SMART System Guide

Installation & Configuration
Network Deployment
Operation & Management

Technical Reference Document

Trademarks

COBS and the combinations of its logo thereof are trademarks of COBS AB, Sweden.
Other product names used in this publication are for identification purposes and maybe the trademarks of their respective companies.

Disclaimer

The contents of this document are provided in connection with COBS products. COBS makes no representations with respect to completeness or accuracy of the contents of this publication and reserves the right to make changes to product descriptions, usage, etc., at any time without notice. No license, whether express, implied, to any intellectual property rights are granted by this publication

Confidentiality

This document should be regarded as confidential, unauthorized copying is not allowed

Contents

1 About This Document

This document describes the configuration, customization, management, operation, maintenance and troubleshooting of the SMART System (SMART AP, SMART1 handset).

1.1 Audience

Who should read this guide? First, this guide is intended for networking professionals responsible for designing and implementing COBS SMART System a wireless enterprise voice and messaging network. Second, network administrators and IT support personnel that need to install, configure, maintain and monitor elements in a "live" SMART System network will find this document helpful. Furthermore, anyone who wishes to gain knowledge on fundamental features in the system can also benefit from this material.

1.2 When Should I Read This Guide

Read this guide before you install the core network devices of SMART System and when you are ready to setup or configure SIP server, NAT aware router, advanced VLAN settings, base stations, CMS, SMART Manager and multi cell setup.

This manual will enable you to set up components in your network to communicate with each other and also deploy a fully functionally SMART System.

1.3 Important Assumptions

This document was written with the following assumptions in mind:

1) You have understanding of network deployment in general
2) You have working knowledge of basic TCP/IP/SIP protocols, Network Address Translation, etc...
3) A proper site survey has been performed, and the administrator have access to these plans and documentation.
4) You are familiar with components such as SMART Manager, CMS and SIP pbx systems in general.

1.4 Abbreviations

For the purpose of this document, the following abbreviations hold:

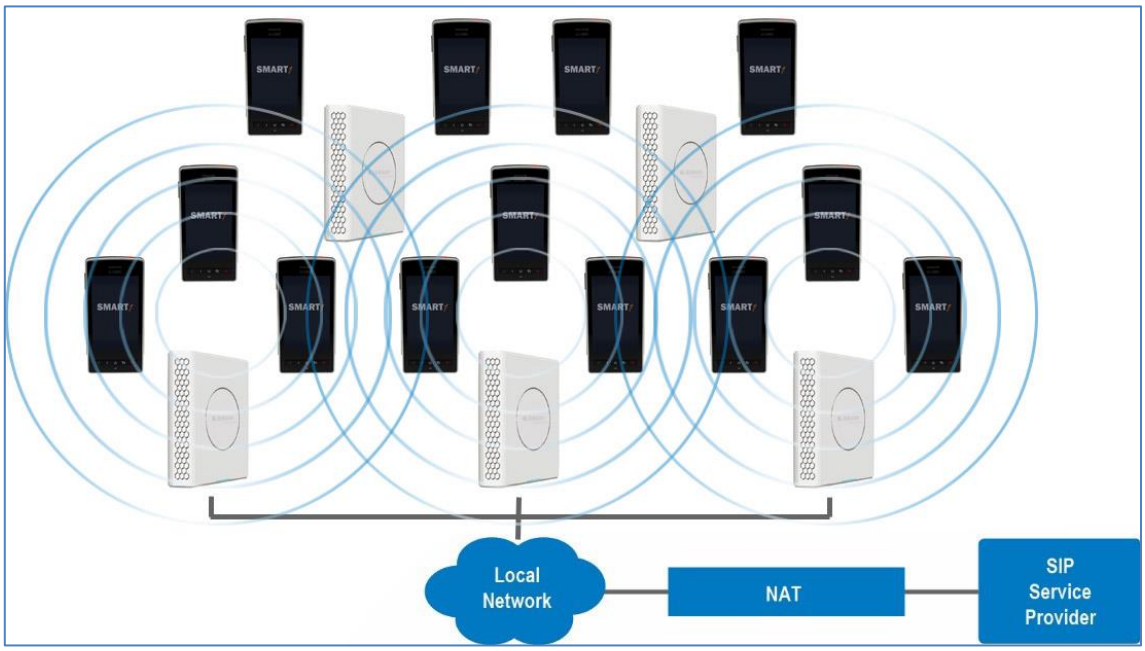
DHCP:	Dynamic Host Configuration Protocol
DNS:	Domain Name Server
HTTP(S):	Hyper Text Transfer Protocol (Secure)
(T)FTP:	(Trivial) File Transfer Protocol
IOS:	Internetworking Operating System
PCMA:	A-law Pulse Code Modulation
PCMU:	mu-law Pulse Code Modulation
PoE:	Power over Ethernet
RTP:	Real-time Transport Protocol
RPORT:	Response Port (Refer to RFC3581 for details)
SIP:	Session Initiation Protocol
SME:	Small and Medium scale Enterprise
VLAN:	Virtual Local Access Network
TOS:	Type of Service (policy based routing)
URL:	Uniform Resource Locator
UA:	User Agent

2 Introduction – System Overview

In a typical telephony and messaging system, the network setup is the interconnection between Base-stations, routers, repeaters, portable parts, etc. The back-bone of the network depends on the deployment scenario but a typical Ethernet network is used. The system has centralized monitoring and maintenance.

The system is easy to scale up and supports from 1 to 256 (512) bases in the same network. Further is it able to support up to 1000 registered handsets. The SMART System setup is illustrated below. Based on PoE interface each base station is easy to install without additional wires other than the from the LAN cable.

The following figure gives a graphical overview of the architecture of the SMART System:



2.1 Hardware Setup

SMART network hardware setup can deployed as follows:

Base-station(s) are connected via Layer 3 and/or VLAN Aware Router depending on the deployment requirements. The Layer 3 router implements the switching function.

The base-stations are typically mounted on walls so that each base-station is separated from each other by up to 50m indoor[1] (300m outdoor). Radio coverage can be extended using repeaters that are installed with same distance to base-station(s).
The base-station antenna mechanism is based on space diversity feature which improves coverage. The base-stations uses complete DECT MAC protocol layer and IP media stream audio encoding feature to provide up to 10 simultaneous calls.

2.2 Components of SMART System

COBS SMART System is made up of (but not limited to) the following components:

- At least one SMART Base Station is connected over an IP network and using DECT as air-core interface.
- COBS SMART1 wireless Handset.
- A WiFi access point

[1] Measured with European DECT radio and depends on local building layout and material

- COBS SMART Configuration Interface; is a management interface for SME VoIP Wireless Solution. It runs on all SMART AP base stations. Each Base station has its own unique settings.

2.2.1 COBS Base Stations

The Base Station converts IP protocol to DECT protocol and transmits the traffic to and from the end-nodes (i.e. wireless handsets) over a channel. It has 12 available channels.
In a multi-cell setup, each base station has:

- 8 channels have associated DSP resources for media streams.
- The remaining 4 channels are reserved for control signalling between IP Base Stations and the SIP/DECT end nodes (or phones).

Base Stations are grouped into clusters. Within each Cluster, Base Stations are synchronized to enable a seamless handover when a user moves from one base station coverage to another. For synchronization purposes, it is not necessary for Base Stations to communicate directly with each other in the system. E.g. a Base Station may only need to communicate with the next in the chain. It is advisable for a Base Station to identify more than one Base Station to guarantee synchronization in the situation that one of the Base Stations fails.
The 4 control signalling channels are used to carry bearer signals that enable a handset to initiate a handover process.

2.2.2 SMART System Administration interface

The SMART System Configuration Interface is a web based administration page used for configuration and programming of the base station and relevant network end-nodes. E.g. handsets can be registered or de-registered from the system using this interface.
The configuration interface can be used as a setup tool for software or firmware download to base stations and handsets. Further, it is used to check relevant system logs that can be useful to administrator. These logs can be used to troubleshoot the system when the system faces unforeseen operational issues.

2.2.3 COBS Wireless Handset

The handset SMART1 is an Android based, lightweight, ergonomically and portable unit compatible with Wideband Audio (G.722), DECT, GAP standard, CAT-iQ audio compliant.
The handset includes touch display with graphical user interface. It can also provide the subscriber with most of the features available for a wired phone, in addition to its roaming and handover capabilities. Refer to the relevant handset manuals for full details handset features.

2.3 Wireless Bands

The bands supported in the SMART System are summarized as follows:

Frequency bands:	1880 – 1930 MHz (DECT)
	1880 – 1900 MHz (10 frequencies) Europe/ETSI
	1910 – 1930 MHz (10 frequencies) LATAM
	1920 – 1930 MHz (5 carriers) US

2.4 System Capacity (in Summary)

SME network capacity of relevant components can be summarised as follows:

Description	Capacity
Min ## of Bases Single Cell Setup	1
Max ## of Bases in Multi-cell Setup	256
Max ## of Users (SIP registrations) per Base	30
Max ## of Users per SMART System	Currently limited to 1000

Multi-cell Setup: Max ## of Synchronisation levels	24
Single Cell Setup: Max ## Simultaneous Calls	10 per Base station
Multi-cell Setup: Max ## of Calls	8 per Base station
Total Max ## Simultaneous Calls (Multi-cell Setup)	Limited to 1000

Quick Definitions

Single Cell Setup: Telephony network composed of one base station
Multi-cell Setup: Telephony network that consists of more than one base station
Synchronisation Level: Is the air core interface between two base stations.

2.5 Advantages of SMART System

They include (but not limited to):

1. Simplicity. Integrating functionalities leads to reduced maintenance and troubleshooting, and significant cost reductions.

2. Flexibility. Single network architecture can be employed and managed. Furthermore, the architecture is amenable to different deployment scenarios, including Isolated buildings for in-building coverage, location with co-located partners, and large to medium scale enterprises deployment for wide coverage.

3. Scalability. SMART network architecture can easily be scaled to the required size depending on customer requirement.

4. Performance. The integration of different network functionalities leads to the collapse of the protocol stack in a single network element and thereby eliminates transmission delays between network elements and reduces the call setup time and packet fragmentation and aggregation delays.

3 Installation of SMART AP

After planning the network, next is to determine the proper places or location the relevant base stations will be installed. Therefore, we briefly describe the how to install the base station in this chapter.

3.1 Package – Contents/Damage Inspection

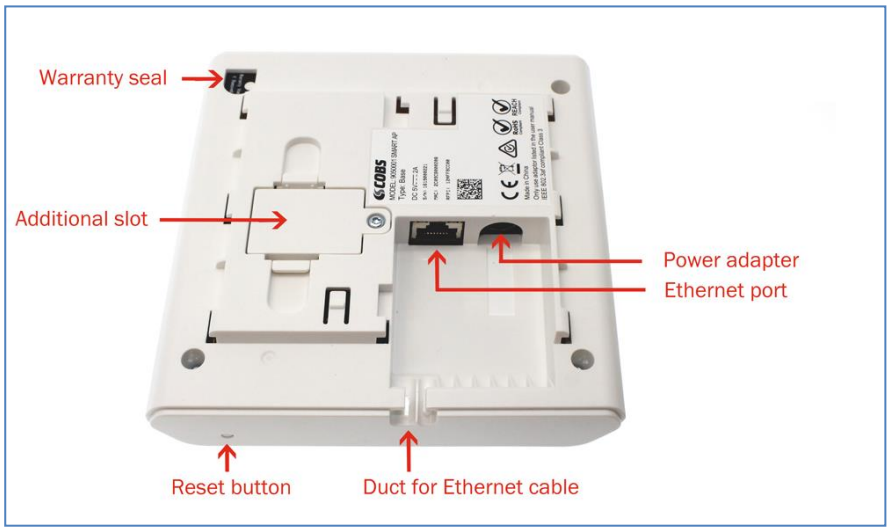
Before Package Is Opened:

Examine the shipping package for evidence of physical damage or mishandling prior to opening. If there is a proof of mishandling prior to opening, you must report it to the relevant support centre of the regional representative or operator.

Contents of Package:

Make sure all relevant components are available in the package before proceeding to the next step.
Every shipped base unit package/box contains the following items:

- 2 x mounting screws and 2 x Anchors
- 1 x Plastic mounting fixture
- SMART AP (Base station)



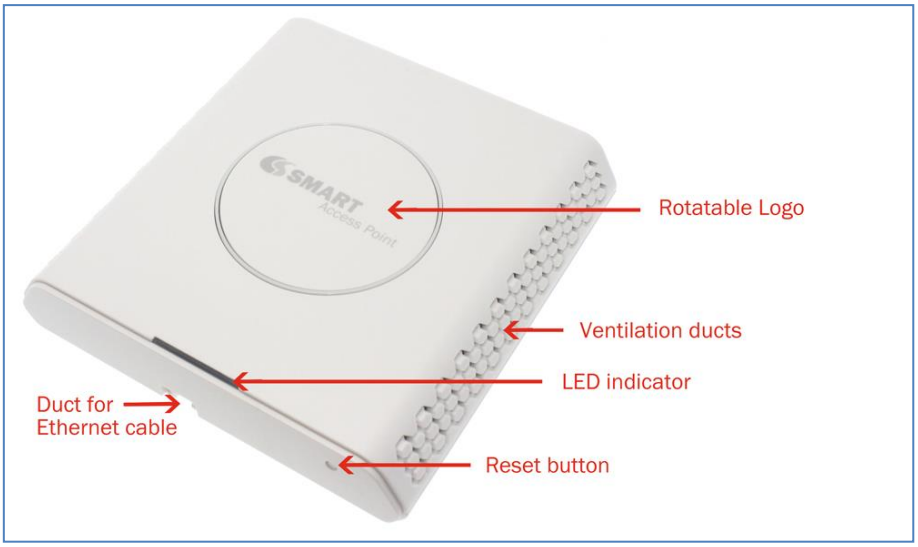
Damage Inspection:

The following are the recommended procedure for you to use for inspection:

1. Examine all relevant components for damage.
2. Make a “defective on arrival – DOA” report or RMA to the operator. Do not move the shipping carton until it has been examined by the operator. If possible send pictures of the damage. The operator/regional representative will initiate the necessary procedure to process this RMA. They will guide the network administrator on how to return the damaged package if necessary.
3. If no damage is found then unwrap all the components and dispose of empty package/carton(s) in accordance with country specific environmental regulations.

3.2 SMART AP Mechanics

The base station front end shows an LED indicator that signals different functional states of the base unit and occasionally of the overall network. The indicator is off when the base unit is not powered.



The table below summarises the various LED states:

LED State	State
Unlit	No power in unit
Unlit/Solid red	Error condition
Blinking green	Initialisation
Solid red	Factory reset warning or long press in BS reset button
Blinking red	Factory setting in progress
Solid green	Ethernet connection available (Normal operation)
Blinking red	Ethernet connect not available OR handset de/registration failed
Solid red	Critical error (can only be identified by COBS Engineers). Symptoms include no system/SIP debug logs are logged, etc.
Orange	Press reset button of base station.
Blinking orange	No IP address received

3.3 SMART AP Base Unit – Reset feature

It is possible to restart or reset the base station unit by pressing a “hidden” reset button on the bottom part of the SMART AP. Alternatively, it can be reset from the SMART System Configuration Interface.

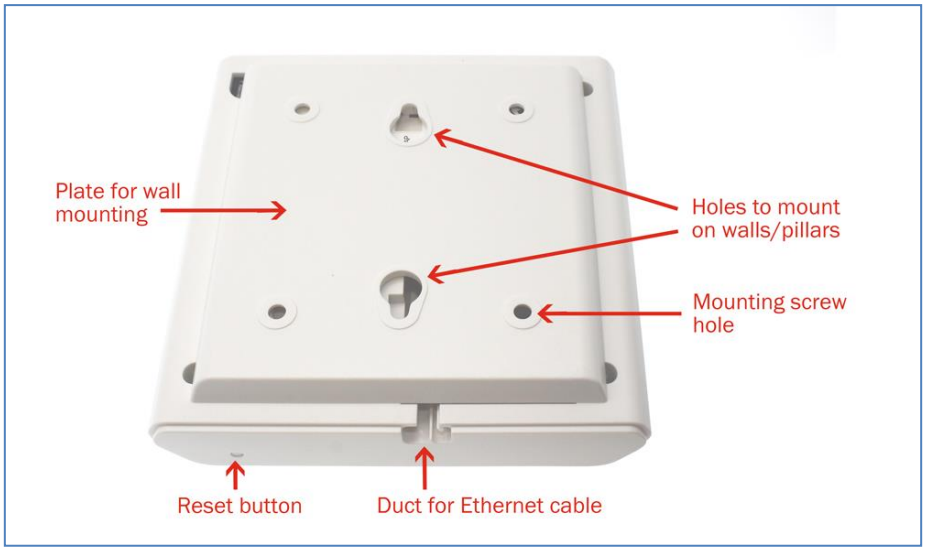
3.4 Installing the SMART AP (Base Station)

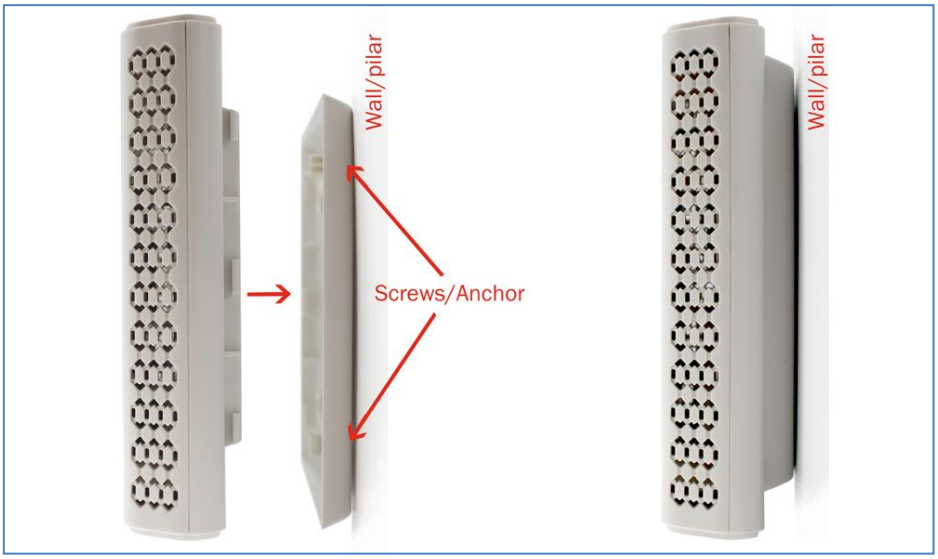
First determine the best location that will provide an optimal coverage taking account the construction of the building, architecture and choice of building materials.
Next, mount the Base Station on a wall to cover range between 50 – 300 meters (i.e. 164 to 984 feet), depending whether it’s an indoor or outdoor installation.

3.4.1 Mounting the Base Stations

We recommend the base station be mounted an angle other than vertical on both concrete/wood/plaster pillars and walls for optimal radio coverage. Avoid mounting the base units upside down as it significantly reduces radio coverage.

Mount the base unit as high as possible to clear all nearby objects (e.g. office cubicles and cabinets, etc.). Avoid all contacts with any high voltage lines.



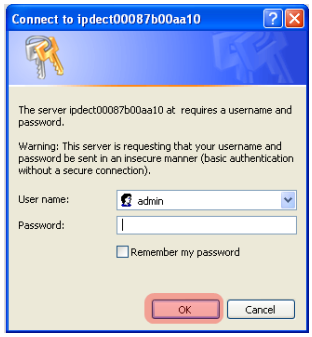


3.5 Login to base stations with your browser

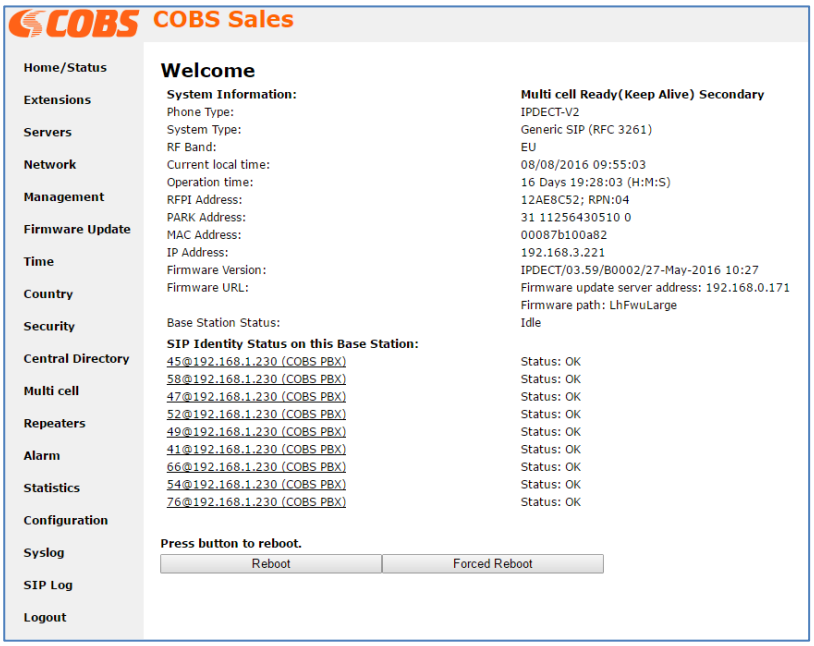
STEP 1 Connect the Base station to a private network via standard Ethernet cable (CAT-5).

STEP 2 Find the base stations IP-address through either the DHCP server or a scanner application. By default the base uses a DHCP assigned IP address.

STEP 3 On the Login page, enter your authenticating credentials (i.e. username and password). By default the username and password is **admin**. Click **OK** button.



STEP 4 Once you have authenticated, the browser will display front end of the SMART System Configuration Interface. The front end will show relevant information of the base station.



4 Making Handset Ready

In this chapter we briefly describe how to prepare the handset for use, install, insert and charge new batteries. Please refer to an accompanying Handset User Guide for more information of the features available in the Handset.

4.1 Package – Contents/Damage Inspection

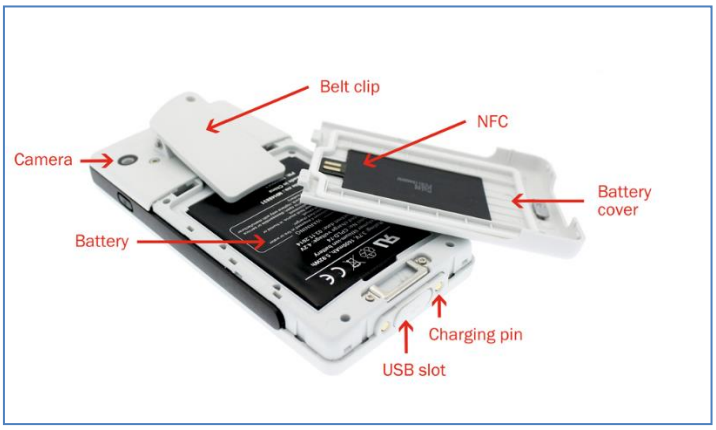
Before Package Is Opened:

Examine the shipping package for evidence of physical damage or mishandling prior to opening. If there is a proof of mishandling prior to opening, you must report it to the relevant support centre of the regional representative or operator.

Contents of Package:

Make sure all relevant components are available in the package before proceeding to the next step.
Every shipped handset package/box contains the following items:

- 1 x Handset
- 1 x Battery
- 1 x Flush rear part (mounted)
- 1 x Belt clip



Damage Inspection:

The following are the recommended procedure for you to use for inspection:

1. Examine all relevant components for damage.
2. Make a “defective on arrival – DOA” report or RMA to the operator. Do not move the shipping carton until it has been examined by the operator. The operator/regional representative will initiate the necessary procedure to process this RMA. They will guide the network administrator on how to return the damaged package if necessary.
3. If no damage is found then unwrap all the components and dispose of empty package/carton(s) in accordance with country specific environmental regulations.

4.2 Before Using the Phone

Here are the pre-cautions users should read before using the Handset:

Installing the Battery

1. Never dispose battery in fires, otherwise it will explode.

2. Never replace the batteries in potentially explosive environments, e.g. close to inflammable liquids/ gases.
3. ONLY use approved batteries and chargers from the vendor or operator.
4. Do not disassemble, customise or short circuit the battery

Using the Charger

Each handset is charged through the use of a handset charger. The charger is a compact desktop unit designed to charge and automatically maintain the correct battery charge levels and voltage.
The charger Handset is powered by AC supply from 110-240VAC that supplies 5.5VDC at 600mA.
When charging the battery for the first time, it is necessary to leave the handset in the charger for at least 10 hours before the battery is fully charged and the handset ready for use.

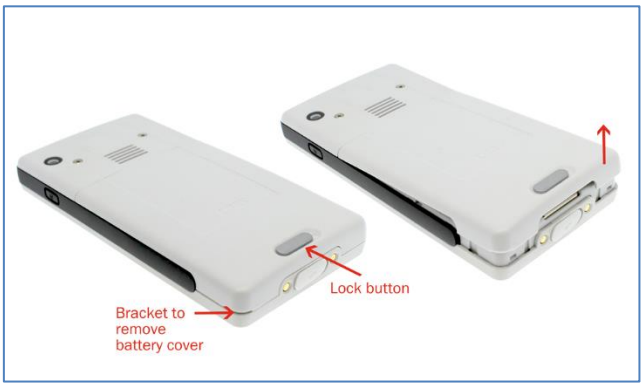
Handset in the Charger

For correct charging, ensure that the room temperature is between 0°C and 25°C/32°F and 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.

The handset will always turn on once it is placed in the charger.

Open Back Cover

1. Unlock the battery LID and lift up the back cover.
2. Remove Back Cover from Handset



Handset IPEI Number

The IPEI number of each handset is found either on a label, which is placed behind the battery, or on the packaging label. First, lift off handset back cover and lift the battery and read the serial number.
The IPEI number is needed to enable service to the handset. It must be programmed into the system database via the SMART System Configuration interface.

Replace Battery

Remove Back Cover from Handset. Remove the old battery and replace with a new one.

4.3 Using the Handset

Please refer handset manual for detailed description of how to use the handset features [1].

5 SMART System Administration Interface

The SMART System Administration Interface is also known as SMART System Configuration. It is the main interface through which the system is managed, configured and debugged.

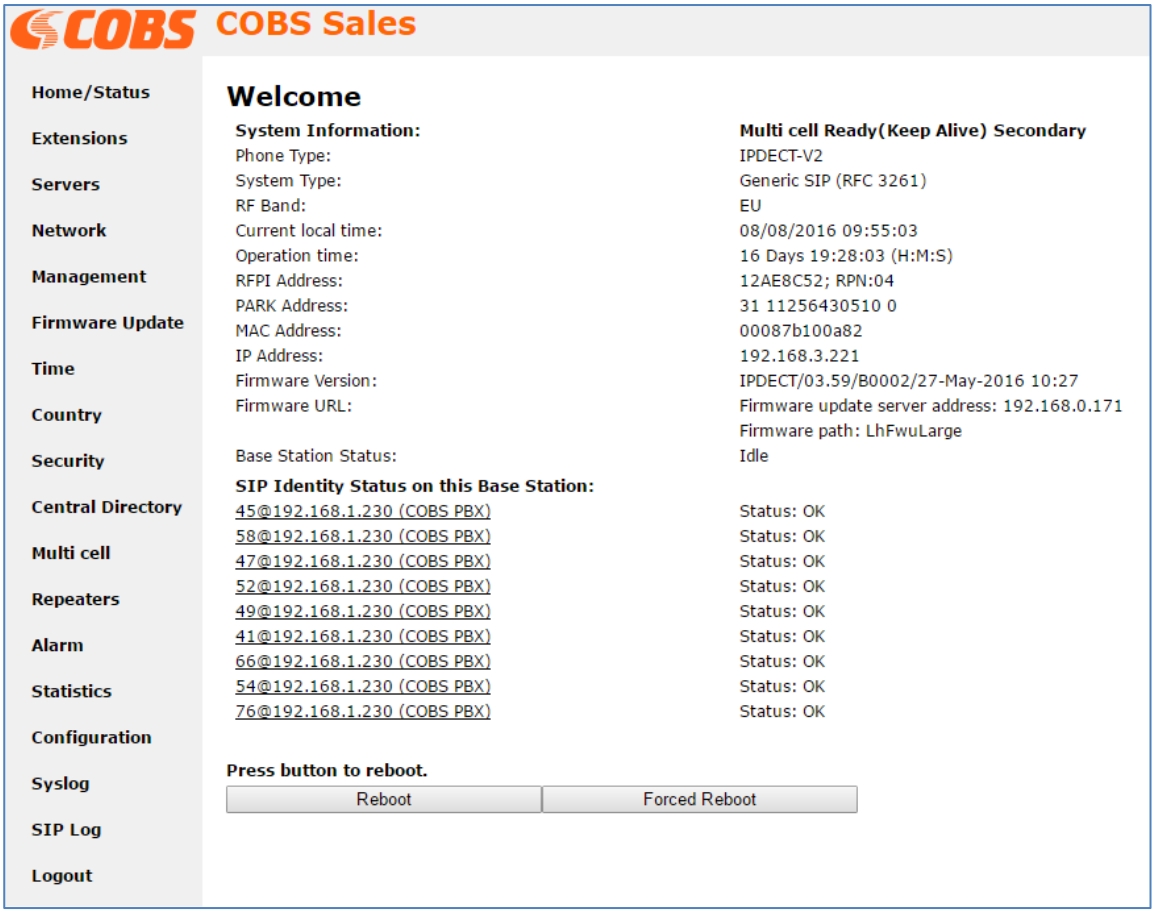
The SMART System Configuration Interface is an in-built HTTP Web Server service residing in each base station. This interface is a user friendly interface and easy to handle even to a first time user.

Note: Enabling secure web is not possible. For secure configuration use secure provisioning.

This chapter seeks to define various variables/parameters available for configuration in the network.

5.1 Web navigation

We describe the left menu in the front end of the SMART System Administration Interface.

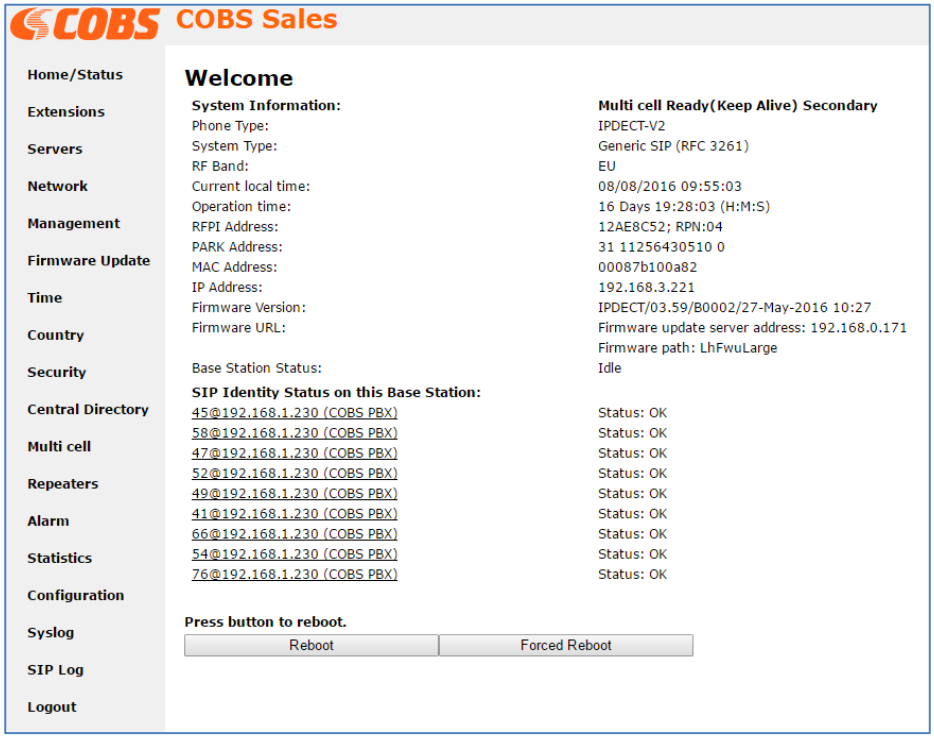


Feature	Description
Home/Status	This is the front end of the Base station's HTTP web interface. This page shows the summary of current operating condition and settings of the Base station and Handset(s).
Extensions	Administration of extensions and handsets in the system
Servers	On this page the user can define which SIP/NAT server the network should connect to.
Network	Typically the user configures the Network settings from here. **NAT provisioning**: allows configuration of features for resolving of the NAT – Network Address Translation. These features enable interoperability with most types of routers.

	DHCP: allows changes in protocol for getting a dynamic IP address. **Virtual LAN:** specifies the Virtual LAN ID and the User priority. **IP Mode:** specifies using dynamic (DHCP) or static IP address for your SME network. **IP address:** if using DHCP leave it empty. Only write in, when you use static IP address. **Subnet mask:** if using DHCP, leave it empty. Only write in, when you use static IP address. **DNS server:** specify if using DHCP, leave it empty. Only write in the DNS server address of your Internet service provider, when you use static IP address. (DNS = Dynamic Name Server) **Default gateway**: if using DHCP, leave it empty. Write in the IP address of your router, when you use static IP address.
Management	Defines the Configuration server address, Management transfer protocol, sizes of logs/traces that should be catalogued in the system, CMS messaging server interface.
Firmware Update	Remote firmware updates (HTTP(s)/TFTP) settings of Base stations and handsets.
Time	Here the user can configure the Time server. It should be used as time server in relevant country for exact time. The time servers have to deliver the time to conform to the Network Time Protocol (NTP). Handsets are synchronised to this time. Base units synchronise to the master using the Time server.
Country	Specifying the country/territory where the SMART System network is located ensures that your phone connection functions properly. Note: The base language and country setting are independent of each other.
Security	The users can administrate certificates and create account credentials with which they can log in or log out of the embedded HTTP web server.
Central Directory	Interface to common directory load of up to 3000 entries using *csv format or configuration of LDAP directory. Note: LDAP and central directory cannot operate at the same time.
Multi cell	Specify to connect base station or chain of base stations to the network. Make sure the system ID for the relevant base stations are the same otherwise the multi-cell feature will not work.
Repeaters	Administration and configuration of repeaters of the system
Alarm	**Currently not used.**
Statistics	Overview of system and call statistics for a system.
Configuration	This shows detail and complete SMART System network settings for base station(s), HTTP/DNS/DHCP/TFTP server, SIP server, etc.
Syslog	Overall network related events or logs are displayed here (only live feed is shown).
SIP Log	SIP related logs can be retrieved from url link. It is also possible to clear logs from this feature.

5.2 Home/Status

We describe the parameters found in the Welcome front end home/status of the SMART System Administration Interface.



Parameter	Description
System information	This base current multi-cell state
Phone Type	Always IPDECT-V2
System Type	This base customer configuration
RF Band	This base RF band setting. The parameter is software defined in production and relates to the radio approvals shown on the label of the base.
Current local time	This base local time
Operation time	Operation is operation time for the base since last reboot
RFPI-Address	This base RFPI address
PARK Address	This base PARK address
MAC-Address	This base MAC address
IP-Address	This base IP address
Firmware version	This base firmware version
Firmware URL	Firmware update server address and firmware path on server
Base Station Status	"Idle" : When no calls on base "In use" : When active calls on base
SIP identity status	List of extensions present at this base station. Format: "extension"@"this base IP address"("server name") followed by status to the right. Below is listed possible status: OK: Handset is ok SIP Error: SIP registration error
Reboot	Reboot after all connections is stopped on base. Connections are active calls, directory access, firmware update active
Forced Reboot	Reboot immediately.

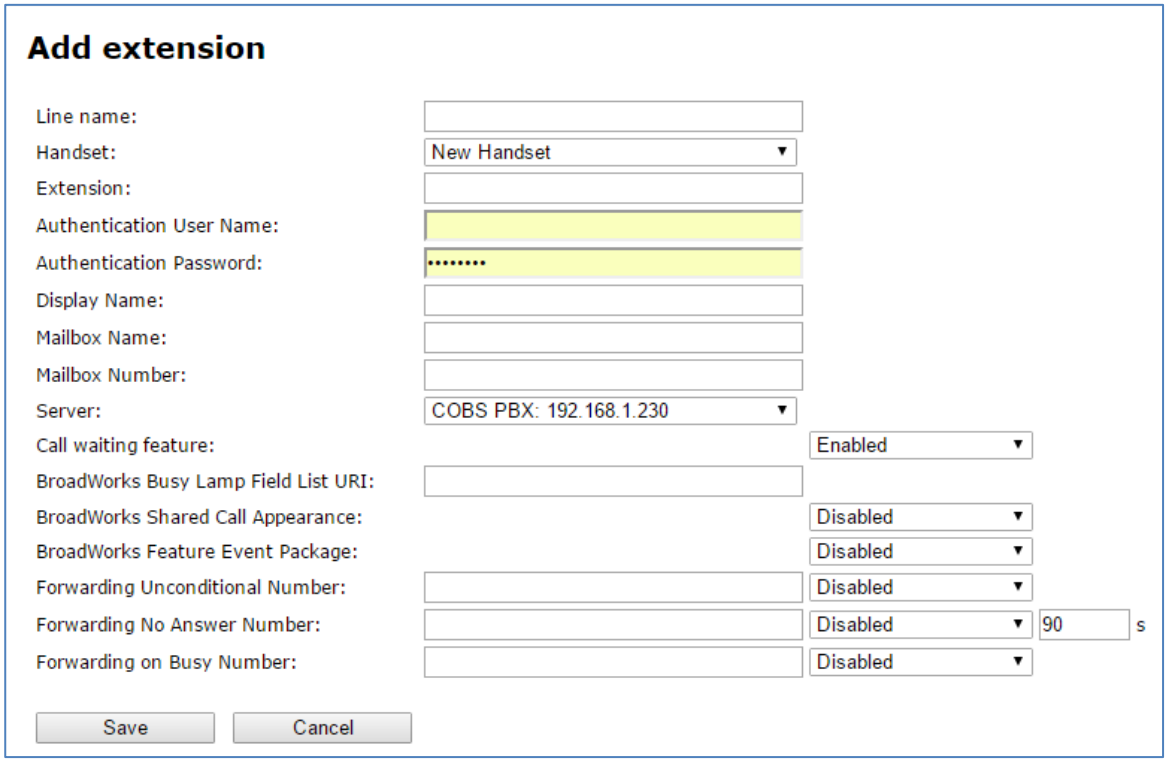
5.3 Extensions

In this section, we describe the different parameters available whenever the administrator is creating extensions for handsets. Note, it is not possible to add extensions if no servers are defined. As well the section describes the administration of extensions and handsets using the extension list and the extension list menu.

The system can handle maximum 1000 extensions matching 1000 handsets which can be divided between servers. When 1000 handsets are registered it is not possible to add more extensions. With active multiline feature the system can handle maximum 1000 extensions. With 4 active lines maximum 250 handsets can be active in the system.

Note: Within servers or even with multi servers, extensions must always be unique. This means same extension number on server 1 cannot be re-used on server 2.

5.3.1 Add extension

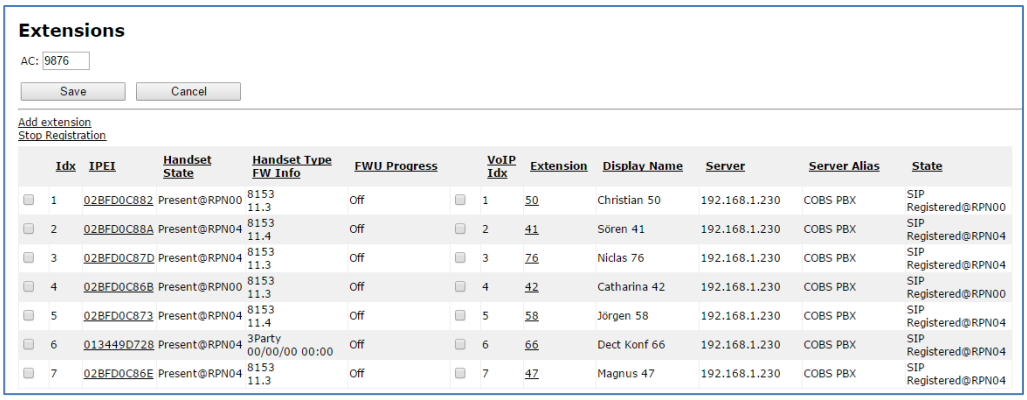


Parameter	Default Value(s)	Description
Extension	Empty	Handset phone number or SIP username depending on the setup. **Possible value(s):** 8-bit string length **Example: 1024, etc.** **Note:** The Extension must also be configured in SIP server in order for this feature to function.
Authentication User Name	Empty	**Username:** SIP authentication username **Permitted value(s):** 8-bit string length
Authentication Password	Empty	**Password:** SIP authentication password. **Permitted value(s):** 8-bit string length
Display Name	Empty	Human readable name used for the given extension **Permitted value(s):** 8-bit string length

Mailbox Name	Empty	Name of centralised system used to store phone voice messages that can be retrieved by recipient at a later time. **Valid Input(s):** 8-bit string Latin characters for the Name
Mailbox Number	Empty	Dialled mail box number by long key press on key 1. **Valid Input(s):** 0 – 9, *, # **Note: Mailbox Number parameter** is available only when it's enabled from SIP server.
Server	Server 1 IP	FQDN or IP address of SIP server. Drop down menu to select between the defined Servers of SMART System Service provider.
Call waiting feature:	Enabled	Used to enable/disable Call Waiting feature. When disabled a second incoming call will be rejected. If enabled a second call will be presented as call waiting.
Broadsoft Feature Event Package	Disabled	If enabled the given SIP extension subscribes for the Broadsoft Application Server Feature Event Package, and it becomes ready for reception of SIP NOTIFY with status on the following Broadsoft Server Services: -Do Not Disturb -Call Forwarding (Always, Busy, No answer) The received status will be displayed in the handset idle display. Reference section 5.3.2
Forwarding Unconditional Number	Empty Disabled	Number to which incoming calls must be re-routed to irrespective of the current state of the handset. Forwarding Unconditional must be enabled to function. **Note:** Feature must be enabled in the SIP server before it can function in the network
Forwarding No Answer Number	Empty Disabled 90	Number to which incoming calls must be re-routed to when there is no response from the SIP end node. Forwarding No Answer Number must be enabled to function. **Note:** Feature must be enabled in the SIP server before it can function in the network Specify delay from call to forward in seconds.
Forwarding On Busy Number	Empty Disabled	Number to which incoming calls must be re-routed to when SIP node is busy. Forwarding On Busy Number must be enabled to function. **Note:** Feature must be enabled in the SIP server before it can function in the network

5.3.1.1 Extensions list

The added extensions will be shown in the extension lists.
The list can be sorted by any of the top headlines, by mouse click on the headline link.



Extensions

AC: 9876

Save Cancel

Add extension
Stop Registration

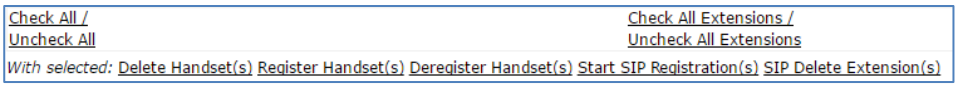
	Idx	IPEI	Handset State	Handset Type FW Info	FWU Progress		VoIP Idx	Extension	Display Name	Server	Server Alias	State
☐	1	02BFD0C882	Present@RPN00	8153 11.3	Off	☐	1	50	Christian 50	192.168.1.230	COBS PBX	SIP Registered@RPN00
☐	2	02BFD0C88A	Present@RPN04	8153 11.4	Off	☐	2	41	Sören 41	192.168.1.230	COBS PBX	SIP Registered@RPN04
☐	3	02BFD0C87D	Present@RPN04	8153 11.3	Off	☐	3	76	Niclas 76	192.168.1.230	COBS PBX	SIP Registered@RPN04
☐	4	02BFD0C86B	Present@RPN00	8153 11.3	Off	☐	4	42	Catharina 42	192.168.1.230	COBS PBX	SIP Registered@RPN00
☐	5	02BFD0C873	Present@RPN04	8153 11.4	Off	☐	5	58	Jörgen 58	192.168.1.230	COBS PBX	SIP Registered@RPN04
☐	6	013449D728	Present@RPN04	3Party 00/00/00 00:00	Off	☐	6	66	Dect Konf 66	192.168.1.230	COBS PBX	SIP Registered@RPN04
☐	7	02BFD0C86E	Present@RPN04	8153 11.3	Off	☐	7	47	Magnus 47	192.168.1.230	COBS PBX	SIP Registered@RPN04

Parameter	Description
Idx	Select / deselect for delete, register and deregister handsets
IPEI	Handset IPEI. IPEI is unique DECT identification number.
Handset State	At which base the handset is registered.
FW info	Firmware version of handset
FWU Progress	**Off:** Always set to off.
Extension	Given extension is displayed
Display Name	Given display name is displayed. If no name given this field will be empty
Server	Server IP or URL
Server Alias	Given server alias is displayed. If no alias given this field will be empty.
State	**SIP** registration state – if empty the handset is not SIP registered.

5.3.1.2 Handset and extension list top/sub-menus

The handset extension list menu is used to control paring or deletion of handset to the system (DECT registration/de-registrations) and to control SIP registration/de-registrations to the system.
Above and below the list are found commands for making operations on handsets/and extensions. The top menu is general operations, and the sub menu is always operating on selected handsets/extensions.

Add extension
Stop Registration



Check All / Uncheck All
Check All Extensions / Uncheck All Extensions
With selected: Delete Handset(s) Register Handset(s) Deregister Handset(s) Start SIP Registration(s) SIP Delete Extension(s)

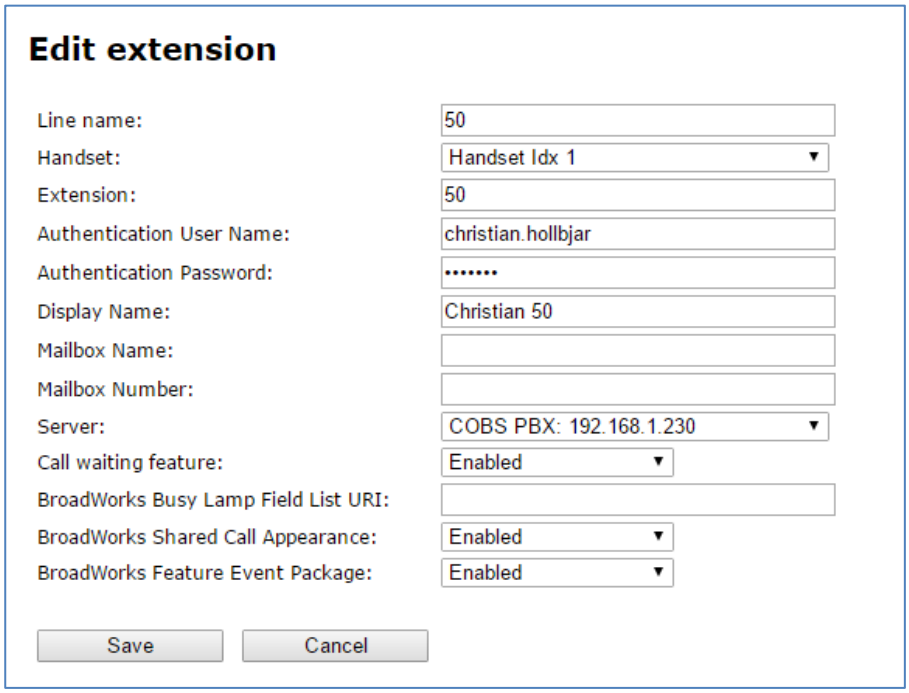
In the below table each command is described.

Actions	Description
Add extension	Access to the “Add extension” sub menu
Stop Registration	Manually stop DECT registration mode of the system. This prevents any handset from registering to the system
Delete Handset(s)	Deregister selected handset(s), but do not delete the extension(s).
Register Handset(s)	Enable registration mode for the system making it possible to register at a specific extension (selected by checkbox)
Deregister Handset(s)	Deregister the selected handset(s) and delete the extension(s).

Note: By power off the handset the handset will SIP deregister the PBX.

5.3.1.3 Edit Extension

To edit extension use the mouse to click the link of the extension.

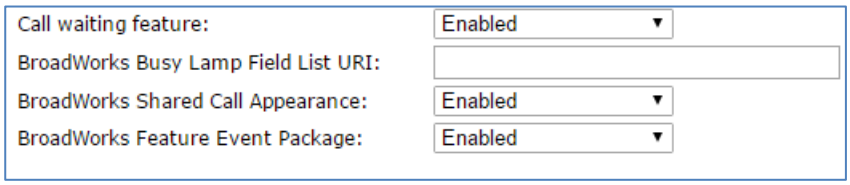


5.3.2 Broadsoft Feature Event Package

If enabled the given SIP extension subscribes for the Broadsoft Application Server Feature Event Package, and it becomes ready for reception of SIP NOTIFY with status on the following Broadsoft Server Services:
-Do Not Disturb
-Call Forwarding (Always, Busy, No answer)
The received status will be displayed in the handset idle display.

After pressing save the extension screen will appear with removed configuration option for the forward feature as shown in the below picture.

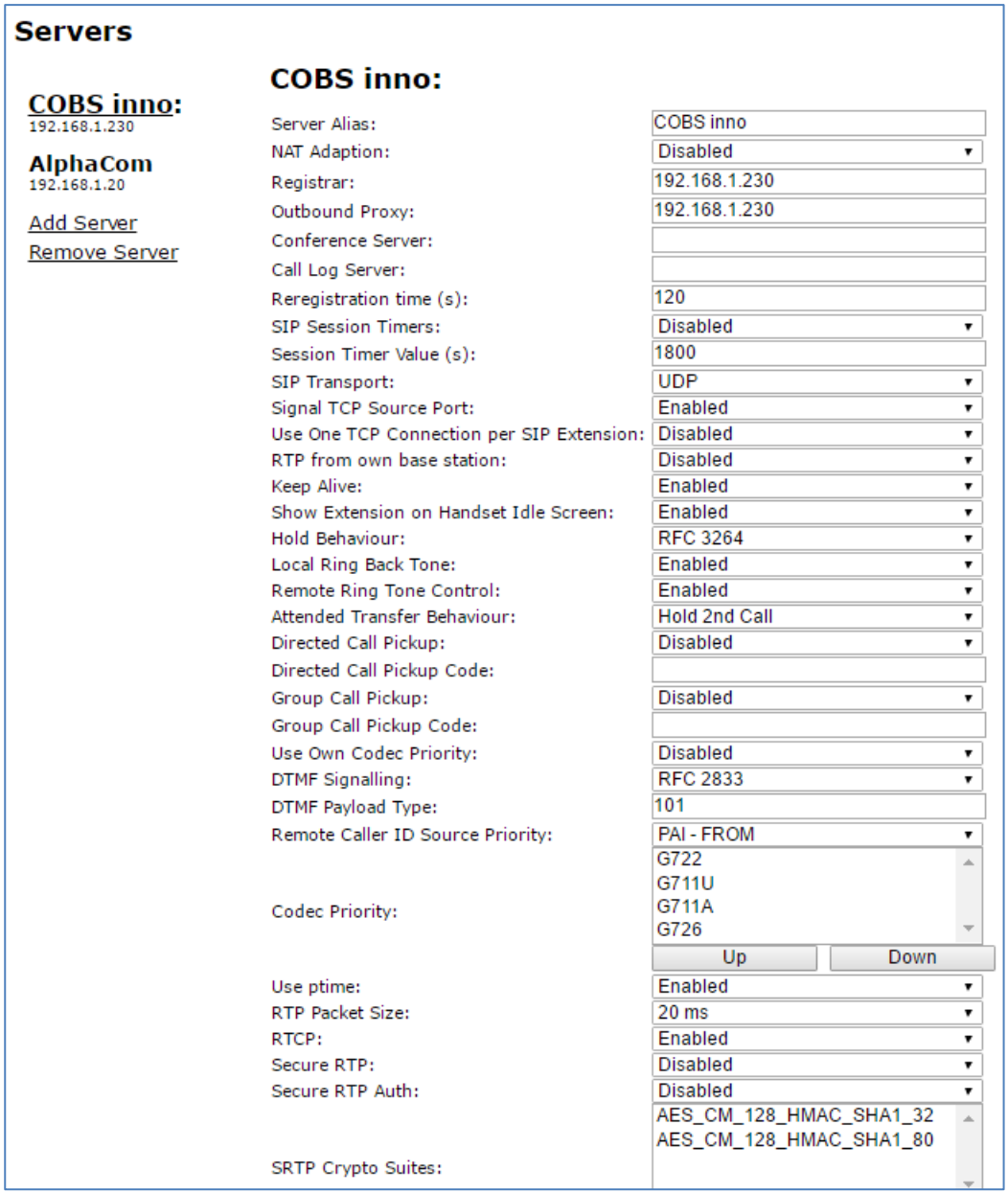
Note: Call forwarding can as well be configured from the handset by the user (for operation refer to the handset guide).



5.4 Servers

In this section, we describe the different parameters available in the Servers configurations menu. Maximum 10 servers can be configured.

Screenshot



Parameter	Default value	Description
Server Alias	Empty	Parameter for server alias
NAT Adaption	Enabled	To ensure all SIP messages goes directly to the NAT gateway in the SIP aware router.
Registrar	Empty	SIP Server proxy DNS or IP address Permitted value(s): AAA.BBB.CCC.DDD:<Port-Number> or <URL>:<Port-Number> **Note:** Specifying the Port Number is optional.
Outbound Proxy	Empty	This is a Session Border Controller DNS or IP address (OR SIP server outbound proxy address) Set the Outbound proxy to the address and port of private NAT gateway so that SIP messages sent via the NAT gateway. Permitted value(s): AAA.BBB.CCC.DDD or <URL> or <URL>:<Port-Number> Examples: “192.168.0.1”, “192.168.0.1:5062”,

		"nat.company.com" and "sip:nat@company.com:5065". If empty call is made via Registar.
Conference Server	Empty	Broadsoft conference feature. Set the IP address of the conference server. In case an IP is specified pressing handset conference will establish a connection to the conference server. If the field is empty the original 3-party local conference on 8630 is used.
Call Log Server	Empty	Broadsoft call log feature. Set the IP address of the XSI call log server. In case an IP is specified pressing handset will use the call log server. If the field is empty the local call log is used
Re-registration time	600	The "expires" value in SIP REGISTER requests. This value indicates how long the current SIP registration is valid, and hence is specifies the maximum time between SIP registrations for the given SIP account. Permitted value(s): A value below 60 sec is not recommended, Maximum value 65636
SIP Session Timers:	Disabled	RFC 4028. A "keep-alive" mechanism for calls. The session timer value specifies the maximum time between "keep-alive" or more correctly session refresh signals. If no session refresh is received when the timer expires the call will be terminated. Default value is 1800 s according to the RFC. Min: 90 s. Max: 65636. If disabled session timers will not be used.
Session Timer Values (s):	1800	Default value is 1800s according to the RFC. If disabled session timers will not be used. Permitted value(s): Minimum value 90, Maximum 65636
SIP Transport	UDP	Select UDP, TCP, TLS 1.0
Signal TCP Source Port	Disabled	When SIP Transport is set to TCP or TLS, a TCP (or TLS) connection will be established for each SIP extension. The source port of the connection will be chosen by the TCP stack, and hence the local SIP port parameter, specified within the SIP/RTP Settings (see 5.5.5) will not be used. The "Signal TCP Source Port" parameter specifies if the used source port shall be signaled explicitly in the SIP messages.
Use One TCP/TLS Connection per SIP Extension:	Disabled	When using TCP or TLS as SIP transport, choose if a TCL/TLS connection shall be established for each SIP extension or if the base station shall establish one connection which all SIP extensions use. Please note that if TLS is used and SIP server requires client authentication (and requests a client certificate), this setting must be set to disabled. 0: Disabled. (Use one TCP/TLS connection for all SIP extensions)

		1: Enabled. (Use one TCP/TLS connection per SIP extensions).
RTP from own base station:	Disabled	If disabled RTP stream will be send from the base, where the handset is located. By enable the RTP stream will always be send from the base, where the SIP registration is made. This setting is typically enabled for operation with Cisco.
Keep Alive	Enabled	This directive defines the window period (30 sec.) to keep opening the port of relevant NAT-aware router(s), etc.
Show Extension on Handset Idle Screen	Enabled	If enabled extension will be shown on handset idle screen.
Hold Behaviour	RFC 3264	Specify the hold behaviour by handset hold feature. RFC 3264: Hold is signalled according to RFC 3264, i.e. the connection information part of the SDP contains the IP Address of the endpoint, and the direction attribute is sendonly, recvonly or inactive dependant of the context RFC 2543: The ”old” way of signalling HOLD. The connection information part of the SDP is set to 0.0.0.0, and the direction attribute is sendonly, recvonly or inactive dependant of the context
Attended Transfer Behaviour	Hold 2nd Call	When we have two calls, and one call is on hold, it is possible to perform attended transfer. When the transfer soft key is pressed in this situation, we have traditionally also put the active call on hold before the SIP REFER request is sent. However, we have experienced that some PBXes do not expect that the 2nd call is put on hold, and therefore attended transfer fails on these PBXes. The "Attended Transfer Behavior" feature defines whether or not the 2nd call shall be put on hold before the REFER is sent. If "Hold 2nd Call" is selected, the 2nd call will be held before REFER is sent. If "Do Not Hold 2nd Call" is selected, the 2nd call will not be held before the REFER is sent
Use Own Codec Priority	Disabled	Default disabled. By enable the system codec priority during incoming call is used instead of the calling party priority. E.g. If base has G722 as top codec and the calling party has Alaw on top and G722 further down the list, the G722 will be chosen as codec for the call.
DTMF Signalling	RFC 2833	Conversion of decimal digits (and ‘*’ and ‘#’) into sounds that share similar characteristics with voice to easily traverse networks designed for voice SIP INFO: Carries application level data along SIP signalling path (e.g.: Carries DTMF digits generated during SIP session OR sending of DTMF tones via data

		packets in the same internet layer as the Voice Stream, etc.). RFC 2833: DTMF handling for gateways, end systems and RTP trunks (e.g.: Sending DTMF tones via data packets in different internet layer as the voice stream) Both: Enables SIP INFO and RFC 2833 modes.
DTMF Payload Type	101	This feature enables the user to specify a value for the DTMF payload type / telephone event (RFC2833).
Remote Caller ID Source Priority	FROM	SIP information field used for Caller ID source: PAI - FROM FROM ALERT_INFO - PAI - FROM
Codec Priority	G.711U G.711A G.726	Defines the codec priority that base stations uses for audio compression and transmission. Possible Option(s): G.711U,G.711A, G.726, G.729, G.722. Note: Modifications of the codec list must be followed by a “reset codes” and “Reboot chain” on the multipage in order to change and update handsets. Note: With G.722 as first priority the number of simultaneous calls per base station will be reduced from 10 (8) to 4 calls. With G.722 in the list the codec negotiation algorithm is active causing the handset (phone) setup time to be slightly slower than if G.722 is removed from the list. With G.729 add on DSP module for the base is required. Contact COBS sales for purchase number 96101203.
RTP Packet size	20ms	The packet size offered as preferred RTP packet size by 8630 when RTP packet size negotiation. Selections available: 20ms, 40ms, 60ms, 80ms
RTCP	Enabled	Real-time Transport Control Protocol is used for monitoring the quality of the established call.
Secure RTP	Disabled	With enable RTP will be encrypted (AES-128) using the key negotiated via the SDP protocol at call setup.
Secure RTP Auth	Disabled	With enable secure RTP is using authentication of the RTP packages. Note: with enabled SRTP authentication maximum 4 concurrent calls is possible per base in a single or multicell system.
SRTP Crypto Suites	AES_CM_128_HMAX_SHA1_32 AES_CM_128_HMAX_SHA1_80	Field list of supported SRTP Crypto Suites. The device is born with two suites.

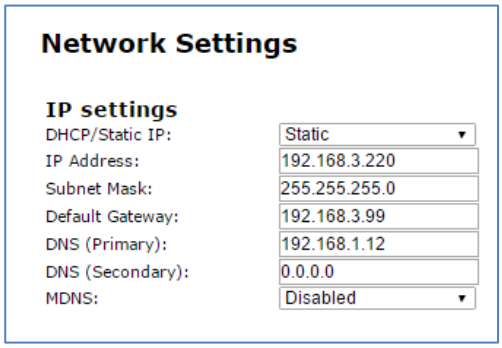
Note: Within servers or even with multi servers, extensions must always be unique. This means same extension number on server 1 cannot be re-used on server 2.

5.5 Network

In this section, we describe the different parameters available in the network configurations menu.

5.5.1 IP Settings

Screenshot



Parameter	Default Values	Description
DHCP/Static IP	DHCP	If DHCP is enabled, the device automatically obtains TCP/IP parameters. **Possible value(s):** Static, DHCP **DHCP:** IP addresses are allocated automatically from a pool of leased address. **Static IP:** IP addresses are manually assigned by the network administrator. If the user chooses DHCP option, the other IP settings or options are not available.
IP Address	NA	32-bit IP address of device (e.g. base station). 64-bit IP address will be supported in the future. **Permitted value(s): AAA.BBB.CCC.DDD**
Subnet Mask	NA	Is device subnet mask. **Permitted value(s): AAA.BBB.CCC.DDD** This is a 32-bit combination used to describe which portion an IP address refers to the subnet and which part refers to the host. A network mask helps users know which portion of the address identifies the network and which portion of the address identifies the node.
Default Gateway	NA	Device's default network router/gateway (32-bit). **Permitted value(s): AAA.BBB.CCC.DDD** e.g. **192.168.50.0** IP address of network router that acts as entrance to other network. This device provides a default route for TCP/IP hosts to use when communicating with other hosts on hosts networks.
DNS (Primary)	NA	Main server to which a device directs Domain Name System (DNS) queries. **Permitted value(s): AAA.BBB.CCC.DDD** or **<URL>** This is the IP address of server that contains mappings of DNS domain names to various data, e.g. IP address, etc. The user needs to specify this option when static IP address option is chosen.
DNS (Secondary)	NA	This is an alternate DNS server.

MDNS	Disabled	Multicast DNS for resolving DNS queries in a local network without a DNS server.

5.5.2 VLAN Settings

Enable users to define devices (e.g. Base station, etc.) with different physical connection to communicate as if they are connected on a single network segment.

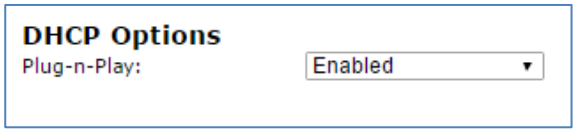
The VLAN settings can be used on a managed network with separate Virtual LANs (VLANs) for sending voice and data traffic. To work on these networks, the base stations can tag voice traffic it generates on a specific "voice VLAN" using the IEEE 802.1q specification.

Screenshot

Parameter	Default Values	Description
VLAN id	0	Is a 12 bit identification of the 802.1Q VLAN. **Permitted value(s):** 0 to 4094 (only decimal values are accepted) A VLAN ID of 0 is used to identify priority frames and ID of 4095 (i.e. FFF) is reserved. Null means no VLAN tagging or No VLAN discovery through DHCP.
VLAN User Priority	0	This is a 3 bit value that defines the user priority. Values are from 0 (best effort) to 7 (highest); 1 represents the lowest priority. These values can be used to prioritize different classes of traffic (voice, video, data, etc). **Permitted value(s):** 8 priority levels (i.e. 0 to 7)
VLAN Synchronization	Disabled	Default disabled. By enabled the VLAN ID is automatic synchronised between the bases in the chain. Bases will be automatic rebooted during the synchronization.

5.5.3 DHCP Options

Screenshot



Parameter	Default Values	Description
Plug-n-Play	Disabled	Enabled: DHCP option 66 to automatically provide PBX IP address to base.

5.5.4 NAT Settings

We define some options available when NAT aware routers are enabled in the network.

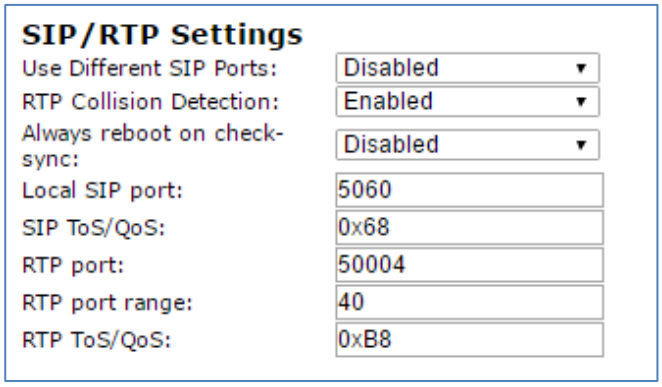
Screenshot

Parameter	Default Values	Description
Enable STUN	Disabled	Enable to use STUN
STUN Server	NA	**Permitted value(s): AAA.BBB.CCC.DDD** (Currently only Ipv4 are supported) or **url**
STUN Bind time Determine	Enabled	
STUN Bind time Guard	80	**Permitted values:** Positive integer default is 90, unit is in seconds
Enable RPORT	Disabled	Enable to use RPORT in SIP messages.
Keep alive time	90	This defines the frequency of how keep-alive are sent to maintain NAT bindings. **Permitted values:** Positive integer default is 90, unit is in seconds

5.5.5 SIP/RTP Settings

These are some definitions of SIP/RTP settings:

Screenshot

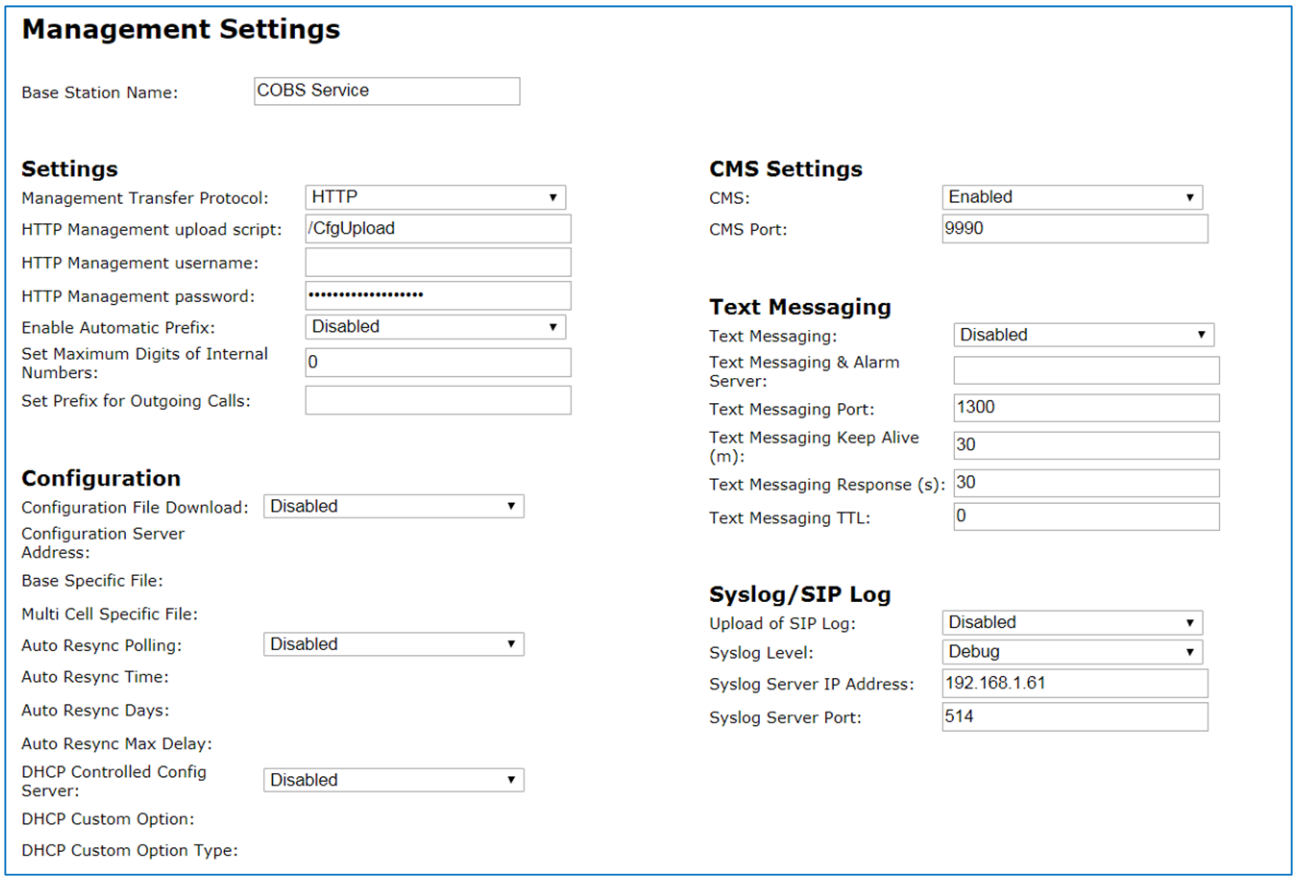


Parameter	Default Values	Description
Use Different SIP Ports	Disabled	If disabled, the Local SIP port parameter specifies the source port used for SIP signalling in the system. If enabled, the Local SIP Port parameter specifies the source port used for first user agent (UA) instance. Succeeding UA's will get succeeding ports.
RTP Collision Detection	Enabled	Enable: If two sources with same SSRC, the following RTX is discarded. Disabled: No check – device will accept all sources.

Local SIP port	5060	The source port used for SIP signalling **Permitted values:** Port number default 5060.
SIP ToS/QoS	0x68	Priority of call control signalling traffic based on both IP Layers of Type of Service (ToS) byte. ToS is referred to as Quality of Service (QoS) in packet based networks. **Permitted values:** Positive integer, default is 0x68
RTP port	50004	The first RTP port to use for RTP audio streaming. **Permitted values:** Port number default 50004 (depending on the setup).
RTP port range	40	The number of ports that can be used for RTP audio streaming. **Permitted values:** Positive integers, default is 40
RTP TOS/QoS	0xB8	Priority of RTP traffic based on the IP layer ToS (Type of Service) byte. ToS is referred to as Quality of Service (QoS) in packet based networks. See RFC 1349 for details. “cost bit” is not supported. o Bit 7..5 defines precedence. o Bit 4..2 defines Type of Service. o Bit 1..0 are ignored. Setting all three of bit 4..2 will be ignored. **Permitted values:** Positive integer, default is 0xB8

5.6 Management Settings Definitions

The administrator can configure base stations to perform some specific functions such as configuration of file transfers, firmware up/downgrades, password management, and SIP/debug logs.



Parameter	Default value	Description
Management Settings		
Base Station Name:	SME VoIP	It indicates the title that appears at the top window of the browser and is used in the multicell page. Maximum characters: 35

SETTINGS		
Management Transfer Protocol	TFTP	The protocol assigned for configuration file and central directory **Valid Input(s):** TFTP, HTTP, HTTPs
HTTP Management upload script	Empty	The folder location or directory path that contains the configuration files of the Configuration server. The configuration upload script is a file located in e.g. TFTP server or Apache Server which is also the configuration server. **Permitted value(s): /<configuration-file-directory>** **Example:** /CfgUpload **Note:** Must begin with (/) slash character. Either / or \ can be used.
HTTP Management user	Empty	Username that should be entered in order to have access to the configuration server. **Permitted value(s):** 8-bit string length

HTTP Management password	Empty	Password that should be entered in order to have access to the configuration server. **Permitted value(s):** 8-bit string length
Enable Automatic Prefix	Disabled	**Disabled**: Feature off. **Enabled**: The base will add the leading digit defined in "Set Prefix for Outgoing Calls". **Enabled + fall through on * and #:** Will enable detection of * or # at the first digit of a dialled number. In case of detection the base will not complete the dialled number with a leading 0. Examples: 1: dialed number on handset * 1234 - > dialed number to the pabx *1234 2: dialed number on handset #1234 - > dialed number to the pabx #1234 3: dialed number on handset 1234 - > dialed number to the pabx 01234
Set Maximum Digits of Internal Numbers	0	Used to detect internal numbers. In case of internal numbers no prefix number will be added to the dialled number.
Set Prefix for Outgoing Calls	Empty	Prefix number for the enabled automatic prefix feature. **Permitted value(s): 1 to 9999**

CONFIGURATION		
Configuration server address	Empty	Server/device that provides configuration file to base station. **Type:** DNS or IP address **Permitted value(s): AAA.BBB.CCC.DDD or <URL>**
Base Specific File	Empty	Base configuration file
Multi Cell Specific File	Empty	The file name must be the chain id of the system. E.g 00087b0a00b3.cfg **Permitted value(s): Format of file is chain ID.cfg**
Configuration File Download	Disabled	Base Specific file: Used when configuring a single cell base Multicell Specific File: Used when configuring a multicell based system. Base and Multicell Specific File: Used on out of factory bases to specify VLAN and Multicell ID and settings.
DHCP Controlled Config Server	Disabled	Provisioning server options. DHCP Option 66: Look for provision file by TFTP boot up server. DHCP Custom Option: Look for provision file by custom option DHCP Custom Option & Option 66: Look for provision file by first custom option and then option 66.
DHCP Custom Option	Empty	By default option 160, but custom option can be defined. An option 160 URL defines the protocol and path information by using a fully qualified domain name for clients that can use DNS.
DHCP Custom Option Type	Empty	URL: URL of server with path. Example of URL: http://myconfigs.com:5060/configs Default configuration file on server must follow the name: MAC.cfg IP Address: IP of server with path.

CMS SETTINGS

CMS:	Enabled	If messaging and alarms server should be enabled.
CMS PORT:	9990	Which port the CMS server is connected on. Defined in the CMS.

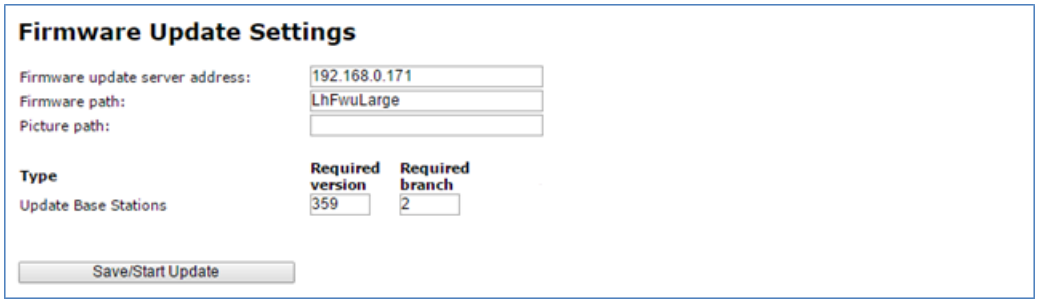
TEXT MESSAGING		
Text Messaging	Disabled	Not used
Text Messaging & Alarm server	Empty	Not used
Text Messaging Port	1300	Not used
Text Messaging Keep Alive (m)	30	Not used
Text Messaging Response (s)	30	Not used
Text Messaging TTL	0	Not used

SYSLOG/SIP LOG		
Upload of SIP Log	Disabled	Enable this option to save low level SIP debug messages to the server. The SIP logs are saved in the file format: **<MAC_Address><Time_Stamp>SIP.log**
Syslog Server IP-Address	Empty	**Permitted value(s): AAA.BBB.CCC.DDD or <URL>**
Syslog Server Port	Empty	Port number of syslog server.
Syslog Level	Off	Off: No data is saved on syslog server Normal Operation: Normal operation events are logged, incoming call, outgoing calls, handset registration, DECT location, and call lost due to busy, critical system errors, general system information. System Analyze: Handset roaming, handset firmware updates status. The system 33nalyse level also contains the messages from normal operation. Debug: Used by COBS for debug. Should not be enabled during normal operation.

There are three ways of configuring the system.
1. Manual configuration by use of the Web server in the base station(s)
2. By use of configuration files that are uploaded from a disk via the “Configuration” page on the Web server.
3. By use of configuration files which the base station(s) download(s) from a configuration server.

5.7 Firmware Update Definitions

In this page, the system administrator can configure how base stations receive their upgrade/downgrade to the relevant firmware. Handsets are upgraded from the SMART Manager. Base station firmware update status is found in the multi cell page.
In this scenario we use the built in TFTP server in the CMS.



Parameter	Default Value(s)	Description
Firmware update server address	Empty	IP address or DNS of firmware update files source **Valid Inputs:** AAA.BBB.CCC.DDD or <URL> **Example:** firmware.cobs.se or 10.10.104.41
Firmware path	LhFwuLarge	Location of firmware on server (or firmware update server path where firmware update files are located). **Example:** /East_Fwu **Note:** Must begin with (/) slash character **Use the default path when upgrading from CMS!**
Picture Path	Empty	Not used at the moment
Update Base Stations : **Required version** **Required branch**	Empty	Version and branch of firmware to be upgraded (or downgraded) on Base station. **Valid Input(s):** 8-bit string length. E.g. 280

5.8 Time Server

In this section, we describe the different parameters available in the Time Server menu.
The Time server supplies the time used for data synchronisation in a multi-cell configuration. As such it is mandatory for a multi-cell configuration. The system will not work without a time server configured. COBS provide a time server in the CMS using the SNTP process.

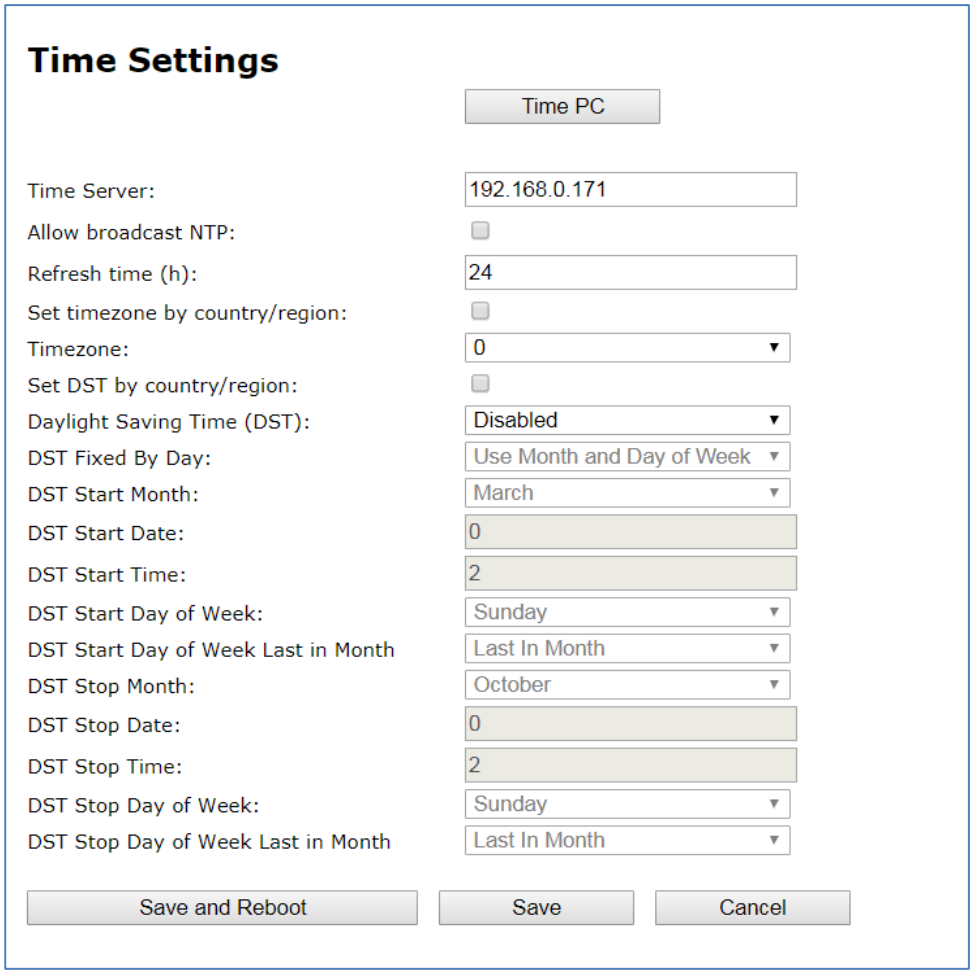
See T100360 “Inst Guide SMART Manager” for more information on best practice to set up time in the SMART System.

As well the time server is used in the debug logs and for SIP traces information pages, and used to determine when to check for new configuration and firmware files.

NOTE: It is not necessary to set the time server for standalone base stations (optional).

Press the “Time PC” button to grab the current PC time and use in the time server fields.

NOTE:
When time server parameters are modified/changed synchronisation between base stations can take up to 15 minutes before all base stations are synchronised, depending on the number of base stations in the system.

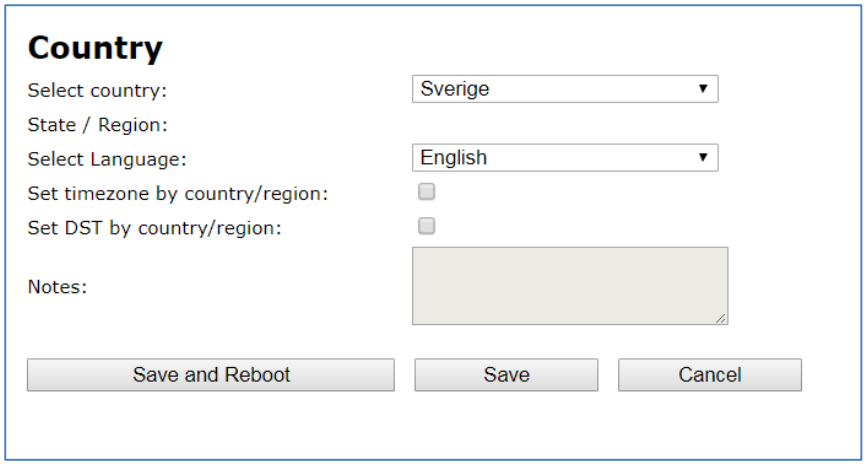


Parameter	Default Values	Description
Time Server	Empty	DNS name or IP address of NTP server. Enter the IP/DNS address of the server that distributes reference clock information to its clients including Base stations, etc. **Valid Input(s):** AAA.BBB.CCC.DDD or URL (e.g. time.server.com) Currently only Ipv4 address (32-bit) nomenclature is supported.
Allow broadcast NTP	Checked	By checked time server is used.
Refresh time (h)	Empty	The window time in hours within which time server refreshes. **Valid Inputs:** positive integer
Set timezone by country/region	Checked	By checked country setting is used (refer to country web page).
Time Zone	0	Refers to local time in GMT or UTC format. **Min:** -12:00 **Max:** +13:00
Set DST by country/region	Checked	By checked country setting is used (refer to country web page).
Daylight Saving Time (DST)	Disabled	The system administrator can Enable or Disable DST manually.

		Automatic: Enter the start and stop dates if you select Automatic.
DST Fixed By Day	Use Month and Date	You determine when DST actually changes. Choose the relevant date or day of the week, etc. from the drop down menu.
DST Start Month	March	Month that DST begins **Valid Input(s):** Gregorian months (e.g. January, February, etc.)
DST Start Date	25	Numerical day of month DST comes to effect when DST is fixed to a specific date **Valid Inputs:** positive integer
DST Start Time	3	DST start time in the day **Valid Inputs:** positive integer
DST Start Day of Week	Monday	Day within the week DST begins
DST Start Day of Week, Last in Month	Last in Month	Specify the week that DST will actually start.
DST Stop Month	October	The month that DST actually stops.
DST Stop Date	1	The numerical day of month that DST turns off. **Valid Inputs:** positive integer (1 to 12)
DST Stop Time	2	The time of day DST stops **Valid Inputs:** positive integer (1 to 12)
DST Stop Day of Week	Sunday	The day of week DST stops
DST Stop Day of Week Last in Month	First in Month	The week within the month that DST will turn off.

5.9 Country

The country setting controls the in-band tones used by the system. To select web interface language go to the management page.



Parameter	Default Values	Description
Select Country	Germany	Supported countries: Australia, Belgium, Brazil, Denmark, Germany, Spain, France, Ireland, Italia, Luxembourg, Nederland, New Zealand, Norway, Portugal, Swiss, Finland, Sweden, Turkey, United Kingdom, US/Canada, Austria

State / Region	NA	Only shown by country selection US/Canada, Australia, Brazil
Select Language	English	Web interface language. Number of available languages: English, Dansk, Italiano, Tyrkie, Deutsch, Portuguese, Hrvatski, Srpski, Slovenian, Nederlands, Francaise, Espanol, Russian, Polski.
Set time zone by country/region	checked	When checked time zone will follow country/region
Set DST by country/region	checked	When checked DST will follow country/region
Notes	Empty	Only showing notes to time setting for countries: US/Canada, Brazil

NOTE: By checked time zone and DST the parameters in web page Time will be discarded.

The following types of in-band tones are supported:

- Dial tone
- Busy tone
- Ring Back tone
- Call Waiting tone
- Re-order tone

5.10 Security

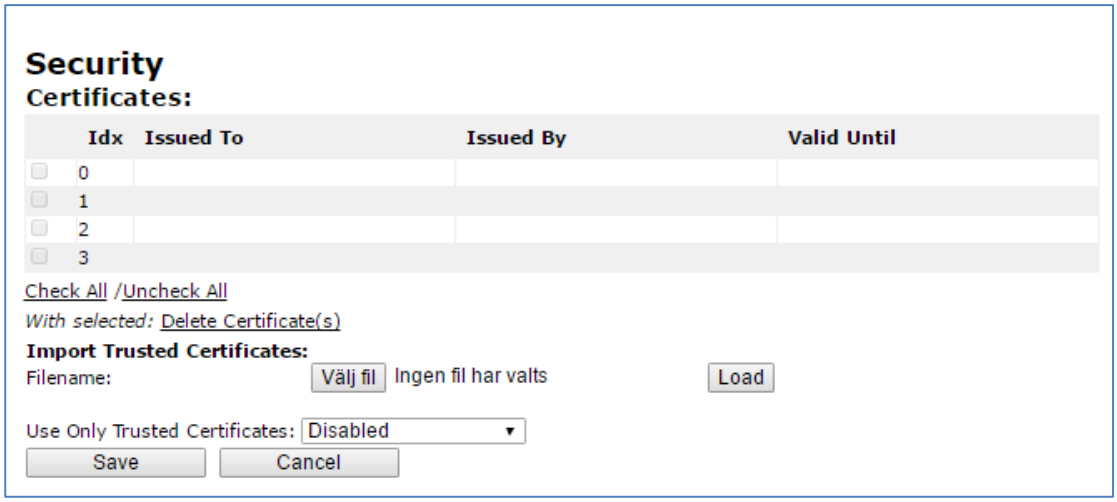
The security section is used for loading of certificates and for selecting if only trusted certificates are used. Furthermore, web password can be configured.
The Security web is divided into three sections: Certificates (trusted), SIP Client Certificates (and keys) and Password administration.

To setup secure fwu and configuration file download select HTTPs for the Management Transfer Protocol (refer to management web).

SIP and RTP security is server dependent and in order to configure user must use the web option Servers (refer to servers web).

5.10.1 Certificates

The certificates list contains the list of loaded certificates for the system. Using the left column check mark it is possible to check and delete certificates. To import a new certificate use the mouse “select file” and browse to the selected file. When file is selected, use the “Load” bottom to load the certificate.
The certificate format supported is DER encoded binary X.509 (.cer).



Certificates list

Parameter	Default Values	Description
Idx	Fixed indexes	Index number
Issued To	Empty	IP address – which is part of the certificate file
Issued To	Empty	Organisation, Company – which is part of the certificate file
Valid Until	Empty	Date Time Year – which is part of the certificate file

By enabling Use Only Trusted Certificates, the certificates the base will receive from the server must be valid and loaded into the system. If no valid matching certificate is found during the TLS connection establishment, the connection will fail. When Use Only Trusted Certificates is disabled, all certificates received from the server will be accepted.
Note: It is important to use correct date and time of the system when using trusted certificates. In case of time/date not defined the certificate validation can fail.

5.10.2 SIP Client Certificates

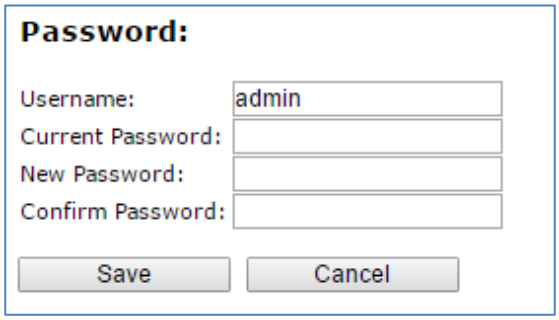
To be able to establish a TLS connection in scenarios, where the server requests a client certificate, a certificate/key pair must be loaded into the base. This is currently supported only for SIP.
To load a client certificate/key pair, both files must be selected at the same time, and it is done by pressing "select files" under "Import SIP Client Certificate and Key Pair" and then select the certificate file as well as the key file at the same time. Afterwards, press load.
The certificate must be provided as a DER encoded binary X.509 (.cer) file, and the key must be provided as a binary PKCS#8 file.

Note: Use Chrome for loading SIP Client Certificates

Screenshot

5.10.3 Password

In the below the password parameters are defined.



Parameter	Default Values	Description
Username	admin	Can be modified to any supported character and number Maximum characters: 15
Current Password	admin	Can be modified to any supported character and number
New Password	Empty	Change to new password Maximum characters: 15
Confirm Password	Empty	Confirm password to reduce accidently wrong changes of passwords

Password valid special signs: @/|<>-_:.!?*+#
Password valid numbers: 0-9
Password valid letters: a-z and A-Z

5.11 Central Directory and LDAP

The SMART System support two types of central directories, a local central directory or LDAP directory.

For both directories caller id look up is made with match for 6 digits of the phone number.

Note: Together with the SMART1 it is probably a better choice to connect directly to the central directoru from the handset.

5.11.1 Local Central Directory

Select local and save for local central directory.

Parameter	Default Values	Description

Local	Local	Drop down menu to select between local central directory and LDAP based central directory
Server	Empty	The parameter is used if directory file is located on server. **Valid Inputs:** AAA.BBB.CCC.DDD or <URL> Refer to appendix for further details.
Filename	Empty	The parameter is used if directory file is located on server. Refer to appendix for further details
Phonebook reload interval (s)	0	The parameter is controlling the reload interface of phonebook in seconds. The feature is for automatic reload the base phonebook file from the server with intervals. It is recommended to specify a conservative value to avoid overload of the base station. With default value setting 0 the reload feature is disabled.

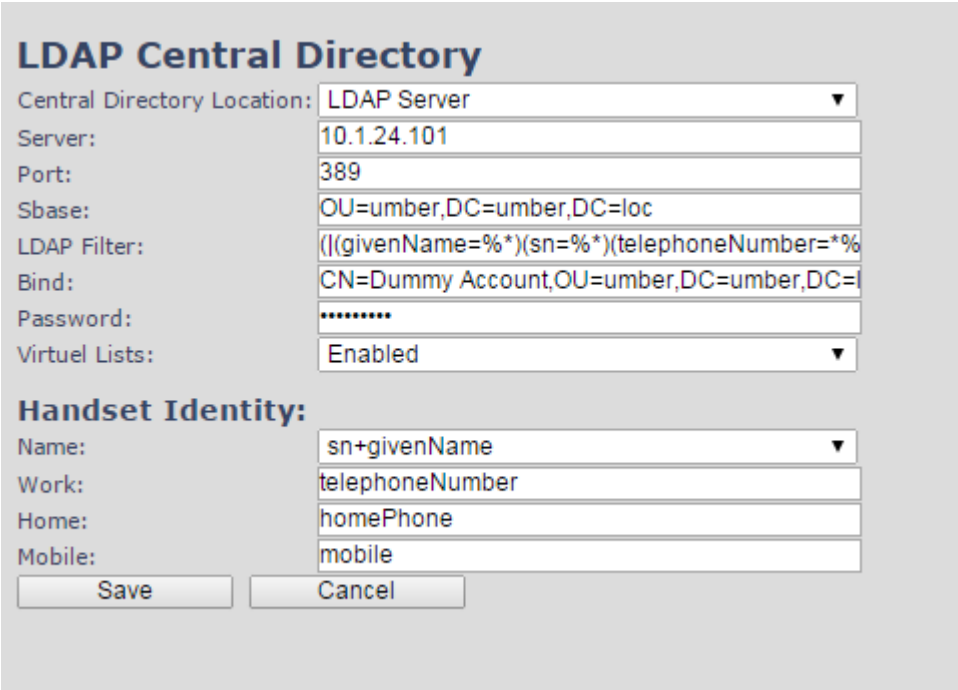
5.11.1.1 Import Central Directory

The import central directory feature is using a browse file approach. After file selection press the load button to load the file. The system support only the original *.csv format. Please note that some excel csv formats are not the original csv format. The central directory feature can handle up to 3000 contacts. For further details of the central directory feature refer to appendix.

5.11.2 LDAP

Select LDAP Server and save for LDAP server configuration.

Screenshot



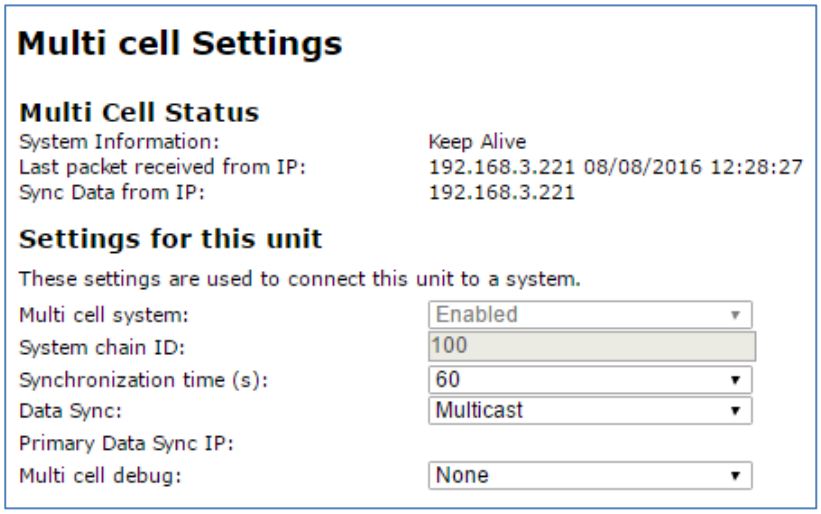
Parameter	Default Values	Description
LDAP Server	LDAP Server	Drop down menu to select between local central directory and LDAP based central directory. LDAP Server is displayed when LDAP server is selected.
Server	Empty	IP address of the LDAP server. **Valid Inputs:** AAA.BBB.CCC.DDD or <URL>
Port	Empty	The server port number that is open for LDAP connections.
Sbase	Empty	Search Base. The criteria depends on the configuration of the LDAP server. Example of the setting is CN=Users, DC=umber, DC=loc
LDAP filter	Empty	LDAP Filter is used to as a search filter, e.g. setting LDAP filter to (|(givenName=%*)(sn=%*)) the IP-DECT will use this filter when requesting entries from the LDAP server. % will be replaced with the entered prefix e.g searching on J will give the filter (|(givenName=J*)(sn=J*)) resulting in a search for given name starting with a J or surname starting with J.
Bind	Empty	Bind is the username that will be used when the IP-DECT phone connects to the server
Password	Empty	Password is the password for the LDAP Server
Virtual Lists	Disabled	By enable, virtual list searching is possible
Name	Empty	The name can be used to specify if sn+givenName or cn (common name) is return in the LDAP search results
Work Number	Empty	Work number is used to specify that LDAP attribute that will be mapped to the handset work number
Home Number	Empty	Home number is used to specify that LDAP attribute that will be mapped to the handset home number
Mobile Number	Empty	Mobile number is used to specify that LDAP attribute that will be mapped to the handset mobile number

5.12 Multi-cell Parameter Definitions

In this section, we describe the different parameters available in the Multi-cell configurations menu.

5.12.1 Settings for Base Unit

Description of Settings for Specific Base units is as follows:



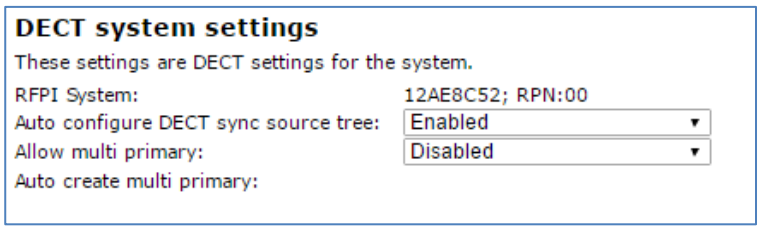
Multicell status covers status of data synchronization. The status “Keep-alive” means normal operation.

Parameter	Default values	Description
Multi cell system	Disabled	Enable this option to allow the Base unit to be set in multi-cell mode (can be set either as master or slave in the multi-cell chain system – refer to **MAC-units in Chain** section for details). **Valid Inputs:** Enable, Disable Must “save and reboot” after change from disabled to enable.
System chain ID	Empty	This is an identifier (in string format e.g. 2275) that is **unique** for a specific multi-cell system. ***The Chain ID value MUST not be equal to a used SIP account.*** The Chain ID use up a SIP account with this value **Note:** There can be several multi-cell systems in SME network. Up to 24 levels of base stations chains are permitted in a setup. **Valid Input:** The Web site allow max 5 digits in this field.
Synchronization time (s)	60 sec	This specifies the period in seconds when elements/nodes (e.g. Base units) in a specific Multi-cell will synchronise to each other. If no keep-alive packets are received within a period of 2*NETWORK_SYNC_TIME, the base will be indicated as lost in the multi cell configuration. The parameter is also used with “Auto create multi primary” feature.
Data Sync:	Multicast	To select between multicast or Peer to Peer data synchronisation mode. The multicast port range and IP addresses used is calculated from the chain id. The multicast feature uses the port range: 49200 – 49999 The multicast feature IP range: 224.1.0.0 – 225.1.0.0 Multicast uses UDP.

Primary Data Sync IP	Empty	IP of base station data sync source – the base handling the data synchronisation. Using multicast this base IP is selected automatically. **NOTE:** Using Peer to Peer mode the IP of the base used for data sync. source MUST be defined. **NOTE:** Using Peer to Peer mode with version below V306 limits the system automatic recovery feature – as there is **no** automatic recovery of the data sync. source in Peer to Peer mode.
Multi cell debug	None	Enable this feature, if you want the system to catalogue low level multi-cell debug information or traces. Options: **Data Sync:** Writes header information for all packets received and sent to be used to debug any special issues. Generates LOTS of SysLog signaling and is only recommended to enable shortly when debugging. **Auto Tree:** Writes states and data related to the Auto Tree Configuration feature. **Both:** Both Data Sync and Auto Tree are enabled. NOTE: Must only be used for debug purpose and not enabled on a normal running system

5.12.2 DECT System Settings

Description of DECT Settings for Specific Base units is as follows:



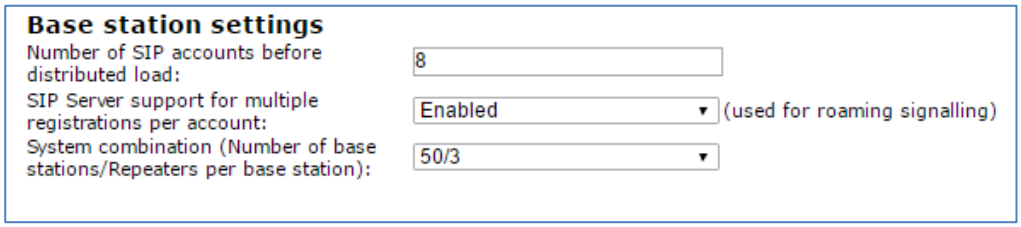
Parameter	Default values	Description
DECT system RFPI	Not able	This is a radio network identity accessed by all Base units in a specific multi-cell system. It composed of 5 octets. It is actually 5 different variables combined together. **RFPI Format:** XX XX XX XX XX (where XX are HEX values)
Allow multi primary:	Disabled	This feature is used for multi-location setups. Allows two or more primary in the same system. The two cells will be unsynchronized and handover will not be possible. “Auto Configure DECT sync source tree” must be enabled for this feature to also be enabled
Auto create multi primary:	Disabled	By enabled the system can generate cells in case a base goes into faulty mode. Two cells will only be generated in case no radio connection between the two cells is present. In order to recover the full system after establish of the faulty base, the system must be rebooted. Allow multi primary must be enabled for this feature to also be enabled.
Auto configure	Enabled	Enable this to allow the system to automatically synchronise the multi-cell chain/tree.

DECT sync source tree		NOTE: Must be enabled in order to allow a new primary recover in case the original primary goes into faulty mode.

Note: To run with a system with two separate primary in two locations “Allow multi primary” and “Auto configure DECT sync source tree” must be enabled. To add the second primary the slave must manually be configured as primary. Alternatively the “Auto create multi primary” must be enabled.

5.12.3 Base System Settings

Description of SIP Settings for Specific Base units is as follows:



Parameter	Default Values	Description
Number of SIP accounts before distributed load	8	The maximum number of handsets or SIP end nodes that are permitted to perform location registration on a specific Base unit before load is distributed to other base units. The parameter can be used to optimize the handset distribution among visible basestations. **Note:** A maximum of 8 simultaneous calls can be routed through each Base unit in a multi-cell setup. **Permitted Input:** Positive Integers (e.g. 6)
SIP Server support for multiple registrations per account	Disabled	Enable this option so it is possible to use same extension (i.e. SIP Account) on multiple phones (SIP end nodes). These phones will ring simultaneously for all incoming calls. When a phone (from a SIP account group) initiates a handover from Base X to Base Y, this phone will de-register from Base X, and register to Base Y after a call. **Note:** Choose **Yes** when the SIP server supports this feature otherwise choose **No** for the Sip server does not support this feature. **Permitted Input:** Yes, No

5.12.4 Base Station Group

The Base station group list various parameter settings for base stations including chain level information.

Base Station Group

	ID	RPN	Version	MAC Address	IP Address	IP Status	DECT sync source	DECT property	Base Station Name
☐	0	00	359.2	00087B100A4F	192.168.3.220	This Unit	Primary:RPN04 (-47dBm ▾	Locked	COBS Service
☐	1	04	359.2	00087B100A82	192.168.3.221	Connected	Select as primary ▾	**Primary**	COBS Sales

Check All /Uncheck All

With selected: Remove from chain

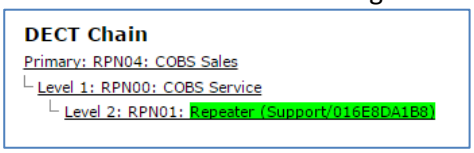
Parameters	Description
ID	Base unit identity in the chained network. **Permitted Output:** Positive Integers
RPN	The Radio Fixed Part Number is an 8-bit DECT cell identity allocated by the installer. The allocated RPN within the system must be geographically unique. **Permitted Output:** 0 to 255 (DEC) **OR** 0x00 to 0xFF (HEX)
Version	Base station current firmware version. **Permitted Output:** positive Integers with dot (e.g. 273.1)
MAC Address	Contains the hardware Ethernet MAC address of the base station. It varies from Base station to Base stations.
IP Status	Current Base station behaviour in the SME network. **Possible Outputs** **Connected:** The relevant Base station(s) is online in the network **Connection Loss:** Base station unexpectedly lost connection to network **This Unit:** Current Base station whose http Web Interface is currently being accessed
DECT Sync source	With setting "Auto configure DECT sync source tree" set to Enable, this three will automatically be generated. If manual configured the administrator should choose the relevant "multi cell chain" level its wants a specific Base unit be placed. Maximum number of "multi-cell chain" levels is 24. Format of the selection: "AAAAAxx: RPNyy (-zz dBm)" AAAAA: indication of sync. source for the base. Can be "Primary" or "Level xx" xx: Sync. source base sync. level yy: Sync. source base RPN zz: RSSI level of sync. source base seen from the actual base "(Any) RPN": When a base is not synchronized to other base. State after reboot of chain.
Dect Property	Base station characteristics in connection to the current multi cell network. **Possible Output(s)** **Primary:** Main Base station unto which all other nodes in the chain synchronises to. **Locked:** The Base unit is currently synchronized and locked to the master Base unit. **Searching:** Base unit in the process of locating to a Master/slave as specified in DECT sync source **Free Running:** A locked Base unit that suddenly lost synchronisation to the Master.

	Unknown: No current connection information from specific Base unit **Assisted lock:** Base has lost DECT sync. source and Ethernet is used for synchronization **Sync. Lost:** Handset has an active DECT connection with the base. But the base has lost DECT sync. source connection. The base will stay working as long as the call is active and will go into searching mode when call is stopped.
Base Station Name	Name from management settings.

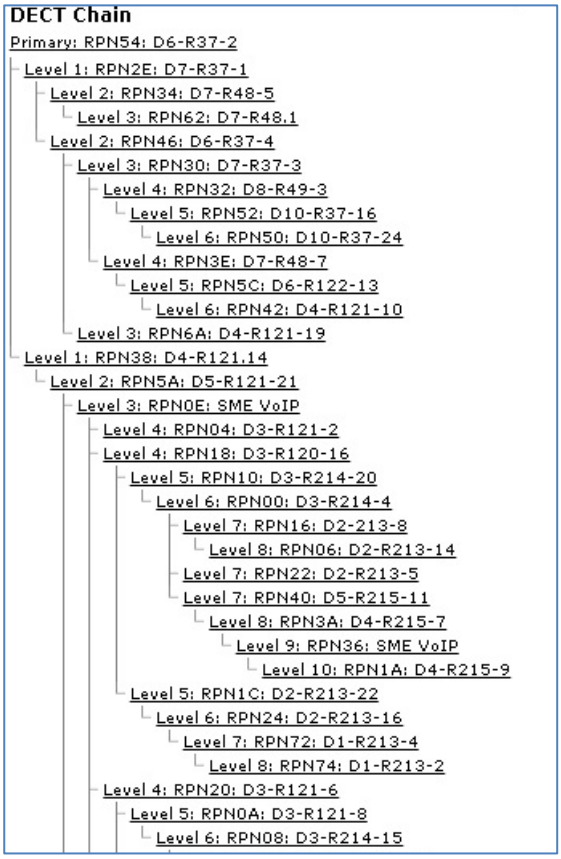
5.12.5 DECT Chain

Below the Base Group Table is the DECT Chain tree. The DECT Chain tree is a graphical presentation of the Base Group table levels and connections. Repeaters are shown with green highlight.

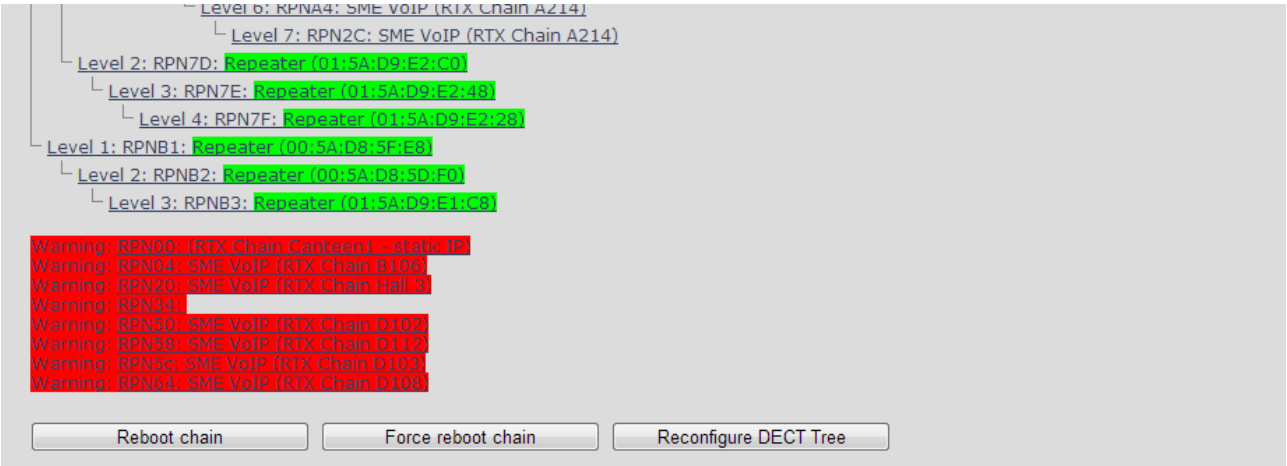
DECT Chain tree of above configuration (note repeaters is still not supported)



Screenshot: Example of part of DECT Chain tree



Screenshot: Example of part of DECT Chain tree with units in Base Group but not in tree by various reasons.



When a base or repeater has not joined the tree it will be shown with read background below the tree.

5.13 Repeaters (not supported)

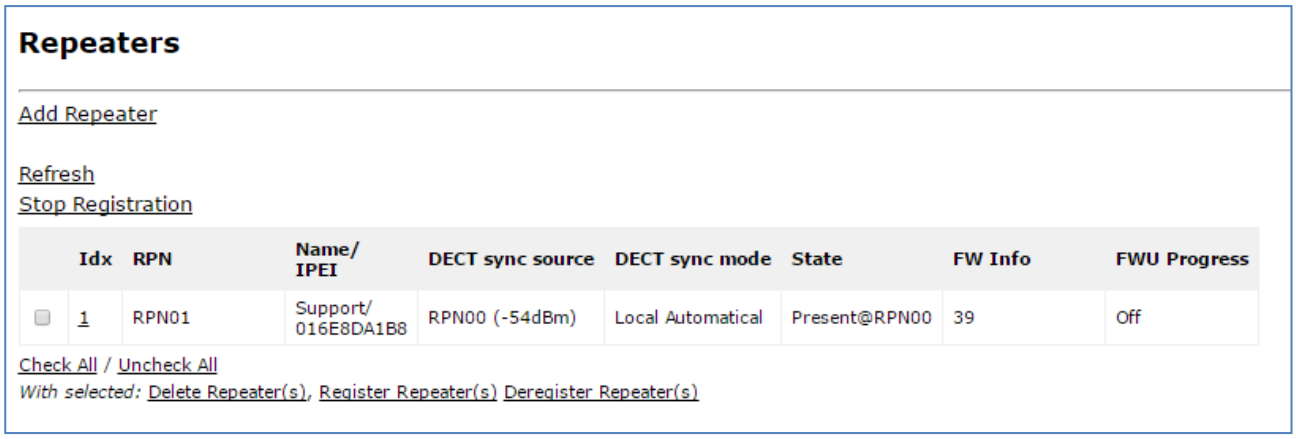
Repeaters are currently not supported in the system.

Within this section we describe the repeater parameters for future use.

5.13.1 Add repeater

From repeaters web select “Add Repeater”

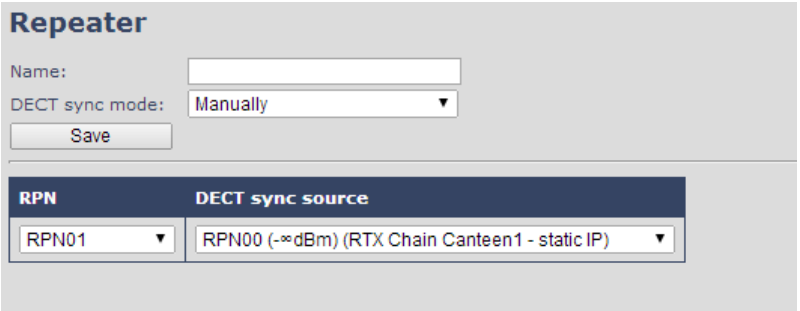
Screenshot



Then select “DECT Sync mode”

Screenshot

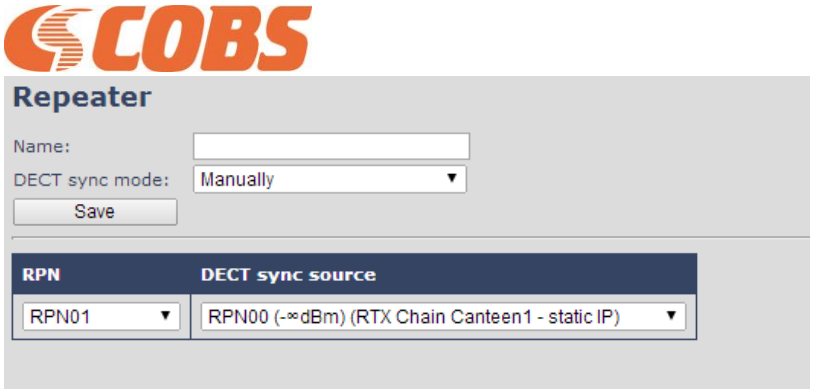
Parameters	Description
Name	Repeater name. If no name specified the field will be empty
DECT sync mode	**Manually:** User controlled by manually assign “Repeater RPN” and “DECT sync source RPN” **Local Automatical:** Repeater controlled by auto detects best base signal and auto assign RPN.



5.13.1.1 Manually

User controlled by manually assign “Repeater RPN” and “DECT sync source RPN”. The parameters are selected from the drop down menu.

Screenshot



Parameters	Description
Idx	System counter
RPN	**SINGLE CELL SYSTEM:** The base has always RPN00, first repeater will then be RPN01, second repeater RPN02 and third RPN03 (3 repeaters maximum per base) **MULTI CELL SYSTEM:** Bases are increment by 2^2 in hex, means first base RPN00 second base RPN04 etc., in between RPN01, 02, 03 addressed for repeaters at Primary base and 05, 06, 07 addressed for Secondary base (3 repeaters maximum per base)
DECT sync source	Select the base or repeater the repeater has to be synchronized to.

5.13.1.2 Local Automatical

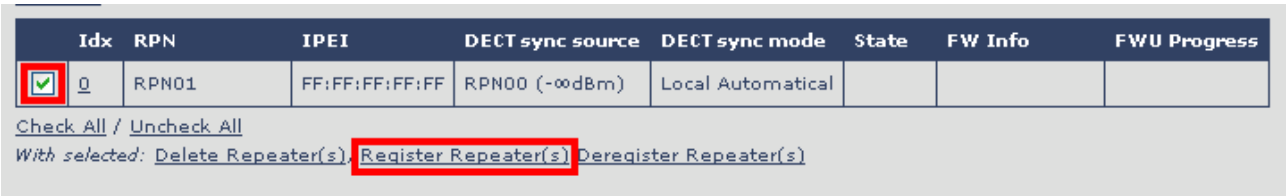
Repeater controlled by auto detects best base signal and auto assign RPN. The RPN and DECT sync source are greyed out.

The repeater RPN is dynamic assigned in base RPN range.
With local automatical mode repeater on repeater (chain) is not supported.

5.13.2 Register Repeater

Adding a repeater makes it possible to register the repeater. Registration is made by select the repeater and pressing register repeater. The base window for repeater registration will be open until the registration is stopped. By stopping the registration all registration on the system will be stopped inclusive handset registration.

Picture 54



5.13.3 Repeaters list

Repeaters

Add Repeater

Refresh
Stop Registration

	Idx	RPN	Name/ IPEI	DECT sync source	DECT sync mode	State	FW Info	FWU Progress
☐	0	RPN01	Office A100/ 005AD85FB0	RPN00 (-26dBm)	Manually	Present@RPN00	39	Off
☐	1	RPN02	Office B120/ 005AD85D90	RPN01 (-34dBm)	Manually	Present@RPN00	39	Off
☐	2	RPN03	Office D130/ 015AD85E80	RPN02 (-34dBm)	Manually	Present@RPN00	39	Off

Check All / Uncheck All
With selected: Delete Repeater(s), Register Repeater(s) Deregister Repeater(s)

Parameters	Description
IDx	Repeater unit identity in the chained network. **Permitted Output:** Positive Integers
RPN	The Radio Fixed Part Number is an 8-bit DECT cell identity allocated by the installer. The allocated RPN within the SME must be geographically unique. **Permitted Output:** 0 to 255 (DEC) **OR** 0x00 to 0xFF (HEX)
Name/IPEI	Contains the name and the unique DECT serial number of the repeater. If name is given the field will be empty.
DECT sync Source	The "multi cell chain" connection to the specific Base/repeater unit. Maximum number of chain levels is 24. Sync. source format: "RPNyy (-zz dBm)" yy: RPN of source zz: RSSI level seen from the actual repeater
DECT sync Mode	**Manually:** User controlled by manually assign "Repeater RPN" and "DECT sync source RPN" **Local Automatical:** Repeater controlled by auto detects best base signal and auto assign RPN. **Chaining Automatical:** Base controlled by auto detects best base or repeater signal and auto assign RPN. This feature will be supported in a future version
State	Present@unit means connected to unit with RPN yy
FW info	Firmware version
FWU Progress	Possible FWU progress states: **Off:** Means sw version is specified to 0 = fwu is off **Initializing:** Means FWU is starting and progress is 0%. **X% :** FWU ongoing **Verifying X%:** FWU writing is done and now verifying before swap "**Conn. term. wait**" (Repeater): All FWU is complete and is now waiting for connections to stop before repeater restart. **Complete HS/repeater:** FWU complete **Error:** Not able to fwu e.g. file not found, file not valid etc

5.14 Alarm (Currently not used)

These settings is for future use and is currently not supported.

5.15 Statistics

The statistic feature is divided into four administrative web pages, which can be access from any base.

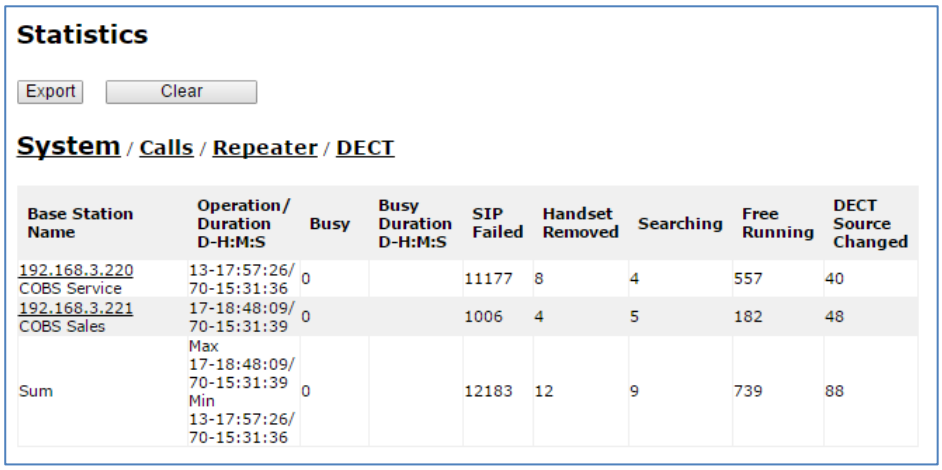
1. System
2. Calls
3. Repeater
4. DECT data

All four views have an embedded export function, which export all data to comma separated file.
By pressing the clear button all data in the full system is cleared.

5.15.1 System data

The system data web is access by pressing the menu Statistics and the data is organised in a table as shown in below example.

Screenshot



Statistics

Export Clear

System / Calls / Repeater / DECT

Base Station Name	Operation/ Duration D-H:M:S	Busy	Busy Duration D-H:M:S	SIP Failed	Handset Removed	Searching	Free Running	DECT Source Changed
192.168.3.220 COBS Service	13-17:57:26/ 70-15:31:36	0		11177	8	4	557	40
192.168.3.221 COBS Sales	17-18:48:09/ 70-15:31:39	0		1006	4	5	182	48
Sum	Max 17-18:48:09/ 70-15:31:39 Min 13-17:57:26/ 70-15:31:36	0		12183	12	9	739	88

The table is organised with headline row, data pr. base rows and with last row containing the sum of all base parameters.

Parameters	Description
Base Station Name	Base IP address and base station name from management settings
Operation/Duration D-H:M:S	Operation is operation time for the base since last reboot. Duration is the operation time for the base since last reset of statistics, or firmware upgrade.
Busy	Busy Count is the number of times the base has been busy.
Busy Duration D-H:M:S	Busy duration is the total time a base has been busy for speech (8 or more calls active).
SIP Failed	Failed SIP registrations count the number of times a SIP registration has failed
Handset Removed	Handset removed count is the number of times a handset has been marked as removed
Searching	Base searching is the number of times a base has been searching for it's sync source
Free Running	Base free running is the number of times a base has been free running
DECT Source Changed	Number of time a base has changed sync source

5.15.2 Call data

Screenshot

Statistics

Export Clear

System / **Calls** / Repeater / DECT

Base Station Name	Operation/ Duration D-H:M:S	Count	Dropped	No Response	Duration D-H:M:S	Active	Max Active	Codec G711U: G711A: G722: G726:	Handover Success	Handover Failed	Audio Not Detected
192.168.3.220 COBS Service	13-17:58:21/ 70-15:32:32	631	1	4	1-02:22:16	0	5	0:30:0:0	215	36	631
192.168.3.221 COBS Sales	17-18:48:09/ 70-15:32:35	666	3	19	8-10:59:52	0	6	0:61:0:0	244	101	666
Sum	Max 17-18:48:09/ 70-15:32:35 Min 13-17:58:21/ 70-15:32:32	1297	4	23	9-13:22:08	0	11	0:91:0:0	459	137	1086

The table is organised with headline row, data pr. base rows and with last row containing the sum of all base parameters.

Parameters	Description
Base Station Name	Base IP address and base station name from management settings
Operation time/Duration	Total operation time for the base since last reboot or reset Duration is the time from data was cleared or system has been firmware upgraded.
Count	Counts number of calls on a base.
Dropped	Dropped calls are the number of active calls that was dropped. E.g. if a user has an active call and walks out of range, the calls will be counted as a dropped call. An entry is stored in the syslog when a call is dropped.
No response	No response calls is the number of calls that have no response, e.g. if a external user tries to make a call to a handset that is out of range the call is counted as no response. An entry is stored in the syslog when a call is no response.
Duration	Call duration is total time that calls are active on the base.
Active	Active call shows how many active calls that are active on the base (Not active DECT calls, but active calls). On one base there can be up to 30 active calls.
Max Active	Maximum active calls are the maximum number of calls that has been active at the same time.
Codecs	Logging and count of used codec types on each call.
Handover Success	Counts the number of successful handovers.
Handover Failed	Counts the number of failed handovers.

5.15.3 Repeater data

Statistics

Export Clear

System / Calls / **Repeater** / DECT

Idx/ Name	Operation D-H:M:S	Busy	Busy Duration D-H:M:S	Max Active	Searching	Recovery	DECT Source Changed	Wide Band	Narrow Band
1/ Support	48-00:32:46	1643	0-00:51:18	12	3	0	0	4457	35739
Sum	48-00:32:46	1643	0-00:51:18	12	3	0	0	4457	35739

The table is organised with headline row, data pr. base rows and with last row containing the sum of all base parameters.

Parameters	Description
Idx/Name	Base IP address and base station name from management settings
Operation D-H:M:S	Total operation time for the repeater since last reboot or reset Duration is the time from data was cleared or system has been firmware upgraded.
Busy	Busy Count is the number of times the repeater has been busy.
Busy Duration D-H:M:S	Busy duration is the total time a repeater has been busy for speech (5 or more calls active).
Max Active	Maximum active calls are the maximum number of calls that has been active at the same time.
Searching	Repeater searching is the number of times a repeater has been searching for it's sync source
Recovery	In case the sync source is not present anymore the repeater will go into lock on another base or repeater and show recovery mode
DECT Source Changed	Number of time a repeater has changed sync source
Wide Band	Number of wideband calls on repeaters
Narrow Band	Number of narrow band calls on repeaters

5.15.4 DECT data

The DECT data is organised in a table as shown in below example.

Statistics

Export Clear

System / Calls / Repeater / **DECT**

	Slot0	Slot1	Slot2	Slot3	Slot4	Slot5	Slot6	Slot7	Slot8	Slot9	Slot10	Slot11
Frequency0	4309	2674	3911	2635	3371	2697	2972	2493	2608	2303	2249	2070
Frequency1	3502	1496	3007	1636	2114	1491	2110	1489	2393	2029	1835	1232
Frequency2	4116	1845	3507	2080	2817	2071	2270	1941	2037	1838	1805	1307
Frequency3	3629	1727	3191	1942	2394	1785	2326	1693	2453	2134	2067	1408
Frequency4	4215	1817	3474	1962	2687	1936	2167	1955	2007	1709	1753	1326
Frequency5	3478	1868	3188	1938	2443	1762	2274	1767	2476	2166	2091	1489
Frequency6	3924	1759	3410	1848	2522	1837	2063	1686	1853	1583	1690	1224
Frequency7	3414	1625	3114	1823	2316	1709	2276	1772	2401	2122	2032	1394
Frequency8	3407	1493	3020	1722	2390	1665	1986	1547	1649	1594	1559	1162
Frequency9	3681	2231	3429	2274	2883	2235	2709	2205	2891	2609	2621	1943

Please note 3 frequencies are manually removed in the example system.

5.16 Settings – Configuration File Setup

This page provides non editable information showing the native format of entire SMART System Configuration parameter settings. The **settings** format is exactly what is used in the configuration file. The configuration file is found in the TFTP server.
The filename for the configuration server is **<MAC_Address>.cfg**. The configuration file is saved in the folder **/Config** in the TFTP sever.

There are three ways to edit the configuration file or make changes to the **settings** page:

1) Using the WEB GUI to make changes. Each page of the HTTP web interface is a template for which the user can customise settings in the configuration file.
2) **Retrieving the relevant configuration file from the TFTP and modify and enter new changes. This should be done with an expert network administrator.**
3) Navigate to the settings page of the WEB GUI interface > copy the contents of settings > save them to any standard text editor e.g. notepad > modify the relevant contents, make sure you keep the formatting intact > Save the file as **<Enter_MAC_Address_of_RFP>.cfg** > upload it into the relevant TFTP server.

For details refer to [3].

An example of contents of settings is as follows:

```
~RELEASE=UMBER_FP_V0054
%GMT_TIME_ZONE%:16
%COUNTRY_VARIANT_ID%:18
%FWU_POLLING_ENABLE%:0
%FWU_POLLING_MODE%:0
%FWU_POLLING_PERIOD%:86400
%FWU_POLLING_TIME_HH%:3
%FWU_POLLING_TIME_MM%:0
%DST_ENABLE%:2
%DST_FIXED_DAY_ENABLE%:0
%DST_START_MONTH%:3
%DST_START_DATE%:1
....
....
```

5.17 Sys log

This page shows live feed of system level messages of the current base station. The messages the administrator see here depends on what is configured at the Management settings. The Debug logs can show only **Boot Log** or **Everything** that is all system logs including boot logs.
The Debug log is saved in the file format **<Time_Stamp>b.log** in a relevant location in the TFTP server as specified in the upload script.
To dump the log simply copy and page the full contents.

5.18 SIP Logs

This page shows SIP server related messages that are logged during the operation of the SME system.

The full native format of SIP logs can be added to the syslog.

NOTE!
Adding SIP logs to the syslog will add a lot of data to the syslog and should only be activated during debug and troubleshooting!

To dump the log simply copy and page the full contents.

6 Setting up a Multi-cell system, best practice

This chapter seeks to describe how to install, add and synchronize one or multiple base stations to the network. There are two main procedures involved:

1) Proper placement of the base stations (which is called network dimensioning). The present chapter does not address this issue.
2) Creating and adding base station profiles to the network via the SME Configuration Tool (to form a multi-cell system).

This chapter describes the second procedure.

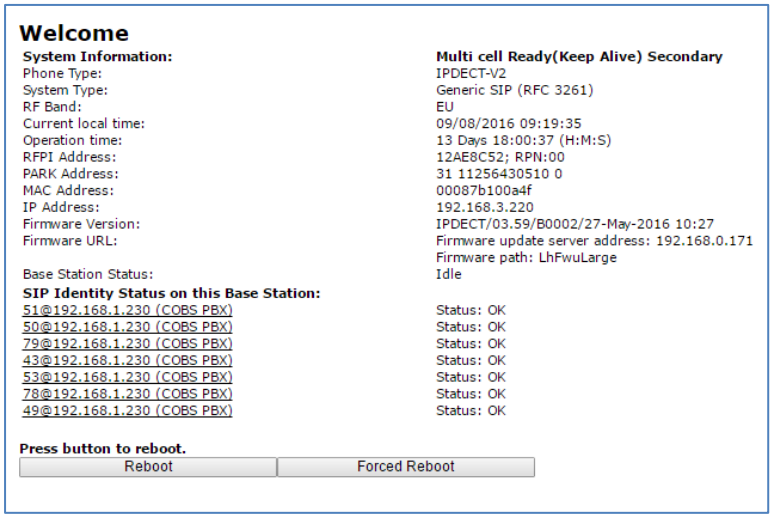
6.1 Adding Base stations

Here are the recommended steps to add Base stations to network:

STEP 1 Connect the Base station to a private network via standard Ethernet cable (CAT-5).

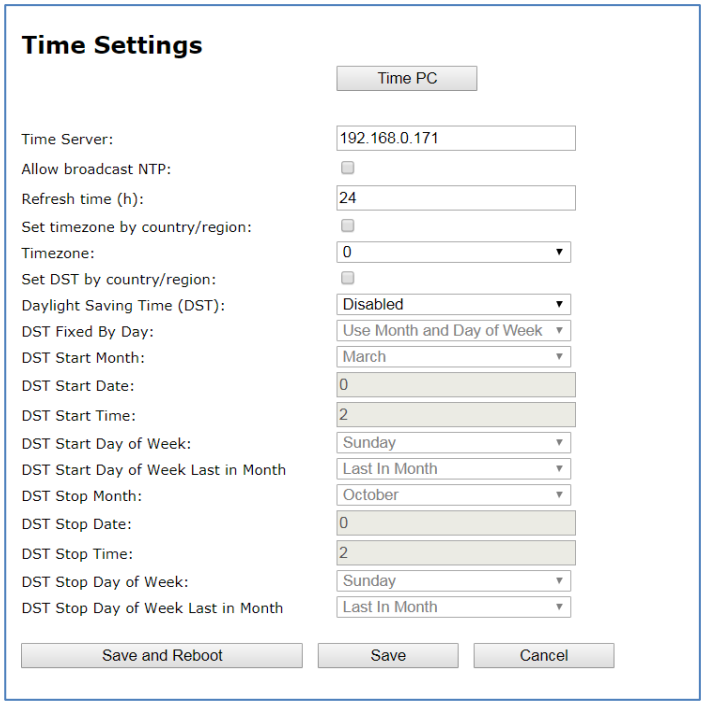
STEP 2 Open browser on the computer and type in the IP address of the base (Given to the base by the DHCP-server). Press "Enter" to access the base Login to base station.

STEP 3 Once you have authenticated, the browser will display front end of the SME Configuration Interface. The front end will show relevant information of the base station.



6.1.1 Time Server Setup

STEP 4 Navigate to the Time settings and configure it. Scroll on the left column and click on **Time** link to open the **Time Settings** Page. Enter the relevant parameters on this page and press the **Save and Reboot** button.
Make sure there is contact to the "Time server" otherwise the Multi-cell feature will not work. The CMS can be used as a timeserver with the correct license.
You can verify whether the Time server is reachable after rebooting the base station by verifying the correct Time Server IP address is still in place.



6.1.2 SIP Server (or PBX Server) Setup

STEP 5 Create the relevant SIP server (or PBX Server) information in the system. Each service provider/customer should refer SIP server vendor information on how to setup SIP servers.

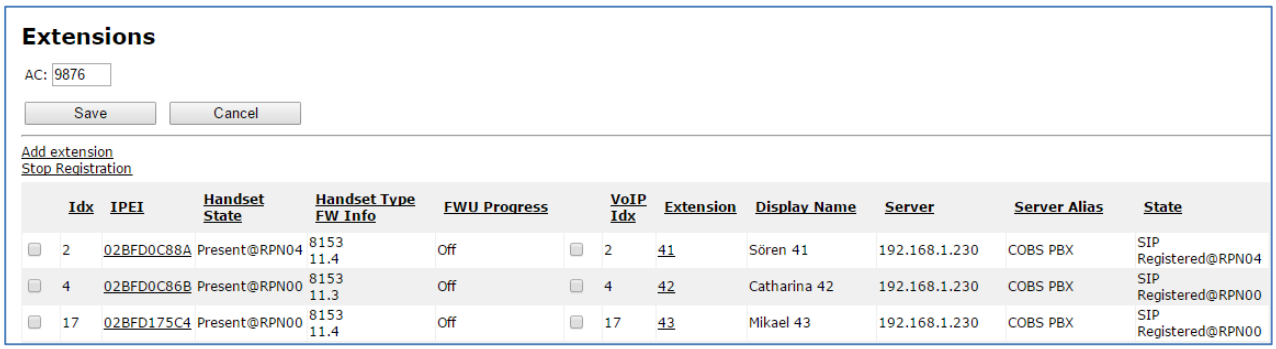
Click the link "**Server"** at the left hand column of home page, you can add your SIP server for base station use.

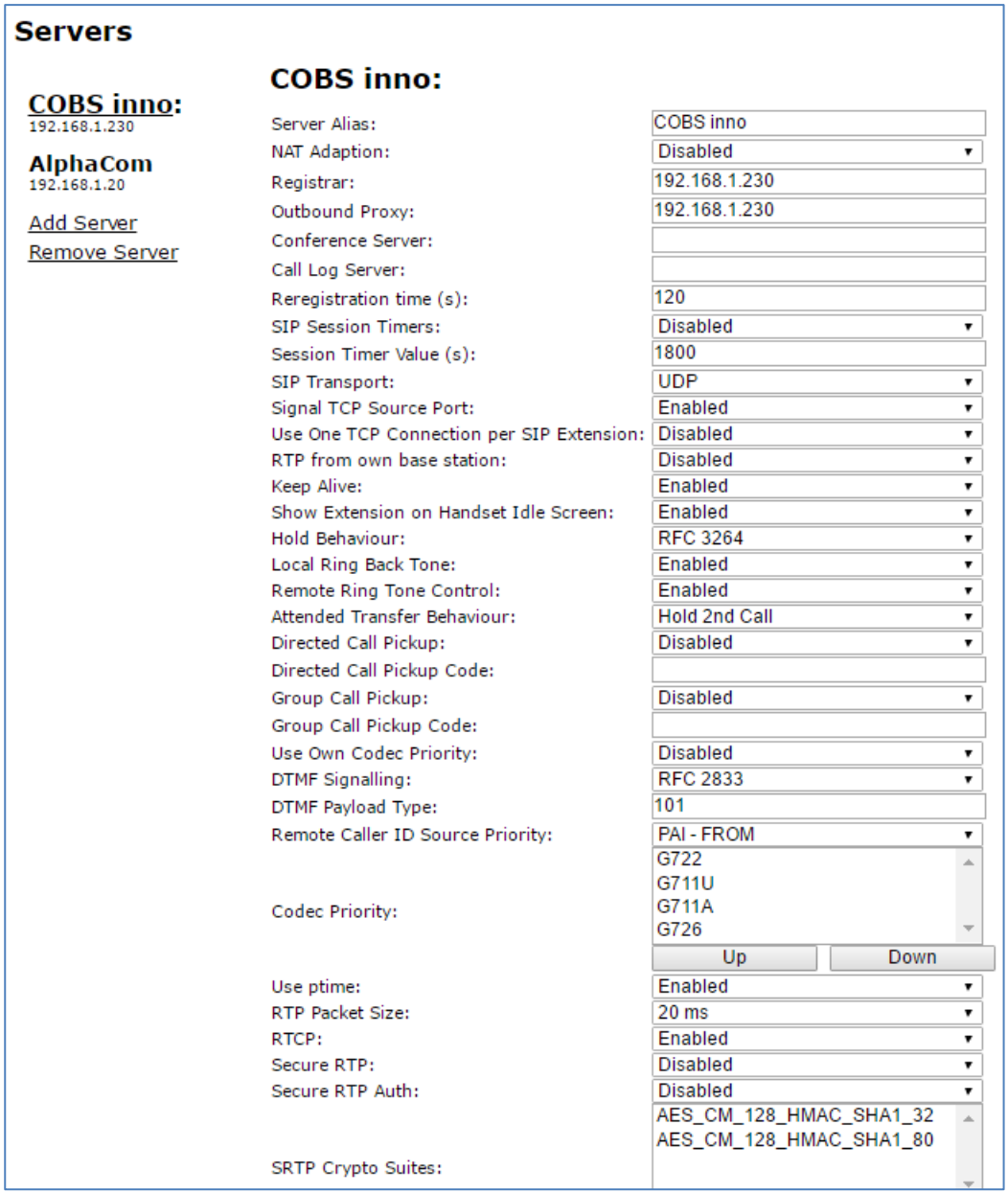
Next, from the Server page, click on the **Add Server** URL and enter the relevant SIP server information (an example is shown below).

Choose "**Disabled**" on NAT adaption parameter if NAT function of the SIP aware router is not enabled. Enter the relevant parameters based on the description in the table below.

Select **Save** button.

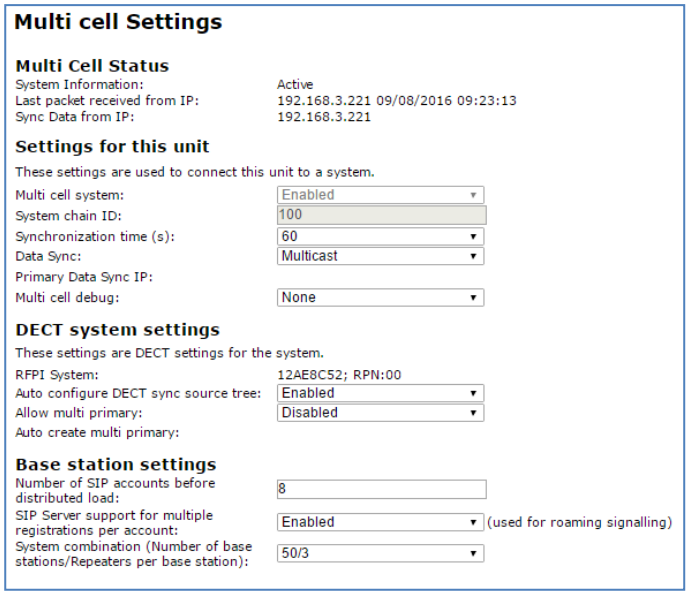
NOTE: On the **extension** page add one extension (no handset needs to be registered). This step is important for allow secondary base to join



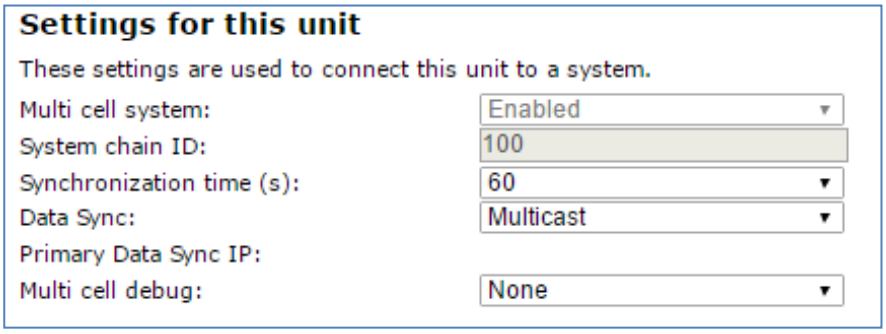


6.1.3 Multi-cell Setup

STEP 6 Click on **Multi Cell** link in the GUI to view the current **Multi cell settings** status of the current base station. Brand new base stations have **Multi cell system** feature disabled by default.

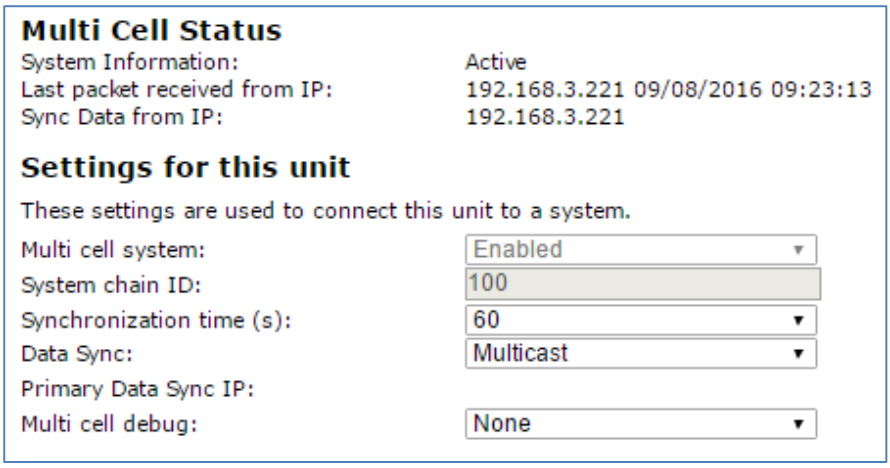


STEP 7 Next, the system administrator needs to create and Enable Multi Settings profile for the current base station. On the **Multi Cell settings** Page, choose **Enable** option from the drop down menu of the **Multi cell system** parameter. Enable the **Multi cell debug** option if the system administrator wants some Multi-cell related logs to be catalogued by the system.



STEP 8 On the same **Multi Cell Settings** page > Enter the relevant values for **System chain ID** and **Synchronization time (s)** respectively. The **System chain ID** is a geographically unique DECT cell identity allocated to bridge several base stations together in a chain. An example is **55555**. The **Synchronization time (s)** parameter is defined as window/period of time in seconds a specific base station synchronises to the master base station unit (by default 60).

Note: Do NOT use a chain ID similar to an extension.



Click on **Save** button to keep modified changes of multi cell settings into the base station.

The parameters are successfully saved

You will be redirected after 3 seconds

NOTE: The Multi Cell data synchronization ONLY works when the relevant **Time Server** is set in the system before Server/Subscriber profile is added or created. Refer to **STEP 5**.

IMPORTANT: Base stations must be rebooted after the time server has been set.

STEP 9 Repeat **STEP 1-3 & 6-8** as explained above for each base stations.

IMPORTANT: It takes up to 5 minutes (synchronization time) to add a new base station to a Multi Cell System.

6.2 Synchronizing the Base stations

STEP 10 On each **System Configuration** interface for the base station(s) navigate to the Home/Status page and Click the Reboot button.

Welcome

System Information:	**Multi cell Ready(Keep Alive) Secondary**
Phone Type:	IPDECT-V2
System Type:	Generic SIP (RFC 3261)
RF Band:	EU
Current local time:	11/10/2016 10:45:32
Operation time:	7 Days 00:27:18 (H:M:S)
RFPI Address:	12AE8C52; RPN:04
PARK Address:	31 11256430510 0
MAC Address:	00087b100a82
IP Address:	192.168.1.226
Firmware Version:	IPDECT/03.62/B0001/01-Sep-2016 16:26
Firmware URL:	Firmware update server address: 192.168.1.232
	Firmware path: LhFwuLarge
Base Station Status:	In Use
SIP Identity Status on this Base Station:	
66@192.168.1.230 (COBS inno)	Status: OK
54@192.168.1.230 (COBS inno)	Status: OK
16@192.168.1.230 (COBS inno)	Status: OK
52@192.168.1.230 (COBS inno)	Status: OK
41@192.168.1.230 (COBS inno)	Status: OK
47@192.168.1.230 (COBS inno)	Status: OK
58@192.168.1.230 (COBS inno)	Status: OK

Press button to reboot.

Reboot | Forced Reboot

This will trigger an "**Are you sure you want to reboot base station?"** dialog window. Click "**OK"** button on this window. A successful restart of the base stations will lead to a display of the page: "**Base station has been reset"**.

STEP 11 Navigate back to the **Multi cell settings** page by clicking **Multi-cell** url link at the left column. The revised **Multi cell settings** page shows the relevant base stations synchronized together. By default, the system uses the first registered base station as the master base unit.

Base Station Group

	ID	RPN	Version	MAC Address	IP Address	IP Status	DECT sync source	DECT property	Ieee1588 state	Base Station Name
	0	00	362.1	00087B100A4F	192.168.1.225	Connected	Select as primary	**Primary**	Off	COBS Service
	1	04	362.1	00087B100A82	192.168.1.226	This Unit	Primary:RPN00 (-47dBm	Locked	Off	COBS Sales
	2	08	0	2C09CB000ED1	0.0.0.0	**Connection lost!**	Select as primary		Off	

Check All /Uncheck All
With selected: Remove from chain

STEP 12 On the Multi-cell settings page, scroll to the **DECT system settings** and Enable or Disable the "**Auto configure DECT sync option source tree**" (See description in the table below). The DECT system RFPI parameter is computed by the system (It's often greyed in a multi-cell system configuration).

DECT system settings

These settings are DECT settings for the system.

RFPI System:	12AE8C52; RPN:04
Auto configure DECT sync source tree:	Enabled
Allow multi primary:	Enabled
Auto create multi primary:	Disabled

STEP 13 Next, on the **MAC-units in chains** section, you can manually configure the synchronisation source tree of the multi-cell system. Multi-cell settings page, scroll to the DECT system settings and Enable or Disable the "**Auto configure DECT sync option source tree**" (See description in the table below). The DECT system RFPI parameter is computed by the system (Its often greyed in a multi-cell system)

Base Station Group

	ID	RPN	Version	MAC Address	IP Address	IP Status	DECT sync source	DECT property	Ieee1588 state	Base Station Name
	0	00	362.1	00087B100A4F	192.168.1.225	Connected	Select as primary	**Primary**	Off	COBS Service
	1	04	362.1	00087B100A82	192.168.1.226	This Unit	Primary:RPN00 (-47dBm	Locked	Off	COBS Sales
	2	08	0	2C09CB000ED1	0.0.0.0	**Connection lost!**	Select as primary		Off	

Check All /Uncheck All
With selected: Remove from chain

6.3 Summary of Procedure – Creating a Chain

We enumerate the short version of how to add 3 base stations units in a multi-cell setup. This can be applied for any number base stations.

This procedure is divided into four (4) main stages. Apply this procedure if all base unit are straight from production.

6.3.1 Stage 1

Skip this stage if relevant base stations are already in the network.

a) Add 3 base stations i.e. RFP1, RFP2, RFP3 > Disable the "Multi cell system" option and "Save"
b) RFP1, RFP2, RFP3: Reboot from the HTTP SME Configuration Main Page
c) RFP1, RFP2, RFP3: Default by pressing reset button 12-sec.

6.3.2 Stage 2

Choosing 1st base unit i.e. RFP1 as Primary

a) RFP1: Define Time server and "Save and reboot" from the **Time** page
b) RFP1: Reboot automatically
c) RFP1: Press "Add server" and define SIP server IP and "Save" from the **Servers** page
d) RFP1: On the **extension** page add one extension (no handset needs to be registered). This step is important for allow secondary base to join
e) RFP1: Multi cell system = enable and "Save" from the **Multi-cell** page
f) RFP1: Reboot (Verify from Debug log "**SYNCMGR: This base is ready to be Primary in a Chain**")

6.3.3 Stage 3

Choose another base unit,RFP2 as Secondary

a) RFP2: Select chain ID same as RFP1.
b) RFP2: Multi cell system = enable and "Save"
c) RFP2: Reboot (Verify from Debug log "**SYNCMGR: This base is ready to join into another Chain**")
d) RFP1, RFP2: Wait 2min for stable Primary-Secondary chain (check for the message: **SYNCMGR: Socket#10 creation success**)

6.3.4 Stage 4

Choose the 3rd base unit, RFP3 as Secondary

e) RFP3: Multi cell system = enable and "Save"
f) RFP3: Reboot (Verify Debug log "**SYNCMGR: This base is ready to join into another Chain**")
g) RFP1, RFP3: Wait 2min for stable Master-Slave chain (**SYNCMGR: Socket#10 creation success**)
h) RFP3: Check mark ID2/RPN08 and select dropdown "1 – RPN: 04" and "Save"
i) RFP3: Reboot (**SYNCMGR: Socket#8 creation success**)

Multi-cell chain of 3 base stations has been created successfully. Next step involves adding extensions to the system.

7 Registration Management - Handset

In this chapter we briefly describe how to register a user and a handsets in the SMART System Network. A precondition for handset registration is a proper configured single or multi-base system.

7.1 Register a user to the system

This section describes how to register the wireless handset to the base station.

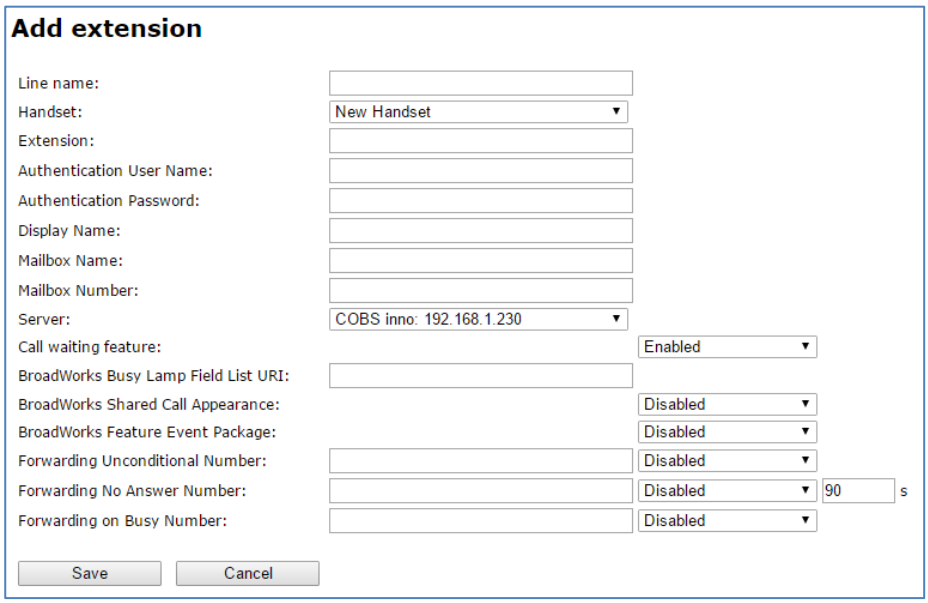
NOTE:

Minimum one server must be registered to the base (system), otherwise a handset cannot be registered to the system.

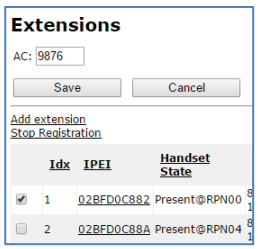
STEP 1 Login to a base station.

STEP 2 Select “Extensions” URL and click “Add extension” link

STEP 3 Fill out the form and click “Save”.



STEP 4 In the extensions list set a Check mark on the extension which shall be assigned to the handset you want to register and click “Register handset (s)”. The base is now open (ready state) for handset registrations for 5 minutes.



STEP 5 Start the registration procedure on the handset.

Please refer to the installation manual of the SMART1 handset.

NOTE:

The unique handset IPEI is displayed on sheet “Extensions” when the handset is successfully registered. The web page must be manually updated by pressing “F5” to see that the handset is registered; otherwise the handset IPEI (International Portable Equipment Identity) isn’t displayed on the web page.

We illustrate how extensions page will be when you register several handsets.

Extensions

AC: 9876

Save Cancel

Add extension
Stop Registration

	Idx	IPEI	Handset State	Handset Type FW Info	FWU Progress	
☐	1	02BFD0C882	Present@RPN00	8153 12.4	Off	☐
☐	2	02BFD0C88A	Present@RPN04	8153 12.4	Off	☐
☐	3	02BFD175AE	Present@RPN00	8153 12.4	Off	☐
☐	4	02BFD0C86B	Present@RPN00	8153 12.4	Off	☐
☐	5	02BFD0C873	Present@RPN04	8153 12.4	Off	☐

8 Base station Firmware Upgrade Procedure

This step-by-step chapter describes how to upgrade or downgrade base stations to the relevant firmware provided by COBS.

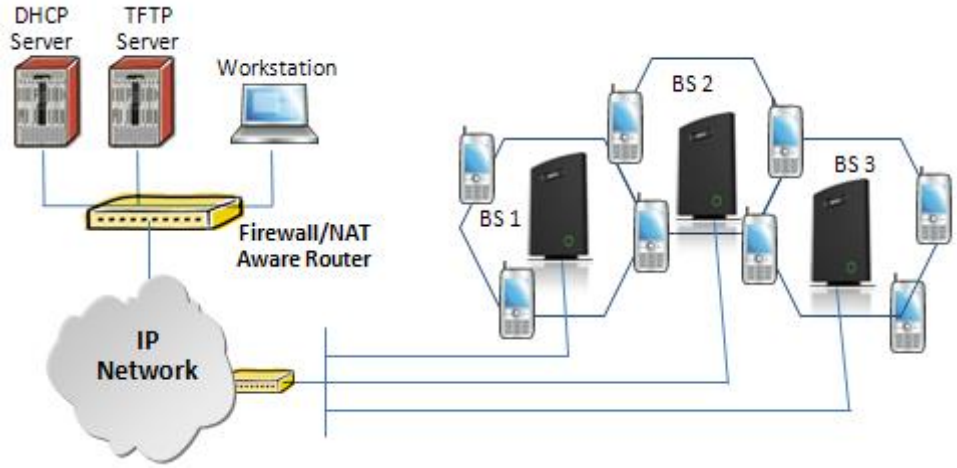
8.1 Network Dimensioning

In principle, a number of hardware and software components should be available or be prepared before base station/handset update can be possible.

The minimum hardware and software components that are required to be able update via TFTP include the following (but not limited to):

- Base stations
- TFTP Server in the CMS, or (Several Windows and Linux applications are available)
- DHCP Server (Several Windows and Linux applications are available)
- Workstation (e.g. Normal terminal or PC)
- Any standard browser (e.g. Firefox or Chrome)
- Public/Private Network

Picture 91

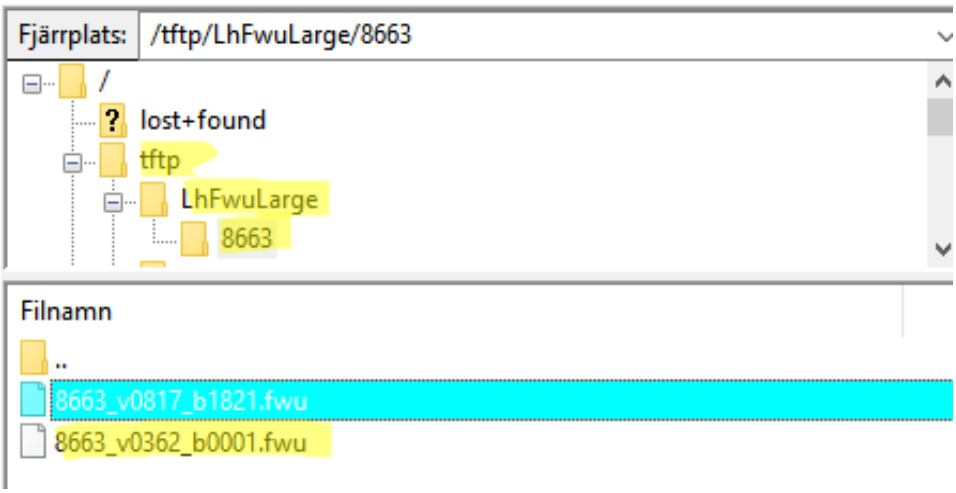


8.2 TFTP Configuration

The easiest way to upgrade base stations are to use built in “Base Firmware” feature in the CMS SMARTCOM process. See T100367E “Installation Guide CMS SMARTCOM” for more information.

This section illustrate TFTP Server configuration using a generic TFTP server.

Create the following relevant folders as shown in the snap shots and choose defaults settings for the remaining options and save.



Picture 92

NOTE: If TFTP server timeout settings are too short firmware upgrade might not complete. Recommended time out setting is more than 3 seconds.

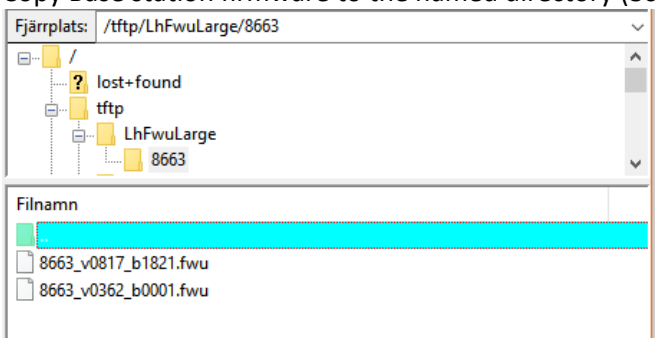
8.3 Create Firmware Directories

The admin from the service provider's side must create the relevant firmware directory in the server where both old and new firmware(s) can be placed in it. (See the STEP above)

8.3.1 Base:

On the TFTP server root, create directory "LhFwuLarge" with sub-folder "8663".

Copy Base station firmware to the named directory (8663).

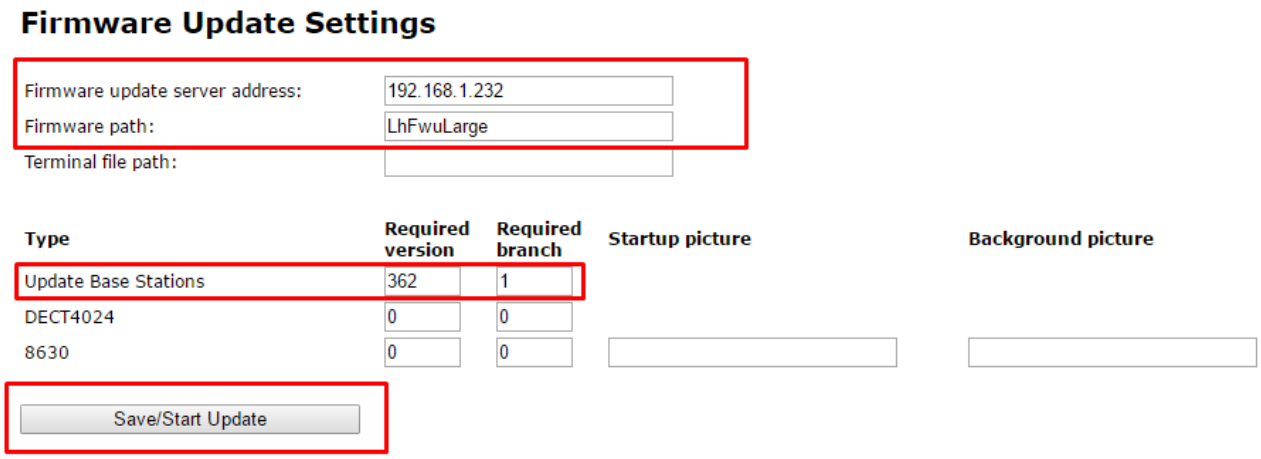


IMPORTANT:

The **LhFwuLarge** directory name cannot be changed.

8.4 Base Station(s) Firmware Upgrade

On the **Firmware Update Settings** page >Enter the TFTP Server address and firmware path > Enter the relevant firmware version of the base station to upgrade or to downgrade. Enter 362 for base version V0362. Enter 1 for branch B0001.



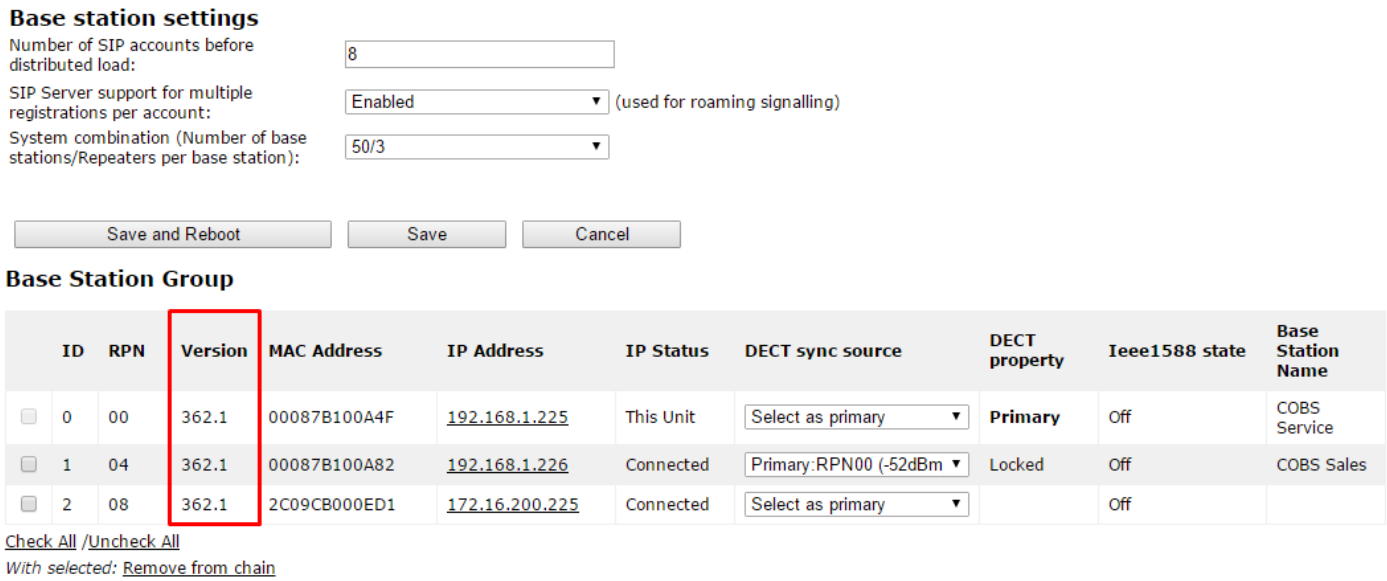
After entering required version choose **Save/Start update** button > select **OK** button from the dialog window to start the update/downgrade procedure.
The relevant base station(s) will automatically reboot and retrieve the firmware specified from the server and update itself accordingly.

The base firmware update behaviour is: Base will fetch the fwu file for approximately 3 minutes, then reboot and start flashing the LED - indicated by LED fast flashing for approximately 3 minutes and reboots in new version.

Note: All on-going voice calls are dropped from the base station(s) immediately the firmware update procedure starts. In a multi-cell setup all bases will update one by one.

8.4.1 Base firmware confirmation

Base station firmware version status in a multicell environment can be seen in the multicell base station group overview page, column 4.



8.4.2 Verification of Firmware Upgrade

Syslog information when Management Syslog level is set to “Debug”

[FWU Downloading File tftp://10.1.24.101/FwuPath/Beatus/BeatusSw_4181_v0202.fwu]
[Base FWU started]
[Base FWU ended with exit code 2101 (NE_FILE_TRANSFER_EOF): End of file]

9 Revision history

Date	Version	Note
2016-10-12	T100361E_RA_COBS SMART System Guide	Initial release
2016-10-31	T100361E_RB_COBS SMART System Guide	Removed some comments.
2016-10-31	T100361E_RC_COBS SMART System Guide	Removed some comments.
2017-05-24	T100361E_RD_COBS SMART System Guide	Revised for FW 3.80B1