the rear of the Handset must not be removed in a potentially explosive environment.
3. Insert the screwdriver into the small crack behind the back cover and lift to open the handset.
4. Lift the battery and read the serial number on the back label.
5. Replace the battery and back cover.

Figure 21 Removing Back Cover from EX Handset



7.4.2 Retrieving Serial Number on Office Handset

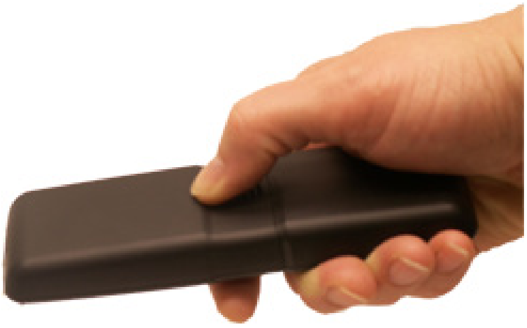
To display the serial or IPEI number on the handset:

1. Press **Menu**
2. Scroll to **Status** and press **Select**
3. Scroll to **Firmware version** and press **Select**
   - The IPEI number will be displayed.
4. Press **Back** and **Exit** to exit the menu

To retrieve the serial number on the Rough/Office Handset.

1. Press down the back cover and slide it towards the bottom of the handset.
2. Lift off the back cover.
3. Lift the battery and read the serial number.
4. Replace the battery and back cover.

Figure 22 Removing Back Cover from Rough/Office Handset



8 Configuring the IP DECT Server 6000

This section provides you with information on how to power up the IP DECT Server 6000 and connect the unit to a computer. It also contains information on how to configure a Server 6000 through the web-based user interface using either DHCP or a static IP address.

☞ *The IP DECT Server 6000 is pre-configured to use a static IP address.*

This section includes information about:

- “Powering up the Server 6000”
- “Connecting a Computer to the Server 6000”
- “Accessing the Server 6000”
- “Configuring the Server 6000 Using Static IP Address”
- “Checking the LED Indicator”

8.1 Powering up the Server 6000

After installing the Server 6000 you need to power up the unit using a local power supply.

Power options for the Server 6000 is 48VDC, 1 W maximum when using local power supply.

8.1.1 Local Power Supply

Powering the Server 6000 with a local power supply can be done using the power input on the unit.

☞ *The power supply for the IP DECT Server 6000 is ordered separately (Part no. 221 110 0225).*

8.2 Connecting a Computer to the Server 6000

The Server 6000 communicates with the computer through a cross-over patch cable.

☞ *The Ethernet port of the Server 6000 is an RJ45 connector.*

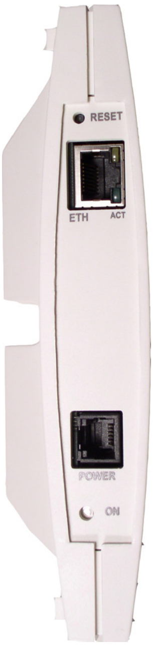


Figure 23 Faceplate showing Ethernet port

To connect the Server 6000 to a computer:

1. Connect the cross-over patch cable to the computer.
2. Connect the cross-over patch cable to the Ethernet (ETH) port of the Server 6000.

8.3 Accessing the Server 6000

The Server 6000 has default IP address: 192.168.0.1

In order for your computer to communicate with the Server 6000, it is necessary to change the computer’s Internet Protocol Properties to the following:

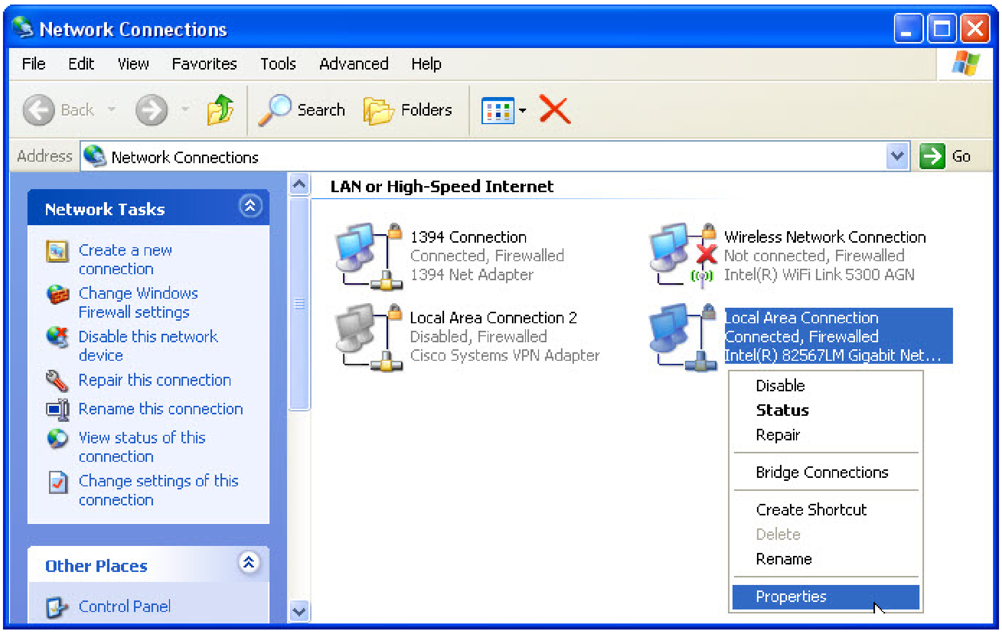
- IP address: **192.168.0.2**
- Subnet mask: **255.255.255.0**

8.3.1 Changing the Internet Protocol Properties using Windows

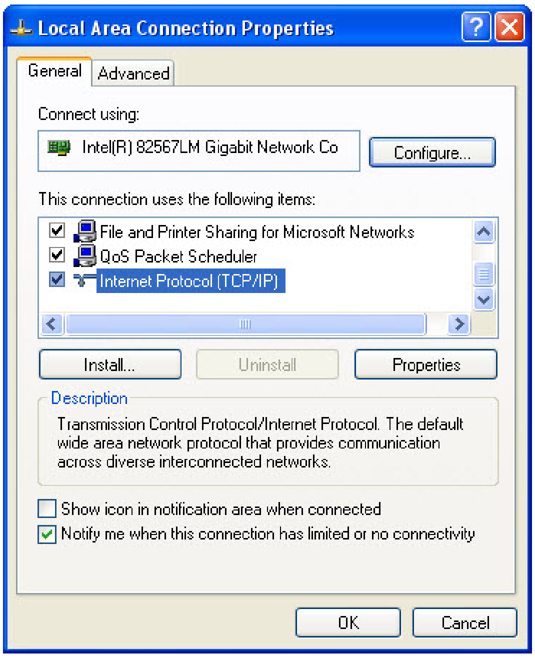
☞ *The example below describes the procedures for changing IP properties using Windows XP. Follow the procedures that are relevant to the Windows version that is installed on your computer.*

To change the IP properties in Windows XP:

1. Click **Start**
2. Point to **Connect To** and then click **Show all connections**.
   - A **Network Connections** window appears.



3. Under **LAN or High-Speed Internet**, right-click **Local Area Connection** and click **Properties**.
   - A **Local Area Connection Properties** dialog box appears.



Local Area Connection Properties

Connect using:

Intel(R) 82567LM Gigabit Network Co

This connection uses the following items:

☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

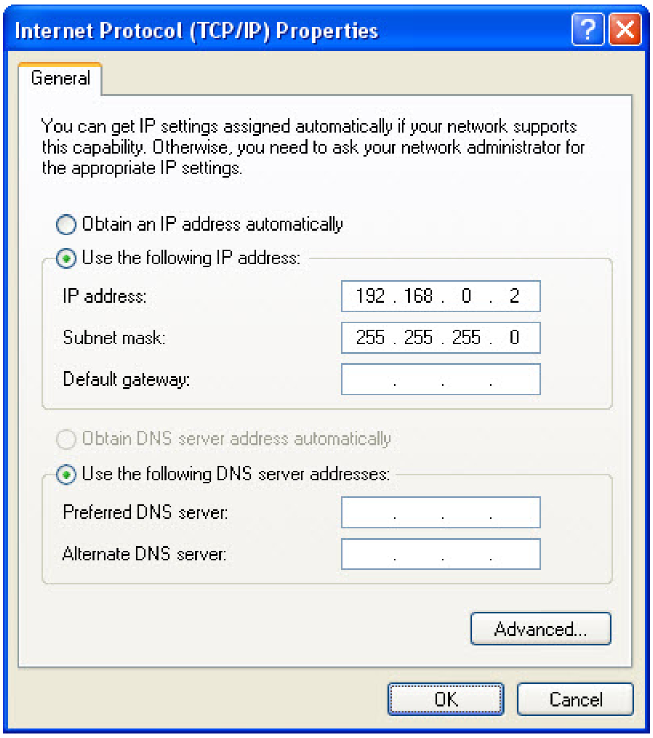
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

4. Under the **General** tab, click **Internet Protocol (TCP/IP)**, and then click **Properties**.

An **Internet Protocol (TCP/IP) Properties** dialog box appears.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 0 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

5. Click **Use the following IP address** and in the **IP address** field, enter **192.168.0.2**.
6. In the **Subnet mask** field, enter **255.255.255.0**
7. Click **OK**.

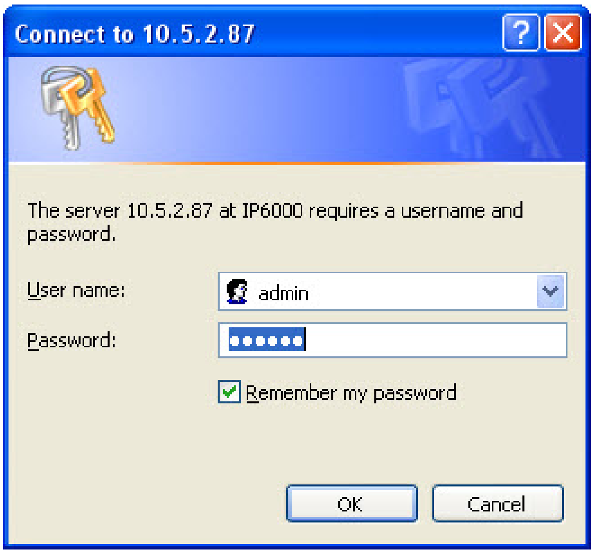
You can now communicate with the IP DECT Server 6000 from your computer using a standard web browser.

8.3.2 Accessing the Server 6000

To access the Server 6000, log into the web interface using a standard web browser.

1. Open a web browser.
2. In the browser's **Address** bar, enter IP address **192.168.0.1**, and press the ENTER key.

The Login page appears.



Connect to 10.5.2.87

The server 10.5.2.87 at IP6000 requires a username and password.

User name: admin

Password: ●●●●●●

☑ Remember my password

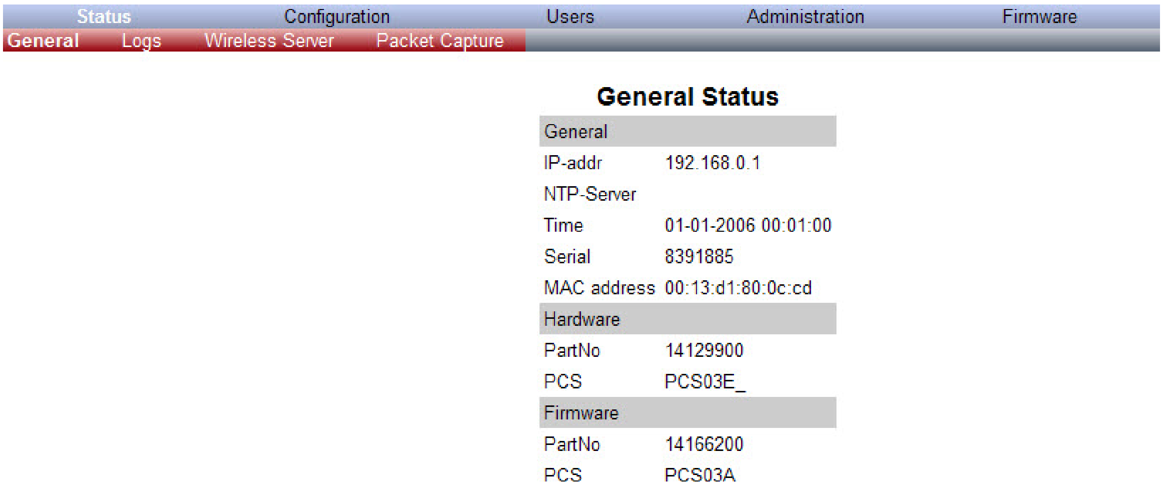
When you access the Server 6000 web interface for the first time, you need to log in with a user name and password.

☞ *The default user name is* ***admin*** *and the default password is* ***ip6000****. It is strongly recommended to change the password, refer to "Changing System User Name and Password".*

To log in:

1. In the **User name** field, enter **admin**.
2. In the **Password** field, enter **ip6000**.
3. Click **OK**.

The General Status page of the Server 6000 web interface is displayed.



General Status

General	
IP-addr	192.168.0.1
NTP-Server	
Time	01-01-2006 00:01:00
Serial	8391885
MAC address	00:13:d1:80:0c:cd
Hardware	
PartNo	14129900
PCS	PCS03E_
Firmware	
PartNo	14166200
PCS	PCS03A

8.4 Configuring the Server 6000 Using a Static IP Address

This section describes how to configure an Server 6000 using a static IP address.

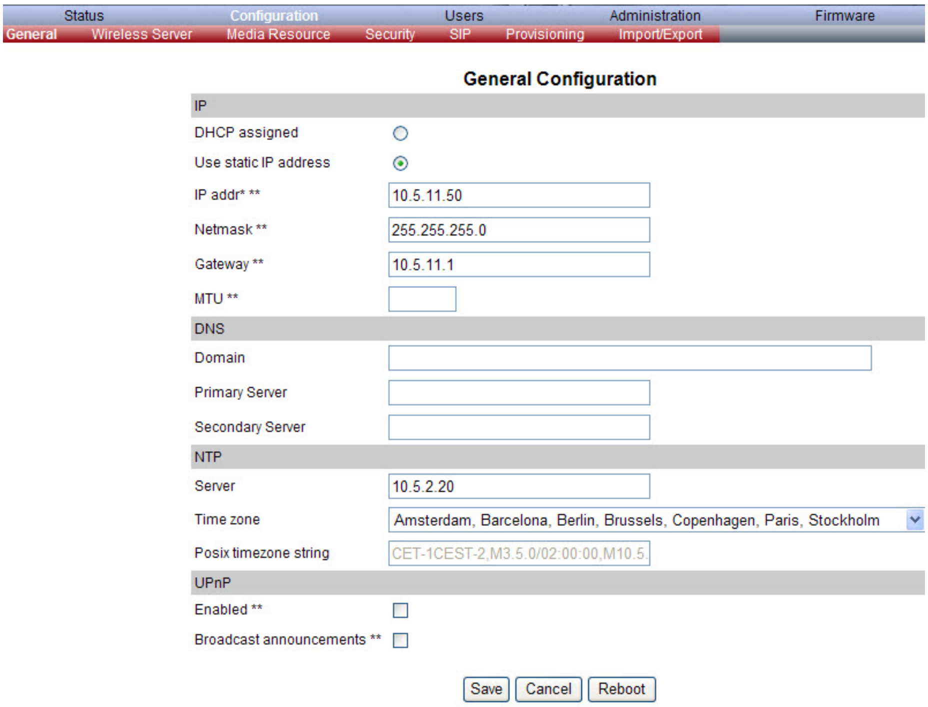
☞ *The Server 6000 is predefined to use a static IP address. It is highly recommended to configure the Server 6000 using a static IP address.*

This section contains information about:

- “General Configuration”
- “Wireless Server Configuration”
- “SIP Configuration”
- “Security Configuration”

8.4.1 General Configuration

You can define IP, DNS and NTP settings for the Server 6000 on the **Configuration > General** page.



General Configuration

IP

DHCP assigned ○

Use static IP address ●

IP addr* ** 10.5.11.50

Netmask ** 255.255.255.0

Gateway ** 10.5.11.1

MTU **

DNS

Domain

Primary Server

Secondary Server

NTP

Server 10.5.2.20

Time zone Amsterdam, Barcelona, Berlin, Brussels, Copenhagen, Paris, Stockholm

Posix timezone string CET-1CEST-2,M3.5.0/02:00:00,M10.5.

UPnP

Enabled ** □

Broadcast announcements ** □

To configure the Server 6000:

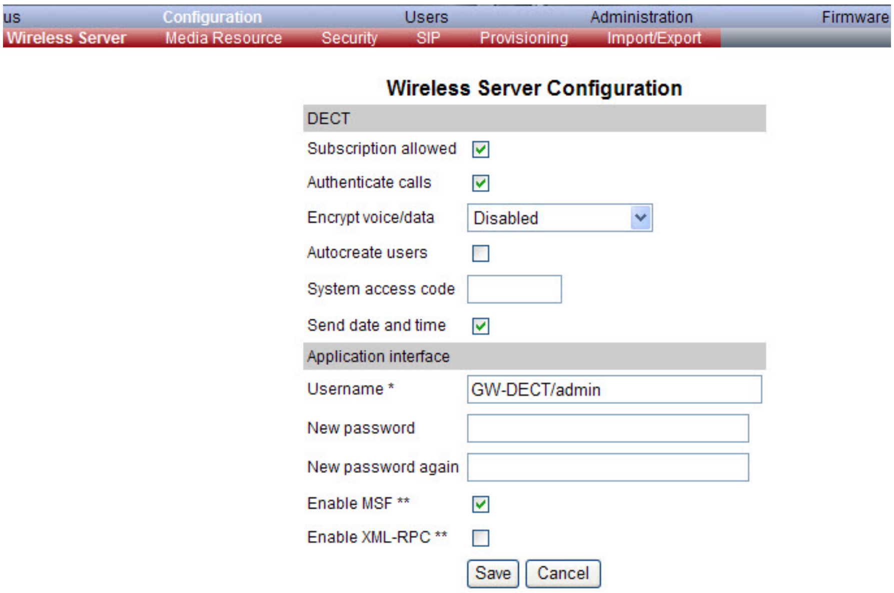
1. Click **Configuration**, and then click **General**.
2. Click **Use Static IP Address**.
3. In the **IP addr** field, enter the IP address of the IP DECT Server 6000.
   - the IP address should be in the same network range as that of the AlphaCom/ACM exchange
   - Contact your system administrator for more information.
4. In the **Netmask** field, enter a new network mask.
   - Contact your system administrator for more information.
5. In the **Gateway** field, enter the IP address of the default gateway.
   - The default gateway serves as an access point to another network. Contact your system administrator for more information.
6. In the **MTU** (Maximum Translation Unit) field, enter the size of the largest packet that your network protocol can transmit (optional).
7. In the **Domain** field, enter the domain name of the system (optional).
8. In the **Primary Server** and **Secondary Server** fields (under **DNS**

- Domain Name System), enter the IP address of the DNS server (optional).

9. In the **Server** field (under **NTP** - Network Time Protocol), enter the IP address of the NTP server from which the system will obtain the current time (optional).
10. From the **Time Zone** dropdown list, select the desired time zone (optional).
11. For **UPnP** (Universal Plug and Play) leave both **Enabled** and **Broadcast announcements** with their default values (optional).
12. Click **Save** to save your general configuration data.

8.4.2 Wireless Server Configuration

On the **Configuration > Wireless Server** page, you can configure the Server 6000 to allow subscription. If the system does not allow subscription, it is not possible to subscribe a handset.



Wireless Server Configuration

DECT

Subscription allowed	☑
Authenticate calls	☑
Encrypt voice/data	Disabled
Autocreate users	□
System access code	
Send date and time	☑

Application interface

Username *	GW-DECT/admin
New password	
New password again	
Enable MSF **	☑
Enable XML-RPC **	□

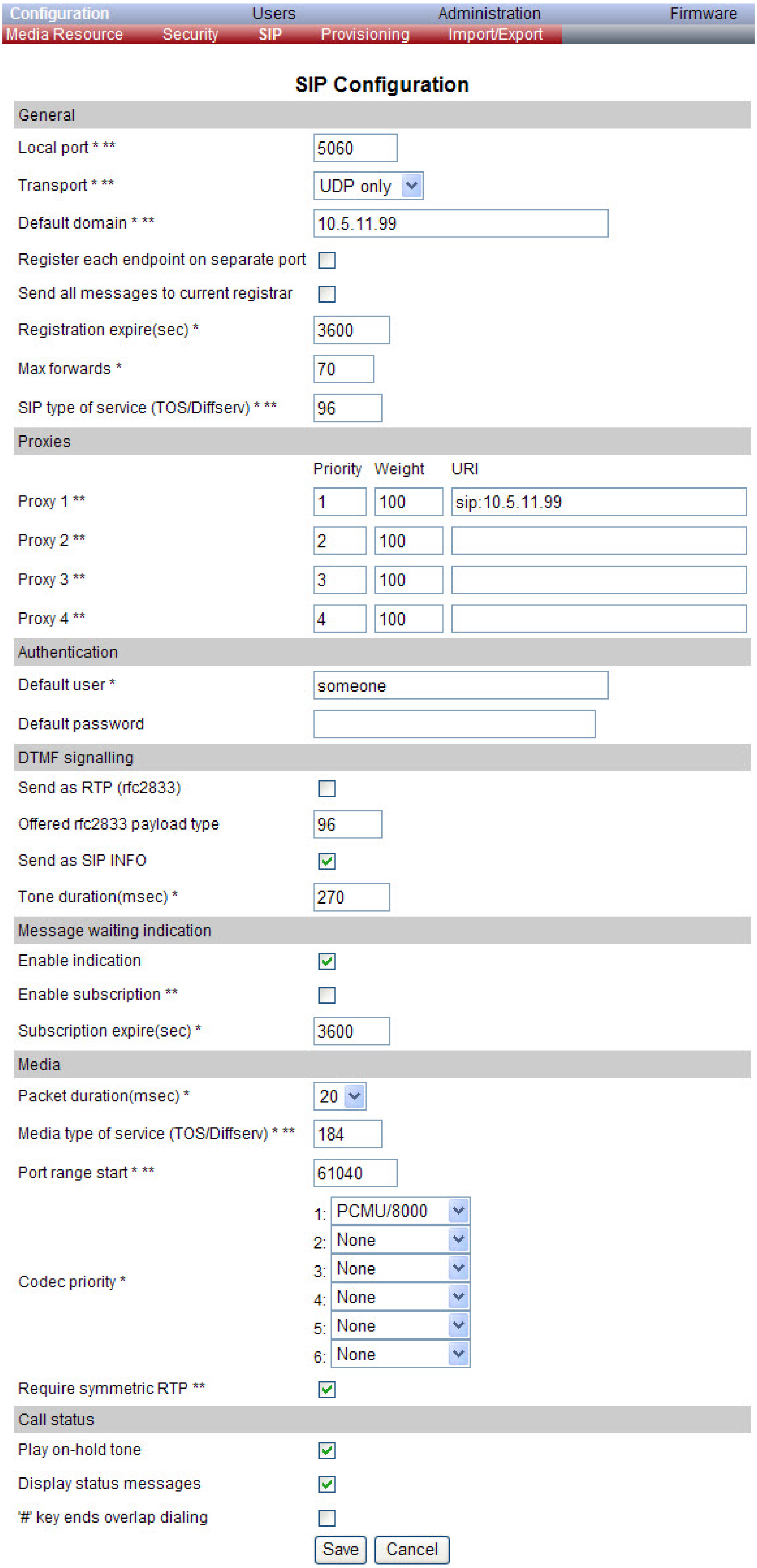
To configure the Server 6000:

1. Click **Configuration**, and then click **Wireless Server**.
2. Check the **Subscription Allowed** checkbox.
   - If this is not checked, you cannot subscribe a handset.
3. Uncheck the **Autocreate users** checkbox
4. Enter an access code in the **System access code** field (optional)
5. Check the **Send date and time** checkbox (optional)
6. For all the fields under **Application interface** leave them with their default values.
7. Click **Save**.

8.4.3 SIP Configuration

On the **Configuration > SIP** page, you can define general SIP settings, information about authentication, DTMF signalling, message waiting indication and media.

1. Click **Configuration**, and then click **SIP**.



SIP Configuration

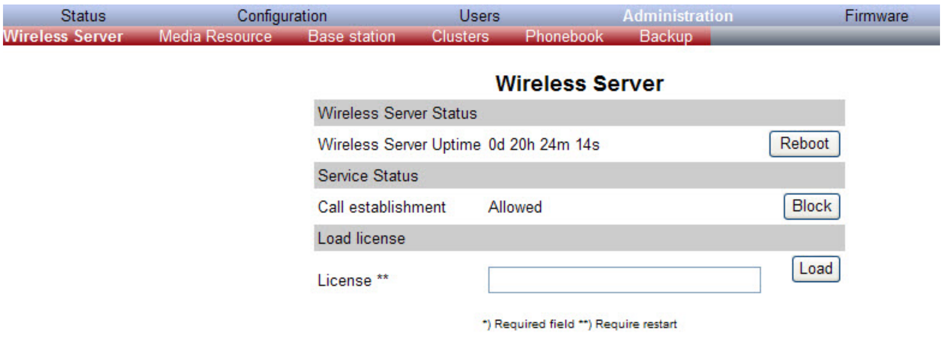
General			
Local port * **	5060		
Transport * **	UDP only		
Default domain * **	10.5.11.99		
Register each endpoint on separate port	□		
Send all messages to current registrar	□		
Registration expire(sec) *	3600		
Max forwards *	70		
SIP type of service (TOS/Diffserv) * **	96		
Proxies			
	Priority	Weight	URI
Proxy 1 **	1	100	sip:10.5.11.99
Proxy 2 **	2	100	
Proxy 3 **	3	100	
Proxy 4 **	4	100	
Authentication			
Default user *	someone		
Default password			
DTMF signalling			
Send as RTP (rfc2833)	□		
Offered rfc2833 payload type	96		
Send as SIP INFO	☑		
Tone duration(msec) *	270		
Message waiting indication			
Enable indication	☑		
Enable subscription **	□		
Subscription expire(sec) *	3600		
Media			
Packet duration(msec) *	20		
Media type of service (TOS/Diffserv) * **	184		
Port range start * **	61040		
Codec priority *	1: PCMU/8000 2: None 3: None 4: None 5: None 6: None		
Require symmetric RTP **	☑		
Call status			
Play on-hold tone	☑		
Display status messages	☑		
'#' key ends overlap dialing	□		

2. In the **Local port** field, enter the local port number. The default local port number is **5060**.
   - The local port is the port on which the Server 6000 listens for incoming SIP signalling.
3. For the **Transport** dropdown list, select **UDP only**.
4. In the **Default domain** field, enter the **IP address of the AlphaCom/ ACM** exchange.
5. Uncheck the **Register each endpoint on separate port** checkbox.
6. Uncheck the **Send all messages to current registrar** checkbox.
7. For the **Registration expire(sec)** field for the number of seconds before a SIP registration is renewed, accept the default value.
8. For the **Max forwards** field, accept the default value.
9. For the **SIP type of service (TOS/Diffserv)** field, accept the default value.
10. It is possible to enter up to four proxies. In the **Proxy 1** field, enter the IP address of the AlphaCom/ACM exchange.
    - The prefix *sip:* will be automatically added to the IP address after the configuration data has been saved, e.g. *sip:10.5.11.99*
    - The proxy is the **SIP URI** of the SIP proxy. The Server 6000 will route all outgoing SIP signalling to the proxy, e.g. SIP registrations and outgoing calls.
11. In the **Default user** field, accept the default value.
12. For the **Default password** field, leave it blank.
    - If no handset specific authentication user name/password is configured, handsets registered on the Server 6000 will use the default user name/password for authentication.
13. Uncheck the **Send as RTP (rfc2833)** checkbox.
    - Real-time Transport Protocol
    - When using the AlphaCom/ACM exchange server, keypad signalling should NOT be sent as RTP packets with DTMF code.
14. For the **Offered rfc2833 payload type** field, leave it as default **96**.
15. Check the **Send as SIP INFO** checkbox.
    - Keypad signalling should be sent as SIP INFO to the AlphaCom/ ACM exchange server.
16. In the **Tone duration(msec)** field for the time length of the tone in milliseconds, accept the default value.
17. Uncheck the **Enable indication** checkbox.
    - We do NOT want to handle MWI messages.
18. Uncheck the **Enable subscription** checkbox.
    - We do NOT want to subscribe to MWI messages from the SIP proxy.
19. For the **Subscription expire(sec)** field, accept the default value.
20. From the **Packet duration (msec)** dropdown list, select **20**.
21. For the **Media type of service (TOS/Diffserv)** field, accept the default value.
22. For the **Port range start** field, enter the value **61040**
23. In the **Codec priority** dropdown lists, select **PCMU/8000** as first priority. For the other priority codecs, select **None**.
24. Check the **Require symmetric RTP** checkbox.
25. Check the **Play on-hold tone** checkbox.
26. Check the **Display status messages** checkbox.
27. Uncheck the **'#' key ends overlap dialing** checkbox.
28. Click **Save** to save your SIP configuration data.

8.4.4 Rebooting the Server 6000

After SIP configuration has been carried out, you should reboot the Server 6000 in the **Administration > Wireless Server** page.

To reboot:



Wireless Server

Wireless Server Status

Wireless Server Uptime 0d 20h 24m 14s

Service Status

Call establishment Allowed

Load license

License **

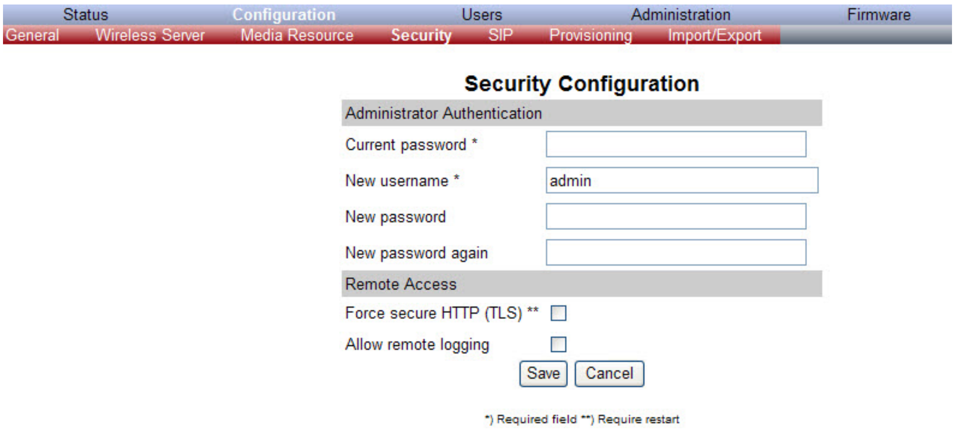
*) Required field **) Require restart

1. Click **Administration**, and then click **Wireless Server**.
2. Click **Reboot** next to **Wireless Server Uptime**.

☞ *After rebooting, change the IP address of your computer to one that is in the same LAN range as that of the Server 6000 or set the TCP/IP properties to obtain an IP address automatically.*

8.4.5 Security Configuration

It is possible to change the password for the Server 6000 from the **Configuration > Security** page.



Security Configuration

Administrator Authentication

Current password *

New username * admin

New password

New password again

Remote Access

Force secure HTTP (TLS) ** □

Allow remote logging □

*) Required field **) Require restart

1. Click **Configuration**, and then click **Security**.
2. In the **Current password** field, enter the current password.
3. In the **New username** field, enter a new username.
4. In the **New password** field, enter a new password.
5. In the **New password again** field, re-enter the new password.
6. Uncheck the **Force secure HTTP (TLS)** checkbox.
7. Uncheck the **Allow remote logging** checkbox.
8. Click **Save**.

8.5 Checking the LED Indicator

Verify that the Server 6000 LED is lighting a steady green, indicating that it is now operational.

9 Configuring the Base Station

This section provides you with information on how to connect the base station to an IP DECT Server 6000 and how to configure the base station through the web-based user interface using either DHCP or a static IP address.

This section includes information about:

- “Powering up the Base Station”
- “Connecting a Computer to the Base Station”
- “Accessing the Base Station”
- ”Configuring the Base Station Using DHCP”
- “Checking the LED Indicator”

9.1 Powering up the Base Station

After installing the base station you need to power it up. The base station uses:

- Power over Ethernet (PoE 802.3af).
- Maximum power supply consumption is 3.0W (IEEE 802.3af class 1 device).

Use a standard PoE adapter or a PoE-enabled port on a switch adhering to PoE 802.3af when connecting the base station to a PoE power source.

9.2 Connecting a Computer to the Base Station

The base station itself has the IP address **192.168.0.1** from factory default settings. The computer communicates with the base station either through a cross-over patch cable or through a network with an identical net mask.

☞ *The LAN port of the base station is an RJ45 connector.*

To connect the computer to the base station:

1. Connect the LAN cable or cross-over patch cable to the PoE switch.
2. Connect the LAN cable or cross-over patch cable to the Ethernet connector on the base station.
3. Connect the PoE switch to the computer.

☞ *If the base station has been used, reset it to factory default settings such that its IP address reverts to* **192.168.0.1**

9.3 Accessing the Base Station

Before accessing the user interface of the base station, communication between the computer and the base station has to be set up by changing the IP properties of the computer to IP address: **192.168.0.2** and Subnet mask: **255.255.255.0** in Windows.

The procedure for doing this is identical to that for the Server 6000, and is described in section 8.3.

After setting up communication between the base station and the computer, access the base station by logging into its web interface using a standard web browser.

1. Open a web browser.
2. In the browser's **Address** bar, enter IP address **192.168.0.1**, and press the **ENTER** key.

The Login page is displayed.

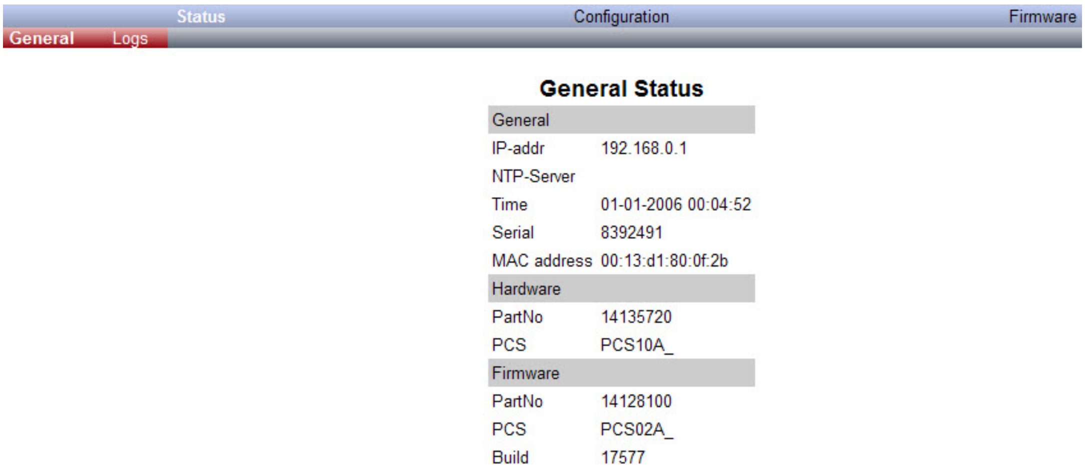
When you access the user interface for the first time, you need to log in with a user name and password.

☞ *The default user name of the system is* **admin** *and the default password of the system is* **ip6000**. *It is strongly recommended to change the password - see "Changing System User Name and Password".*

To log in:

1. In the **User Name** field, enter **admin**.
2. In the **Password** field, enter **ip6000**.
3. Click **OK**.

The Base Station **General Status** page is displayed.



General Status

General	
IP-addr	192.168.0.1
NTP-Server	
Time	01-01-2006 00:04:52
Serial	8392491
MAC address	00:13:d1:80:0f:2b
Hardware	
PartNo	14135720
PCS	PCS10A_
Firmware	
PartNo	14128100
PCS	PCS02A_
Build	17577

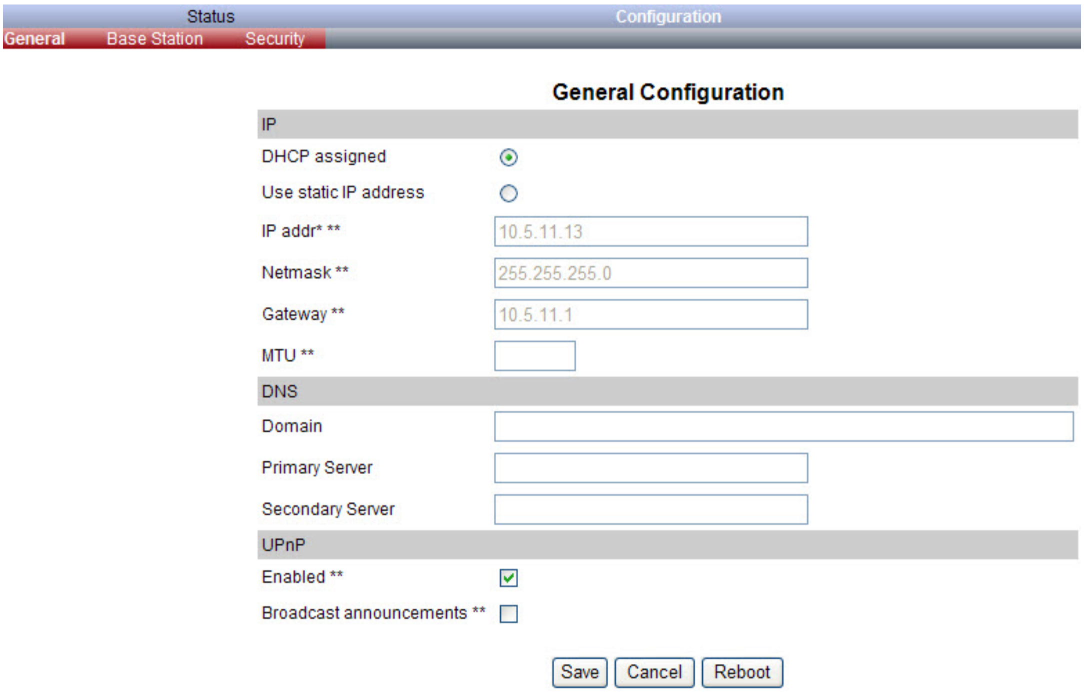
9.4 Configuring the Base Station Using DHCP

This section describes how to configure a base station using DHCP.

☞ *It is strongly recommended to configure the base station using DHCP.*

9.4.1 General Configuration

On the **General Configuration** page, you can define DNS settings for the base station.



General Configuration

IP

DHCP assigned	●
Use static IP address	○
IP addr* **	10.5.11.13
Netmask **	255.255.255.0
Gateway **	10.5.11.1
MTU **	

DNS

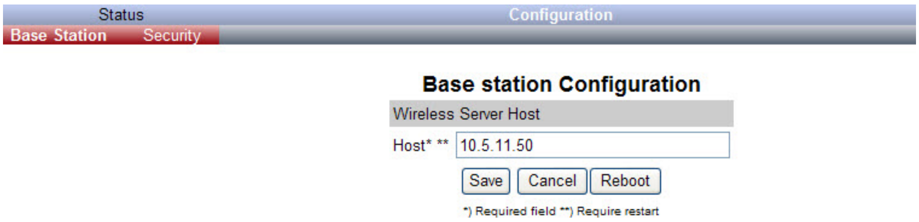
Domain	
Primary Server	
Secondary Server	

UPnP

Enabled **	☑
Broadcast announcements **	□

1. Click **Configuration**, and then click **General**.
2. Click the **DHCP assigned** radio button.
3. For the **MTU** (Maximum Translation Unit) field, for entering the size of the largest packet that your network protocol can transmit, leave it blank.
4. Leave the following fields blank:
   - **Domain**
   - **Primary Server**
   - **Secondary Server**
5. For **UPnP** (Universal Plug and Play) leave both **Enabled** and **Broadcast announcements** with their default values (optional).
6. Click **Save**.

9.4.2 Base Station Configuration



Base station Configuration

Wireless Server Host

Host* ** 10.5.11.50

*) Required field **) Require restart

To configure the base station:

1. Click **Configuration**, and then click **Base Station**.
2. In the **Host** field, enter the **IP address of the Server 6000**.
3. Click **Save**.
4. Click **Reboot** to enable the configuration changes.

9.4.3 Security Configuration

The procedures for administrating username and password for the base station is identical to that for the Server 6000, and are described in section 8.4.5.

- Click **Configuration**, and then click **Security**.

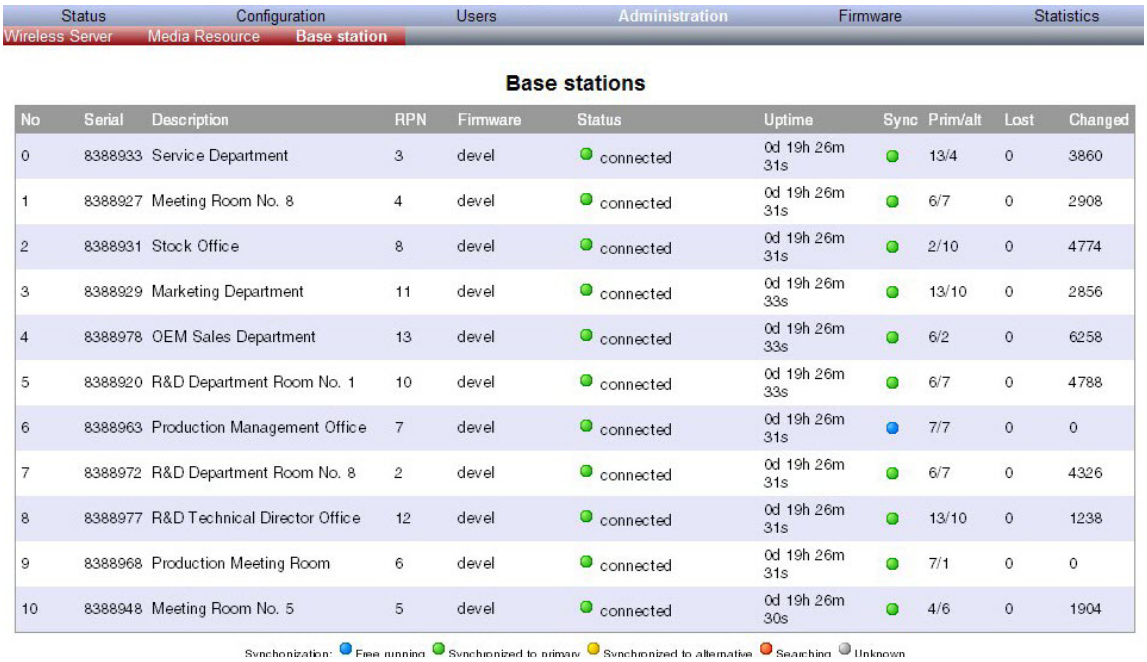
You will now be able to change your password, etc.

9.4.4 Synchronization Ways Configuration

The synchronization ways of the base station have to be defined in the **Administration > Base station** page of the Server 6000.

You will now have to connect the base station to a PoE switch that is on the same network as the Server 6000 and the AlphaCom/ACM exchange.

1. Log into the web interface for the Server 6000.
2. Click **Administration**, and then click **Base station**.

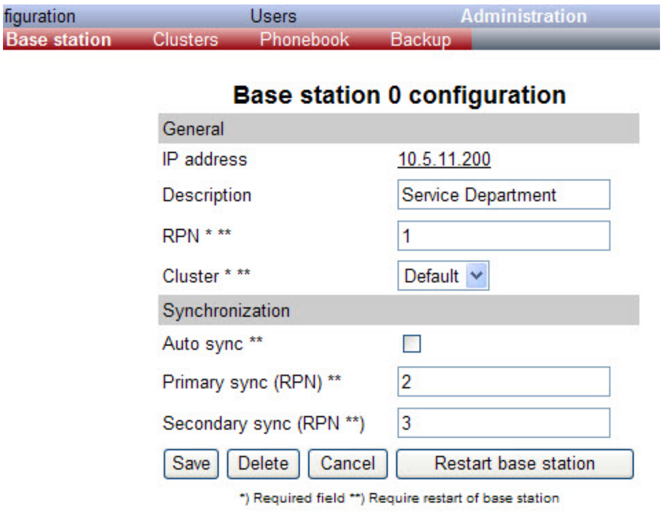


Base stations

No	Serial	Description	RPN	Firmware	Status	Uptime	Sync	Prim/alt	Lost	Changed
0	8388933	Service Department	3	devel	🟢 connected	0d 19h 26m 31s	🟢	13/4	0	3860
1	8388927	Meeting Room No. 8	4	devel	🟢 connected	0d 19h 26m 31s	🟢	6/7	0	2908
2	8388931	Stock Office	8	devel	🟢 connected	0d 19h 26m 31s	🟢	2/10	0	4774
3	8388929	Marketing Department	11	devel	🟢 connected	0d 19h 26m 33s	🟢	13/10	0	2856
4	8388978	OEM Sales Department	13	devel	🟢 connected	0d 19h 26m 33s	🟢	6/2	0	6258
5	8388920	R&D Department Room No. 1	10	devel	🟢 connected	0d 19h 26m 33s	🟢	6/7	0	4788
6	8388963	Production Management Office	7	devel	🟢 connected	0d 19h 26m 31s	🔵	7/7	0	0
7	8388972	R&D Department Room No. 8	2	devel	🟢 connected	0d 19h 26m 31s	🟢	6/7	0	4326
8	8388977	R&D Technical Director Office	12	devel	🟢 connected	0d 19h 26m 31s	🟢	13/10	0	1238
9	8388968	Production Meeting Room	6	devel	🟢 connected	0d 19h 26m 31s	🟢	7/1	0	0
10	8388948	Meeting Room No. 5	5	devel	🟢 connected	0d 19h 26m 30s	🟢	4/6	0	1904

Synchonization: 🔵 Free running 🟢 Synchronized to primary 🟡 Synchronized to alternative 🔴 Searching ⚪ Unknown

3. Click the relevant base station in the list to open the Configuration page.



Base station 0 configuration

General	
IP address	10.5.11.200
Description	Service Department
RPN * **	1
Cluster * **	Default
Synchronization	
Auto sync **	□
Primary sync (RPN) **	2
Secondary sync (RPN **)	3

*) Required field **) Require restart of base station

4. In the **RPN** field, type the Radio Part Number of the base station.
   - The Radio Part Number can be a number between 0 and 255. See your site plan. The default value of the RPN is the base station number. It is recommended that the number starts with 1.
5. For **Cluster**, leave as **Default**.
6. Check the **Auto sync** checkbox if you are deploying and want to find a sync way for the first base station.
   - Auto sync is only to be used in a deployment situation. When selecting Auto sync, radio part numbers in the **Primary sync (RPN)** and **Secondary sync (RPN)** fields are not taken into consideration.
7. In the **Primary sync (RPN)** field, enter the radio part number of the base station you want to synchronize on.
   - See your site plan.
8. In the **Secondary sync (RPN)** field, enter the radio part number of the base station, you want to synchronize on.
   - See your site plan.
9. Click **Save**.
10. Click **Restart base station** to enable the configuration changes.

To check the sync state of the base station, refer to “Sync State of Base Station”.

9.5 Checking the LED Indicator

Verify that the base station LED is lighting a steady green, indicating that the base station is now operational.

10 Handset Registration and Subscription

This section provides information about handset registration and subscription. You must register and subscribe a handset before you can use it.

☞ *This section only describes how to register handsets on the Server 6000. You also need to register the users on the call handler/AlphaCom/ACM. For registering users on the call handler/AlphaCom/ACM, refer to the relevant user and system guides.*

When registering handset, information on handsets settings such as the serial number (IPEI), name, etc. is entered into the system database. When subscribing handsets you subscribe a registered handset to the system for usage. If the handset is not registered in the system database, subscription of the handset is not possible.

This section includes information about:

- "Registering Handsets"
- "Subscribing Handsets"

10.1 Registering Handsets

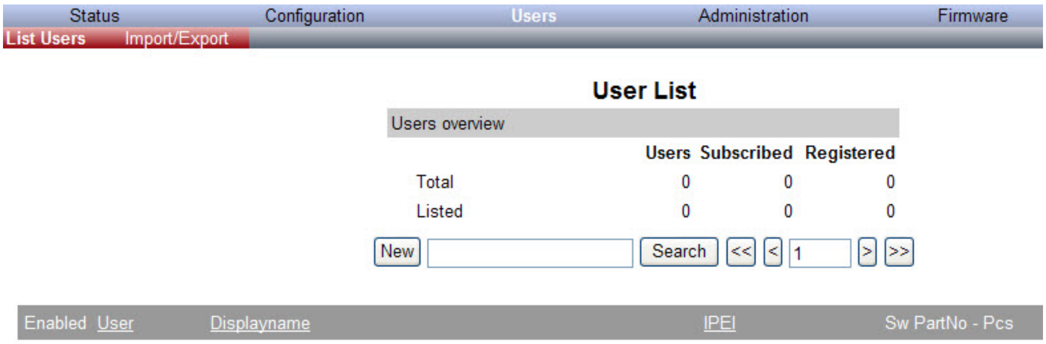
The **Users** page of the web-based interface of the Server 6000 is used to register handsets.

Each handset in the wireless solution must be programmed with the serial number (IPEI) before it can operate. This serial number must be registered in the **Users** page of the web-based user interface of the Server 6000. The serial number is a unique fingerprint of each handset. The serial number is programmed into the handset during the manufacturing process and cannot be changed by field personnel.

☞ *The Server 6000 will not provide any service to a handset if its serial number is not registered in the web-based user interface.*

To register a handset:

1. Click **Users**, and then click **List Users**.



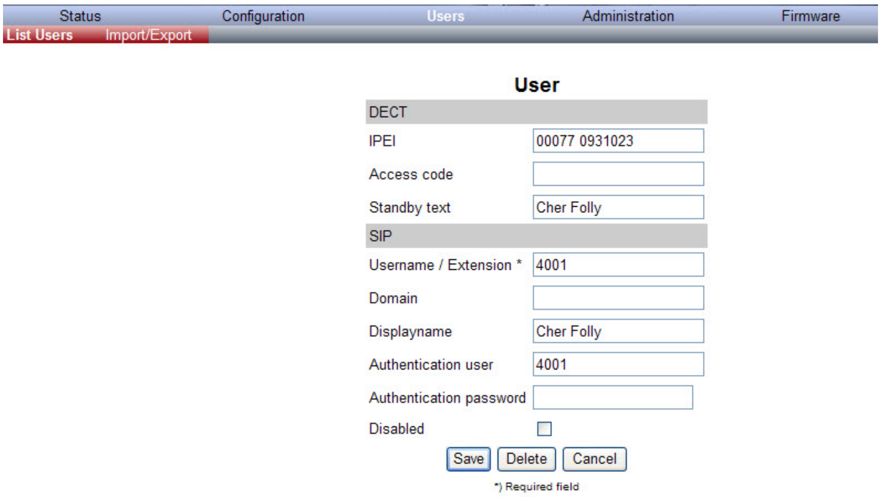
User List

Users overview

	Users	Subscribed	Registered
Total	0	0	0
Listed	0	0	0

Enabled	User	Displayname	IPEI	Sw PartNo - Pcs

2. Under **User List**, click **New**.



User

DECT	
IPEI	00077 0931023
Access code	
Standby text	Cher Folly
SIP	
Username / Extension *	4001
Domain	
Displayname	Cher Folly
Authentication user	4001
Authentication password	
Disabled	□

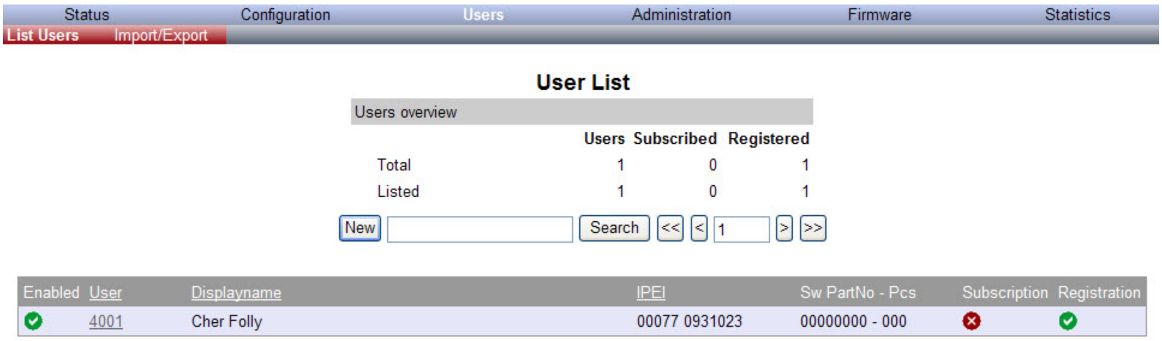
*) Required field

The data configured for each handset can be split into two categories: DECT data which is necessary for the correct handling of the DECT protocol stack, and SIP data which is necessary for the handling of a SIP user agent.

For Rough/Office handsets, it is NOT necessary to enter the IPEI number as the auto-subscription feature will locate the IPEI numbers automatically.

3. In the **IPEI** field, enter the IPEI number (serial number) of the **EX handset**.
   - The serial number consist of a five-digit handset type (manufacturer code) and a seven-digit handset number.
   - For more general information about the IPEI number (serial number) and how to retrieve it, refer to "Retrieving the Serial Number of the Handset".
   - To view the IPEI number for EX handset, enter ***99984*** and then press ✓ - the number starts with 00077...
4. In the **Access code** field, enter the authentication code (AC) (optional)
   - The authentication code is a subscription password of a maximum of eight digits, defined by the technicians and can be used when connecting the handset to an Server 6000. The authentication code is a subscription PIN code for the individual handset.
5. In the **Standby text** field, enter a text to be displayed when the handset is on hook (optional).
6. In the **Username/Extension** field, enter a directory number.
   - The value of this field should be the same as the AlphaCom/ACM directory number.
7. Leave the **Domain** field blank.
8. In the **Displayname** field, enter the name to be displayed (caller ID), e.g. John Doe in John Doe<sip:1234@example.com> (optional).
9. In the **Authentication user** field, enter a directory number (optional).
   - This should be the same as the directory number registered in the AlphaCom/ACM exchange.
   - The user name will override the **Default user** field under **SIP Configuration** (refer to "SIP Configuration").
10. Leave the **Authentication password** field blank.
    - This is not necessary for an AlphaCom/ACM configuration.
    - The password will override the **Default Password** field under SIP Configuration (refer to "SIP Configuration").
11. Uncheck the **Disabled** checkbox.
12. Click **Save** to save the registration data.
13. Click **OK** on the next page.

The newly registered user/handset is now listed:



User List

Users overview

	Users	Subscribed	Registered
Total	1	0	1
Listed	1	0	1

Enabled	User	Displayname	IPEI	Sw PartNo - Pcs	Subscription	Registration
✓	4001	Cher Folly	00077 0931023	00000000 - 000	✗	✓

Repeat the whole procedure to register each new handset.

10.2 Subscribing Handsets

The subscription procedure for EX, Rough and Office Handsets is carried out on the handset itself.

☞ *Subscription of handsets requires the use of each registered handset.*

☞ *For subscriptions to work, the system must allow subscriptions to be made (refer to "Server 6000 Configuration"). Some systems also require an Authentication Code (AC). If more than one system currently permits subscription, you will need to know the ID of the system (ARI code) to which you wish to subscribe. Authentication Codes and system IDs (ARI code on the label at the rear of the Server 6000) may be provided by the system administrator.*

Before subscribing handsets you need to ensure:

- that handset battery has been charged (see "Charging Battery"). Low battery could cause subscription problems.
- that the handsets have been registered to the system (see "Registering Handsets").

10.2.1 Subscribing an EX Handset

To Subscribe a EX Handset:

1. Press **MENU** and go to **MENU LOGIN**.
2. Press ✓ and go to **SUBSCRIPTION CREATE**.
3. Press ✓ .
   - The handset will start searching for the ARI code or serial number of the Server 6000.
4. Use the **< >** keys to scroll between the ARI codes if there is more than one Server 6000 available.
   - During subscription, the handset searches for free positions and carries out subscription on the first free position.
5. As soon as the correct ARI code of the Server 6000 appears in the display, press ✓ .
   - The ARI code can be found on the label at the back of the Server 6000.
6. Enter the AC (if required) using the keypad, and press ✓ .

An antenna symbol and user name should appear on the display to indicate a successful subscription. If not, the subscription has failed and the procedure should be repeated.

10.2.1.1 Subscribing EX Handset to Different Systems

The handset can be subscribed (connected) to a maximum of 10 different systems.

☞ *To be able to log on to a system, subscription to the system must be established.*

Changing to another System Automatically Using Auto Login A

☞ *Auto Login A should only be used when systems are separate with no overlaps.*

To change to another system automatically:

1. Press **MENU** and go to **MENU LOGIN**.
2. Press ✓ and go to **SELECT LOGIN**.
3. Press ✓ and go to **SELECT LOGIN AUTO A**.
4. Press ✓ .

The handset automatically selects a system.

The selected system is marked with an **A**.

Changing to another System Automatically Using Auto Login B

☞ *Auto Login B can be used in separate systems which overlap each other.*

To change to another system automatically:

1. Press **MENU** and go to **MENU LOGIN**.
2. Press ✓ and go to **SELECT LOGIN**.
3. Press ✓ and go to **SELECT LOGIN AUTO B**.
4. Press ✓ .

The handset automatically selects a system.

The selected system is marked with a **B**.

Changing to another System Manually

To change to another system:

1. Press **MENU** and go to **MENU LOGIN**.
2. Press ✓ and go to **SELECT LOGIN** to subscribe to a system.
   - The actual chosen system is marked with an ***** or an **A** (if Auto Login is selected).
3. Press ✓ and use the **< >** keys to scroll between the IDs of the different systems to find the system to which you want to connect.
   - Under **SELECT LOGIN**, only subscriptions are displayed. Free positions are not displayed.
4. Press ✓ to confirm.

10.2.2 Rough/Office Handset Subscription

A handset can be subscribed to more than one system and will automatically log on to the relevant system. If a handset is subscribed to two or more systems, you can use Auto Login type A to change between the systems automatically.

☞ *Auto Login A should only be used in separate systems without overlaps.*

If a handset loses signal from the system (the display shows a no-signal icon), after 20 seconds the handset will start searching for an alternative system available from the Login list and automatically change to this system.

☞ *When using Auto Login A, any call will be dropped when changing to an alternative system.*

☞ *Subscription of handsets requires the use of each registered handset.*

☞ *For subscriptions to work, the system must allow subscriptions to be made (refer to "6000 Server Configuration"). Some systems also require an Authentication Code (AC). If more than one system currently permits subscription, you will need to know the ID of the system (ARI code) to which you wish to subscribe. Consult the system administrator for Authentication Codes and system IDs (ARI code on the label at the rear of the Server 6000).*

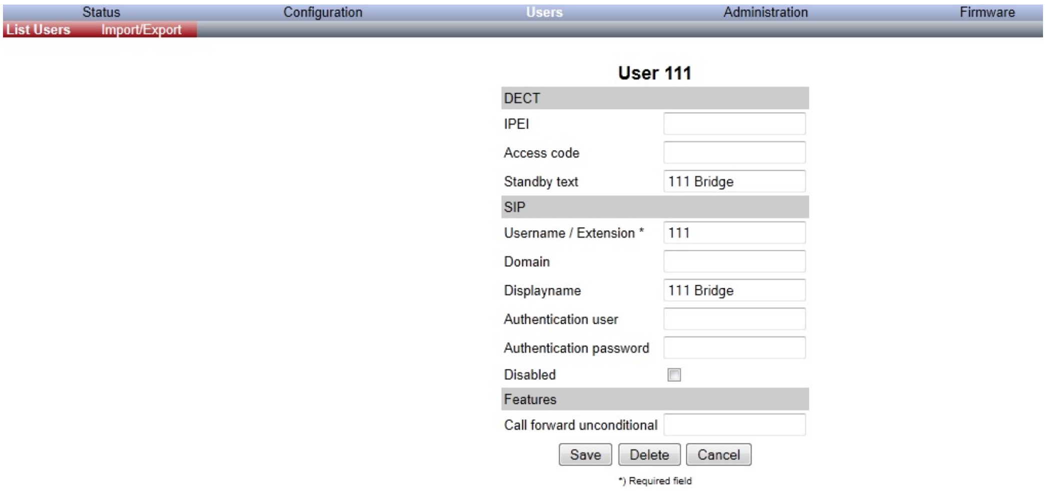
Before subscribing handsets you need to ensure that:

- the handset battery has been charged (see "Charging Battery"). Low battery could cause subscription problems.
- the handsets have been registered to the system (see "Registering Handsets").

10.2.3 Subscribing a Rough Handset

Before starting the subscription process, register the handset in the IP DECT server:

1. Select **Users** > **List Users** and click **New** to define a new user without entering the IPEI number

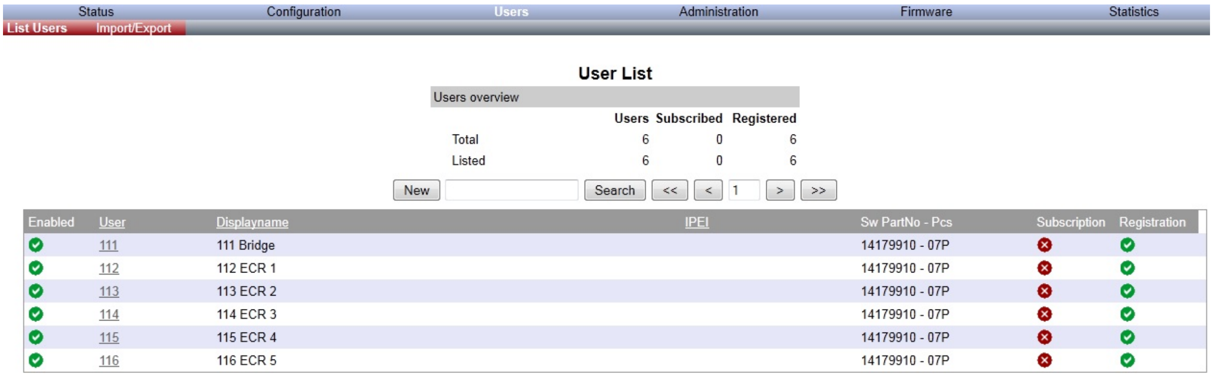


User 111

DECT	
IPEI	
Access code	
Standby text	111 Bridge
SIP	
Username / Extension *	111
Domain	
Displayname	111 Bridge
Authentication user	
Authentication password	
Disabled	□
Features	
Call forward unconditional	

*) Required field

After registering the handsets, the User List on the DECT server may look something like this:



User List

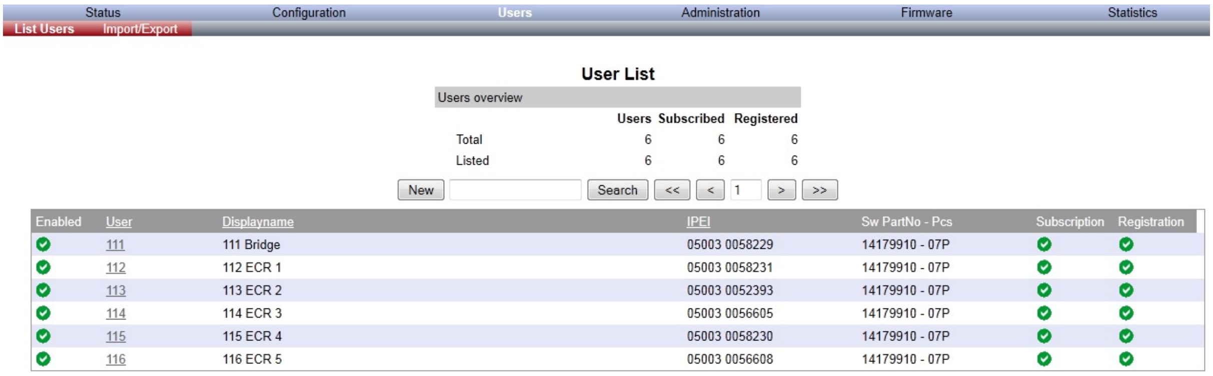
Users overview	Users	Subscribed	Registered
Total	6	0	6
Listed	6	0	6

Enabled	User	Displayname	IPEI	Sw PartNo - Pcs	Subscription	Registration
✓	111	111 Bridge		14179910 - 07P	✗	✓
✓	112	112 ECR 1		14179910 - 07P	✗	✓
✓	113	113 ECR 2		14179910 - 07P	✗	✓
✓	114	114 ECR 3		14179910 - 07P	✗	✓
✓	115	115 ECR 4		14179910 - 07P	✗	✓
✓	116	116 ECR 5		14179910 - 07P	✗	✓

To subscribe the handset to the system:

1. Turn on the handset
2. Press **Menu**
3. Scroll to **Settings** and press **Select**
4. Scroll to **Advanced** and press **Select**
5. Scroll to **Login** and press **Select**
6. Scroll to **Create login** and press **Select**
7. When the handset's ARI number appears, press **Select**
8. Press **OK** when asked for the AC (Authentication Code)
   - AC is normally not required
   - **Connecting...** is displayed as the handset acquires the user ID from the user list
9. When **Connecting...OK** is displayed, press **OK**
10. Press the Back button to return to the main page to check that the handset is now subscribed to the system

The **List Users** page on the DECT server should now automatically display the IPEI number of the subscribed handset:



User List

Users overview	Users	Subscribed	Registered
Total	6	6	6
Listed	6	6	6

Enabled	User	Displayname	IPEI	Sw PartNo - Pcs	Subscription	Registration
✓	111	111 Bridge	05003 0058229	14179910 - 07P	✓	✓
✓	112	112 ECR 1	05003 0058231	14179910 - 07P	✓	✓
✓	113	113 ECR 2	05003 0052393	14179910 - 07P	✓	✓
✓	114	114 ECR 3	05003 0056605	14179910 - 07P	✓	✓
✓	115	115 ECR 4	05003 0058230	14179910 - 07P	✓	✓
✓	116	116 ECR 5	05003 0056608	14179910 - 07P	✓	✓

10.2.4 Subscribing an Office Handset

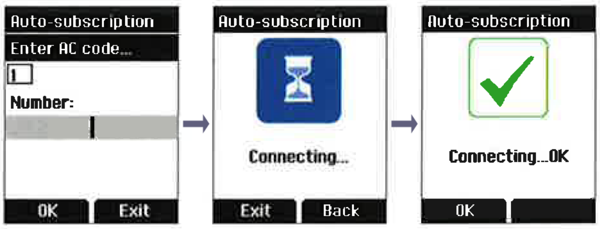
Before starting the subscription process, register the handset in the IP DECT server without the IPEI number as for the Rough handset above.

The **Auto-subcription** feature is used to subscribe an Office Handset. Some systems may require an Authentication Code (AC).

To subscribe the handset to the system:

1. Turn on the handset

2. Press **OK** to start Auto-subscription
   - **Connecting...** will be displayed



3. When **Connecting...OK** is displayed, press **OK**

The handset is now subscribed to the system and the **List Users** page on the DECT server should now automatically display the IPEI number of the subscribed handset.

10.2.4.1 Subscribing Office Handset to Different Systems

The handset can be subscribed (connected) to a maximum of 10 different systems.

☞ *To be able to log on to a system, subscription to the system must be established.*

Changing to another System Automatically Using Auto Login A

Auto Login A should only be used when systems are separate, with no overlaps.

☞ *To activate Auto login, your handset must be subscribed to at least two systems.*

To change to another system automatically:

1. Press **Menu** to enter the main menu.
2. Scroll to **Settings** and press **Select**.
3. Scroll to **Advanced** and press **Select**.
4. Scroll to **Login** and press **Select**.
5. Scroll to **Auto login** and press **Select**.
6. If **Off** is already set, press **Change** to select **On**.
7. Press **R** to return to standby mode.
   - The handset automatically selects a system.
   - The selected system is marked with an **A**.

Changing to another System Manually

To change to another system manually:

1. Press **Menu** to enter the main menu.
2. Scroll to **Settings** and press **Select**.
3. Scroll to **Advanced** and press **Select**.
4. Scroll to **Login** and press **Select**.
5. Scroll to **Select login** and press **Select**.
6. Scroll to the desired login and press **Select**.

11 Handset Management

This section provides information about handset management such as viewing handset configuration, deregistering handsets and changing user configurations using the web-based user interface. It also provides information about unsubscribing handsets, exporting/restoring/importing handset registration data and handset adjustment.

This section includes information about:

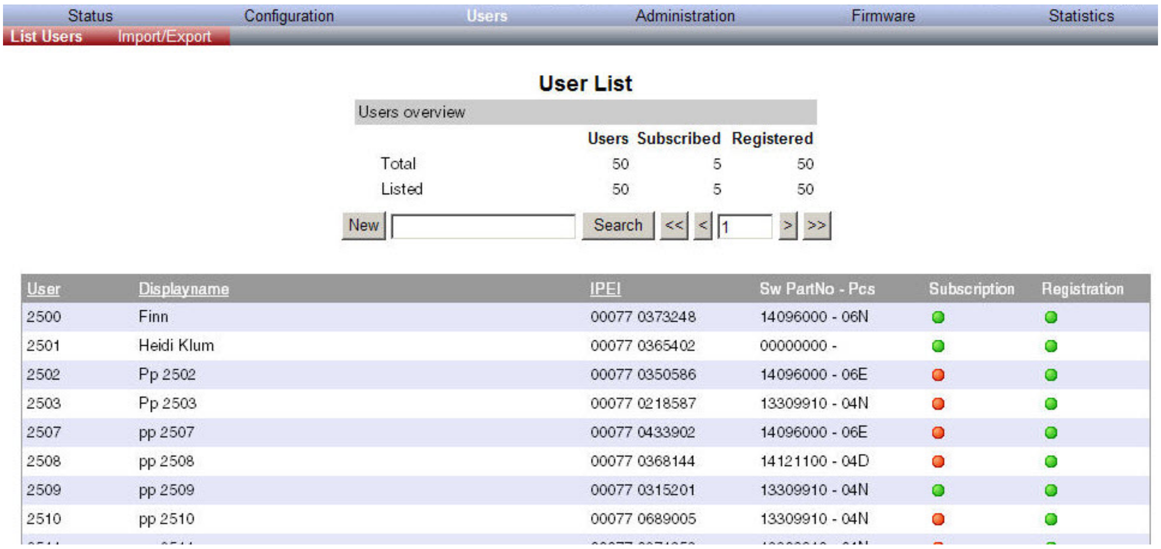
- “Viewing Handset/User Configuration”
- “Searching for Handset/User Information”
- “Unsubscribing Handsets”
- “Deleting Handsets from the List (Deregistering)”
- “Changing User Configurations”
- “Exporting Handset Registration Data”
- “Restoring Handset Registration Data”
- “Importing Handset Registration Data - CSV Format”

11.1 Viewing Handset/User Configuration

Through the web-based user interface, it is possible to view all the user configurations of the wireless system.

To view user configuration:

- Click **Users**, and then click **List Users**.



User List

Users overview

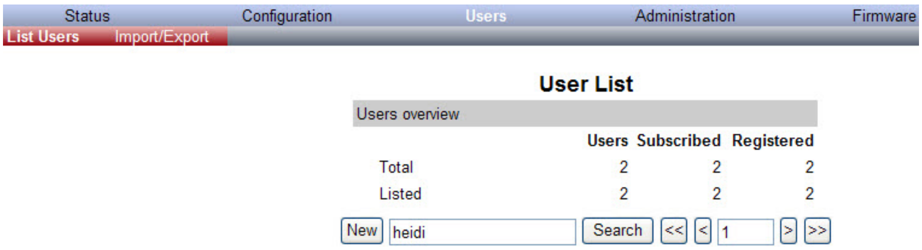
	Users	Subscribed	Registered
Total	50	5	50
Listed	50	5	50

User	Displayname	IPEI	Sw PartNo - Pcs	Subscription	Registration
2500	Finn	00077 0373248	14096000 - 06N	🟢	🟢
2501	Heidi Klum	00077 0365402	00000000 -	🟢	🟢
2502	Pp 2502	00077 0350586	14096000 - 06E	🔴	🟢
2503	Pp 2503	00077 0218587	13309910 - 04N	🔴	🟢
2507	pp 2507	00077 0433902	14096000 - 06E	🔴	🟢
2508	pp 2508	00077 0368144	14121100 - 04D	🔴	🟢
2509	pp 2509	00077 0315201	13309910 - 04N	🟢	🟢
2510	pp 2510	00077 0689005	13309910 - 04N	🔴	🟢

11.2 Searching for Handset/User Information

Through the web-based user interface, it is possible to search for a registered handset/user in the system.

1. Click **Users**, and then click **List Users**.
2. In the **Search** field, type the beginning of a user name, display name or IPEI number to search for in the text field, and then click **Search**.



User List

Users overview

	Users	Subscribed	Registered
Total	2	2	2
Listed	2	2	2

heidi

1

11.3 Unsubscribing Handsets

☞ *Removing a subscription from the system requires a password. The default password is 0000.*

11.3.1 EX Handset

To unsubscribe a handset:

1. Press **MENU**.
2. Press **<** and go to **MENU LOGIN**.
3. Press ✓ .
4. Press **<** and go to **SUBSCRIPTION REMOVE**.
5. Press ✓ .
6. Enter password: **0000**
7. Press ✓ .
8. If the handset is subscribed to more than one system, select the system ARI in question.

The handset is now unsubscribed.

11.3.2 Rough/Office Handset

Logins can be removed from the system in use and from the 9 other systems (if connected).

☞ *Removing a login requires a password. The default password is **0000**.*

To remove a Login:

1. Press **Menu** to enter the main menu.
2. Scroll to **Settings** and press **Select**.
3. Scroll to **Advanced** and press **Select**.
4. Scroll to **Login** and press **Select**.
5. Scroll to **Remove login** and press **Select**.
6. Scroll to the desired login and press **Select**.
7. Enter the **password** and press **Ok**.

☞ *If the system in use is removed, it is necessary to select one of the remaining systems or to subscribe to a new one.*

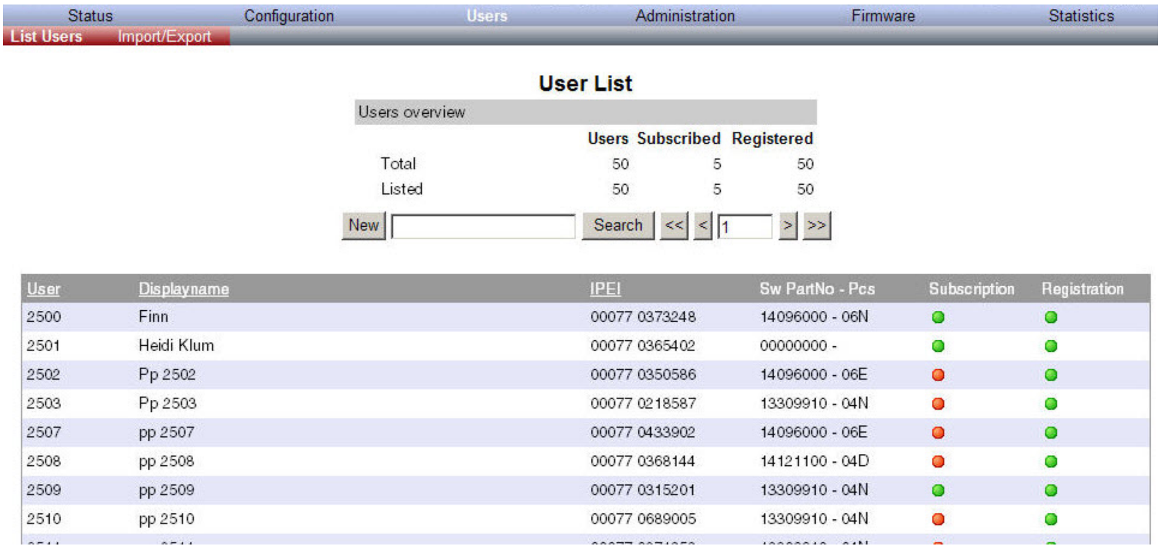
11.4 Deleting Users/Handsets from the List (Deregistering)

You can deregister handsets from the Server 6000.

This is necessary when:

- you have to replace the user/handset due to loss or breakage.
- you want to assign the handset to a user with a different phone number.

1. Click **Users**, and then click **List Users**.



User List

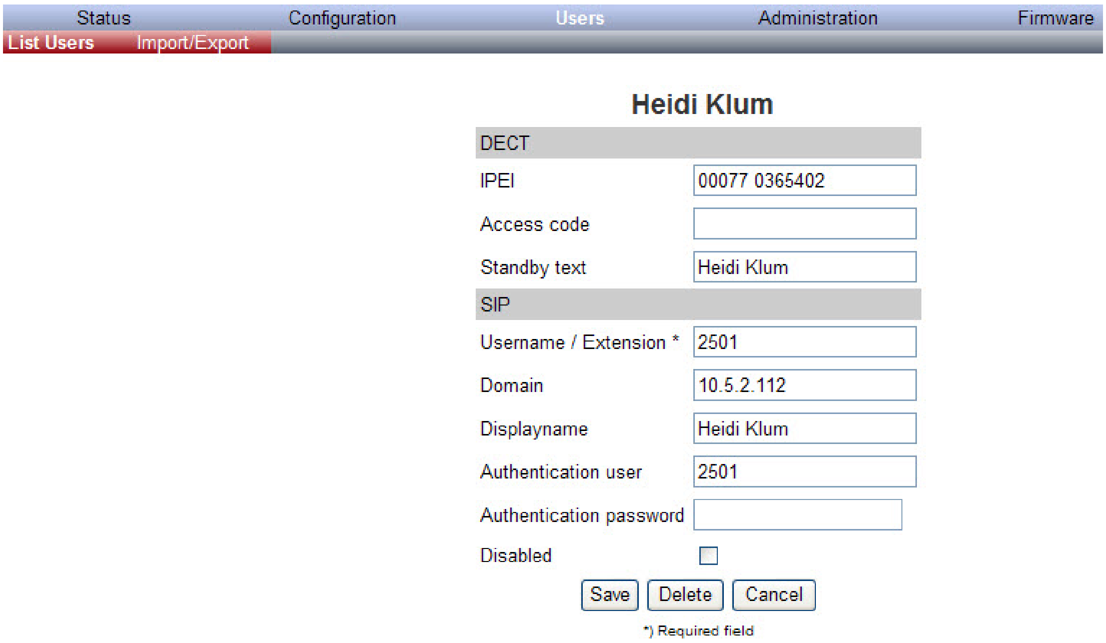
Users overview

	Users	Subscribed	Registered
Total	50	5	50
Listed	50	5	50

User	Displayname	IPEI	Sw PartNo - Pcs	Subscription	Registration
2500	Finn	00077 0373248	14096000 - 06N	🟢	🟢
2501	Heidi Klum	00077 0365402	00000000 -	🟢	🟢
2502	Pp 2502	00077 0350586	14096000 - 06E	🔴	🟢
2503	Pp 2503	00077 0218587	13309910 - 04N	🔴	🟢
2507	pp 2507	00077 0433902	14096000 - 06E	🔴	🟢
2508	pp 2508	00077 0368144	14121100 - 04D	🔴	🟢
2509	pp 2509	00077 0315201	13309910 - 04N	🟢	🟢
2510	pp 2510	00077 0689005	13309910 - 04N	🔴	🟢

2. Select the user/handset you wish to delete by clicking on the user information, for example, user 2501 “Heidi Klum”.

The following page is displayed:



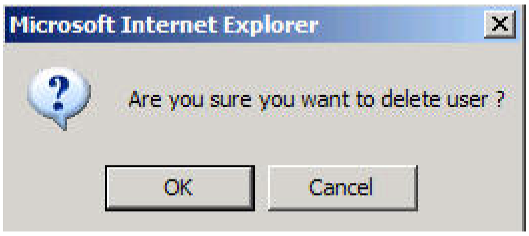
Heidi Klum

DECT	
IPEI	00077 0365402
Access code	
Standby text	Heidi Klum
SIP	
Username / Extension *	2501
Domain	10.5.2.112
Displayname	Heidi Klum
Authentication user	2501
Authentication password	
Disabled	□

*) Required field

3. Click **Delete**.

A warning box will appear.



Microsoft Internet Explorer

Are you sure you want to delete user ?

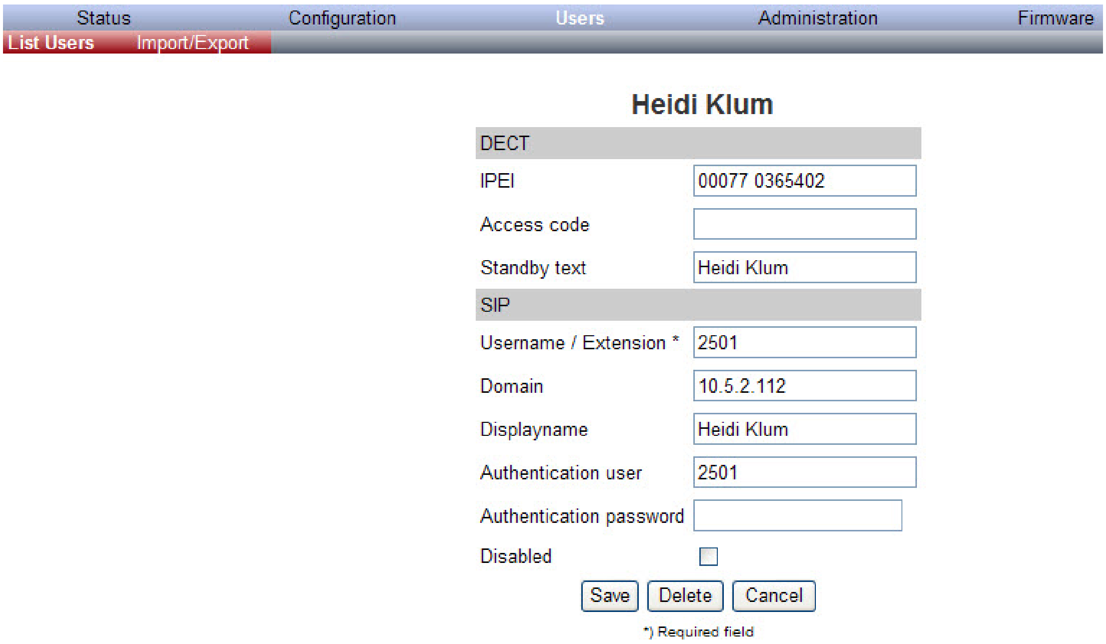
4. Click **OK** to confirm.

The user/handset will now be deregistered from the system.

11.5 Changing User Configurations

You can change user configurations, such as the AC (authentication code) using the web-based user interface.

1. Click **Users**, and then click **List Users**.
2. Select the handset you wish to change by clicking on the user information, for example, user 2501 “Heidi Klum”.



Heidi Klum

DECT	
IPEI	00077 0365402
Access code	
Standby text	Heidi Klum
SIP	
Username / Extension *	2501
Domain	10.5.2.112
Displayname	Heidi Klum
Authentication user	2501
Authentication password	
Disabled	□

*) Required field

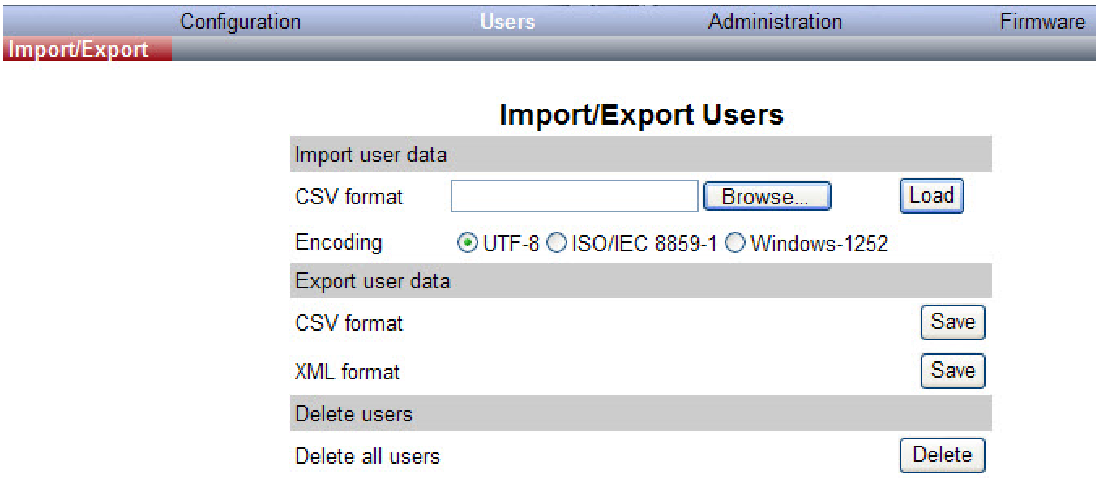
3. Change the settings accordingly, and then click **Save**.

The new settings will now be enabled in the system.

11.6 Exporting Handset Registration Data

You can export handset registration data using the web-based user interface. It is possible to export a user database with subscriptions and without subscriptions (configuration data only).

- Click **Users**, and then click **Import/Export**.



Import/Export Users

Import user data

CSV format

Encoding ● UTF-8 ○ ISO/IEC 8859-1 ○ Windows-1252

Export user data

CSV format

XML format

Delete users

Delete all users

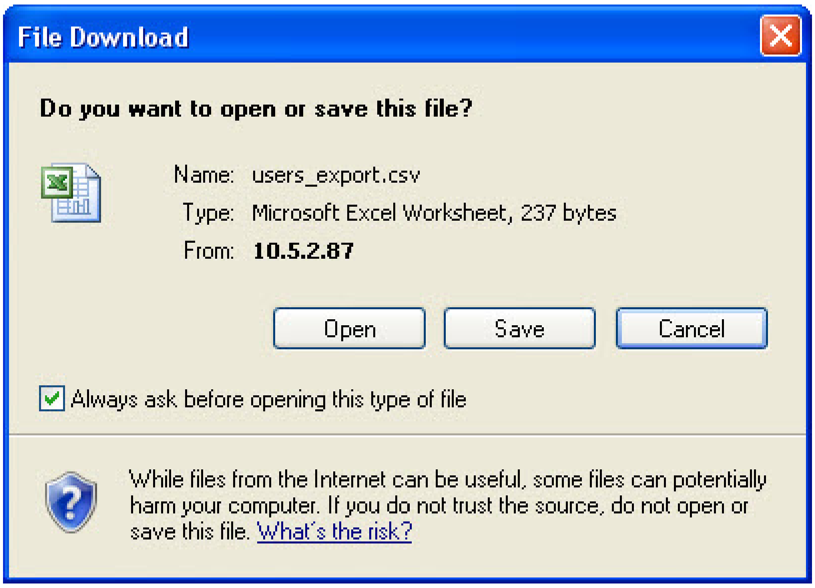
Under **Export User Data** do one of the following:

- export user data in CSV format
- export user data in XML format, click **Save** for **XML format**.

To export user data in CSV format:

1. Click **Save** for **CSV format**.

A File Download dialog box appears.



Do you want to open or save this file?

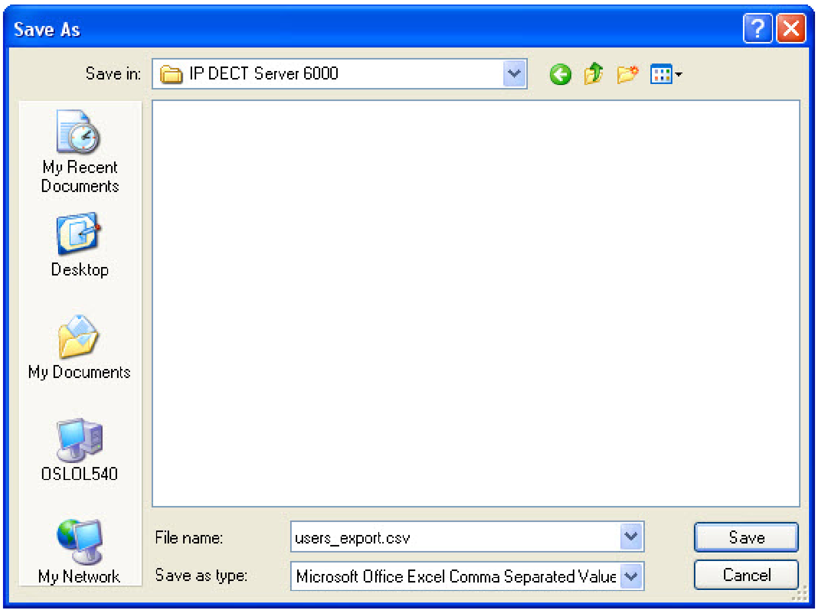
Name: users_export.csv
Type: Microsoft Excel Worksheet, 237 bytes
From: **10.5.2.87**

☑ Always ask before opening this type of file

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

2. Click **Save** to confirm.

A Save As dialog box appears.



Save As

Save in: IP DECT Server 6000

File name: users_export.csv

Save as type: Microsoft Office Excel Comma Separated Value

3. Select the folder and the name the file should be saved as, and then click **Save**.

11.7 Importing Handset Registration Data - CSV Format

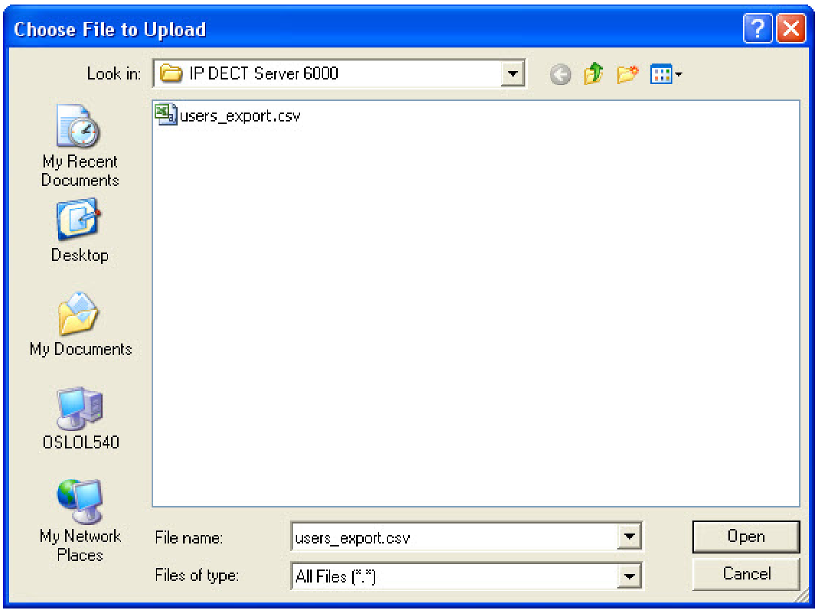
You can import handset registration data in CSV format. To be able to import the data correctly, you must create a file containing the following information and punctuation:

#IPEI,access code,standby text,username,domain,displayname, authenticate user,authenticate password,local number

☞ *If you want to leave out some of the information, e.g. standby text, you must retain the commas, e.g.:* **#IPEI,access code,,username,domain,displayname, authenticate user,authenticate password,local number**.

1. Click **Users**, and then click **Import/Export**.
   - Under **Import user data**, you have a choice of different Encoding types such as UTF-8, ISO/IEC 8859-1, and Windows-1252.
2. Click **Browse** to find the CSV file with handset registration data.

A **Choose File to Upload** dialog box appears.



Choose File to Upload

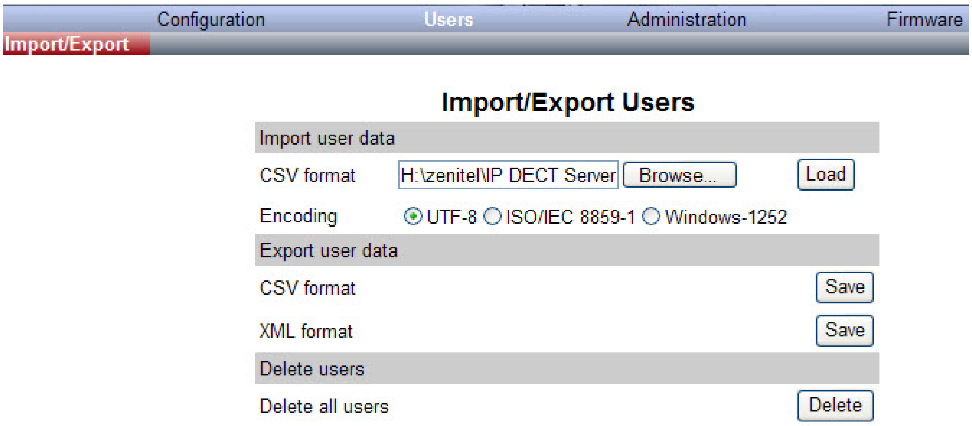
Look in: IP DECT Server 6000

users_export.csv

File name: users_export.csv

Files of type: All Files (*.*)

3. Select the desired file, and then click **Open**.



Import/Export Users

Import user data

CSV format: H:\zenitel\IP DECT Server

Encoding: ● UTF-8 ○ ISO/IEC 8859-1 ○ Windows-1252

Export user data

CSV format

XML format

Delete users

Delete all users

4. Click **Load**.
5. Click **OK**.

☞ *It is not possible to import handset registration data that is already registered in the system.*

12 System Management

This section provides you with information about system management using the web-based user interface of the IP DECT Server 6000.

Through the web-based user interface of the Server 6000, it is possible to define and view different settings of the system, read statistics, make a backup of the configuration file, update system software, and reset the system.

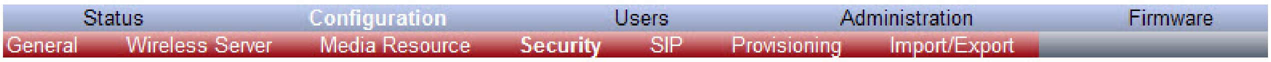
12.1 IP DECT Server 6000

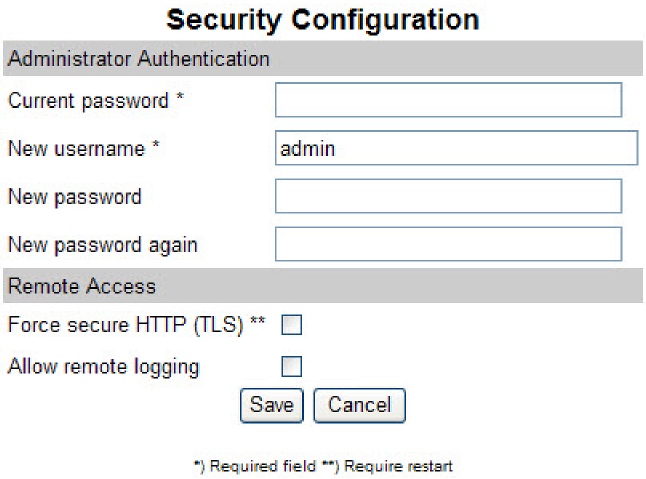
12.1.1 Changing System User Name and Password

From the user interface it is possible to change the user name and password for the system.

Log into the user interface of the Server 6000.

1. Click **Configuration**, and then click **Security**.





Security Configuration

Administrator Authentication

Current password *	
New username *	admin
New password	
New password again	

Remote Access

Force secure HTTP (TLS) **	□
Allow remote logging	□

*) Required field **) Require restart

2. In the **Current password** field, type the current password.
3. In the **New username** field, type a new user name.
4. In the **New password** field, type a new password
5. In the **New password again** field, type the new password again to confirm it.
6. Uncheck the **Force secure HTTP (TLS)** checkbox.
7. Uncheck the **Allow remote logging** checkbox.
8. Click **Save** to change the user name and password.

12.1.2 Reading System Information

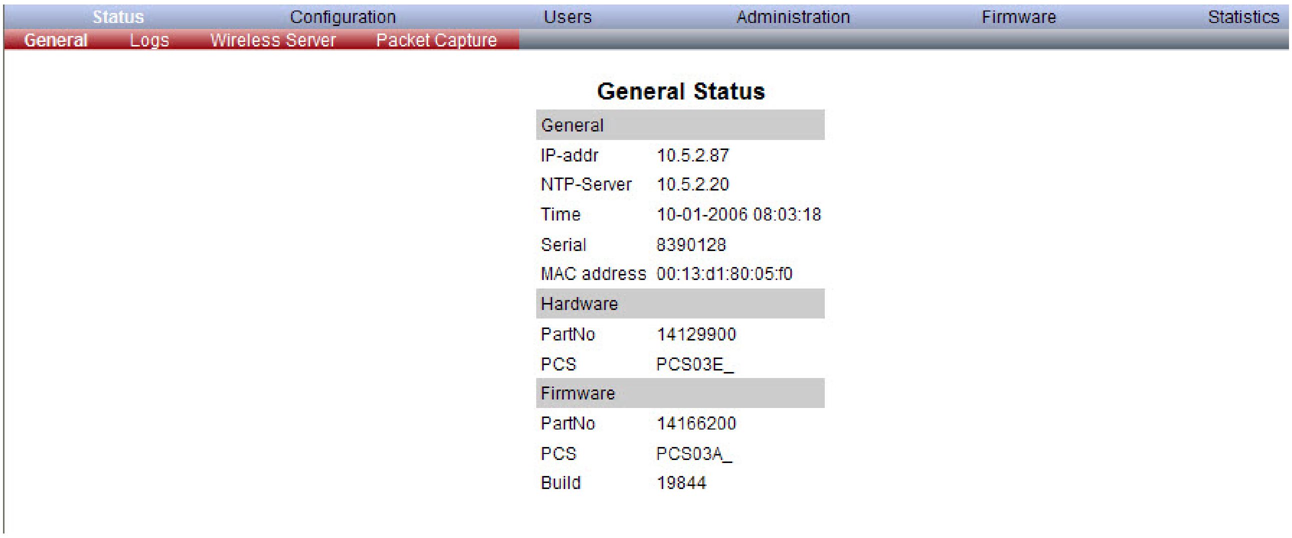
Under **Status**, it is possible to get general information about hardware version, firmware and message logging. This information is useful for troubleshooting. The web-based user interface of the wireless server provides an overview of the solution, e.g. how the base stations are functioning.

12.1.2.1 General Status Information

This page provides general system information such as hardware, firmware and OS Status information.

Log into the web interface of the Server 6000.

- Click **Status**, and then click **General**.



General Status

General	
IP-addr	10.5.2.87
NTP-Server	10.5.2.20
Time	10-01-2006 08:03:18
Serial	8390128
MAC address	00:13:d1:80:05:f0
Hardware	
PartNo	14129900
PCS	PCS03E_
Firmware	
PartNo	14166200
PCS	PCS03A_
Build	19844

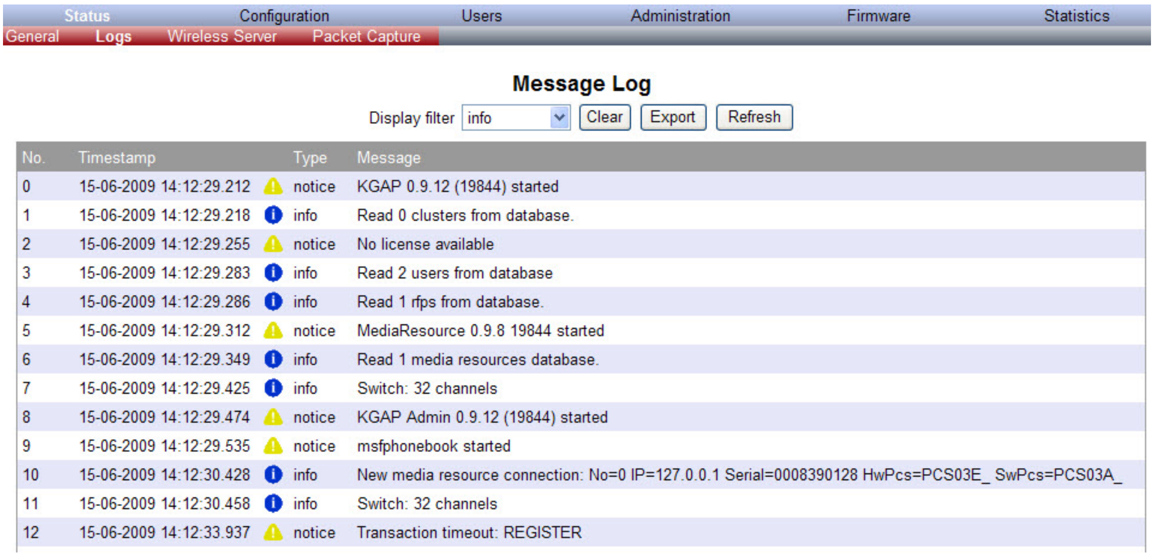
On the **Status/General** page you can read information about:

- firmware and hardware being used
- MAC address (physical number) of the system
- NTP Server from which the system receives its time information
- time information - (if a time server is valid)

12.1.2.2 Logs Information

This page provides logs information such as base station connections and different types of status.

1. Click **Status**, and then click **Logs**.



Message Log

Display filter: info

No.	Timestamp		Type	Message
0	15-06-2009 14:12:29.212	⚠	notice	KGAP 0.9.12 (19844) started
1	15-06-2009 14:12:29.218	ⓘ	info	Read 0 clusters from database.
2	15-06-2009 14:12:29.255	⚠	notice	No license available
3	15-06-2009 14:12:29.283	ⓘ	info	Read 2 users from database
4	15-06-2009 14:12:29.286	ⓘ	info	Read 1 rfps from database.
5	15-06-2009 14:12:29.312	⚠	notice	MediaResource 0.9.8 19844 started
6	15-06-2009 14:12:29.349	ⓘ	info	Read 1 media resources database.
7	15-06-2009 14:12:29.425	ⓘ	info	Switch: 32 channels
8	15-06-2009 14:12:29.474	⚠	notice	KGAP Admin 0.9.12 (19844) started
9	15-06-2009 14:12:29.535	⚠	notice	msfphonebook started
10	15-06-2009 14:12:30.428	ⓘ	info	New media resource connection: No=0 IP=127.0.0.1 Serial=0008390128 HwPcs=PCS03E_ SwPcs=PCS03A_
11	15-06-2009 14:12:30.458	ⓘ	info	Switch: 32 channels
12	15-06-2009 14:12:33.937	⚠	notice	Transaction timeout: REGISTER

2. From the **Display filter** dropdown list, select **emergency**, **critical**,

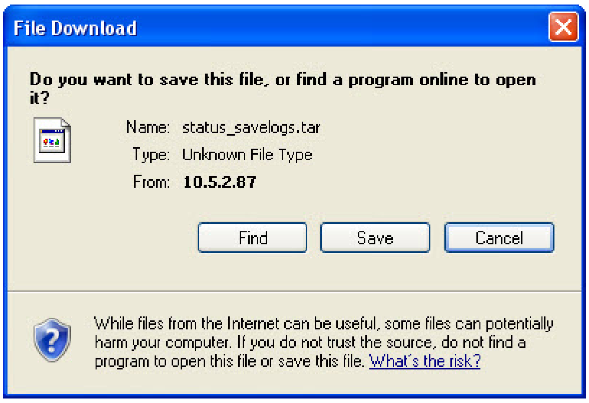
error, **warning**, **notice**, **info**, or **debug** depending on the logs you want to view.

The meaning of the different types of status are:

- emergency - errors causing the system to malfunction for all calls
- critical - events that do not occur under normal operation, causing minor malfunction
- error - events that do not occur under normal operation, causing minor malfunction
- warning - events that do not occur under normal operation, may cause malfunction
- notice/info - events that occur under normal operation, relevant to an administrator
- debug - events that occur under normal operation, may be relevant to an administrator

3. Click **Export** if you want to save the logs in a file.

A **File Download** dialog box appears.

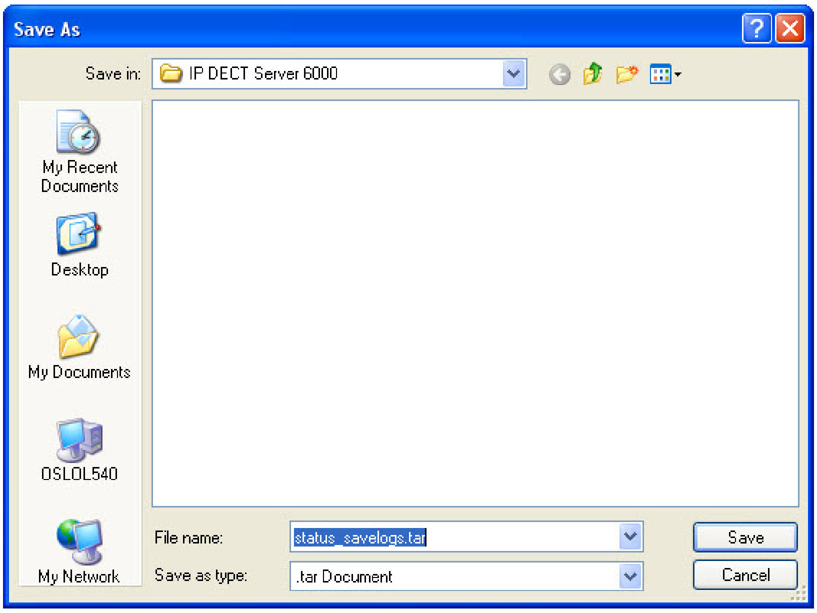


Do you want to save this file, or find a program online to open it?

Name: status_savelogs.tar
Type: Unknown File Type
From: 10.5.2.87

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

4. Click **Save**.
A **Save As** dialog box appears.



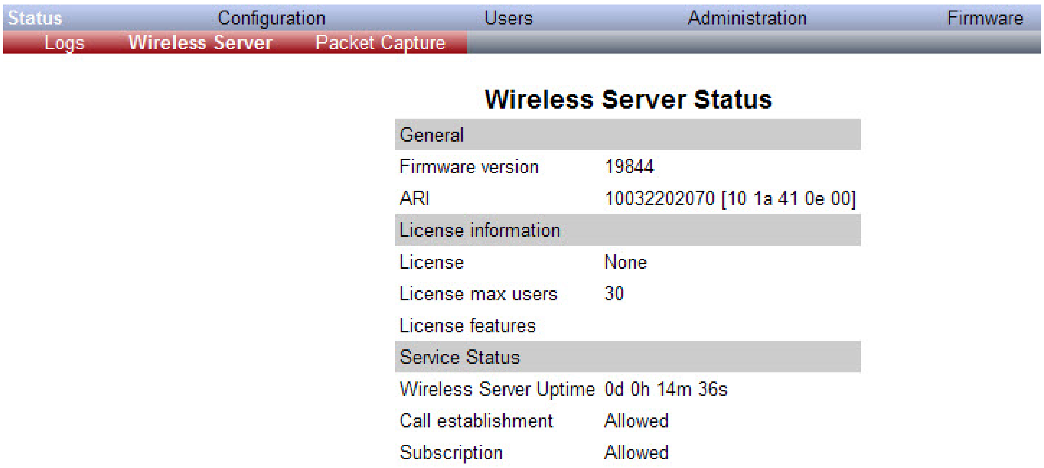
File name: status_savelogs.tar
Save as type: .tar Document

5. Indicate the folder and the name the file should be saved as, and then click **Save**.
The log files can now be sent to authorized technicians for further support and troubleshooting.

12.1.2.3 Wireless Server Information

This page provides information about the firmware version, ARI code, license information, and service status of the Server 6000.

- Click **Status**, and then click **Wireless Server**.



Wireless Server Status

General	
Firmware version	19844
ARI	10032202070 [10 1a 41 0e 00]
License information	
License	None
License max users	30
License features	
Service Status	
Wireless Server Uptime	0d 0h 14m 36s
Call establishment	Allowed
Subscription	Allowed

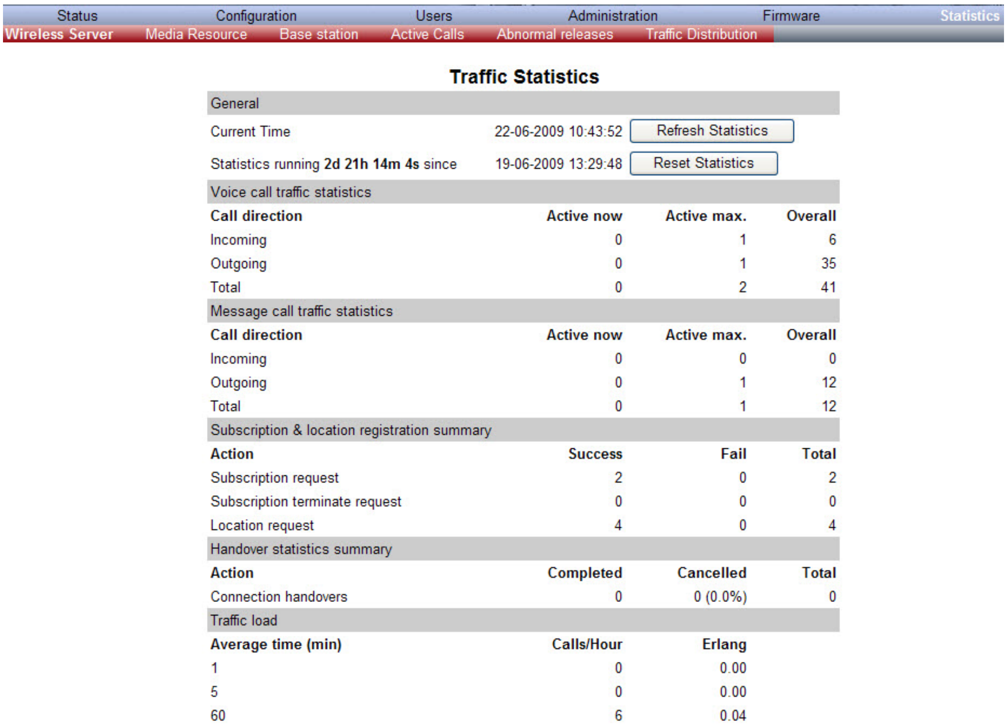
12.1.3 Reading Statistics

Under **Statistics**, it is possible to view statistic information about the Server 6000 such as base stations, calls, handovers and abnormal releases in the system. From this, you can get an overview of how the system is running.

12.1.3.1 Wireless Server

This page is useful for getting information about traffic on the Server 6000 such as voice call traffic and message call traffic and it provides a summary of subscription and handover statistics. It also provides information about the traffic load (Erlang) of the installation.

- Click **Statistics**, and then click **Wireless Server**.

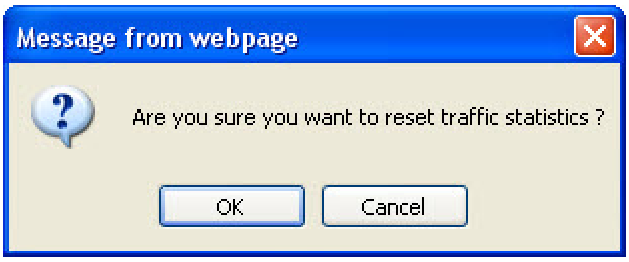


Traffic Statistics

General			
Current Time	22-06-2009 10:43:52	Refresh Statistics	
Statistics running **2d 21h 14m 4s** since	19-06-2009 13:29:48	Reset Statistics	
Voice call traffic statistics			
Call direction	**Active now**	**Active max.**	**Overall**
Incoming	0	1	6
Outgoing	0	1	35
Total	0	2	41
Message call traffic statistics			
Call direction	**Active now**	**Active max.**	**Overall**
Incoming	0	0	0
Outgoing	0	1	12
Total	0	1	12
Subscription & location registration summary			
Action	**Success**	**Fail**	**Total**
Subscription request	2	0	2
Subscription terminate request	0	0	0
Location request	4	0	4
Handover statistics summary			
Action	**Completed**	**Cancelled**	**Total**
Connection handovers	0	0 (0.0%)	0
Traffic load			
Average time (min)	**Calls/Hour**	**Erlang**	
1	0	0.00	
5	0	0.00	
60	6	0.04	

If you want to delete all statistic traffic information:

1. Click **Reset Statistics**
   - A warning message appears.



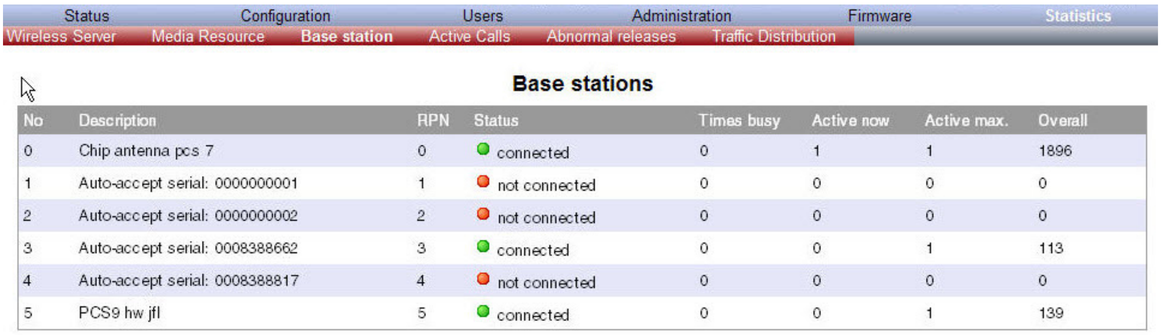
Are you sure you want to reset traffic statistics ?

2. Click **OK** to confirm.

12.1.3.2 Base Station

This page provides statistic information about the base station.

- Click **Statistics**, and then click **Base Station**.



Base stations

No	Description	RPN	Status	Times busy	Active now	Active max.	Overall
0	Chip antenna pcs 7	0	● connected	0	1	1	1896
1	Auto-accept serial: 0000000001	1	● not connected	0	0	0	0
2	Auto-accept serial: 0000000002	2	● not connected	0	0	0	0
3	Auto-accept serial: 0008388662	3	● connected	0	0	1	113
4	Auto-accept serial: 0008388817	4	● not connected	0	0	0	0
5	PCS9 hw jfl	5	● connected	0	0	1	139

12.1.3.3 Active Calls

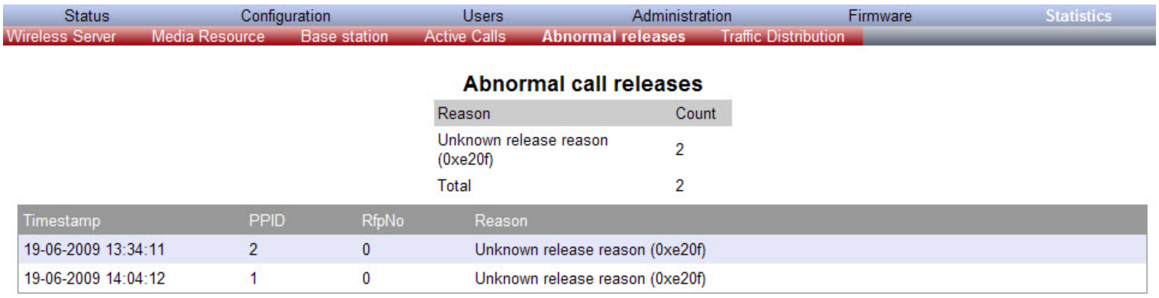
This page provides statistic information about active calls in the Server 6000 installation.

- Click **Statistics**, and then click **Active Calls**.

12.1.3.4 Abnormal Releases

This page provides statistic information about abnormal call releases in an Server 6000 installation.

- Click **Statistics**, and then click **Abnormal Releases**.



Abnormal call releases

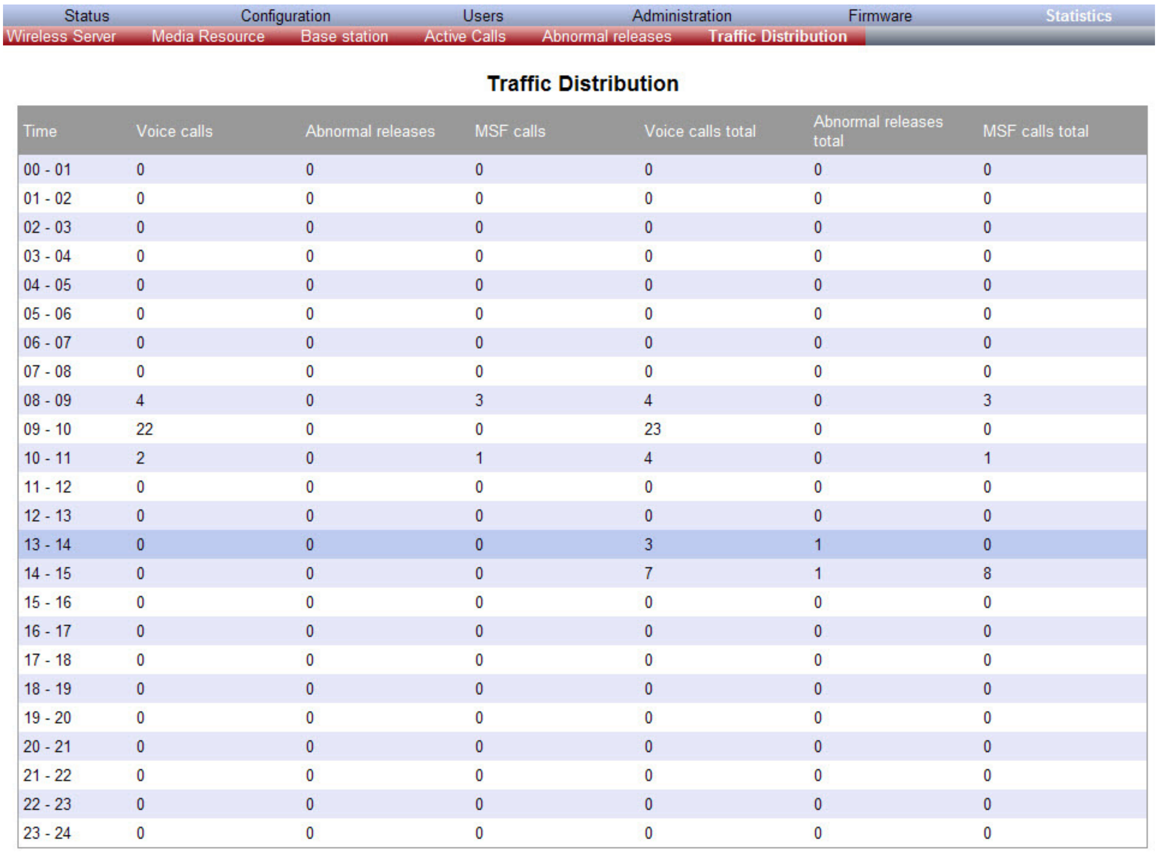
Reason	Count
Unknown release reason (0xe20f)	2
Total	2

Timestamp	PPID	RfpNo	Reason
19-06-2009 13:34:11	2	0	Unknown release reason (0xe20f)
19-06-2009 14:04:12	1	0	Unknown release reason (0xe20f)

12.1.3.5 Traffic Distribution

This page provides statistic information about traffic distribution during the last 24 hours in an Server 6000 installation.

- Click **Statistics**, and then click **Traffic Distribution**.



Traffic Distribution

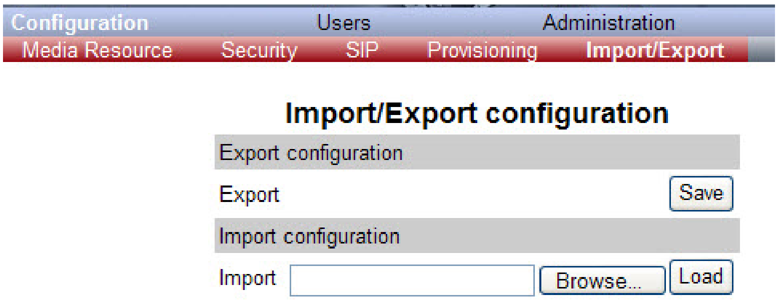
Time	Voice calls	Abnormal releases	MSF calls	Voice calls total	Abnormal releases total	MSF calls total
00 - 01	0	0	0	0	0	0
01 - 02	0	0	0	0	0	0
02 - 03	0	0	0	0	0	0
03 - 04	0	0	0	0	0	0
04 - 05	0	0	0	0	0	0
05 - 06	0	0	0	0	0	0
06 - 07	0	0	0	0	0	0
07 - 08	0	0	0	0	0	0
08 - 09	4	0	3	4	0	3
09 - 10	22	0	0	23	0	0
10 - 11	2	0	1	4	0	1
11 - 12	0	0	0	0	0	0
12 - 13	0	0	0	0	0	0
13 - 14	0	0	0	3	1	0
14 - 15	0	0	0	7	1	8
15 - 16	0	0	0	0	0	0
16 - 17	0	0	0	0	0	0
17 - 18	0	0	0	0	0	0
18 - 19	0	0	0	0	0	0
19 - 20	0	0	0	0	0	0
20 - 21	0	0	0	0	0	0
21 - 22	0	0	0	0	0	0
22 - 23	0	0	0	0	0	0
23 - 24	0	0	0	0	0	0

12.1.4 Exporting / Backing Up the Configuration File

This section provides information about exporting and saving the configuration data of the Server 6000, registration and subscription data of the handset and system information.

When you save the configuration data, you are able later to get an overview of the Wireless Server which is useful for troubleshooting.

1. Click **Configuration**, and then click **Import/Export**.

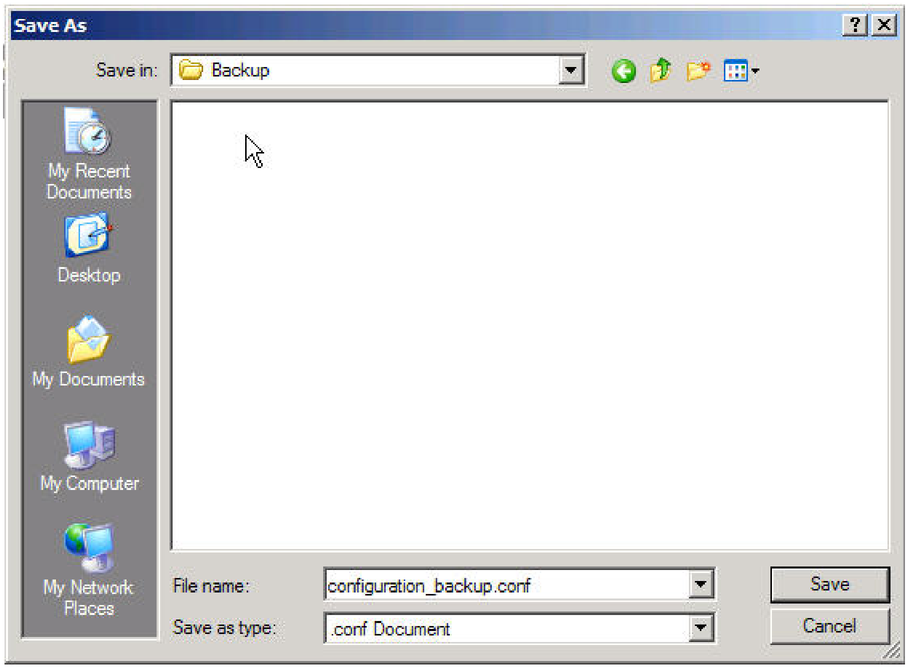


2. Click **Save** to export the configuration file.

A **File Download** dialog box appears.

3. Click **Save** to save the file to a specific folder.

A **Save As** dialog box appears.

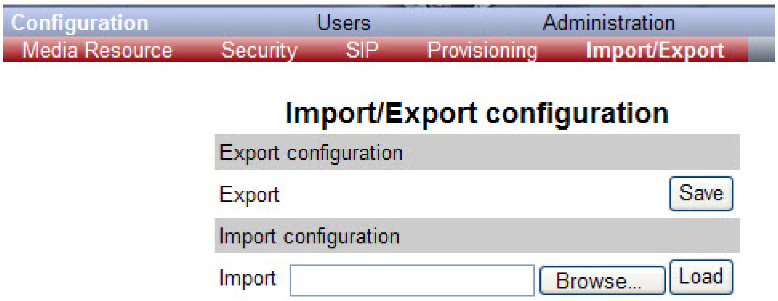


4. Indicate in which folder and under what name the file should be saved, and then click **Save**.

12.1.5 Importing/Restoring the Configuration File

This section describes how to import or restore a configuration file.

1. Click **Configuration**, and then click **Import/Export**.



Import/Export configuration

Export configuration

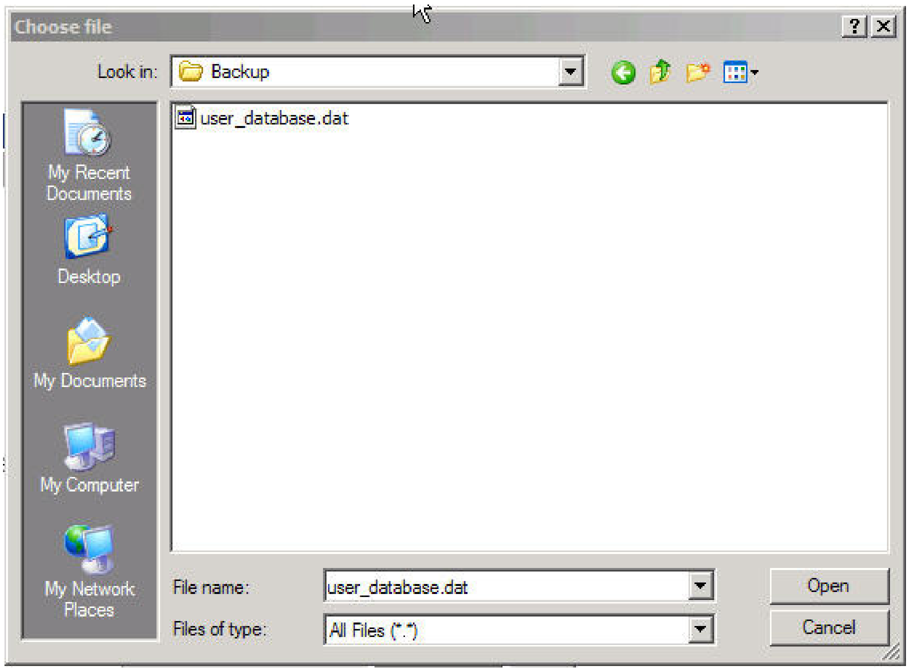
Export

Import configuration

Import

2. Click **Browse**.

A **Choose File to Upload** dialog box appears.



3. Select the desired file, and then click **Open**.
4. Click **Load**.
5. Click **OK**.

The configuration file should now be imported and restored to the system.

12.1.6 Updating the Server 6000

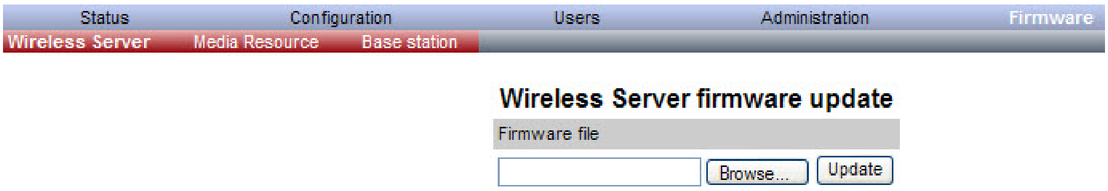
The firmware of the Server 6000 can be updated from a file that is loaded to the system.

☞ *Contact your distributor for the latest firmware.*

Updating the firmware is done through the web interface of the Server 6000.

12.1.6.1 Updating Server 6000 Firmware

1. Click **Firmware**, and then click **Wireless Server**.

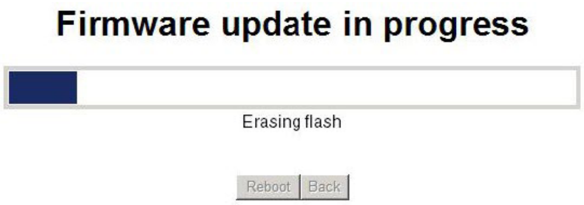


2. Click Browse.

A **Choose File to Upload** dialog box appears.

3. Select the firmware update file, and then click **Open**.
4. Click **Update**.

Wait for the system to finish updating.



Firmware update in progress

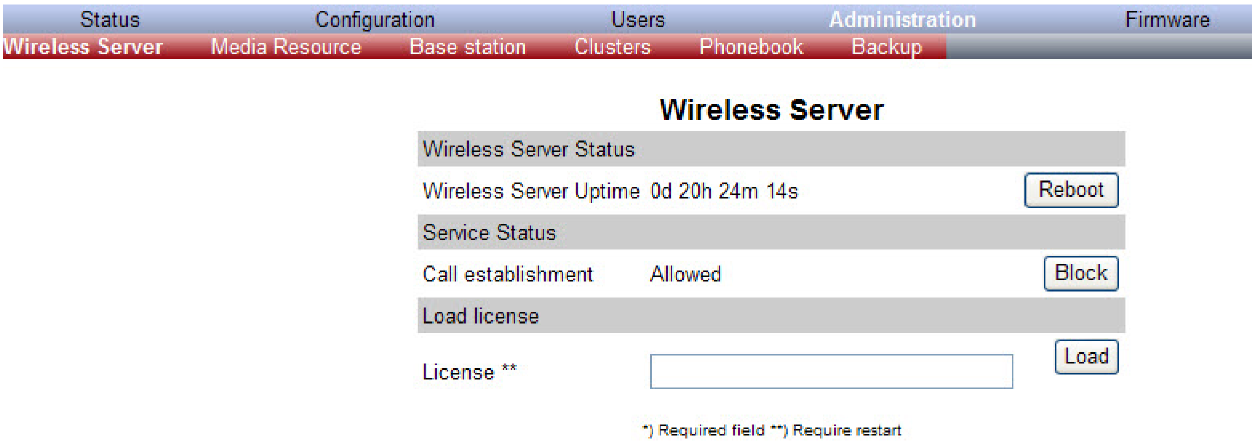
Erasing flash

✋ ***Do not cut the power during the updating process.***

5. Click **Reboot** to update the Server 6000 firmware.

Optionally, you can block new calls during a firmware update by doing the following:

1. Click **Administration**, and then click **Wireless Server**.



Wireless Server

Wireless Server Status

Wireless Server Uptime 0d 20h 24m 14s

Service Status

Call establishment Allowed

Load license

License **

*) Required field **) Require restart

2. Under **Service Status** click **Block**.

If you have blocked new calls during a firmware update, enable new calls again by doing the following:

3. Click **Allow**.

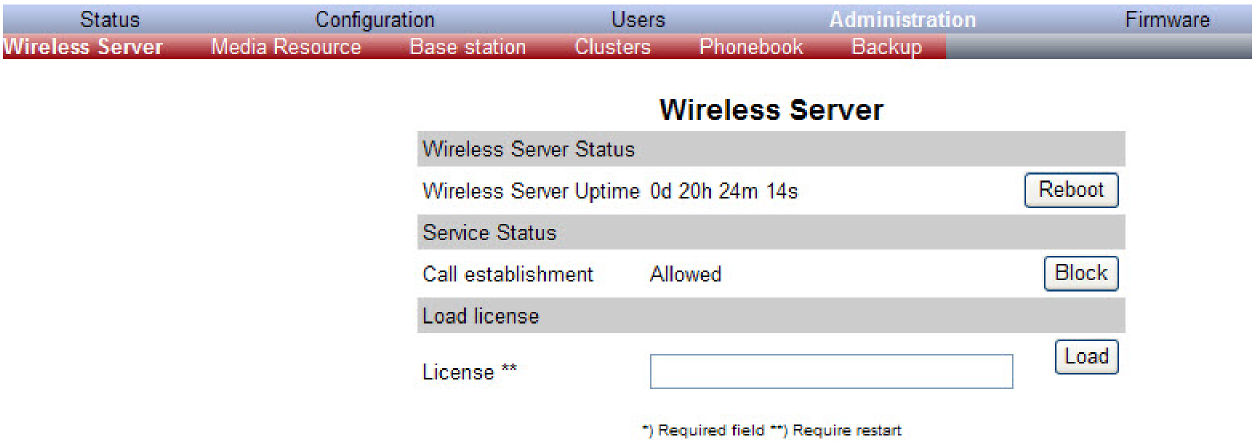
12.1.7 Rebooting/Restarting the Server 6000

Some configuration changes require a reboot in order to take effect. You must reboot the system after the following procedures:

- configuring
- uploading configuration data
- uploading firmware

When rebooting the Server 6000, all calls are terminated and the 6000 is reset.

1. Click **Administration**, and then click **Wireless Server**.



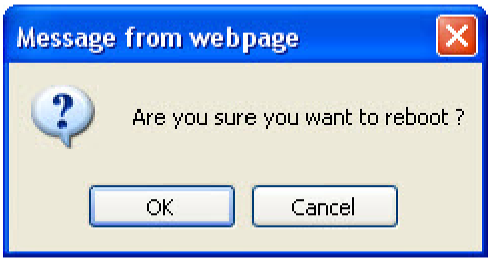
Wireless Server

Wireless Server Status	
Wireless Server Uptime	0d 20h 24m 14s
Service Status	
Call establishment	Allowed
Load license	
License **	

*) Required field **) Require restart

2. For **Wireless Server Uptime** click **Reboot**.

A warning box appears.



Message from webpage

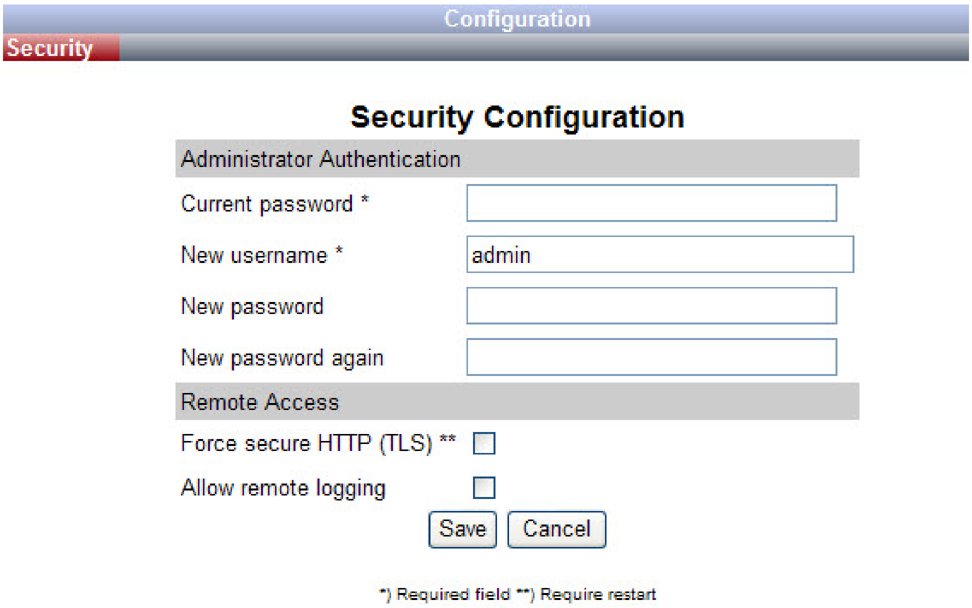
Are you sure you want to reboot ?

3. Click **OK**.

12.2 Base Station

12.2.1 Changing System User Name and Password

It is possible to change the user name and password for the system from the web interface of the Base Station.



Security Configuration

Administrator Authentication

Current password *	
New username *	admin
New password	
New password again	

Remote Access

Force secure HTTP (TLS) ** □

Allow remote logging □

*) Required field **) Require restart

1. Click **Configuration**, and then click **Security**.
2. In the **Current password** field, enter the current password.
3. In the **New username** field, enter a new username.
4. In the **New password** field, enter a new password.
5. In the **New password again** field, re-enter the new password.
6. Uncheck the **Force secure HTTP (TLS)** checkbox.
7. Uncheck the **Allow remote logging** checkbox.
8. Click **Save**.

12.2.2 Reading System Information

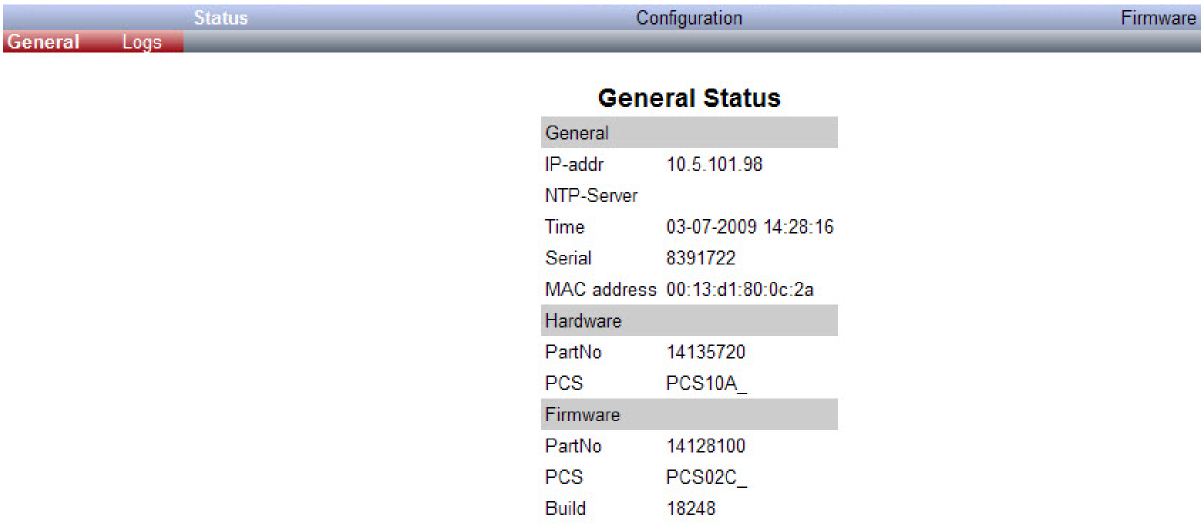
Under Status it is possible to get general information about hardware version, firmware and message logging. This information is useful in case of troubleshooting.

12.2.2.1 General Status Information

This page provides general system information such as hardware, firmware and OS Status information.

Log into the web interface of the Base Station.

- Click **Status**, and then click **General**.



General Status

General	
IP-addr	10.5.101.98
NTP-Server	
Time	03-07-2009 14:28:16
Serial	8391722
MAC address	00:13:d1:80:0c:2a
Hardware	
PartNo	14135720
PCS	PCS10A_
Firmware	
PartNo	14128100
PCS	PCS02C_
Build	18248

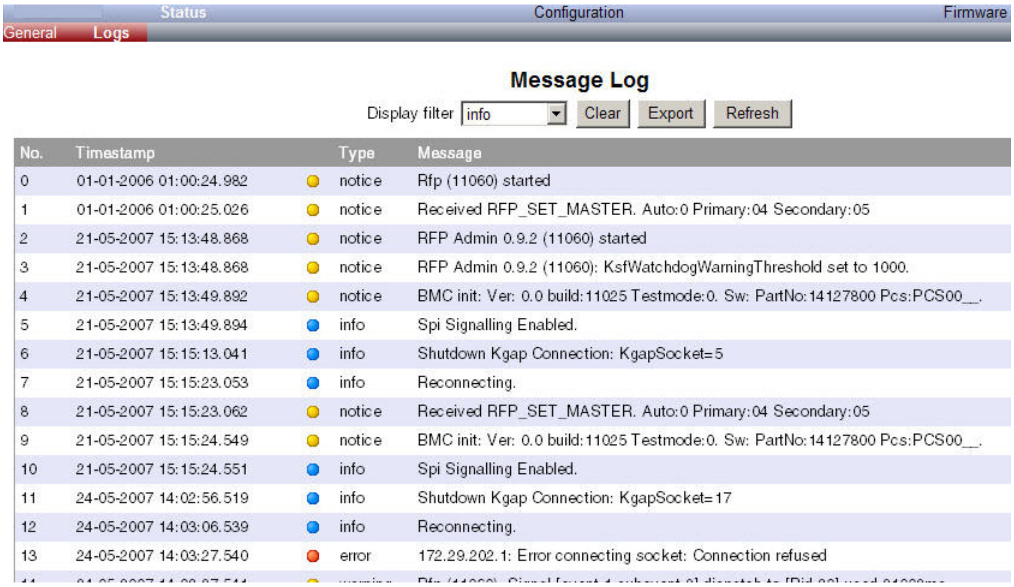
On the **Status/General** page you can read information about:

- firmware and hardware being used
- MAC address (physical number) of the system
- NTP Server from which the system receives its time information
- Time for time information - (if a time server is valid)

12.2.2.2 Logs Information

This page provides logs information such as base station connection and different types of status.

1. Click **Status**, and then click **Logs**.



Message Log

Display filter: info

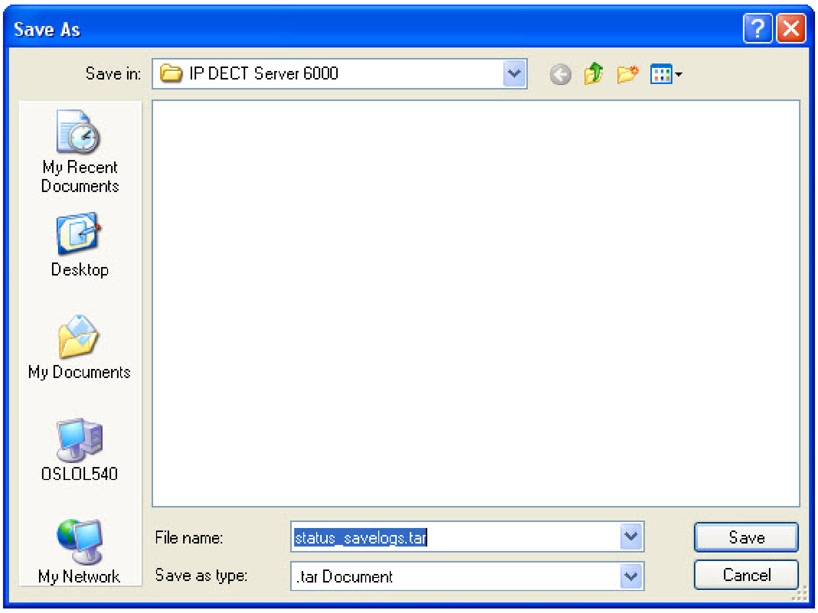
No.	Timestamp		Type	Message
0	01-01-2006 01:00:24.982	●	notice	Rfp (11060) started
1	01-01-2006 01:00:25.026	●	notice	Received RFP_SET_MASTER. Auto:0 Primary:04 Secondary:05
2	21-05-2007 15:13:48.868	●	notice	RFP Admin 0.9.2 (11060) started
3	21-05-2007 15:13:48.868	●	notice	RFP Admin 0.9.2 (11060): KsfWatchdogWarningThreshold set to 1000.
4	21-05-2007 15:13:49.892	●	notice	BMC init: Ver: 0.0 build:11025 Testmode:0. Sw: PartNo:14127800 Pcs:PCS00__.
5	21-05-2007 15:13:49.894	●	info	Spi Signalling Enabled.
6	21-05-2007 15:15:13.041	●	info	Shutdown Kgap Connection: KgapSocket=5
7	21-05-2007 15:15:23.053	●	info	Reconnecting.
8	21-05-2007 15:15:23.062	●	notice	Received RFP_SET_MASTER. Auto:0 Primary:04 Secondary:05
9	21-05-2007 15:15:24.549	●	notice	BMC init: Ver: 0.0 build:11025 Testmode:0. Sw: PartNo:14127800 Pcs:PCS00__.
10	21-05-2007 15:15:24.551	●	info	Spi Signalling Enabled.
11	24-05-2007 14:02:56.519	●	info	Shutdown Kgap Connection: KgapSocket=17
12	24-05-2007 14:03:06.539	●	info	Reconnecting.
13	24-05-2007 14:03:27.540	●	error	172.29.202.1: Error connecting socket: Connection refused

2. From the **Display filter** dropdown list, select **emergency**, **critical**, **error**, **warning**, **notice**, **info**, or **debug** depending on the logs you want to view.

The meaning of the different types of status are:

- **emergency** - errors causing the system to malfunction for all calls
- **critical** - events that do not occur under normal operation, causing minor malfunction
- **error** - events that do not occur under normal operation, causing minor malfunction
- **warning** - events that do not occur under normal operation, may cause malfunction
- **notice/info** - events that occur under normal operation, relevant to an administrator
- **debug** - events that occur under normal operation, may be relevant to an administrator

3. Click **Export** if you want to save the logs in a file.
4. Click **Save** when a **File Download** dialog box appears.
   - A **Save As** dialog box appears.



File name: status_savelogs.tar

Save as type: .tar Document

5. Select the folder and the name the file should be saved as, and then click **Save**.

The log files can now be sent to authorized technicians for further support and troubleshooting.

12.2.3 Synchronization State of Base Station

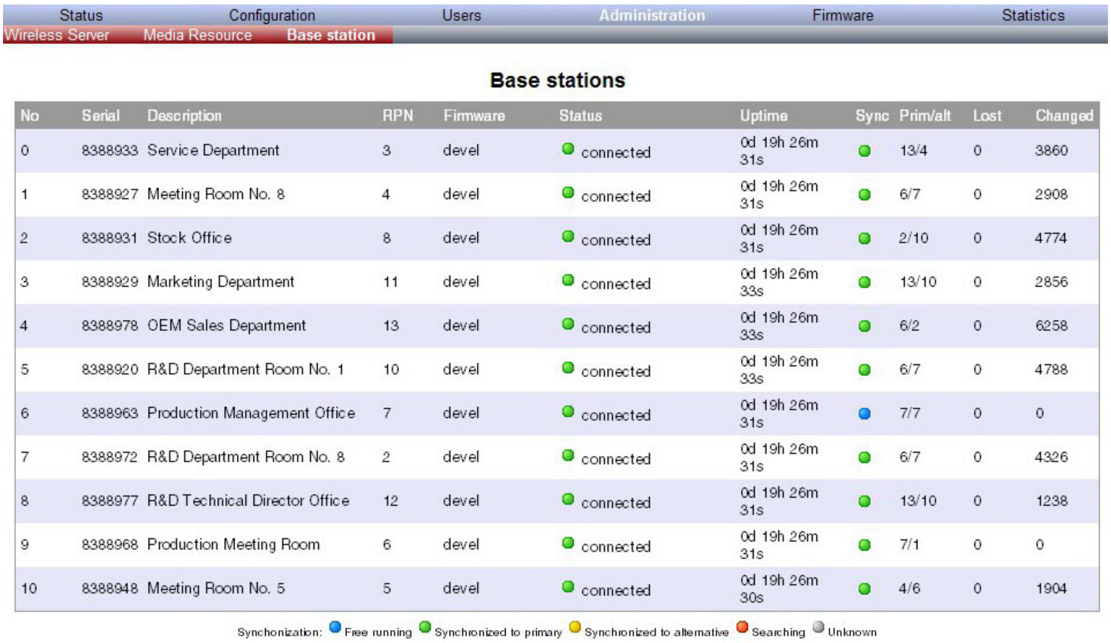
You can get information about the synchronization state of the base station, i.e. the uptime and to which radio unit it synchronizes on. This is useful when you want to get an overview of the base stations and in case of problem solving.

Information about the synchronization state of the base station can be retrieved from the web interface of the Server 6000.

12.2.3.1 Checking Sync State

In the web interface of the Server 6000:

- Click **Administration**, and then click **Base Station**.



Base stations

No	Serial	Description	RPN	Firmware	Status	Uptime	Sync	Prim/alt	Lost	Changed
0	8388933	Service Department	3	devel	🟢 connected	0d 19h 26m 31s	🟢	13/4	0	3860
1	8388927	Meeting Room No. 8	4	devel	🟢 connected	0d 19h 26m 31s	🟢	6/7	0	2908
2	8388931	Stock Office	8	devel	🟢 connected	0d 19h 26m 31s	🟢	2/10	0	4774
3	8388929	Marketing Department	11	devel	🟢 connected	0d 19h 26m 33s	🟢	13/10	0	2856
4	8388978	OEM Sales Department	13	devel	🟢 connected	0d 19h 26m 33s	🟢	6/2	0	6258
5	8388920	R&D Department Room No. 1	10	devel	🟢 connected	0d 19h 26m 33s	🟢	6/7	0	4788
6	8388963	Production Management Office	7	devel	🟢 connected	0d 19h 26m 31s	🔵	7/7	0	0
7	8388972	R&D Department Room No. 8	2	devel	🟢 connected	0d 19h 26m 31s	🟢	6/7	0	4326
8	8388977	R&D Technical Director Office	12	devel	🟢 connected	0d 19h 26m 31s	🟢	13/10	0	1238
9	8388968	Production Meeting Room	6	devel	🟢 connected	0d 19h 26m 31s	🟢	7/1	0	0
10	8388948	Meeting Room No. 5	5	devel	🟢 connected	0d 19h 26m 30s	🟢	4/6	0	1904

Synchronization: 🔵 Free running 🟢 Synchronized to primary 🟡 Synchronized to alternative 🔴 Searching ⚪ Unknown

At the bottom of the page, there is a color description of the various sync states.

The sync states of the base stations are as follows:

- Blue: Free running (Sync Master)
- Green: Synchronized to primary (Primary Sync Master)
- Yellow: Synchronized to secondary (Secondary Sync Master)
- Red: Searching (not in sync with any radio unit)
- Grey: Unknown (not connected - base station removed from installation)

Double-click a base station in the list to check the RSSI values of the base stations it is synchronizing on (Primary sync or Secondary sync).

12.2.4 Updating the Base Station Firmware

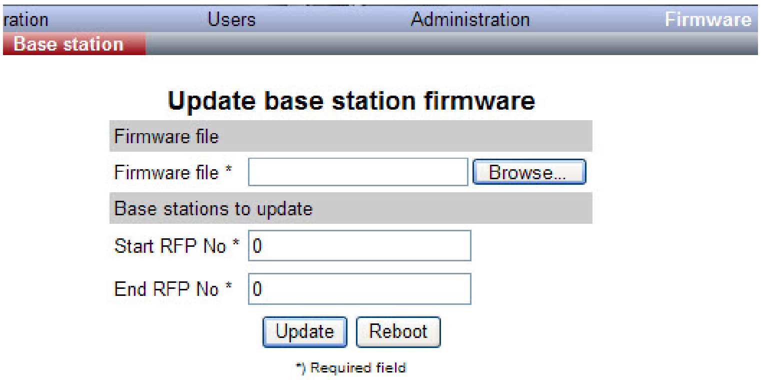
To update the firmware, you have to load a file to the system. Contact your distributor for the latest firmware.

The base station firmware is updated from the **Firmware** page of the Server 6000.

You can specify a range of base stations to be updated with the new firmware.

To update the base station firmware:

1. Click **Firmware**, and then click **Base Station**.



Update base station firmware

Firmware file

Firmware file * [ ] Browse...

Base stations to update

Start RFP No * 0

End RFP No * 0

Update Reboot

*) Required field

2. Next to the **Firmware file** field, click **Browse**.
   - A **Choose File to Upload** dialog box appears.
3. Select the firmware update file, and then click **Open**.
   - The file has the extension **.bin**.
4. In the **Start RFP No** field, type the number of the first base station to be updated.
   - You can check base station numbers under **Administration > Base station**.
5. In the **End RFP No** field, type the number of the last base station to be updated.
6. Click **Update**.

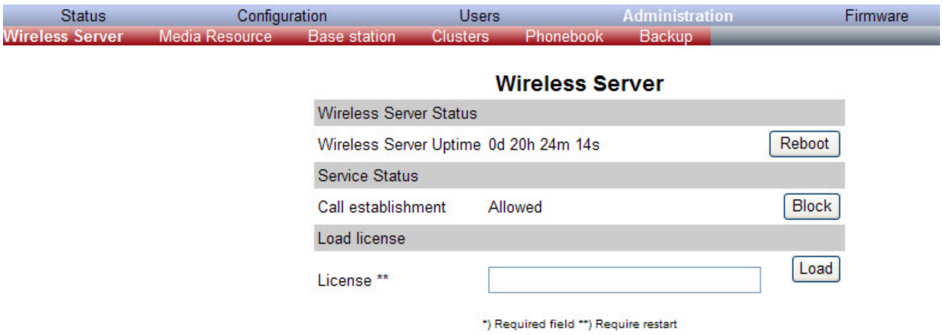
Wait for the system to finish uploading. All base stations in the range specified will be updated.

☞ *You can check the update status under Administration > Base station while the update is progressing. Each update takes approximately 30 seconds.*

7. When the update is completed, click **Reboot** to enable the changes.

Optionally, you can block new calls during a firmware update by doing the following:

1. Click **Administration**, and then click **Wireless Server**.



Wireless Server

Wireless Server Status

Wireless Server Uptime 0d 20h 24m 14s Reboot

Service Status

Call establishment Allowed Block

Load license

License ** [ ] Load

*) Required field **) Require restart

2. Under **Service Status** for **Call establishment**, click **Block**.

If you have blocked new calls during a firmware update, enable new calls again by doing the following:

3. Under **Service Status**, for **Call establishment**, click **Allow**.

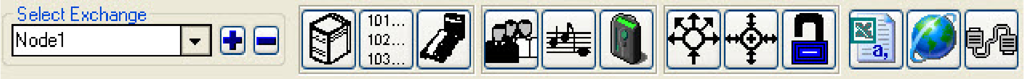
13 Configuring the AlphaCom/ACM Exchange

The AlphaCom/ACM exchange has to be configured to be able to communicate with the Server 6000. This is carried out using the AlphaPro configuration tool.

The configuration procedures are as follows:

- Adding a DECT User/Handset
- Updating the Exchange

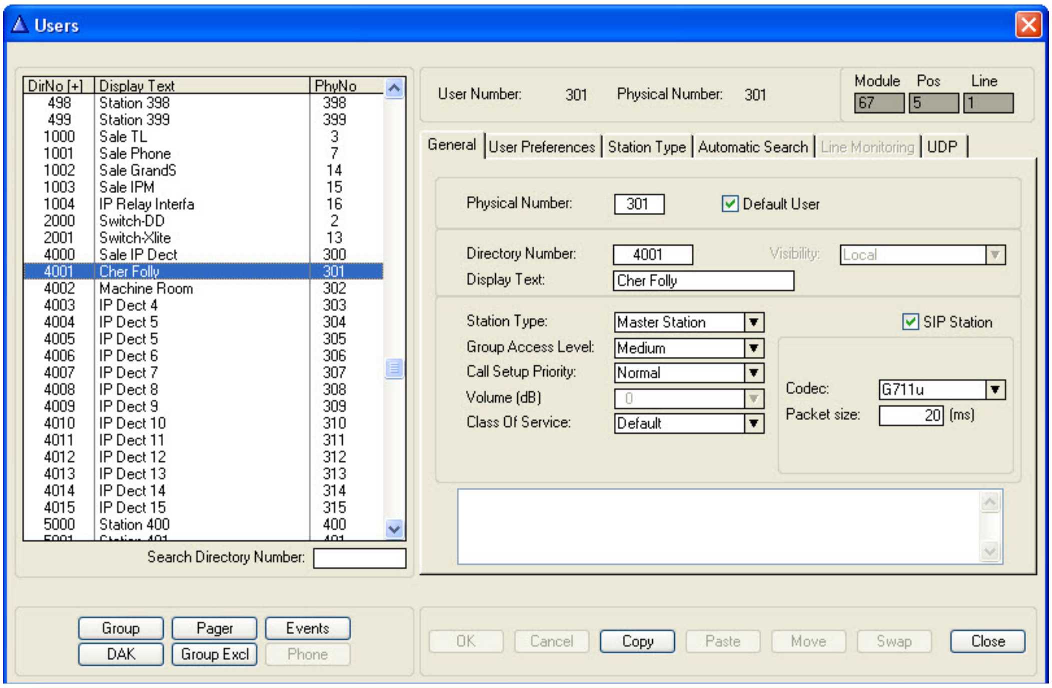
To configure the AlphaCom/ACM exchange, start the AlphaPro software tool on your computer.



☞ *The following procedure for adding a DECT user/handset is only valid for an AlphaCom/ACM exchange with AMC board version 10.55 and above.*

13.1 Adding a DECT User/Handset

1. From the AlphaPro menu bar, click the **Users & Stations** icon.



DirNo [+]	Display Text	PhyNo
498	Station 398	398
499	Station 399	399
1000	Sale TL	3
1001	Sale Phone	7
1002	Sale GrandS	14
1003	Sale IPM	15
1004	IP Relay Interfa	16
2000	Switch-DD	2
2001	Switch-Xlite	13
4000	Sale IP Dect	300
4001	Cher Folly	301
4002	Machine Room	302
4003	IP Dect 4	303
4004	IP Dect 5	304
4005	IP Dect 5	305
4006	IP Dect 6	306
4007	IP Dect 7	307
4008	IP Dect 8	308
4009	IP Dect 9	309
4010	IP Dect 10	310
4011	IP Dect 11	311
4012	IP Dect 12	312
4013	IP Dect 13	313
4014	IP Dect 14	314
4015	IP Dect 15	315
5000	Station 400	400
5001	Station 401	401

Search Directory Number:

User Number: 301 Physical Number: 301

Module	Pos	Line
67	5	1

Physical Number: 301 ☑ Default User

Directory Number: 4001 Visibility: Local

Display Text: Cher Folly

Station Type: Master Station

Group Access Level: Medium

Call Setup Priority: Normal

Volume (dB) 0

Class Of Service: Default

☑ SIP Station

Codec: G711u

Packet size: 20 (ms)

2. Select the directory number corresponding to the handset number that was registered on the Server 6000.
3. Check the **SIP Station** checkbox.
4. Enter the text of your choice in the **Display Text** field.
5. Click **OK**

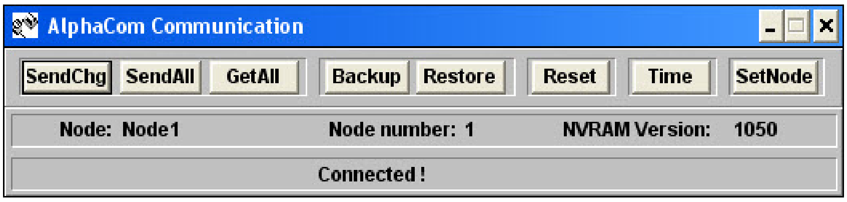
13.2 Updating the Exchange

Log on to the AlphaCom/ACM exchange.

To update the exchange:

- Click **SendAll**

Reset the AMC board when the transfer is completed.



Node: Node1 Node number: 1 NVRAM Version: 1050

Connected !

You should now be able to use the IP DECT handsets as mobile intercom stations and make calls to/from any stations connected to the AlphaCom/ACM exchange.

A Acronyms

AC	Authentication Code
ACM	AlphaCom Marine
	- VINGTOR’s IP exchange
AlphaCom	STENTOFON’s IP exchange
ARI	Access Rights Identity - Serial number of the IP DECT Server 6000
dB	Decibel
DECT	Digital Enhanced Cordless Telecommunications
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EIRP	Equivalent Isotropically Radiated Power
ETSI	European Telecommunications Standards Institute
GAP	Generic Access Profile
IP	Internet Protocol
IPEI	International Portable Equipment Identity - Serial number of the handset
WS	Wireless Server
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Control - hardware address of a device connected to a network
MTU	Maximum Translation Unit
MWI	Message Waiting Indicator
NTP	Network Time Protocol
PBX	Private Branch eXchange
PoE	Power over Ethernet
PSTN	Public Switched Telephone Network
RFP	Radio Fixed Part
RSSI	Received Signal Strength Indicator
RTP	Real-time Transport Protocol
SIP	Session Initiated Protocol
VoIP	Voice over Internet Protocol
WLAN	Wireless Local Area Network
WRFP	Wireless Radio Fixed Part - Wireless Repeater

B Regulatory Notices

This section contains important safety regulations for the Server 6000.

B.1 International Regulatory Information

This product has been marked with the CE mark. This mark indicates compliance with EEC Directives 89/336/EEC, 73/23/EEC 1999/5/EC. A full copy of the Declaration of Conformity can be obtained from Zenitel Norway AS, P.O. BOX 4498 NYDALEN, NO-0403 Oslo, Norway.

Cesky [Czech]:
Váš dodavatel tímto prohlašuje, že tento produkt je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.

Dansk [Danish]:
Deres leverandør erklærer herved, at udstyret overholder de væsentlige krav og øvrige relevante krav i direktiv 1 999/5/EF.

Deutsch [German]:
Hiermit erklärt Ihr Lieferant, dass sich das Gerät in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1 999/5/EGbefindet.

Eesti [Estonian]:
Käesolevaga kinnitab Teie tarnija, et seade on vastavuses direktiivi 1999/5/EÜ põhinõuetega ning nimetatud direktiivist tulenevate teiste asjakohaste sätetega.

English:
Hereby, your supplier declares that this product is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Español [Spanish]:
Por medio de la presente su proveedor declara que este producto cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.

Ellivtiai [Greek]:
ME THN IIAPOYEA, O IIPOMHOETHE EAE AHACNEI OTI TO EYFKEKPIMENO IIPOION EYMMOPMENETAI IIPOE TIE OYEIMEIE AIIAITHEEIE KAI TIE AOIIIEE EXETIKEE AIATAZEEIE THE OAHFIAE 1999/5/EK.

Français [French]:
Par la présente votre fournisseur déclare que l’appareil conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.

Italiano [Italian]:
Con la presente il Suo fornitore dichiara che questo prodotto è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

Íslenska (Icelandic):
Hér með lýsir birgirinn þinn því yfir að þessi vara sé í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC

Latviski [Latvian]:
Piegadatajs pazino, ka šis produkts atbilst Direktivas 1999/5/EK pamatprasibam un citiem attiecigajiem tas noteikumiem.

Lietuviu [Lithuanian]:
Šiuo jusu tiekejas deklaruoja, kad šis produktas atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.

Nederlands [Dutch]:
Hierbij verklaart uw leverancier dat dit product in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn1999/5/EG.

Malti [Maltese]:
Ghalhekk, il-fornitur jiddikjara li dan il-prodott jikkonforma mal-htigijietijiet essenzjali u ma provvedimenti relevanti ohrajn li hemm fid-Dirrettiva 1999/5/EC.

Magyar [Hungarian]:
Alulírott, beszállító nyilatkozom, hogy ez atermék megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak

Norsk [Norwegian]:
Din leverandør erklærer herved at dette produkt er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

Polski [Polish]:
Niniejszym dostawca oswiadcza, ze produkt ten jest zgodne z podstawowymi wymaganiami oraz innymi stosownymi postanowieniami Dyrektywy 1 999/5/WE.

Português [Portuguese]:
Por este meio, o seu fornecedor declara que este produto está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

Slovensko [Slovenian]:
Dobavitelj izjavlja, da je ta izdelek v skladu z bistvenimi zahtevami in ostalimi relevantnimi dolocili direktive 1999/5/ES.

Slovensky [Slovak]:
Dodávatel zároven vyhlasuje, že tento produkt splna základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.

Suomi [Finnish]:
Täten toimittajanne vakuuttaa, että tämä tuote on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Svenska [Swedish]:
Härmed intygar leverantören att denna produkt står iöverensstämmelse

med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1 999/5/EG.

Explosive Device Proximity Warning

Warning
Do not operate your wireless network device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.

Waarschuwing
Gebruik dit draadloos netwerkapparaat alleen in de buurt van onbeschermde ontstekers of in een omgeving met explosieven indien het apparaat speciaal is aangepast om aan de eisen voor een dergelijk gebruik te voldoen.

Varoitus
Älä käytä johdotonta verkkolaitetta suojaamattomien räjäytysnallien läheisyydessä tai räjäytysalueella, jos laitetta ei ole erityisesti muunnettu sopivaksi sellaiseen käyttöön.oen.

Attention
Ne jamais utiliser un équipement de réseau sans fil à proximité d’un détonateur non blindé ou dans un lieu présentant des risques d’explosion, sauf si l’équipement a été modifié à cet effet.

Warnung
Benutzen Sie Ihr drahtloses Netzwerkgerät nicht in der Nähe ungeschützter Sprengkapseln oder anderer explosiver Stoffe, es sei denn, Ihr Gerät wurde eigens für diesen Gebrauch modifiziert und bestimmt.

Avvertenza
Non utilizzare la periferica di rete senza fili in prossimità di un detonatore non protetto o di esplosivi a meno che la periferica non sia stata modificata a tale proposito.

Advarsel
Ikke bruk den trådløse nettverksenheten nært inntil uisolerte fenghetter eller i et eksplosivt miljø med mindre enheten er modifisert slik at den tåler slik bruk.

Aviso
Não opere o dispositivo de rede sem fios perto de cápsulas explosivas não protegidas ou num ambiente explosivo, a não ser que o dispositivo tenha sido modificado para se qualificar especialmente para essa utilização.

¡Advertencia!
No utilizar un aparato de la red sin cable cerca de un detonador que no esté protegido ni tampoco en un entorno explosivo a menos que el aparato haya sido modificado con ese fin.

Varning!
Använd inte den trådlösa nätverksenheten i närheten av oskyddade tändhattar eller i en explosiv miljö om inte enheten modifierats för att kunna användas i sådana sammanhang.

The WEEE Marking on this equipment indicates that the product must not be disposed of with unsorted waste, but must be collected separately.

Appropriate RF safety/installation information

The product is intended to be installed by authorized personal. The product shall be installed in accordance with FCC rules.

RF Exposure Statement

The EUT is considered as a mobile device according to OET Bulletin 65, Edition 97-01. Therefore distance to human body of min. 20 cm is determined.

The internal/external antennas used for this mobile transmitter must provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

WARNING

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures. The above warning is inserted for regulatory reasons. If any customer believes that they have an interference problem, either because their product seems to cause interference or suffers from interference, they should contact their distributor immediately. The distributor will assist with a remedy for any problems.

Safety WARNING!

Only qualified service personnel may install this equipment. The instructions in this manual are intended for use by qualified service personnel only.

Only qualified persons should service the system.

The installation and service of this hardware is to be performed only by service personnel having appropriate training and experience necessary to be aware of hazards to which they are exposed in performing a task and of measures to minimize the danger to themselves or other persons.

Electrical shock hazards from the telecommunication network and AC mains are possible with this equipment. To minimize risk to service personnel and users, the system must be connected to an outlet with a third-wire Earth.

Service personnel must be alert to the possibility of high leakage currents becoming available on metal system surfaces during power line fault events near network lines. These leakage currents normally safely flow to Protective Earth via the power cord. Therefore, it is mandatory that connection to an earthed outlet is performed first and removed last when cabling to the unit. Specifically, operations requiring the unit to be powered down must have the network connections (exchange lines) removed first.

B.2 Important Safety Instructions

Before using your telephone equipment, you should always follow basic safety instruction to reduce the risk of fire, electrical shock and injury to persons, and damage to property.

- Read and understand all instructions.
- Follow all warnings and instructions including those marked on the product.
- Unplug this product before cleaning. Do not use liquid cleaners or aerosol cleaners. Use damp cloth for cleaning.
- Do not install the telephone equipment in the bathroom or near a wash bowl, kitchen sink, or laundry tub, in a wet basement, or near a swimming pool.
- The product should be operated only from the type of power source indicated on the instructions. If you are not sure of the type of power supply, consult your dealer or local power company.
- Do not overload wall outlets and extension cords as this can result in fire or electrical shock.
- Never push objects of any kind into this product through cabinet slots as they may touch dangerous voltage points or short out parts that could result in fire, electrical shock, or injury. Never spill liquid of any kind into this product.
- To reduce the risk of electrical shock or burns, do not disassemble this product. Opening or removing covers may expose you to dangerous voltages, dangerous electrical current, or other risks. Incorrect reassemble can cause electrical shock when the appliance is subsequently used. If the product needs repair, consult your dealer.
- This product does not support connections to outside plant.
- Refer servicing to qualified service personnel under the following conditions:
  - If liquid has been spilled into the product
  - If the product has been exposed to rain or water
  - If the product does not operate normally when following the operating instructions in the manual. Adjust only those controls that are covered by the operation instructions. Improper adjustment of other controls may result in damage and will often require extensive work by qualified service personnel to restore the product to normal operation.
  - If the product has been dropped or cabinet has been damaged
  - If the product exhibits a distinct change in performance

Warning

- Avoid using the telephone during an electrical storm. There may be a risk of electrical shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
- Do not place the unit near microwave ovens, radio equipment, or non-ground connected televisions. These appliances may cause electrical interference to the base or handset.
- Installation must be performed in accordance with all relevant national wiring rules.

- Plug acts as Disconnect Device - The socket outlet to which this apparatus is connected must be installed near the equipment and must always be readily accessible.
- The system will not operate in the event of a blackout. Please keep a backup phone for emergencies.

Intrinsic safety

Do not install the unit in conditions where there is a danger of electrically ignited explosions.

Exposure to sunlight, heat and moisture

Do not expose the unit to direct sunlight for long periods. Keep away from excessive heat and moisture.

Spare parts and accessories

Use only approved spare parts and accessories. The operation of non-approved parts cannot be guaranteed and may even cause damage.

RF compliance information

The user manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

NOTICES

FCC Note: This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IC Note: Operation is subject to the following two conditions: (1) This device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device. The term “IC:” before the certification/registration number only signifies that the Industry Canada technical specifications were met.

Privacy of communications may not be ensured when using this telephone.

Information to user: The user manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

LIMITED WARRANTY

This limited, non-transferable warranty is provided to the original purchaser. The product is warranted to be free from defects in materials and workmanship under normal installation, use and service for a period of one (1) year from the date of purchase as shown on the purchaser’s receipt.

Our obligation under this warranty is limited to repair or replacement (at our option) of the product or any part(s) which are defective provided that the product is returned to the original place of purchase or an authorized service location during the warranty period. Products returned must be accompanied by a copy of the purchase receipt. In the absence of a purchase receipt, the warranty period shall be one (1) year from the date of manufacture. Repair or replacement of the product is your sole and exclusive remedy.

If the product is repaired, reconditioned component parts or materials may be used. If the product is replaced, we may replace it with a new or reconditioned product of the same or similar design. The repaired product will be warranted for either (a) 90 days or (b) the remainder of the original one (1) year warranty period, whichever is longer.

This warranty does not apply to the defects outside of our control, including but not limited to acts of God, fire, flood and damage while in transit to service facility. We do not warranty that the product will be compatible with any telephone equipment, systems or party lines.

This warranty shall be void if the product is damaged as a result of defacement, misuse, abuse, neglect, accident, destruction or alteration of the serial number, improper electrical voltages or currents, repair, alteration or maintenance by any person or party other than our authorized service facility, or any violation of instructions furnished by us.

This warranty is also void if this product is removed from the country in which it was purchased by the original purchaser, if it is used in a country in which it is not registered for use, or if it is used in a country for which it was not designed. Due to variations in telephone systems and communications laws, this product may be illegal for use in some countries. We assume no responsibilities for damages or penalties incurred resulting from the use of this product in a manner or location other than that for which it was intended.

THIS LIMITED WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED. ANY IMPLIED WARRANTIES INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, SHALL BE LIMITED TO THE DURATION OF THIS WRITTEN LIMITED WARRANTY. WE DISCLAIM ANY LIABILITY FOR DAMAGES FOR LOSS OF USE OF THE PRODUCTS, LOSS OF TIME, INCONVENIENCE, INJURY TO ANY PERSON, OR DAMAGE TO PROPERTY CAUSED BY THE PRODUCT, LOSS OF REVENUE OR PROFIT OR DAMAGES FOR ANY FAILURE TO PERFORM. IN NO EVENT SHALL WE BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES EVEN IF WE ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Some states do not allow limitations on how long an implied warranty lasts, so the above limitations may not apply to you. This warranty is the sole and exclusive warranty provided for the product. There are no other express warranties. This warranty gives you specific legal rights, and you may also have other rights, which vary from state to state.

www.stentofon.com

Zenitel Norway AS
P.O. Box 4498 Nydalen
NO-0403 OSLO
Norway

DOC NO.

A100K10652

support@stentofon.com
support@vingtor.com

STENTOFON and VINGTOR products are developed and marketed by Zenitel Norway AS. The company's Quality Assurance System is certified to meet the requirements in NS-EN ISO 9001:2008. Zenitel Norway AS reserves the right to modify designs and alter specifications without prior notice, in pursuance of a policy of continuous improvement. © 2009 Zenitel Norway AS.