SME VoIP System Guide for RTX9431 / D200 / 8328 SIP-DECT SINGLE BASE STATION / RFP 14 Base Station NA series

Installation & Configuration
Network Deployment
Operation & Management

Technical Reference Document
Version 4.9

Trademarks

Disclaimer

The contents of this document are provided about RTX products. RTX 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.

Table of Contents

1 About This Document

This document describes the configuration, customization, management, operation, maintenance and troubleshooting of the SME VoIP System (RTX9431 base, RTX8630 handset, RTX8430 handset, RTX8830 ruggedized handset and RTX4024 Repeater) in RTX generic mode. For customer, specific modes refer to specific customer agreements, which describe the software operational deviations from this document.

1.1 Audience

Who should read this guide? First, this guide is intended for networking professionals responsible for designing and implementing RTX based enterprise networks.
Second, network administrators and IT support personnel that need to install, configure, maintain, and monitor elements in a "live" SME VoIP network will find this document helpful. Furthermore, anyone who wishes to gain knowledge on fundamental features in the Beatus 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 VoIP SME System and when you are ready to setup or configure SIP server, NAT aware router, advanced VLAN settings, base stations, and multi cell setup.

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

1.3 Important Assumptions

This document was written with the following assumptions in mind:

1) You understand 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.

1.4 What's Inside This Guide

We summarize the contents of this document in the table below:

WHERE IS IT?	CONTENT	PURPOSE
CHAPTER 2	Introduction – System Overview	To gain knowledge about the different elements in a typical SME VoIP Network
CHAPTER 3	Installation of Base station/Repeater	Considerations to remember before unwrapping and installing base units and repeaters
CHAPTER 4	Making Handsets Ready	To determine precautions to take in preparing handsets for use in the system
CHAPTER 5	SME VoIP Administration Interface	To learn about the Configuration Interface and define full meaning of various parameters needed to be setup in the system.
APPENDIX – HOW-TO SETUP A DUAL-CELL SYSTEM	Multi-Cell Setup & Management	Learn how to add servers and setup multiple bases into a multi-cell network
APPENDIX – ADDING EXTENSIONS	Registration Management – Handsets	Learn how to register handset and extensions to base stations

APPENDIX – FIRMWARE UPGRADE	Firmware Upgrade/Downgrade Management	Provides the procedure of how to upgrade firmware to base stations and/or handsets and/or repeaters
APPENDIX – MULTILINE FEATURE	Multiline	Allows the same handset to have more then one number/line
APPENDIX – FUNCTIONALITY OVERVIEW	System Functionality Overview	To gain detail knowledge about the system features.

1.5 What's Not in This guide

This guide provides overview material on network deployment, how-to procedures, and configuration examples that will enable you to begin configuring your VoIP SME System.

It is not intended as a comprehensive reference to all detail and specific steps on how to configure other vendor specific components/devices needed to make the SME VoIP System functional. For such a reference to vendor specific devices, please contact the respective vendor for documentation.

1.6 Abbreviations

For this document, the following abbreviations hold:

DHCP: Dynamic Host Configuration Protocol
DNS: Domain Name Server
DLC: Data Link Control
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

1.7 References/Related Documentation

RTX8430 Handset_Manual_Operations_v4.6
RTX8630 Handset_Manual_Operations_v4.6
RTX8631_Handset_Manual_Operations_v4.6
RTX8632_Handset_Manual_Operations_v4.6
RTX8633_Handset_Manual_Operations_v4.6
RTX8830_Handset_Manual_Operations_v4.6
RTX8663 SME VoIP System Guide_SIP_V4.6
How to Deploy SME VOIP System v1.4
Provisioning of SME VoIP System (23)

1.8 Document History

REVISION	AUTHOR	ISSUE DATE	COMMENTS
1.0	DKO	14-08-2019	
1.1	TWL	7-Nov-2019	Add the FCC and ISEDC warning message
1.2	TWL	11-Dec-2019	Add Avaya model D200 in model variant.
1.3	QCC	16-Jun-2021	Add Mitel model RFP 14 Base Station NA
1.4	QCC	30-May-2023	Add Alcatel model 8328 SIP-DECT SINGLE BASE STATION

1.9 What is new

What new features have been added.

VERSION	FEATURE
V420	uaCSTA
	LDAP over SSL
	SME VoIP handset – login(for GDPR)
V430	TLS 1.2
	Secure Syslog
V440	LLDP Support
V450	Firmware update warning
	New Generic statistics
	8660 – 8663 Mixed mode
	Diagnostics Logging
V460	RTX BTLE Beacon support

1.10 Documentation Feedback

We always strive to produce the best and we also value your comments and suggestions about our documentation. If you have any comments about this guide, please enter them through the Feedback link on the RTX website. We will use your feedback to improve the documentation.

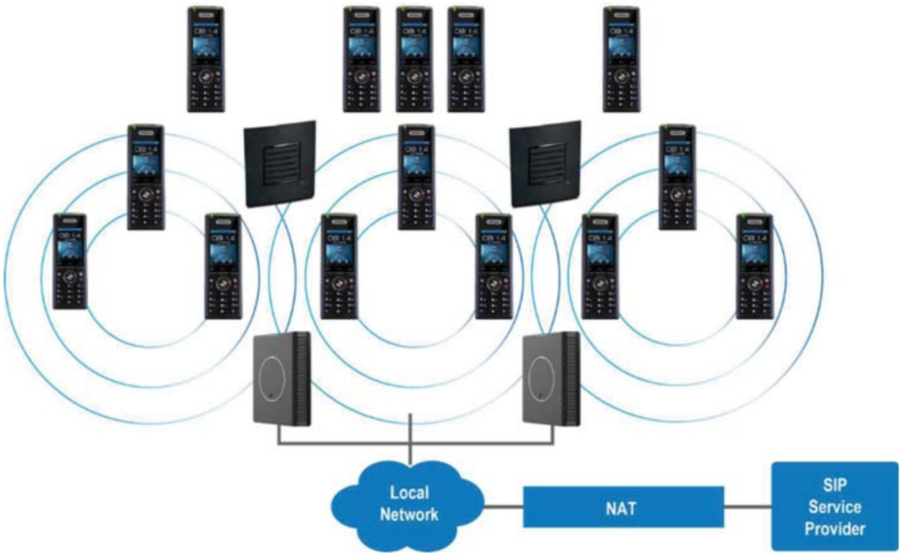
2 Introduction – System Overview

In a typical telephony system, the network setup is the interconnection between Base-stations, “fat” routers, repeaters, portable parts, etc. The backbone of the network depends on the deployment scenario, but a ring or hub topology is used. The network has centralized monitoring, and maintenance system.

The model variant is included RTX9431 D200 (Avaya model), RFP 14 Base Station NA (Mitel model) and 8328 SIP-DECT SINGLE BASE STATION (Alcatel model).

The system is easy to scale up and supports from 1 to 249 bases in the same network. Further it can support up to 20 registered handsets (RTX8630, RTX8830 and RTX8430). The Small and Medium Scale Enterprise (SME) VoIP system setup is illustrated below. Based on PoE interface each base station is easy to install without additional wires other than the LAN cable. The system supports the IP DECT CAT-IQ repeater RTX4024 with support up to 5 channels simultaneous call sessions.

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



2.1 Hardware Setup

SME network hardware setup can be 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 mounted on walls or lamp poles 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). Repeaters are range extenders and cannot be used to solve local call capacity issues. In this case additional bases must be used.
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.

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

2.2 Components of SME VoIP System

RTX SME VoIP system is made up of (but not limited to) the following components:

- At least one RTX Base Station is connected over an IP network and using DECT as air-core interface.
- RTX IP DECT wireless Handset.
- RTX SME VoIP Configuration Interface; is a management interface for SME VoIP Wireless Solution. It runs on all IP DECT Base stations. Each Base station has its own unique settings.

2.2.1 RTX 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 dual-cell setup, each base station has:

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

If two Base Stations are used, they are grouped into a cluster. Within the Cluster, Base Stations are synchronized to enable a seamless handover when a user moves from one base station coverage to the other. It is necessary for Base Stations to communicate directly with each other in the system in order to guarantee synchronization in the situation that one of them fails.

The 4 control signaling channels are used to carry bearer signals that enable a handset to initiate a handover process.

2.2.2 SME VoIP Administration Server/Software

This server is referred to as SME VoIP Configuration Interface.
The SME VoIP 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, repeaters 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 RTX Wireless Handset

The handset is a lightweight, ergonomically, and portable unit compatible with Wideband Audio (G.722), DECT, GAP standard, CAT-iq audio compliant.
The handset includes color 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 SME VoIP are summarized as follows:
Frequency bands:
1880 – 1930 MHz (DECT)
1880 – 1900 MHz (10 carriers) Europe/ETSI
1910 – 1930 MHz (10 carriers) LATAM
1920 – 1930 MHz (5 carriers) US

Transmit Power: 23.7 dBm in Europe mode.

2.4 System Capacity (in Summary)

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

DESCRIPTION	CAPACITY
Min ## of Bases Single Cell Setup	1
Max ## of Bases in Dual-cell Setup (configurable)	2
Single/Dual-Cell Setup: Max ## of Repeaters	1 base and 6 repeaters per base
Dual-Cell Setup: Total Max ## of Repeaters	12
Max ## of Users (SIP registrations) per Base	30
Max ## of Users per SME VoIP System	limited to 1000
Dual-cell Setup: Max ## of Synchronization levels	24
Single Cell Setup: Max ## Simultaneous Calls	10 per Base station
Dual-Cell Setup: Max ## of Calls	20 per system
Total Max ## Simultaneous Calls (Dual-cell Setup)	Limited to 1000
Repeater: Max ## of Calls (Narrow band)	10
Repeater: Max ## of Calls (G722)	4

Quick Definitions

Single Cell Setup: SME telephony network composed of one base station

Dual-cell Setup: Telephony network that consists of two base stations

Synchronization Level: Is the air core interface between two base stations.

2.5 Advantages of SME VoIP 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. SME 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 Base Stations/Repeater

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 center 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:

- Box for Base station (DC+PoE) unit + PSU
    - 1 x Base Station unit
    - 1 x Ethernet cable 1m
    - 1 x Power supply single plug
    - 1 x Quick guide
    - 1 x Safety sheet

Depending on the manufacturer P/N, the DC adaptor type may vary as listed below:

Manufacturer P/N	DC adaptor plug type by countries
S008ACM0500200	Multi-plug
S010WB0500200	UK
S010WV0500200	EU
S010WU0500200	US
S010WS0500200	AU

- Box for PoE only Base station unit
    - 1 x Base Station unit
    - 1 x Ethernet cable 1m
    - 1 x Quick guide
    - 1 x Safety sheet

- Spare accessories
    - PSU single plug
    - PSU multi plug

Please note that mounting screws and anchors are not added in the packaging.

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 the operator has examined it. 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 RTX Base Station Mechanics

RTX9431 can operate on a maximum temperature of 50℃. With such small dimensions as 109mm (height) and 93mm (width), it allows the user to mount the device on the wall or easily leave it standing on any furniture. (please see image below for more details).

Alternative mechanics casing.

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 summarizes the various LED states:

LED STATE	STATE
UNLIT	No power in unit
UNLIT/SOLID RED	Error condition
BLINKING GREEN	Initialization
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 RTX 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 RTX Base Unit – Reset feature

It is possible to restart or reset the base station unit by pressing a knob at the bottom side of the unit (see image below). Alternatively, it can be reset from the SME Configuration Interface. We do not recommend this; but unplugging and plugging the Ethernet cable back to the PoE port of the base station also resets the base unit.

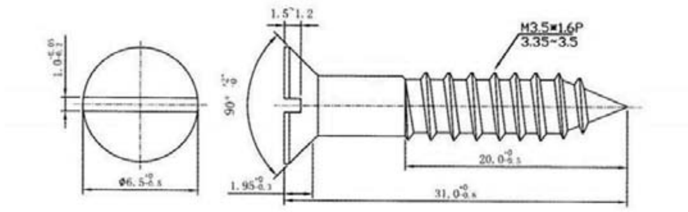
3.4 Installing the Base Station

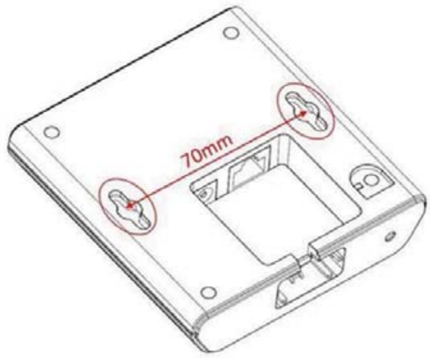
First determine the best location that will provide an optimal coverage taking account the construction of the building, architecture, and choice of building materials.
Next, mount the Base Station on a wall to cover range between 50 – 300 meters (i.e. 164 to 984 feet), depending whether it's an indoor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

3.4.1 Mounting the Base Stations/Repeaters:

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

As mentioned before, the screws and anchors are not included in the packaging. Therefore, you will have to provide your own two pieces of screws M3.5 x 31mm. The distance between them is 70mm (please see the images below). The height of wall mount is suggested to be less than or equal to 2 meters.





Mount the base unit as high as possible (not more than 2m) to clear all nearby objects (e.g. office cubicles and cabinets, etc.). Occasionally extend coverage to remote offices/halls with lower telephony users by installing Repeaters.
Make sure that when you fix the base stations with screws, the screws do not touch the PCB on the unit. Secondly, avoid all contacts with any high voltage lines.

3.5 Find IP of Base Station

To find IP of the installed base station two methods can be used; Using handset Find IP feature or browser IPDECT feature.

3.5.1 Using handset Find IP feature

On the handset press “Menu” key followed by the keys: *47* to get the handset into find bases menu. The handset will now scan for 8660 / 9431 bases. Depending on the amount of powered on bases with active radios and the distance to the base it can take up to minutes to find a base.

- Use the cursor down/up to select the base MAC address for the base that you want to connect to
- The base IP address will be shown in the display below the MAC address of the device

The feature is also used for deployment.

3.5.2 Using browser IPDECT

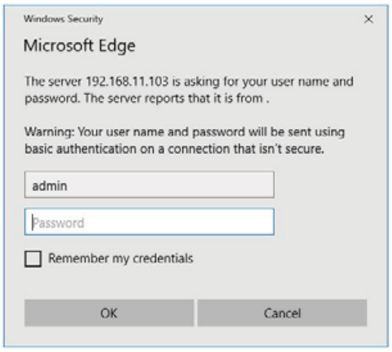
Open any standard browser and enter the address:
http://ipdect<MAC-Address-Base-Station>
for e.g. http://ipdect00087B00AA10. This will retrieve the HTTP Web Server page from the base station with hardware address **00087B00AA10**.
This feature requires an available DNS server.

3.6 Login to Base SME Configuration Interface

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

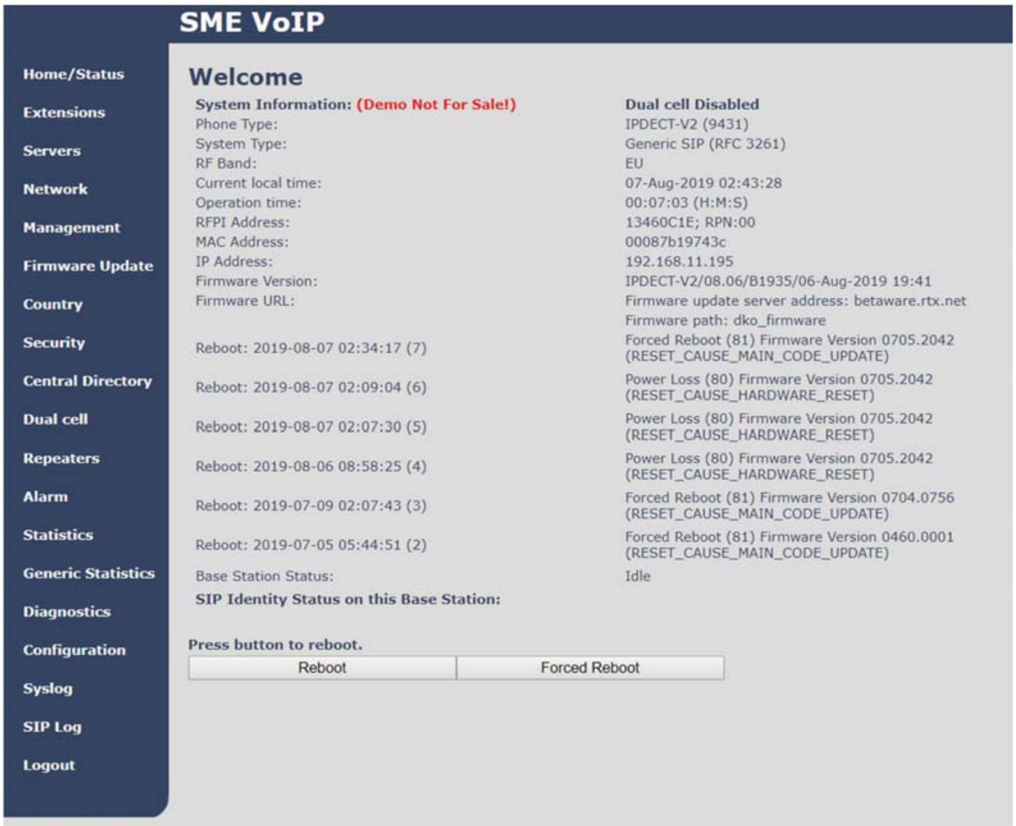
2. Use the IP find menu in the handset (Menu * 4 7 *) to determine the IP-address of the base station by matching the MAC address on the back of the base station with the MAC address list in the handset

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



4. 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.

Screenshot:



4 Making Handset Ready

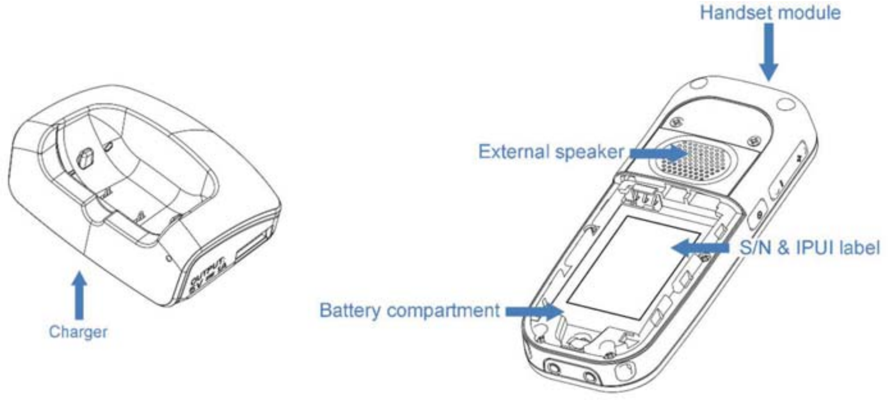
In this chapter, we briefly describe how to prepare the handset for use, install, insert and charge new batteries. Please refer to an accompanying Handset User Guide for more information of the features available in the Handset.

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 center 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 Handset hook
- 1 x A/C Adaptor
- 1 x Battery
- 1 x charger
- 1 x Handset Unit, 1 x Battery cover



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 the operator has examined it. 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

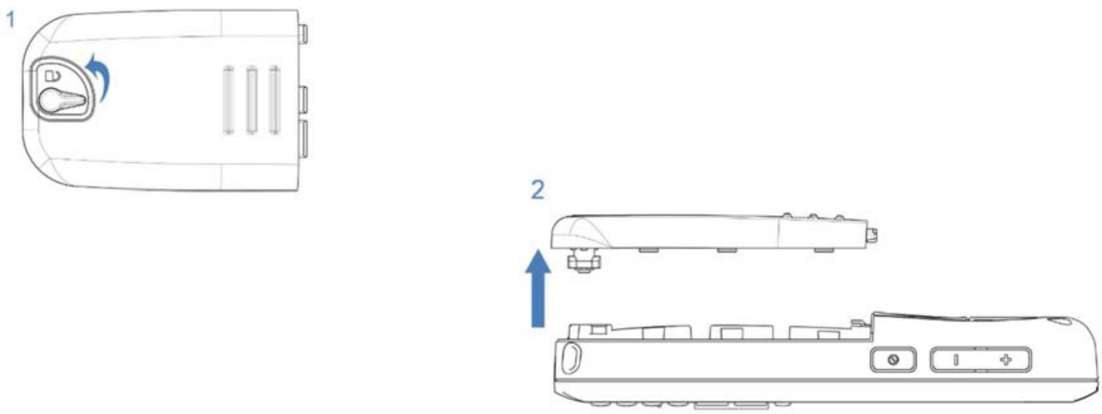
1. Never dispose battery in fires, otherwise it will explode.
2. Never replace the batteries in potentially explosive environments, e.g. close to inflammable liquids/ gases.
3. ONLY use approved batteries and chargers from the vendor or operator.
4. Do not disassemble, customize, or short circuit the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

Using the Charger
Each handset is charged using 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 5℃ and 25℃/41°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.
If the handset is turned off when placed in charger, only the LED indicates the charging. When handset is turned off, the LED flashes at a low frequency while charging and lights constantly when the charging is finished. There will be response for incoming calls.
If the handset is turned on when charging, the display shows the charging status.

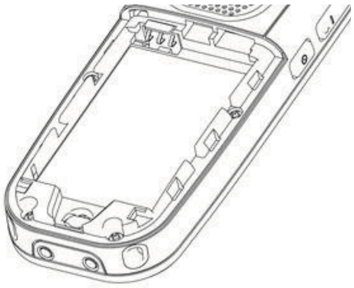
Open Back Cover

1. Press down the back cover and slide it towards the bottom of the handset.
2. Remove Back Cover from Handset



- Handset Serial Number

The serial number (IPEI/IPUI 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 serial number is needed to enable service to the handset. It must be programmed into the system database via the SME VoIP 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 to the handset manual for detailed description of how to use the handset feature.

5 SME VoIP Administration Interface

The SME VoIP Administration Interface is also known as SME VoIP Configuration. It is the main interface through which the system is managed and debugged.

The SME VoIP 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.

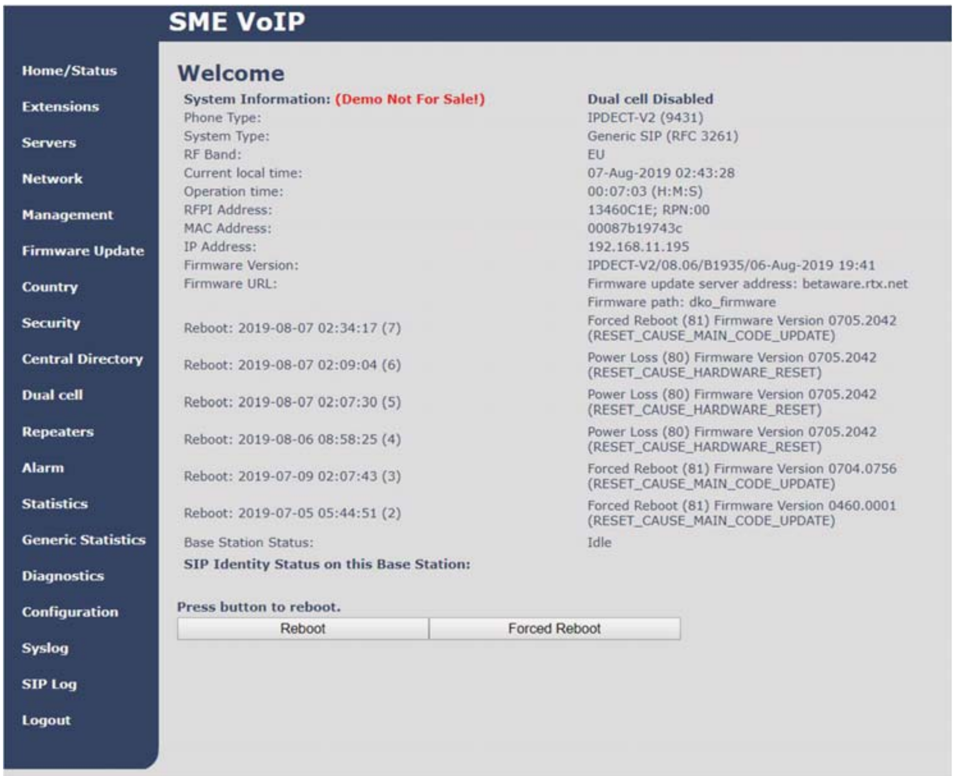
NOTE: Enabling secure web is not possible. For secure configuration use, secure provisioning.

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 SME VoIP Administration Interface. For detailed overview of each parameter from the menu bar, please see the next chapters.

Screenshot



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	Network settings can be configured in this menu such as IP settings, NAT, SIP, VLAN,etc.
MANAGEMENT	Defines the Configuration server address, Management transfer protocol, sizes of logs/traces that should be catalogued in the system.
FIRMWARE UPDATE	Remote firmware updates (HTTP(s)/TFTP) settings of Base stations and handsets.
LOCATION GATEWAY	If Location Gateway is connected, this parameter will be added to the menu bar, serving for administration of Location Gateways
COUNTRY	Specifying the country/territory where the SME network is located ensures that your phone connection functions properly. **Note:** The base language and country setting are independent of each other. Time settings: Here the user can configure the Time server. It should be used as time server in relevant country for exact time. The time servers must 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.
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.
DUAL CELL	Specify to connect up to two base stations to the network. Make sure the system ID for the relevant base stations are the same otherwise the dual-cell feature will not work.
LAN SYNC	Allows base stations to connect over LAN PTP Sync, this makes it possible to have greater distance between the base stations, compared to Air Sync.
REPEATERS	Administration and configuration of repeaters of the system
ALARM	Administration and configuration of the alarm settings on the system. This controls the settings for alarms that can be sent to the handsets. This feature is only available on certain types of handsets.
STATISTICS	Overview of system and call statistics for a system.
GENERAL STATISTICS	Overview of general parameter statistics of the system
DIAGNOSTICS	Overview of Base stations and Extensions diagnostics
CONFIGURATION	This shows detail and complete SME 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.
LOGOUT	Logout of the web interface.

5.2 Home/Status

We describe the parameters found in the Welcome front-end home/status of the SME VoIP Administration Interface.

Screenshot:

PARAMETER	DESCRIPTION
SYSTEM INFORMATION	Status of the base (Single cell as the Dual cell is not activated)
PHONE TYPE	Always IPDECT
SYSTEM TYPE	Customer configuration of the base
RF BAND	RF band setting of the base The parameter is defined in production and relates to the radio approvals shown on the label of the base.
CURRENT LOCAL TIME	Local Time of the base
OPERATION TIME	Operation is operation time for the base since last reboot
RFPI-ADDRESS	RFPI address of the base
MAC-ADDRESS	MAC address of the base
IP-ADDRESS	IP address of the base
FIRMWARE VERSION	Firmware version of the base
FIRMWARE URL	Firmware update server address and firmware path on server
REBOOT	Shows the last reboots of the base station and the reason for reboot
BASE STATION STATUS	"Idle": When no calls on base "In use": When active calls on base
SIP IDENTITY STATUS	Shows 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 Error: SIP registration error
REBOOT	Reboot after all connections are 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 in multiline maximum 200 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 Group call

Call Group is a SIP extension where multiple handsets are associated. All handsets that subscribe to a given extension (and hence Call Group) can receive incoming calls and initiate outgoing calls on the given extension. It is possible for any handset to perform any call action which is possible without the Call Group feature. That is, call actions as Hold, transfer etc. are possible if the PBX supports them.

When an incoming call arrives to a given Call Group, all Call Group subscribed handsets will alert. Thus, if a Call Group contains 20 handsets, all 20 handsets will alert.
An alerting handset cannot receive another incoming call, and therefore if a handset subscribes for multiple Call Groups, and a call arrives for a 2nd Call Group while the handset is alerting, the handset will not receive this call. If DND is enabled for a given handset, it will not receive the incoming call.

For outgoing calls, it can be selected in the handset which line (i.e. Call Group) to use for the call. The maximum number of lines is 20. For any outgoing actions, the settings for the selected line (SIP extension) will be used.

NOTE: Group call, does not work with paired headset.

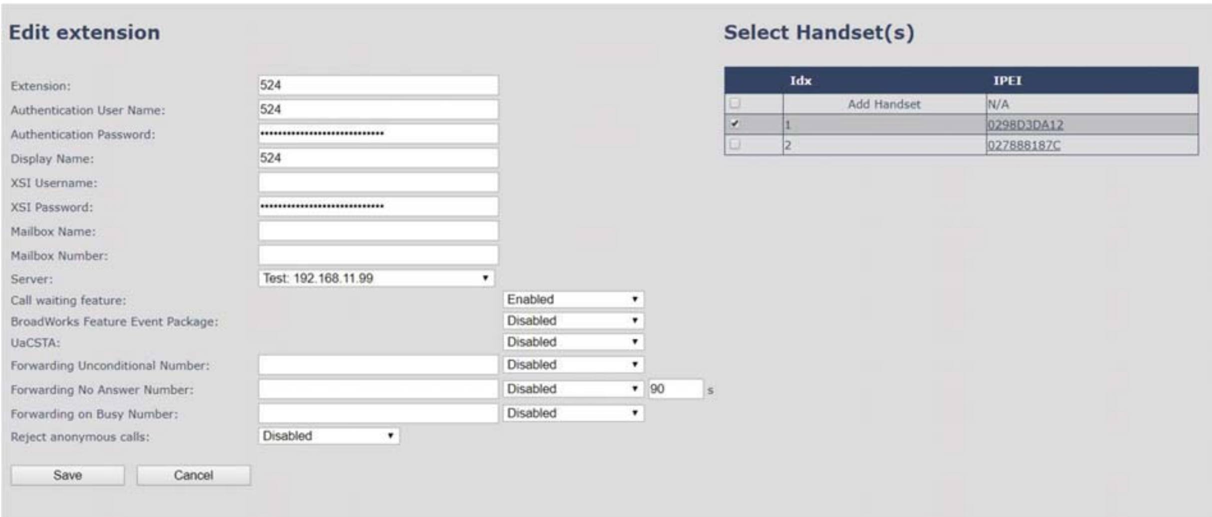
5.3.2 Add extension

1. Click add extension

Screenshot:

2. Fill in the required information

Screenshot:



PARAMETER	DEFAULT VALUE(S)	DESCRIPTION
EXTENSION	Empty	Handset phone number 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
XSI USERNAME	Empty	**Username:** SIP authentication username **Permitted value(s):** 8-bit string length
XSI PASSWORD	Empty	**Password:** SIP authentication password. **Permitted value(s):** 8-bit string length

MAILBOX NAME	Empty	Name of centralized system used to store phone voice messages that can be retrieved by recipient later. **Valid Input(s):** 8-bit string Latin characters for the Name
MAILBOX NUMBER	Empty	Dialed 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 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.
BROADWORKS FEATURE EVENT PACKAGE	Disable	Enable/Disable Broadworks features
UACSTA	Disabled	Enable/Disable uaCSTA support
FORWARDING UNCONDITIONAL NUMBER	Empty	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 **Note:** Feature will be automatically disabled in case the handset or extension is part of a group
FORWARDING NO ANSWER NUMBER	Empty	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. **Note:** Feature will be automatically disabled in case the handset or extension is part of a group
FORWARDING ON BUSY NUMBER	Empty	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 **Note:** Feature will be automatically disabled in case the handset or extension is part of a group
REJECT ANONYMOUS CALLS	Disabled	Calls from anonymous numbers will automatically be rejected. Enable to rejects anonymous calls

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

When an extension is added (or edited) it can be selected (right side check box) which handsets shall subscribe to the given extension, and hence be a part of this call group, see above figure. It is also possible to choose to add a new handset entry at this point, and if this is done, DECT registration for the new entry can be enabled afterwards on the handsets subpage.

5.3.2.1 *Extension list*

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

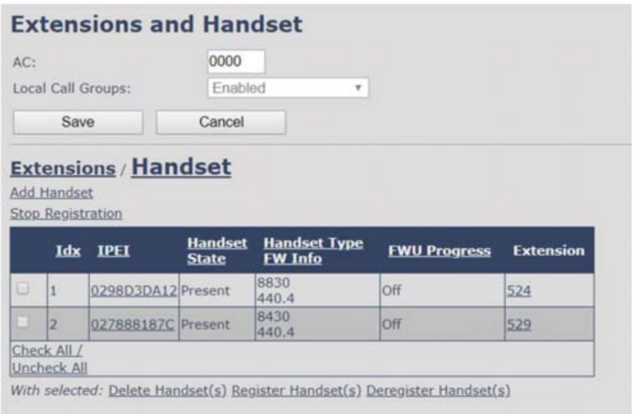
Screenshot

PARAMETER	DESCRIPTION
IDX	Index of handsets ; Select / deselect for delete, register and deregister handsets
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.
IPEI	Handset IPEI. IPEI is a unique DECT identification number. Group call: One extension can be associated to up to 20 IPEI's. The IPEI's will be listed in this cell.

5.3.2.2 *Handset list*

The added handsets will be shown in the handset lists.
The list can be sorted by any of the top headlines (Extensions / Handset), by mouse click on the headline link.

Screenshot



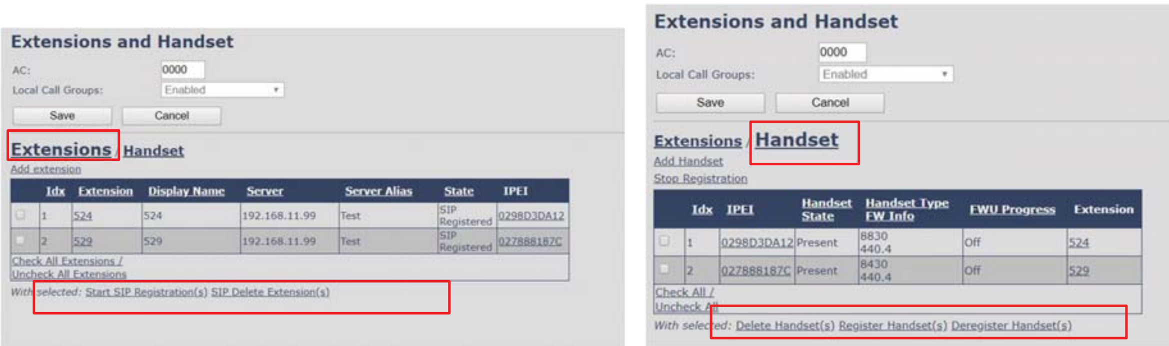
PARAMETER	DESCRIPTION
IDX	Index of handsets ; Select / deselect for delete, register and deregister handsets

IPEI	Handset IPEI. IPEI is unique DECT identification number.
HANDSET STATE	The state of the given handset: **Present:** The handset is DECT located at the base **Detached:** The handset is detached from the system (e.g. powered off) **Removed:** The handset has been out of sight for a specified amount of time (~one hour).
HANDSET TYPE FW INFO	Handset type and firmware version of handset
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 "**Waiting for charger**" (HS)): All FWU is complete and is now waiting for handset restart. **Complete HS:** FWU complete **Error:** Not able to fwu e.g. file not found, file not valid etc
EXTENSION	Given extension is displayed. Group call: The cell will show all the extensions associated with this handset and IPEI.

5.3.2.3 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.

Screenshot



In the below table, each command is described.

ACTIONS	DESCRIPTION
ADD EXTENSION / ADD HANDSET	Access to the "Add extension" or "Add Handset" 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).
START SIP REGISTRATION(S)	Manually start SIP registration for selected handset(s).
DELETE SIP EXTENSION(S)	Deregister the selected handset(s) and delete the extension(s).

NOTE: By powering off the handset, the handset will SIP deregister from the PBX.

5.3.3 Edit Extension

To edit an extension simply click the extension number that you want to edit.

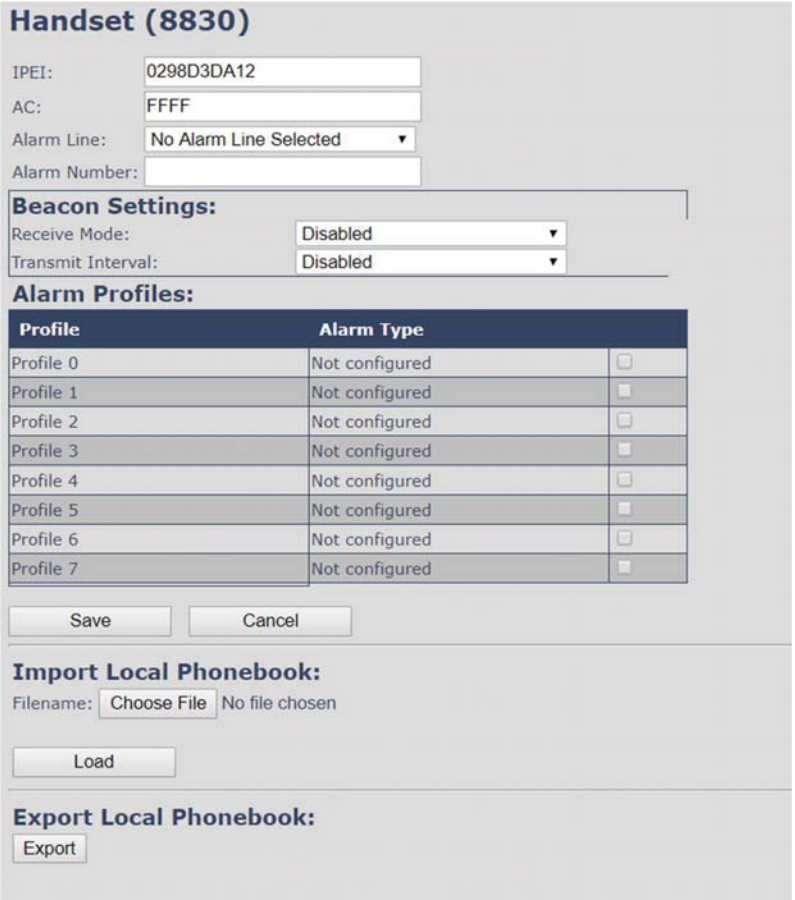
Screenshot:

Editing the extension will open the same configuration possibilities as “Add extension”. Refer to the previous chapter (5.3.2) for more details.

5.3.4 Edit Handset

Use the mouse to click the handset IPEI link to open the handset editor window.

Screenshot



PARAMETER	DEFAULT VALUE(S)	DESCRIPTION
IPEI	Handset IPEI	Shows the handset IPEI. For an already registered handset changing the IPEI will deregister the handset at next handset location update.
AC	Handset AC code	Shows the handset AC code. AC code is used at handset registration. Changing the AC code for an already registered handset will have no effect.
ALARM LINE	No Alarm Line Selected	The line of multiline to be used for alarm call feature
ALARM NUMBER	Empty	Number to be dialed in case of handset alarm key is pressed (Long keypress > 3 seconds on navigation center key)
RECEIVE MODE	Disabled	**NOTE:** This feature is only shown if Handset has BTLE. (RTX8630 and RTX8430 is not supported) Enter Proximity: Leave Proximity: Enter or Leave Proximity:
TRANSMIT INTERVAL	Disabled	**NOTE:** This feature is only shown if Handset has BTLE. (RTX8630 and RTX8430 is not supported)

		Short: Step1: Step2: Step3: Step4: Step5: Long:
ALARM PROFILES	Not configured	Check the wanted alarm profiles for the particular handset.
IMPORT LOCAL PHONEBOOK		Import phonebook from csv file to this specific extension
EXPORT LOCAL PHONEBOOK		Exports this extensions phonebook as csv file NB: Home is not exported as this is considered private data.

5.3.4.1 Import local phonebook

The import local phonebook feature is using a browse file approach. After file selection press the load button to load the file. The system supports only the original *.csv format. Please note that some excel csv formats are not the original csv format.

Screenshot

NOTE: The local phonebook can have 100 entries for RTX863x and RTX8830 and 50 entries for RTX8430.

5.3.4.2 Export local phonebook

The Export local phonebook feature makes it possible to retrieve all contracts from a specific phone to a .CSV file.

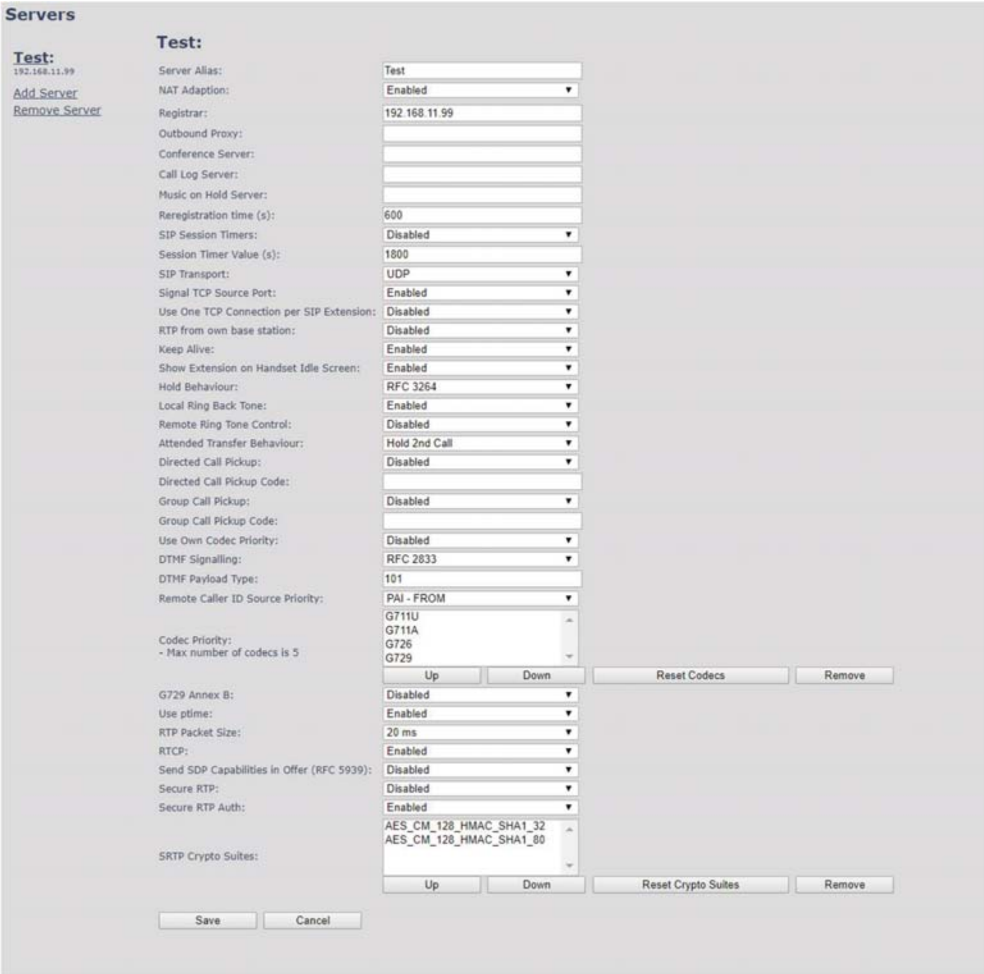
Screenshot

Press the export button and save the .CSV file on you PC or Server.

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	Disabled	To ensure all SIP messages go directly to the NAT gateway in the SIP aware router. If the system receives a SIP response to a REGISTER request with a “Via” header that includes the “received” parameter (ex: “Via: SIP/2.0/UDP 10.1.1.1:4540;received=68.44.20.1”), the base will adapt its contact information to the IP address from the “received” parameter. Thus, the base will issue another REGISTER request with the updated contact information. If NAT Adaption is disabled, the “received” parameter is ignored.
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 Registrar.
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
MUSIC ON HOLD SERVER	Empty	Add the address of a server for ensuring music is on when call is on hold
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
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 5.5.6) 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 behavior by handset hold feature. RFC 3264: Hold is signaled 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 sent only, recvonly or inactive dependent of the context RFC 2543: The ”old” way of signaling HOLD. The connection information part of the SDP is set to 0.0.0.0, and the direction attribute is sent only, recvonly or inactive dependent of the context
LOCAL RING BACK TONE	Enabled	In case the server doesn’t play local ring back tone the handset will do it.
REMOTE RING TONE CONTROL	Enabled	Sometimes call distinguished ringing. It enables the server to control what ring tone that is used on the handsets.
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 PBX’s do not expect that the 2nd call is put on hold, and therefore attended transfer fails on these PBX’s. The "Attended Transfer Behavior" feature defines whether 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
DIRECT CALL PICKUP	Disabled	This is Part of BroadWorks SCA feature. Enabled a direct call pickup code is sent to the Handsets
DIRECT CALL PICKUP CODE	Empty	Code used to direct call pick up
GROUP CALL PICKUP	Disabled	Enable for a call group pickup
GROUP CALL PICKUP CODE	Empty	Code used to pick up a group call
USE OWN CODEC PRIORITY	Disabled	Default disabled. By enablbling 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 signaling 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 use 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 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. To use G.729, add on DSP module must be installed in all base stations. Contact your local dealer for price information.
G729 Annex B		Enable/Disable Annex B of codec G729 **Note:** Both parts have to support it in order to avoid noise and any other kind of voice interruption
USE PTIME	Enabled	Use the RTP Packet size, chosen in the below setting.
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	Enable/Disable RTCP
SEND SDP CAPABILITIES IN OFFER (RFC 5939)	Disabled	Enable to support RFC 5939
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 are possible per base in a single or multicell system.

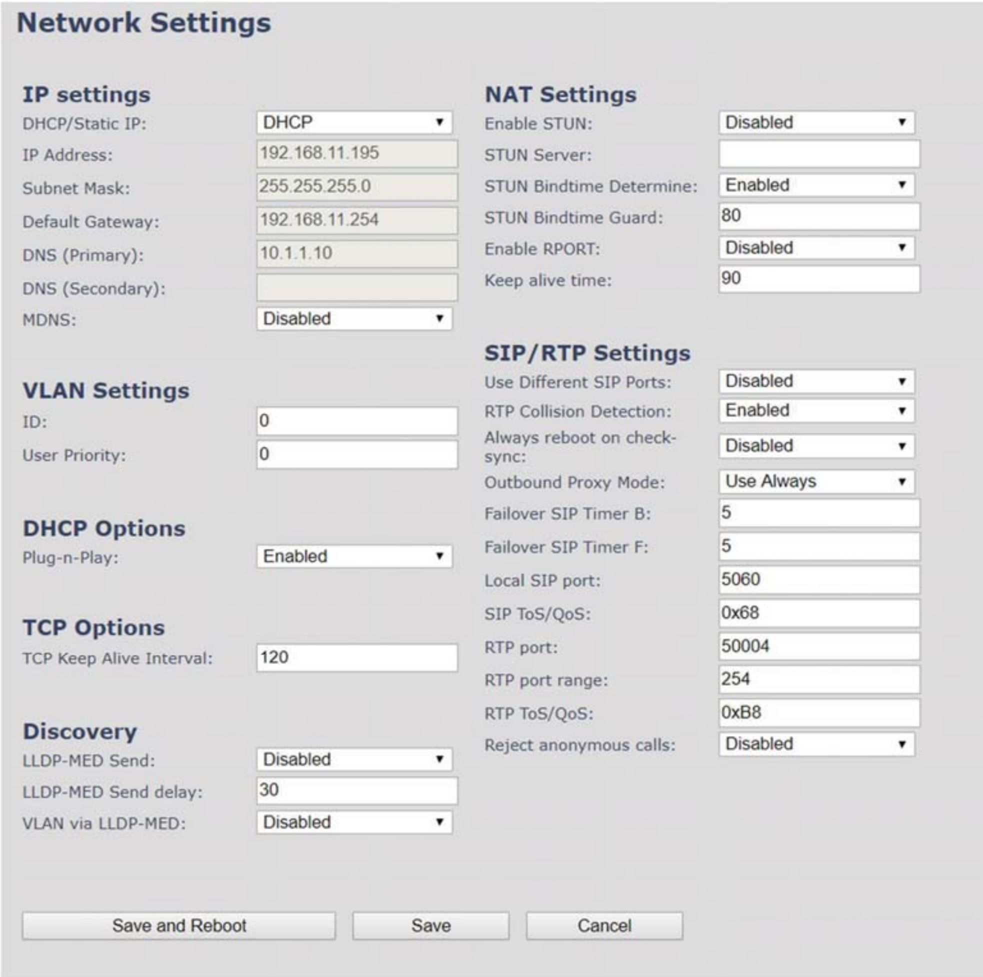
SRTP CRYPTO SUITES	AES_CM_128_HMAX_SHA1_32 AES_CM_128_HMAX_SHA1_80	Field list of supported SRTP Crypto Suites. The device is born with two suites.

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

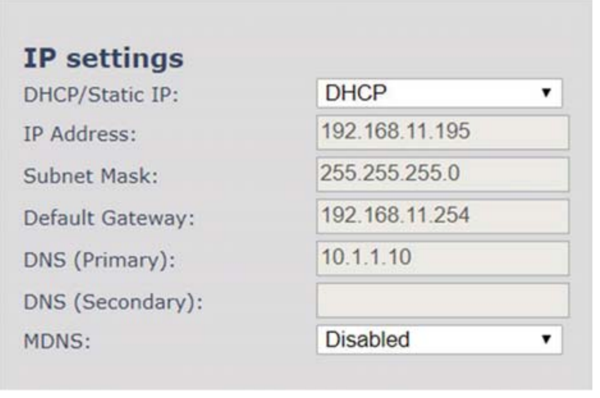
In this section, we describe the different parameters available in the network configurations menu.

Screenshot



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:** the network administrator manually assigns IP addresses. If the user chooses DHCP option, the other IP settings or options are not available.
IP ADDRESS	N/A	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	N/A	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	N/A	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 another network. This device provides a default route for TCP/IP hosts to use when communicating with other hosts on hosts networks.
DNS (PRIMARY)	N/A	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)	N/A	This is an alternate DNS server.
MDNS	Disabled	Enable to allow Multicast Domain Name system (MDNS)

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 synchronized between the bases in the chain. Bases will be automatic rebooted during the synchronization.

For further help on VLAN configuration refer to Appendix.

5.5.3 DHCP Options

Screenshot

PARAMETER	DEFAULT VALUES	DESCRIPTION
PLUG-N-PLAY	Enabled	Enabled: DHCP option 66 to automatically provide PBX IP address to base.

5.5.4 Static IP settings

If there is no DHCP server present you need to set a static IP. When you plug-in the LAN cable and the Base station don’t get IP from a DHCP server it uses RFC3927 Static IP fall back.

Static IP address fall back - RFC3927
If a base station boots without a DHCP server on the network, it boots up using static IP as defined in RFC3927.
Base continuously request IP and after 3min. the base enters static IP address in range: 169.254.x.x

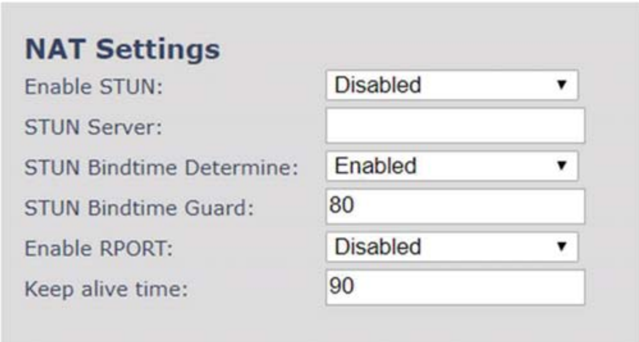
To find base static IP use "Find IP" handset feature.
To access the web interface, set the PC to static IP in the same subnet as the base station and you can now access the web interface.

NOTE: "Find IP" go to menu and press *47*, then the handset with start searching for base stations.

5.5.5 NAT Settings

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

Screenshot

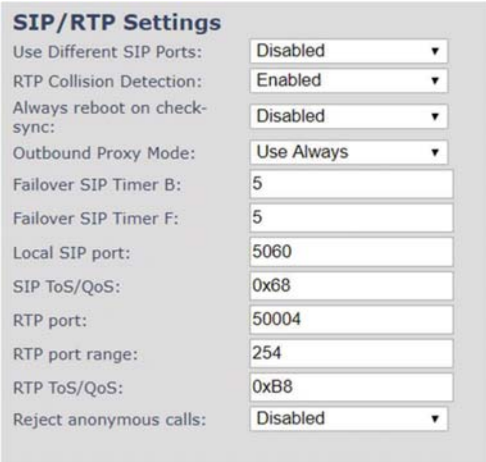


PARAMETER	DEFAULT VALUES	DESCRIPTION
ENABLE STUN	Disabled	Enable to use STUN
STUN SERVER	N/A	**Permitted value(s): AAA.BBB.CCC.DDD** (Currently only Ipv4 is supported) or **URL** (e.g.: firmware.rtx.net).
STUN BINDTIME DETERMINE	Enabled	
STUN BINDTIME GUARD	80	**Permitted values:** Positive integer default is 80, 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

5.5.6 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 signaling 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.
ALWAYS REBOOT ON CHECK-SYNC	Disabled	Reboot base station when new configuration I loaded.
OUTBOUND PROXY MODE	Use Always	Use Always: All outbound calls are sent to outbound proxy Only Initial request: Only use outbound proxy for initial SIP requests
FAILOVER SIP TIMER B	5	When the time expires and the corresponding SIP transaction fails, failover will be triggered
FAILOVER SIP TIMER F	5	When the time expires and the corresponding SIP transaction fails, failover will be triggered
LOCAL SIP PORT	5060	The source port used for SIP signaling **Permitted values:** Port number default 5060.
SIP TOS/QOS	0x68	Priority of call control signaling 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	254	The number of ports that can be used for RTP audio streaming. **Permitted values:** Positive integers, default is 254
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
REJECT ANONYMOUS CALLS	Disabled	If disabled, all calls will be received. If enabled, calls not registered will be automatically rejected

5.5.7 TCP Options

Screenshot

PARAMETER	DEFAULT VALUES	DESCRIPTION
TCP KEEP ALIVE INTERVAL	120s	Specifies the interval the client waits before sending a keep-alive message on a TCP connection.

5.5.8 Discovery

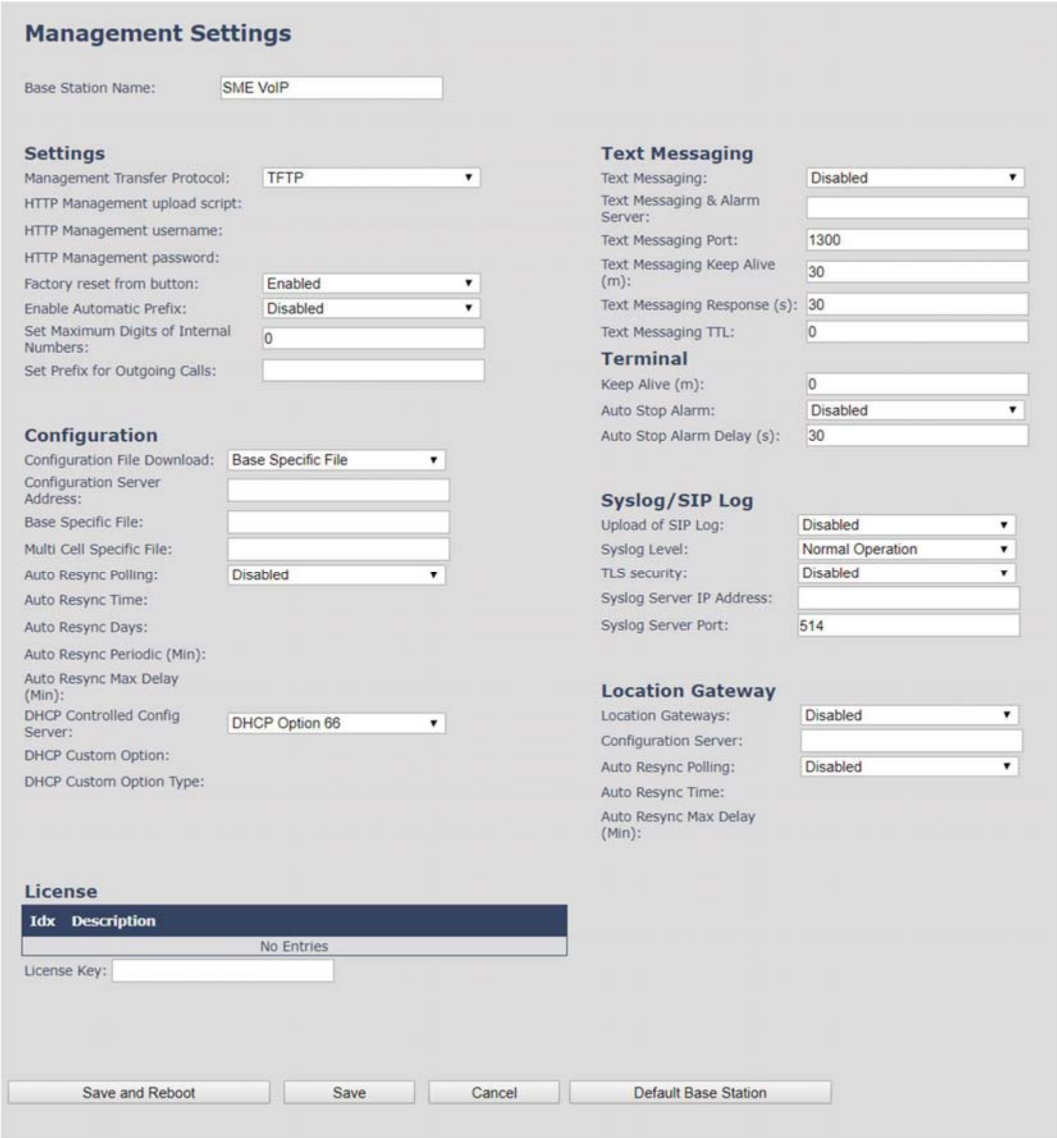
The following parameters of the "Discovery" section are explained

PARAMETER	DEFAULT VALUES	DESCRIPTION
LLDP-MED SEND	Disabled	If "Enabled", the BS will send 5 LLDP-MED messages when started.
LLDP-MED SEND DELAY	30	Sends messages every 30 seconds to inform the network about its LLDP-MED data **Note:** This option works only if the first parameter is enabled (LLDP-MED SEND)
VLAN VIA LLDP-MED	Disabled	If "Enabled", the BS will try to retrieve a VLAN ID from the received LLDP-MED from a switch **Note:** This feature is available only if the first parameter is enabled (LLDP-MED SEND)

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.

Screenshot



5.6.1 Settings:

PARAMETER	Default value	Description
BASE STATION NAME:	SME VoIP	It indicates the title that appears at the top window of the browser and is used in the dualcellpage. Maximum characters: 35
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 USERNAME	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
FACTORY RESET FROM BUTTON	Enabled	If enabled a factory reset will be possible by pressing the button on the BS If disabled, no action will be present by pressing the button on the BS
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 dialed number. In case of detection the base will not complete the dialed 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 FOR INTERNAL NUMBERS	0	Used to detect internal numbers. In case of internal numbers, no prefix number will be added to the dialed number.
SET PREFIX FOR OUTGOING CALLS	Empty	Set the prefix for outgoing calls. Users need to dial this prefix to get an outside line.

5.6.2 Configuration:

PARAMETER	Default value	Description
CONFIGURATION FILE DOWNLOAD	Base Specific File	Base Specific file: Used when configuring a single cell base Base and Multicell Specific File: Used on out of factory bases to specify VLAN and settings.
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**
AUTO RESYNC POLLING	Disabled	Enable to have the base station look for new configuration file, with a predefined time interval
AUTO RESYNC TIME	00:00	Time when the base station shall load the configuration file 24 hour setting
AUTO RESYNC DAYS	0	Number of days between Auto Resync
AUTO RESYNC PERIODIC (MIN)	0	Number of minutes between Auto Resync

AUTO RESYNC DELAY	15	Delay time in sec, to prevent all base station asking for configuration fin at the same time.
DHCP CONTROLLED CONFIG SERVER	DHCP Option 66	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.

5.6.3 Text messaging:

PARAMETER	DEFAULT VALUE	DESCRIPTION
TEXT MESSAGING	Disabled	Disable/enable messaging using a Message/Alarm server Enable Without Server. With this setting handset can send messages to other handsets, which support messaging.
TEXT MESSAGING & ALARM SERVER	Empty	**Permitted value(s): AAA.BBB.CCC.DDD or <URL>**
TEXT MESSAGING PORT	1300	Port number of message server.
TEXT MESSAGING KEEP ALIVE (M)	30	This defines the frequency of how keep-alive are sent **Permitted values:** Positive integer, unit is in minutes
TEXT MESSAGING RESPONSE (S)	30	This defines the frequency of how response timeout **Permitted values:** Positive integer, unit is in seconds
TEXT MESSAGING TTL	0	This defines the text messaging time to live **Permitted values:** Positive integer, unit is in seconds

5.6.4 Terminal:

PARAMETER	DEFAULT VALUE	DESCRIPTION
KEEP ALIVE (M)	0	If different from "0" the handset sends a (emergencyLocationMsg) containing the RSSI measurements with interval "x" that is set. **Permitted values:** Positive integer, unit is in minutes
AUTO STOP ALARM	Disabled	Enable to activate "AUTO STOP ALARM DELAY"
AUTO STOP ALARM DELAY (S)	30	Handset automatically stops alarm announcement (emergencySms) after "x" sec.

5.6.5 Syslog/SIP Log:

PARAMETER	DEFAULT VALUE	DESCRIPTION
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 LEVEL	Normal Operation	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 analyze level also contains the messages from normal operation. Debug: Used by RTX for debug. Should not be enabled during normal operation.
TLS SECURITY	Disabled	If enabled, it uses encrypted TCP, else - UDP
SYSLOG SERVER IP ADDRESS	Empty	**Permitted value(s): AAA.BBB.CCC.DDD or <URL>**
SYSLOG SERVER PORT	514	Port number of syslog server.

5.6.6 Location Gateway

PARAMETER	DEFAULT VALUE	DESCRIPTION
LOCATION GATEWAYS:	Disabled	Enable to allow Location Gateways onto the system. When enabled "Location Gateway" menu will be shown on main menu on the left.
CONFIGURATION SERVER:	Empty	**Permitted value(s): AAA.BBB.CCC.DDD or <URL>**

5.6.7 License:

PARAMETER	DEFAULT VALUE	DESCRIPTION
LICENSE	None	This feature allows administrators to register RTX8930 genetic headsets to the system. License key must be obtained from authorized resellers and only license matching the systems provider code will work.

There are three ways of configuring the system.

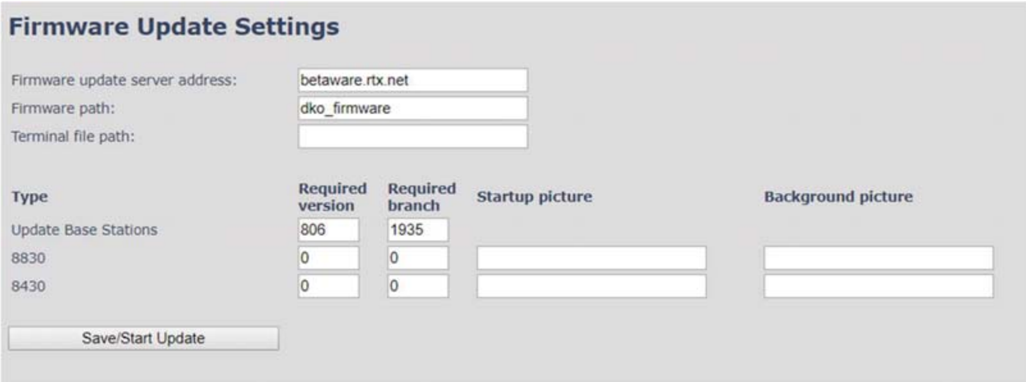
1. Manual configuration by use of the Web server in the base station(s)
2. By use of configuration files that are uploaded from a disk via the "Configuration" page on the Web server.
3. By use of configuration files which the base station(s) download(s) from a configuration server.

For detailed information See Appendix D.

5.7 Firmware Update

In this page, the system administrator can configure how base stations and SIP nodes upgrade/downgrade to the relevant firmware. Handset firmware update status can be found in the extensions page and repeater firmware update status in the repeater page. Base firmware update status is found in the home/status page.

Screenshot

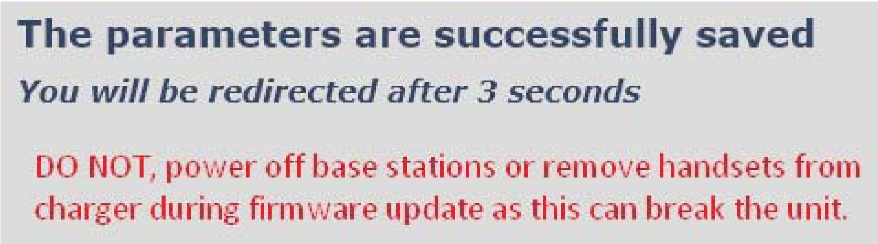


PARAMETER	DEFAULT VALUE(S)	DESCRIPTION
FIRMWARE UPDATE SERVER ADDRESS	Empty	IP address or DNS of firmware update files source **Valid Inputs:** AAA.BBB.CCC.DDD or <URL> **Example:** firmware.rtx.net or 10.10.104.41
FIRMWARE PATH	Empty	Location of firmware on server (or firmware update server path where firmware update files are located). Example: RTXFWU
TERMINAL FILE PATH	Empty	Location of image (folder where background and start up image are located). Example: Images
REQUIRED VERSION	Empty	Version of firmware to be upgraded (or downgraded) on handset, repeater, or base station. **Valid Input(s):** 8-bit string length. E.g. 400 **Note: Value version 0** will disable firmware upgrade **Note:** Two handset types will be serial firmware upgraded. First type 8630 then type 8430.
REQUIRED BRANCH	Empty	Branch of firmware to be upgraded (or downgraded) handset, repeater or base station. **Valid Input(s):** 8-bit string length. E.g. 01
STARTUP PICTURE	Empty	Name of the startup picture you want on the handsets when they are powered up. **NOTE:** Image have same resolution as the screen on the handset(s), this can be found in the handset datasheets If the image does not have the same resolution as the screen, it will be placed in the top left corner. To small the rest of the screen will be black. To large only the left portion of the image will be shown. **NOTE:** Only .BMP is files are supported. **NOTE:** Changing startup picture is not available for new GUI (RTX8631/RTX8632 and RTX8633)
BACKGROUND PICTURE	Empty	Name of the background picture you want on the handsets when they are powered up. **NOTE:** Images have same resolution as the screen on the handset(s), this can be found in the handset datasheets. If the image does not have the same resolution as the screen, it will be placed in the top left corner. To small the rest of the screen will be black. To large only the left portion of the image will be shown **NOTE:** Only .BMP is files are supported. **NOTE:** Changing background picture is not available for new GUI (RTX8631/RTX8632 and RTX8633)

5.7.1 Warning message when firmware upgrading

A warning message will be displayed when starting firmware upgrade.

Screenshot



5.8 Location Gateways

In this section we describe the different setting for Location gateways.

NOTE: to activate Location gateways it must be enabled on the management page (Please see chapter 5.6 for more details)

5.8.1 Register Location gateway

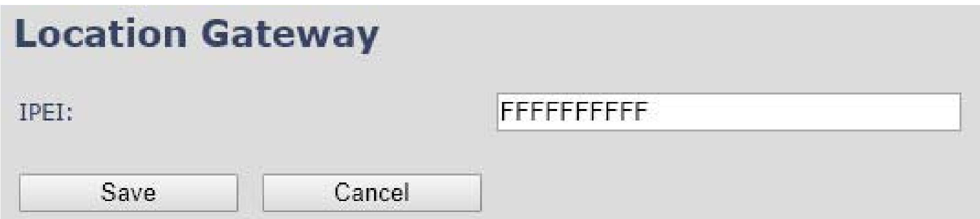
Once you have enabled the feature from the Management menu, please follow the steps below in order to add the Location Gateway:

Step 1: Select Add Location Gateway extension

Screenshot

Step 2: Press save and leave the IPEI: FFFFFFFFF

Screenshot



Step 3: Check the box on the Location gateways that you want to register

Screenshot

5.9 Country/Time Settings

In this section, we describe the different parameters available in the Country/Time settings menu.

The country setting controls the following in-band tones used by the system:

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

The Time server supplies the time used for data synchronisation in a dual-cell configuration. As such it is mandatory for a dual-cell configuration. The system **will not work** without a time server configured.

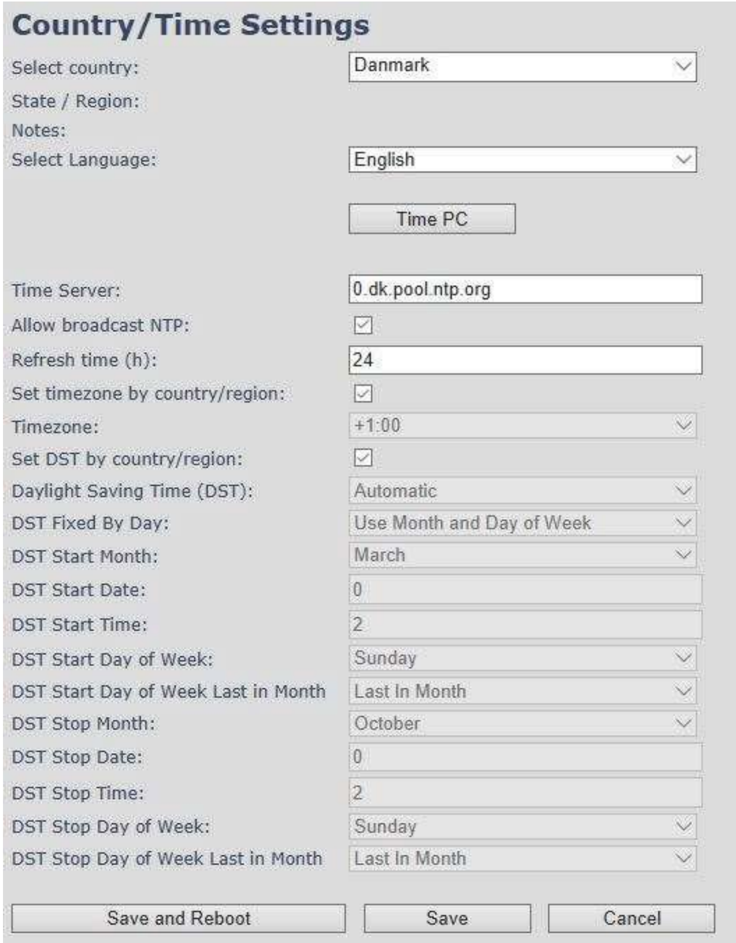
As well the time server is used in the debug logs and for SIP traces information pages and used to determine when to check for new configuration and firmware files.

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 or type the IP address of an NTP server that is closer to you (find it via Google).

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. Changing time settings will require a reboot of system.

Screenshot



PARAMETER	DEFAULT VALUES	DESCRIPTION
SELECT COUNTRY	US/Canada	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	N/A	Only shown by country selection US/Canada, Australia, Brazil
SELECT LANGUAGE	English	Web interface language. Number of available languages: English, Dansk, Italiano, Türkçe, Deutsch, Portuguese, Hrvatski, Srpski, Slovenian, Nederland's, Francaise, Espanyol, Russian, Polski.
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, Handsets, 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)	24	The window time in hours within which time server refreshes. **Valid Inputs:** positive integer
SET TIME ZONE BY COUNTRY/REGION	Checked	By checked country setting is used (refer to country web page).
TIMEZONE	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)	Automatic	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 Day of week	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	0	Numerical day of month DST comes to effect when DST is fixed to a specific date **Valid Inputs:** positive integer
DST START TIME	2	DST start time in the day **Valid Inputs:** positive integer
DST START DAY OF WEEK	Sunday	Day within the week DST begins
DST START DAY OF WEEK, LAST IN MONTH	Second First In Month	Specify the week that DST will actually start.
DST STOP MONTH	October	The month that DST actually stops.
DST STOP DATE	0	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	Last in Month	The week within the month that DST will turn off.

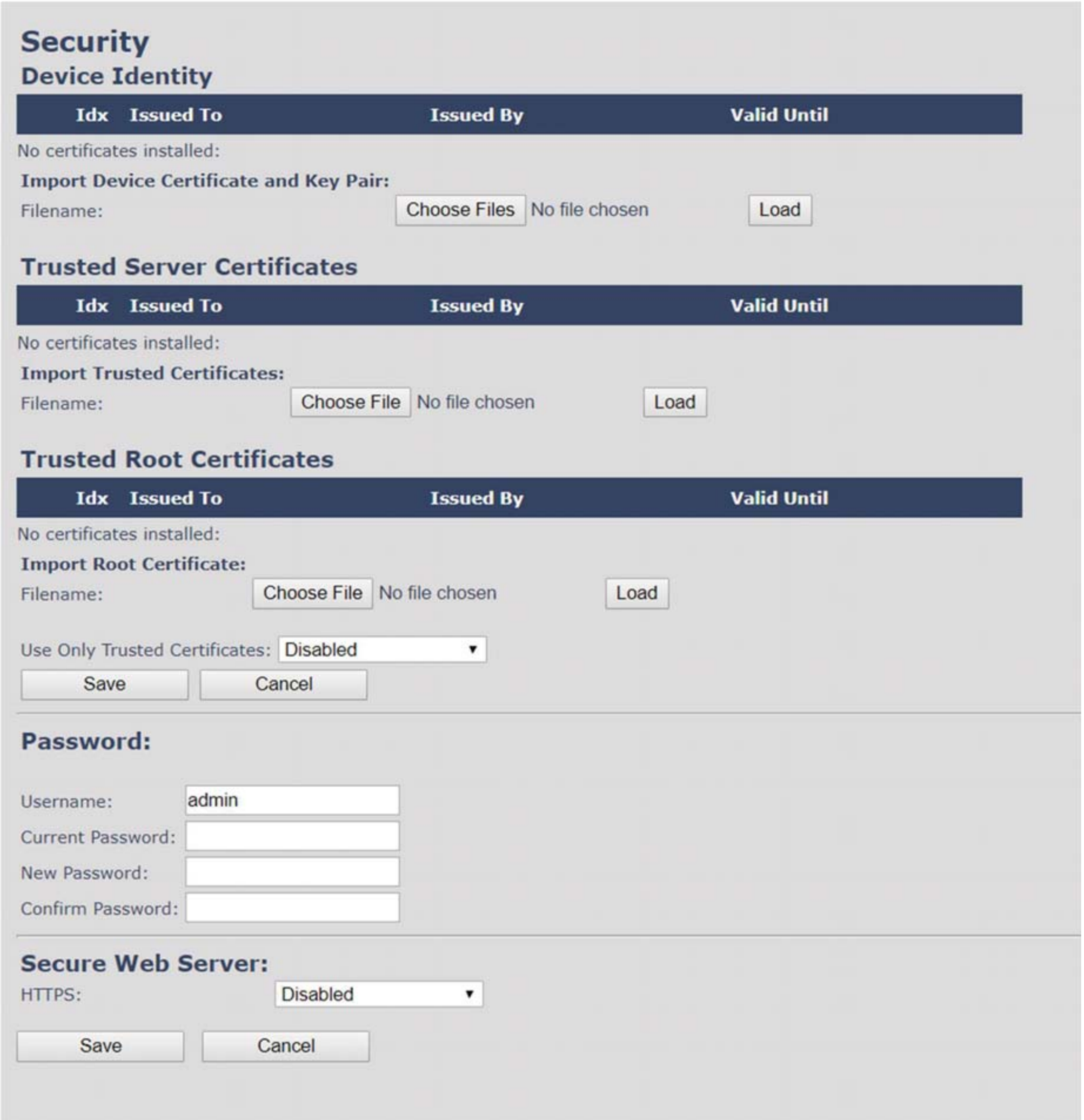
NOTE: By checked time zone and DST the parameters in web page Time will be discarded.

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 chapter 5.6).

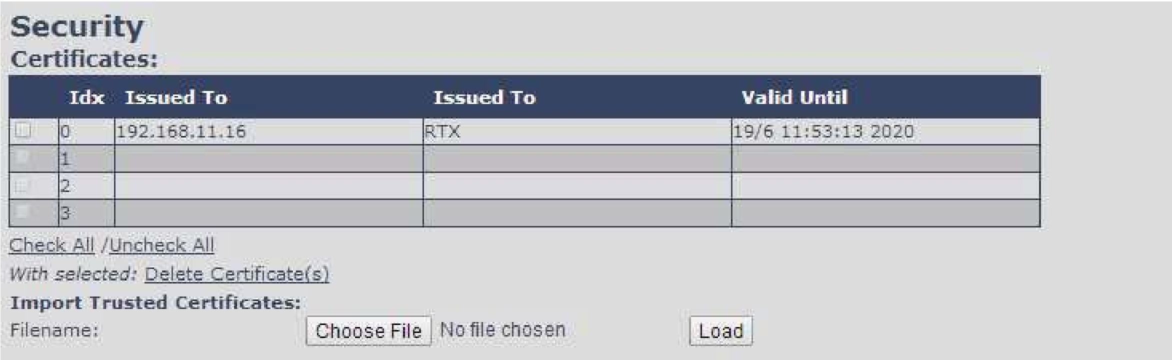
SIP and RTP security are dependent servers and in order to configure them , the user must use the web option Servers (refer to chapter 5.4)
Screenshot



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 to click on “Choose file” and browse to the selected file. When file is selected, use the “Load” button to load the certificate.
The certificate format supported is DER encoded binary X.509 (.cer).

Screenshot



5.10.2 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	Organization, Company – which is part of the certificate file
VALID UNTIL	Empty	Date Time Year – which is part of the certificate file

Screenshot

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.

5.10.3 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 "Choose 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 Certificate
Screenshot

5.10.4 Device identity

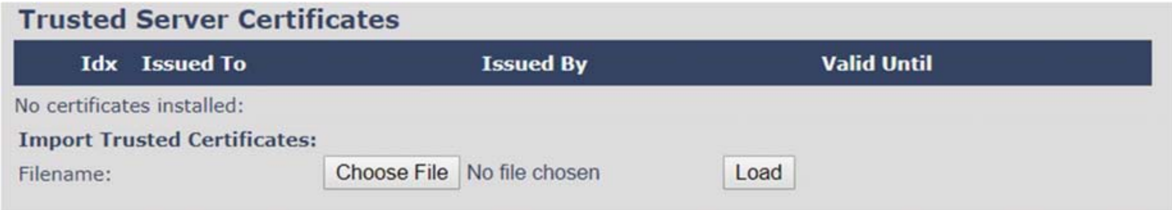
The certificate and personal key used by the base when acting as server or when the server requires client authentication in the SSL handshake procedure.

Screenshot

5.10.5 Trusted Server Certificates

Intermediate certificates (non-root certificates) trusted by the base. Used to validate a received certificate chain (or a chain of trust) in scenarios where only the root certificate is sent by the server during the SSL handshake procedure

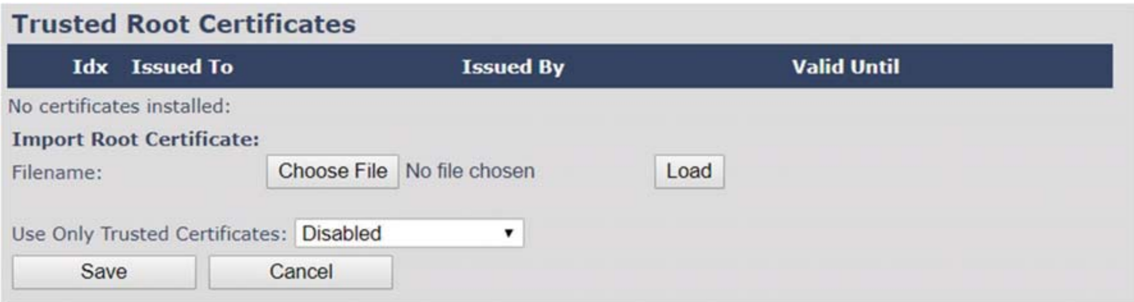
Screenshot



5.10.6 Trusted Root Certificates

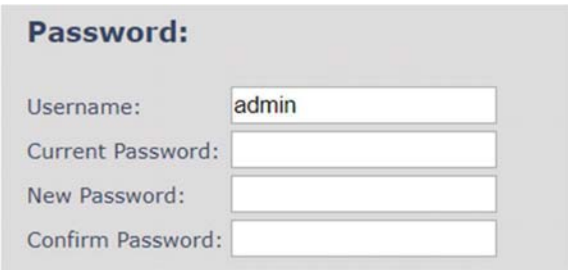
Root certificates (self-signed) trusted by the base. Used to validate received root certificates sent by the server during the SSL handshake procedure.

Screenshot



5.10.7 Password

In the below settings the password parameters are defined.



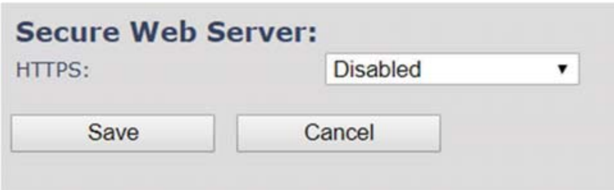
PARAMETER	Default Values	Description
USERNAME	Admin	Can be modified to any supported character and number Maximum characters: 15
CURRENT PASSWORD	Admin	Can be modified to any supported character and number
NEW PASSWORD	Empty	Change to new password Maximum characters: 15
CONFIRM PASSWORD	Empty	Confirm 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

5.10.8 Secure Web Server

This setting allows all communication with the Web Server to be encrypted.

Screenshot



PARAMETER	DEFAULT VALUES	DESCRIPTION
HTTPS	Disabled	Enable to use HTTPS for Web Server Communication.

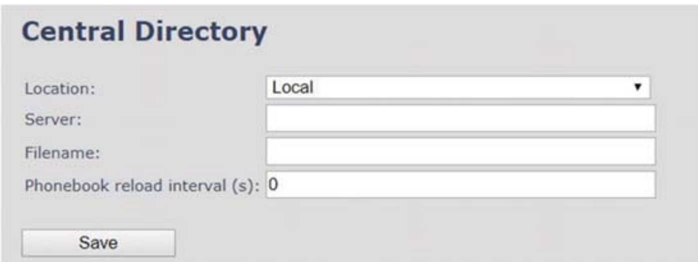
5.11 Central Directory and LDAP

The SME VOIP system supports 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.

5.11.1 Local Central Directory

Select local and save for local central directory.

Screenshot



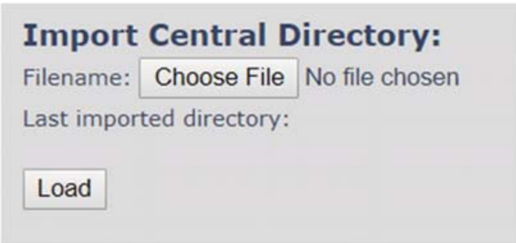
PARAMETER	DEFAULT VALUES	DESCRIPTION
LOCAL	Local	Drop down menu to select between local central directory, LDAP based central directory and xml server

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 supports 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 (Max file size 100kb). For further details of the central directory feature refer to appendix.

Screenshot

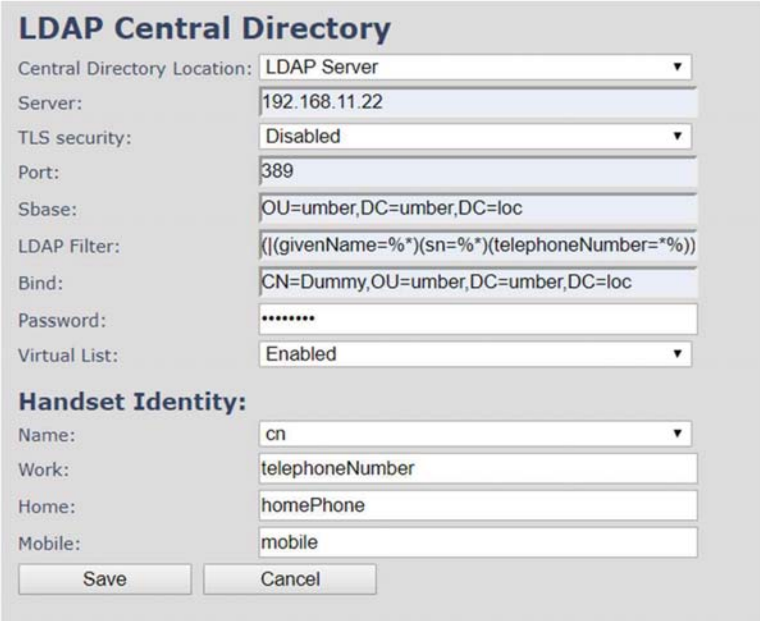


5.11.2 LDAP

Select LDAP Server and save for LDAP server configuration.

Screenshot

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>
TLS SECURITY	Disabled	If enabled, it uses encrypted TCP, else - UDP
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
VIRTUEL LISTS	Enabled	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

5.11.3 Characters supported

The below table shows which characters are supported in the communication between RTX9431 and handset.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0				0	@	P	`	p	€	İ		°	À	Đ	à	đ
1			!	1	A	Q	a	q	ı	'	¡	±	Á	Ñ	á	ñ
2			"	2	B	R	b	r	‚	'	¢	Č	Â	Ò	â	ò
3			#	3	C	S	c	s	ƒ	"	£	č	Ã	Ó	ã	ó
4			$	4	D	T	d	t	„	"	¤	´	Ä	Ô	ä	ô
5			%	5	E	U	e	u	…	▪	¥	µ	Å	Õ	å	õ
6			&	6	F	V	f	v	†	–	¦	¶	Æ	Ö	æ	ö
7			'	7	G	W	g	w	‡	—	§	·	Ç	×	ç	÷
8			(	8	H	X	h	x	ˆ	˜	¨	¸	È	Ø	è	ø
9			)	9	I	Y	i	y	Ř	ř	Ů	Ď	É	Ù	é	ù
A			*	:	J	Z	j	z	Š	š	ů	ď	Ê	Ú	ê	ú
B			+	;	K	[	k	{	‹	›	«	»	Ë	Û	ë	û
C			,	<	L	\	l	|	Œ	œ	Ě	Ť	Ì	Ü	ì	ü
D			-	=	M	]	m	}	Ş	ş	ě	ť	Í	Ý	í	ý
E			.	>	N	^	n	~	Ž	ž	Ň	ň	Î	Þ	î	þ
F			/	?	O	_	o	Ğ	ğ	Ÿ	¯	¿	Ï	ß	ï	ÿ

5.12 Dual-cell Parameter Definitions

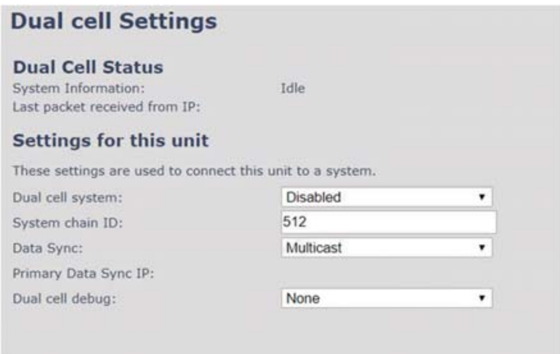
NOTE: To join one Base Station in a dual-cell system, you need to have one handset added to the system. For details and Step-by-Step guide to dual cell, please see Appendix

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

5.12.1 Settings for Base Unit

Description of Settings for Specific Base units is as follows:

Screenshot



Dual-Cell status covers status of data synchronization. The status “Keep-alive” means normal operation, as well as “Idle”.

PARAMETER	DEFAULT VALUES	DESCRIPTION
DUAL CELL SYSTEM	Disabled	Enable this option to allow the Base unit to be set in dual-cell mode (can be set either as master or slave in the dual-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	512	This is an identifier (in string format e.g. 2275) that is **unique** for a specific dual-cell system. The Chain ID value MUST not be equal to a used SIP account. The Chain ID uses up a SIP account with this value. **NOTE:** Chain ID is used as SIP account for check Sync. Default value is 512, which means extension 512 must not be used – unless the chain ID is modified. Chain ID can be modified by provisioning only. **Note:** There can be several dual-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.
DATA SYNC:	Multicast	To select between multicast or Peer to Peer data synchronization 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. **For multi-cast operation make sure that Multicast/IGMP is enabled on your switch(es), else use Peer-to-peer mode.**
PRIMARY DATA SYNC IP	Empty	IP of base station data sync source – the base handling the data synchronization. Using multicast this base IP is selected automatically. The data sync feature uses the port range: 49200 – 49999 **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.
DUAL CELL DEBUG	None	Enable this feature, if you want the system to catalogue low level dual-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:

Screenshot

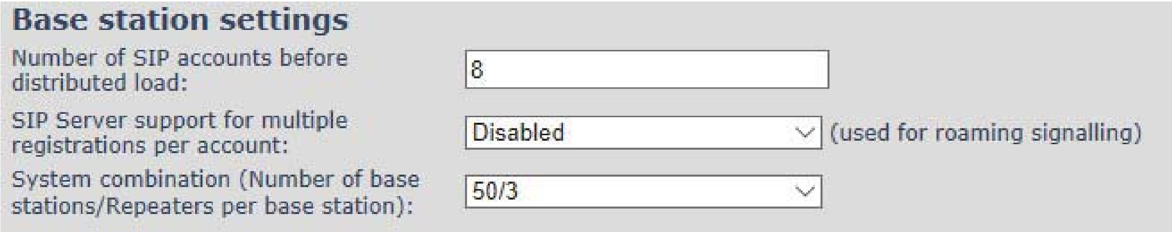
PARAMETER	DEFAULT VALUES	DESCRIPTION
DECT SYSTEM RFPI	Not able	This is a radio network identity accessed by all Base units in a specific multi-cell system. It composed of 5 octets. It is actually 5 different variables combined together. **RFPI Format:** XX XX XX XX XX (where XX are HEX values)
ALLOW 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 establishing of the faulty base, the system must be rebooted. Allow multi primary must be enabled for this feature to also be enabled.
AUTO CONFIGURE DECT SYNC SOURCE TREE	Enabled	Enable this to allow the system to automatically synchronize the multi-cell chain/tree. NOTE: Must be enabled in order to allow a new primary to recover in case the original primary goes into faulty mode.

NOTE: To run with a system with two separate primaries 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:

Screenshot



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 base stations. **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	Disable 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. Permitted Input: Disabled: No SIP de-registration will be made when a handset roams to another base station Enabled: The old SIP registration will be deleted with a SIP Deregistration, when a handset roams to another base station
SYSTEM COMBINATION (NUMBER OF BASE STATIONS/REPEATERS PER BASE STATION):	50/3	Select between basic base configurations. 50/3 : 50 bases and 3 repeaters 127/1 : 127 bases and 1 repeater 254/0 : 254 bases and 0 repeater The configuration cannot be modified after a system is established. The configuration must be set during first multicell configuration.

5.12.4 Base Station Group

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

Screenshot:

Base Station Group

	ID	RPN	Version	MAC-Address	IP-Address	IP Status	DECT sync source	DECT property	Base Station Name
☐	0	00	280	00087B0A00B3	192.168.11.159	This Unit	Select as primary	**Primary**	1
☐	1	04	280	00087B09FECA	192.168.11.116	Connected	Primary:RPN00 (-24dBm)	Locked	2
☐	2	08	280	00087B09FE45	192.168.11.113	Connected	Level 1:RPN04 (-24dBm)	Locked	3
☐	3	0C	280	00087B09FF08	192.168.11.109	Connected	Level 2:RPN08 (-24dBm)	Locked	4
☐	4	10	280	00087B09FE4A	192.168.11.166	Connected	Level 3:RPN0C (-24dBm)	Locked	5
☐	5	14	280	00087B079205	192.168.11.133	Connected	Level 4:RPN10 (-24dBm)	Locked	6

Check All / Uncheck All
With selected: Remove from chain

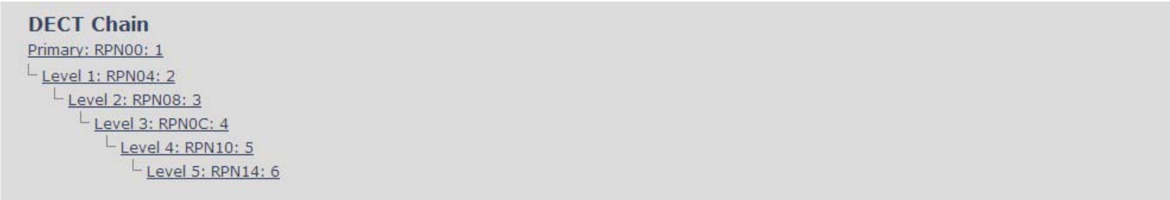
PARAMETERS	DESCRIPTION
ID	Base unit identity in the chained network. **Permitted Output:** Positive Integers
RPN	The Radio Fixed Part Number is an 8-bit DECT cell identity allocated by the installer. The allocated RPN within the SME must be geographically unique. **Permitted Output:** 0 to 255 (DEC) **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 behavior 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 another 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 synchronizes 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 synchronization to the Master. **Unknown:** No current connection information from specific Base unit

	Assisted lock: Base has lost DECT sync. source and Ethernet are 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

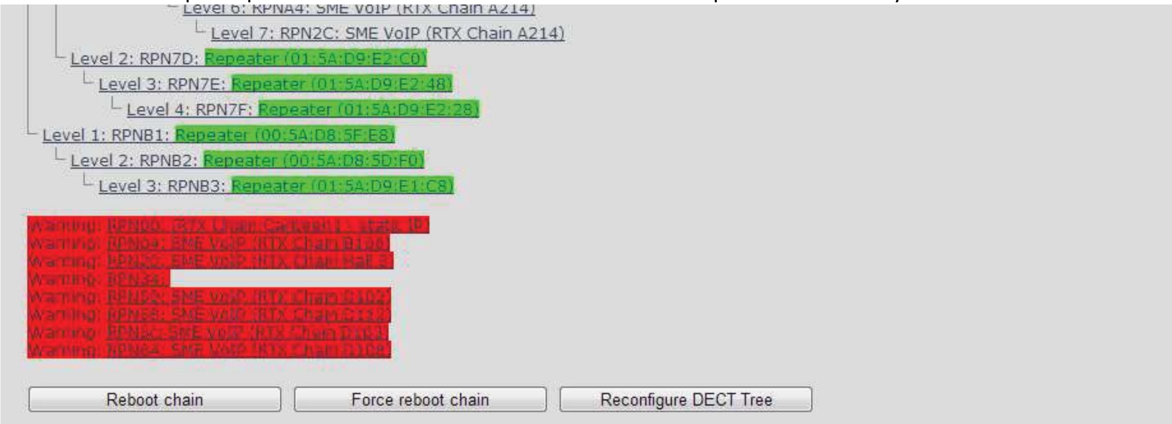
Below the Base Group Table is the DECT Chain tree. The DECT Chain tree is a graphical presentation of the Base Group table levels and connections. Repeaters are shown with green highlight.

Screenshot: DECT Chain tree of above configuration



Screenshot: Example of part of DECT Chain tree with repeaters

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.

5.12.6 RTX8660 -RTX8663 Mixed mode

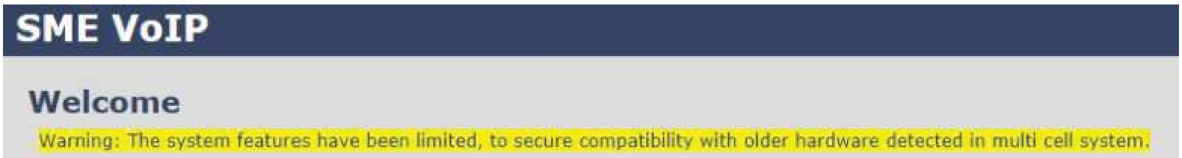
RTX8663 base station can be added to existing systems using RTX8660 base station. Because the RTX8663 have more powerful hardware and additional features, there will be some limitations.

A system running mixed mode, is limited to RTX8660 features.

NOTE: LAN SYNC will not work in mixed mode.

The system will display a warning message on the Home/Status page.

Screenshot:



5.13 LAN SYNC

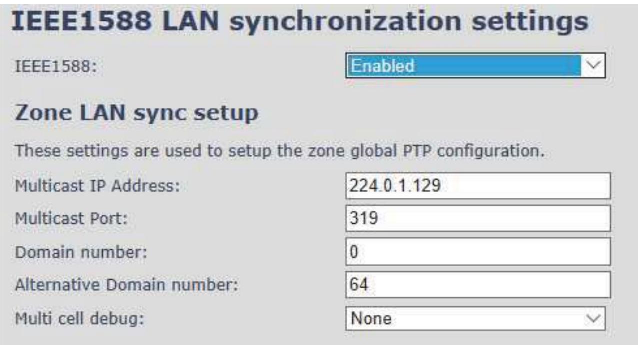
NOTE: To join one Base Station in a dual-cell system, you need to have one handset added to the system. For details and Step-by-Step guide to dual cell, please see Appendix

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

5.13.1 Settings for Base Unit

Description of Settings for Specific Base units is as follows:

Screenshot:



PARAMETERS	DEFAULT VALUES	DESCRIPTION
MULTICAST IP ADDRESS	224.0.1.129	IP address of the multicast group. The IP address must start with 224.0.xx.xx this cannot be changed. To be compliant with IEEE1588, this port must be default value. Before setup, make sure no other devise uses the given IP. **NOTE:** this should only be changed in case other IEEE1588 equipment is on the network and using this specific IP address.
MULTICAST PORT	319	Define the port that the system must communicate on To be compliant with IEEE1588, this port must be default value. **NOTE:** this should only be changed in case other IEEE1588 equipment is on the network and using this specific port.
DOMAIN NUMBER	0	Domain number is used to set what domain this specific base station belongs to. Valid input: 0-127
ALTERNATIVE DOMAIN NUMBER	64	Alternative domain is only used in case the primary sync source from the main domain fails, this the base station will sync with the alternative domain. Must NOT have same value as domain number. Valid input: 0-127
MULTI CELL DEBUG MODE	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. **IEEE1588 Debug:** Writes IEEE1588 debug information **NOTE:** Must only be used for debug purpose and not enabled on a normal running system

5.13.2 Base station group

The Base station group list various parameter settings for base stations.

Screenshot:

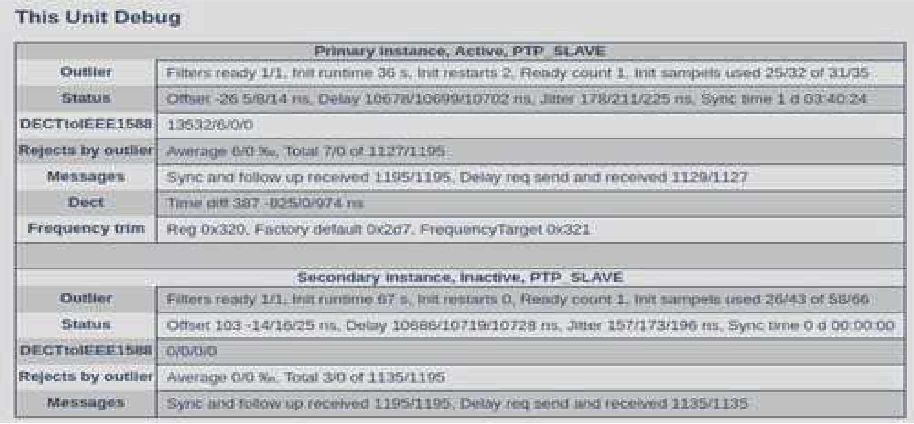
Base Station Group

ID	Status	Prefered Role	Current Role	Sync. Source	Alt. Sync. source	Nwk. Jitter [ns] (min/avg/max)	Nwk. Delay [ns] (min/avg/max)	IP Status	Base Station Name
0	Primary	Primary	Primary	LAN:Primary	LAN:ID:3	(0/0/0)	(0/0/0)	This Unit	ATI-8
1	Locked	Automatic	Secondary	LAN:ID:0	LAN:ID:3	(190/193/215)	(10678/10692/10702)	Connected	ATI-13
2	Locked	Automatic	Secondary	LAN:ID:0	LAN:ID:3	(189/210/223)	(10679/10695/10698)	Connected	ATI-7
3	Locked	Automatic	Secondary	LAN:ID:0	LAN:Primary	(177/200/206)	(10689/10721/10723)	Connected	ATI-12

PARAMETERS	DESCRIPTION
ID	Base unit identity in the chained network. **Permitted Output:** Positive Integers
STATUS	Base station characteristics in connection to the current multi cell network. Possible Output(s) **Primary:** Main Base station into which all other nodes in the chain synchronizes to. **Locked:** The Base unit is currently synchronized and locked to the master Base unit. **Searching:** Base unit in the process of locating a Master/slave as specified in DECT sync source **Free Running:** IEEE master is found, and is DECT synchronizing
PREFERED ROLE	**Disabled:** Disable this base station from the chain **Primary:** The base station that is used for main sync, it is possible to select more than one base station as primary. NOTE: It is recommended to use base stations that is closest to the backbone as primary **Secondary:** Base stations that never will be selected as primary. **Automatic:** System finds primary sync source **Alt. Primary:** Backup for primary base station in case it fails.
CURRENT ROLE	The current role of the base station
SYNC SOURCE	Shows what base station this specific base station is synchronized with
ALT. SYNC SOURCE	Alternative sync source in case main sync source fails
NWK JITTER [MS] (MIN/AVG/MAX)	Measures how the IEEE1588 packets are received, the lower the Jitter is the better
MWK DELAY [MS] (MIN/AVG/MAX)	Measures the time it takes an IEEE packet to travel from primary to Slave base station in ms.
IP STATUS	Current Base station behavior 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
BASE STATION NAME	Name from management settings.

5.13.3 This unit debug

Screenshot:



This Unit Debug

Primary instance, Active, PTP_SLAVE	
Outlier	Filters ready 1/1, Init runtime 36 s, Init restarts 2, Ready count 1, Init sampels used 25/32 of 31/35
Status	Offset -26 5/8/14 ns, Delay 10678/10699/10702 ns, Jitter 178/211/225 ns, Sync time 1 d 03:40:24
DECTtoIEEE1588	13532/6/0/0
Rejects by outlier	Average 6/0 ‰, Total 7/0 of 1127/1195
Messages	Sync and follow up received 1195/1195, Delay req send and received 1129/1127
Dect	Time diff 387 -825/0/974 ns
Frequency trim	Reg 0x320, Factory default 0x2d7, FrequencyTarget 0x321
Secondary instance, Inactive, PTP_SLAVE	
Outlier	Filters ready 1/1, Init runtime 67 s, Init restarts 0, Ready count 1, Init sampels used 26/43 of 58/66
Status	Offset 103 -14/16/25 ns, Delay 10686/10719/10728 ns, Jitter 157/173/196 ns, Sync time 0 d 00:00:00
DECTtoIEEE1588	0/0/0/0
Rejects by outlier	Average 0/0 ‰, Total 3/0 of 1135/1195
Messages	Sync and follow up received 1195/1195, Delay req send and received 1135/1135

Debug information is used only by RTX to debug IEEE1588 network issues.

In case debug is needed, sent this information to RTX support team.

5.14 Repeaters

Within this section we describe the repeater parameters, and how to operate the repeater.

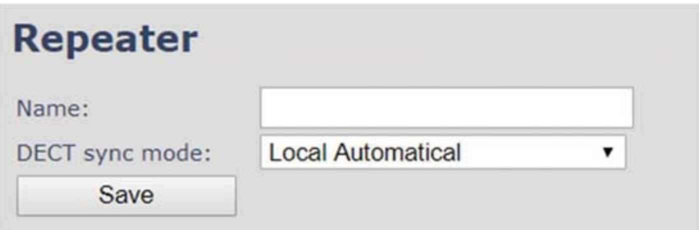
5.14.1 Add repeater

In order to add a repeater to the system, select "Add Repeater"

Screenshot

Thereafter the following window with the specific parameters will be visible

Screenshot



PARAMETERS	DEFAULT VALUES	DESCRIPTION
NAME	Empty	Repeater name. If no name specified, the field will be empty
DECT SYNC MODE	Local Automatical	**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.

5.14.1.1 Manually

If the mode is chosen to be "Manually", the assigned parameters "Repeater RPN" and "DECT sync source RPN" must be selected by the drop-down menu.

Screenshot

After saving the configurations above, the repeater will be visible on the main "Repeaters" menu with the following parameters:

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) DUAL 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)
NAME/IPEI	Name and IPEI number of the repeater
DECT SYNC MODE	DECT Sync mode – Manually or Automatic
STATE	State of the repeater Enabled/Disabled
FW INFO	Firmware version
FWU PROGRESS	How many percentages of the firmware is loaded / Off if no firmware is being loaded

Good practice when adding repeaters to a Dual Cell system is to use manually registration, because then you can control what base station the repeater(s) connects to.

5.14.1.2 Local Automatical

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

Screenshot

Repeater

Name: RPN2

DECT sync mode: Local Automatical

Save

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

5.14.2 Register Repeater

Adding a repeater makes it possible to register the repeater. Registration is made by selecting the repeater via the checkbox 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 including handset registration.

	Idx	RPN	Name/ IPEI	DECT sync source	DECT sync mode	State	FW Info	FWU Progress
☐	2		RPN2/ FFFFFFFFFF		Local Automatical	Enabled		

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

5.14.3 Repeaters list

Screenshot

Repeaters

Add Repeater

Refresh
Stop Registration

	Idx	RPN	Name/ IPEI	DECT sync source	DECT sync mode	State	FW Info	FWU Progress
☐	1	RPN02	RPN1/ 015AD85E80	RPN00 (-26dBm)	Local Automatical	Present@RPN00	41.1	Off
☐	2	RPN01	RPN2/ 005AD85D90	RPN00 (-26dBm)	Local Automatical	Present@RPN00	41.1	Off
☐	3	RPN03	/ 0298D024A0	RPN00 (-26dBm)	Local Automatical	Present@RPN00	41.1	Off

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

The number of repeaters allowed on each base station is mentioned above in 5.14.1.1.
System combination: 50/3 – 127/1 -254/0.
If the system combination is set to 127/1 or 254/0 you can still register more than one repeater, but it will not get a DECT Sync source and have no function.

Example:
System combination 50/3:
Base stations are named RPN00 – RPN04 – RPN08. Etc. jumping 4 numbers each time (HEX numbers)
Repeaters connect to base station RPN00 will be called RPN01 – RPN02 – RPN03 (HEX numbers)
Repeaters connect to base station RPN04 will be called RPN05 – RPN06 – RPN07 (HEX numbers)

Etc.

System combination 127/1:
Base stations are named RPN00 – RPN02 – RPN04. Etc. jumping 2 numbers each time (HEX numbers)
Repeaters connect to base station RPN00 will be called RPN01 (HEX numbers)
Repeaters connect to base station RPN02 will be called RPN05 (HEX numbers)
Etc.

System combination 254/0:
Repeater registration not possible.

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 not given the field will be empty.
DECT SYNC SOURCE	The "dual cell chain" connection to the specific Base/repeater unit. Maximum number of chain levels is 12. 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.

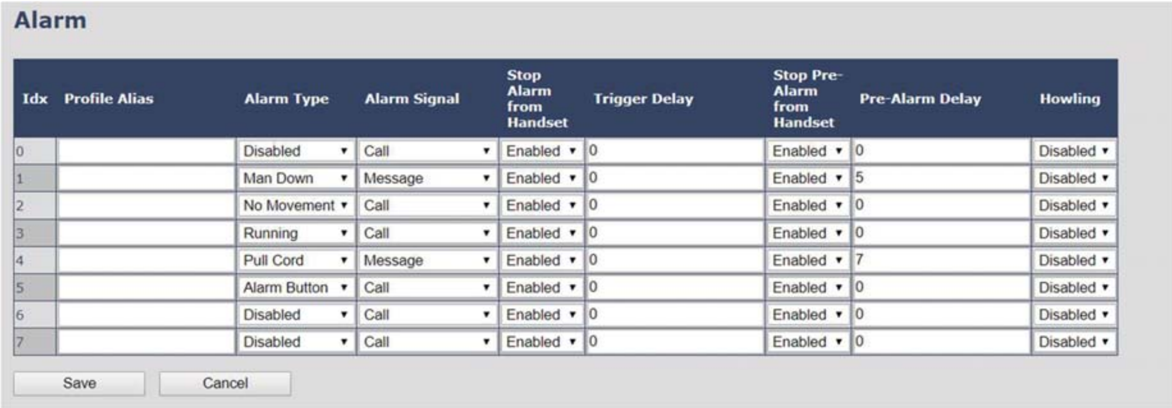
For detailed description on how to operate repeaters please see Repeater HOW-TO guide. Link is found in Appendix.

5.15 Alarm

In the Alarm Settings menu, it is controlled how an alarm appears on the handset. For example, if the handset detects "Man Down", then it is defined in this menu what alarm signal this type of alarm will send out and if a pre-alarm shall be signaled etc.

The Alarm is activated by a long press on the Alarm key (3 sec).

Screenshot



Alarm

Idx	Profile Alias	Alarm Type	Alarm Signal	Stop Alarm from Handset	Trigger Delay	Stop Pre-Alarm from Handset	Pre-Alarm Delay	Howling
0		Disabled	Call	Enabled	0	Enabled	0	Disabled
1		Man Down	Message	Enabled	0	Enabled	5	Disabled
2		No Movement	Call	Enabled	0	Enabled	0	Disabled
3		Running	Call	Enabled	0	Enabled	0	Disabled
4		Pull Cord	Message	Enabled	0	Enabled	7	Disabled
5		Alarm Button	Call	Enabled	0	Enabled	0	Disabled
6		Disabled	Call	Enabled	0	Enabled	0	Disabled
7		Disabled	Call	Enabled	0	Enabled	0	Disabled

Save Cancel

All configuration of the handset Alarm Settings is done from the base station. The concept is that on the "Alarm" page on the web server, eight different alarm profiles can be configured. Afterwards for each handset, it can be selected which of the configured alarm profiles, the given handset shall subscribe to. When this is done the selected alarm, profiles are sent to the handset.

See section 5.3.4: Edit handset.

PARAMETERS	DEFAULT VALUES	DESCRIPTION
IDX		Indicates the index number of a specific alarm.
PROFILE ALIAS	Empty	An alias or user-friendly name to help identify the different profiles when selecting which profiles to enable for the individual handsets.
ALARM TYPE	Disabled	The type of alarm is dependent of what kind of event that has triggered the alarm on the handset. The type of alarms supported is handset related. **RTX8632/RTX8633:** Alarm button **RTX8830:** Alarm button Man Down No Movement Running Pull Cord Emergency Button Disabled
ALARM SIGNAL	Call	The way the alarm is signaled as it received on the handset. **Message:** A text message to an alarm server. **Call:** An outgoing call to the specified emergency number. **Beacon message:** Sends a beacon to the alarm server which sends a message to the handset
STOP ALARM FROM HANDSET	Enabled	**Enable/Disable** the possibility to stop/cancel the alarm from the handset.
TRIGGER DELAY	0	The period from when the alarm has fired until the handset shows a pre-alarm warning. If set to 0, there will be no pre-alarm warning, and the alarm will be signaled immediately. The alarm algorithm typically needs about 6 sec. to detect e.g. man down etc.

STOP PRE-ALARM FROM HANDSET	Enabled	**Enable/Disable** the possibility to stop/cancel the pre-alarm from the handset.
PRE-ALARM DELAY	0	The period from the pre-alarm warning is shown until the actual alarm is signaled. The maximum value is 255.
HOWLING	Disabled	**Enable/Disable** if howling shall be started in the handset, when the alarm is signaled. If disabled, only the configured signal is sent (call or message).

NOTE: The alarm feature is only available on some types of handsets (e.g. RTX8632, RTX8633 and RTX8830)
After configuration, the handset must be rebooted.

5.15.1 Use of Emergency Alarms

As described above, it can be configured if it shall be possible to stop an alarm from the handset. If the possibility to stop an alarm from the handset is disabled, it is ensured that an alarm is not stopped before someone at e.g. an emergency center has received the alarm and reacted upon it.

The behavior of a handset when an alarm "is sent" depends on the configured Alarm Signal:

- **Call:** When the Alarm Signal is configured as "Call", the handset will make a call to the specified emergency number, and the alarm is considered stopped when the call is terminated. If it is not allowed to stop the alarm from the handset, it will not be possible to terminate the call from handset, and the alarm will be considered as stopped only when the remote end (e.g. the emergency center) terminates the call.
- **Message:** When the Alarm Signal is configured as "Message", the handset will send an alarm message to the specified alarm server, and enable auto answer mode. If Howling is enabled, the handset will also start the Howling tone. The alarm will not stop until a call is made, and since auto answer mode is enabled, the emergency center can make the call, and the person with the handset does not have to do anything to answer the call, it will answer automatically. Again, the alarm is considered stopped, when the call is terminated with the same restrictions as for the Call alarm signal.

All type of alarms have the same priority. This means that once an alarm is active, it cannot be overruled by another alarm until the alarm has been stopped. However, if the alarm is not yet active, i.e. if it is in "pre-alarm" state and an alarm configured with no pre-alarm is fired, then the new alarm will become active and stop the pending alarm.
Alarms with no pre-alarm are considered important, and there is no possibility to cancel them before they are sent, and therefore alarms with no pre-alarm, are given higher priority than alarms in pre-alarm state.

The Emergency Button could be an example of an alarm which would be configured without pre-alarm. Thus, when the Emergency Button is pressed you want to be sure the alarm is sent. However, if another alarm was already in pre-alarm state, it could potentially be cancelled, and if the Emergency Button alarm was ignored in this case, no alarm would be sent. This is the reason alarms with no pre-alarm, are given higher priority than alarms in pre-alarm state.

For detailed description on how to alarm please see Alarms HOW-TO guide. Link is found in Appendix.

5.16 Statistics

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

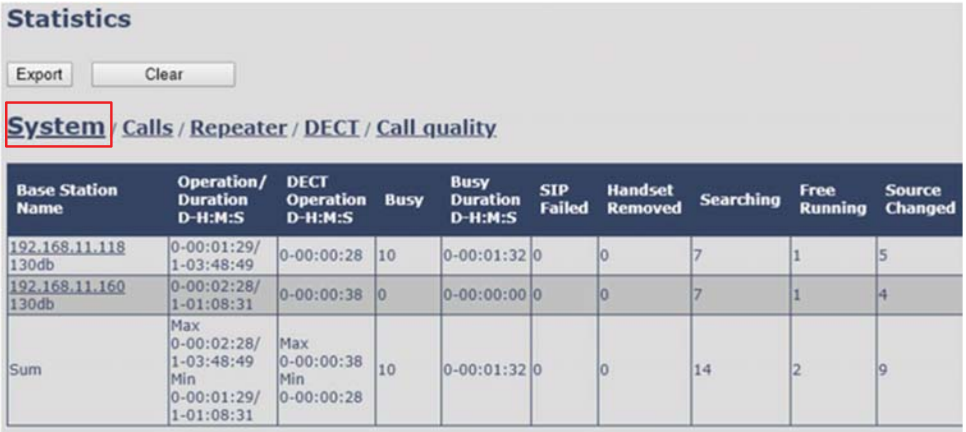
1. System
2. Calls
3. Repeater
4. DECT data
5. Call quality

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

5.16.1 System data

The system data web is accessed by http://ip/SystemStatistics.html and data is organized in a table as shown in below example.

Screenshot



Statistics

Export Clear

System / Calls / Repeater / DECT / Call quality

Base Station Name	Operation/ Duration D-H:M:S	DECT Operation D-H:M:S	Busy	Busy Duration D-H:M:S	SIP Failed	Handset Removed	Searching	Free Running	Source Changed
192.168.11.118 130db	0-00:01:29/ 1-03:48:49	0-00:00:28	10	0-00:01:32	0	0	7	1	5
192.168.11.160 130db	0-00:02:28/ 1-01:08:31	0-00:00:38	0	0-00:00:00	0	0	7	1	4
Sum	Max 0-00:02:28/ 1-03:48:49 Min 0-00:01:29/ 1-01:08:31	Max 0-00:00:38 Min 0-00:00:28	10	0-00:01:32	0	0	14	2	9

The table is organized 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 its sync source
FREE RUNNING	Base free running is the number of times a base has been free running
DECT SOURCE CHANGED	Number of times a base has changed sync source

5.16.2 Free Running explained

First, state Free running is NOT an error state, but is a simple trigger state, indicating that some changes have to be made to ensure continuous DECT synchronization.

The state Free running tells the application that the base has not received any synchronization data from its synchronization source base station in the last 10 seconds.

The reason for this can be several:

1. The two bases are using the same DECT slots and can therefore not see each other.
2. Many simultaneous voice or data calls.
3. Suddenly change of environment (Closing a fire door)
4. Distortion of DECT frequency (around 1.8MHz) Either by other DECT systems or other equipment.

When the Free running state is trigged, several recovery mechanisms are activated:

1. Move DECT slot to avoid using same DECT slot as its synchronization source base state.
2. Use information from all other base station, how they are seeing this base station in the DECT air. This is marked by changing to state Assisted lock

The state Assisted lock can be stabile for a long time and normally change to state Locked again.
The state Free Running can also change back to state Locked again.

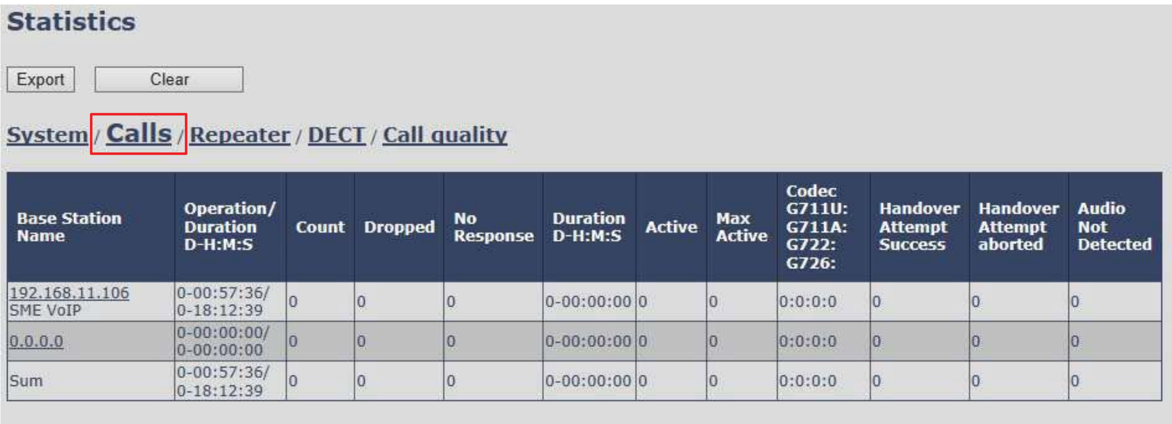
If the base is in state Free running and the synchronization source base station is not seen and no data is available for the assisted lock mechanism, the base station will change to a new state after 2 minutes:

1. If the base station does NOT have any active calls, the base will change to state Searching.
2. If the base station has an active call, this base will change to state Sync lost. After the call is released, the state will change to state Searching.

5.16.3 Call data

The call data web is accessed by http://ip/CallStatistics.html and data are organized in a table as shown in below example.

Screenshot


Statistics

Export Clear

System / Calls / Repeater / DECT / Call quality

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 Attempt Success	Handover Attempt aborted	Audio Not Detected
192.168.11.106 SME VoIP	0-00:57:36/ 0-18:12:39	0	0	0	0-00:00:00	0	0	0:0:0:0	0	0	0
0.0.0.0	0-00:00:00/ 0-00:00:00	0	0	0	0-00:00:00	0	0	0:0:0:0	0	0	0
Sum	0-00:57:36/ 0-18:12:39	0	0	0	0-00:00:00	0	0	0:0:0:0	0	0	0

The table is organized 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 were dropped. E.g. if a user has an active call and walks out of range, the call will be counted as a dropped call. An entry is stored in the syslog when a call is dropped.

NO RESPONSE	No response calls are the number of calls that have no response, e.g. if an 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 ATTEMPT SUCCESS	Counts the number of successful handovers.
HANDOVER ATTEMPT FAILED	Counts the number of failed handovers.
AUDIO NOT DETECTED	Counts the number of times where audio connection was not established.

5.16.4 Repeater data

Screenshot

Idx/ Name	Operation D-H:M:S	Busy	Busy Duration D-H:M:S	Max Active	Searching	Recovery	Source Changed	Wide Band	Narrow Band
1/ RPN1	0-00:00:50	0	0-00:00:00	0	0	0	1	0	0
2/ RPN2	0-00:00:00	0	0-00:00:00	0	0	0	0	0	0
3/	0-00:00:00	0	0-00:00:00	0	0	0	0	0	0
Sum	0-00:00:50	0	0-00:00:00	0	0	0	1	0	0

The table is organized 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 have been active at the same time.
SEARCHING	Repeater searching is the number of times a repeater has been searching for its 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 times a repeater has changed sync source
WIDE BAND	Number of wideband calls on repeaters
NARROW BAND	Number of narrowband calls on repeaters

5.16.5 DECT data

The DECT data web is accessed by http://ip/DectStatistics.html and data is organized in a table as shown in below example.

Screenshot

Statistics

Export Clear

System / Calls / Repeater / DECT / Call quality

	Slot0	Slot1	Slot2	Slot3	Slot4	Slot5	Slot6	Slot7	Slot8	Slot9	Slot10	Slot11
Frequency0	1666	1542	1595	1590	1647	1645	1646	1635	1616	1541	1543	1622
Frequency1	1159	1184	1205	1170	1191	1164	1184	1151	1164	1074	1205	1199
Frequency2	1234	1193	1213	1199	1260	1227	1209	1163	1211	1224	1226	1294
Frequency3	1059	1175	1153	1128	1091	1171	1069	1119	1176	1141	1123	1101
Frequency4	933	1044	984	1029	1022	996	1012	1004	996	957	937	1031
Frequency5	1060	1090	986	962	1030	983	975	980	947	985	982	987
Frequency6	1073	981	1017	1013	1066	959	1013	974	978	992	1019	962
Frequency7	1049	1060	981	995	1065	1082	1005	1033	1017	949	1085	1068
Frequency8	968	972	941	968	988	964	941	963	975	912	934	961
Frequency9	1349	1398	1292	1336	1279	1313	1338	1293	1348	1248	1331	1320

PARAMETERS	DESCRIPTION
FREQUENCY	Number of the DECT slot frequency
SLOTX	Number of connections that have been active on each frequency

5.16.6 Call quality

The Call quality web is accessed by http://ip/CallQuality.html and the data is organized in a table as shown in below example.

Screenshot

Statistics

Export Clear

System / Calls / Repeater / DECT / Call quality

Base Station Name	Type	Call count	Local/remote side	Jitter [ms]	Round trip latency [ms]	Packet loss [%]	R-value	MOS-value
192.168.11.106 SME VoIP	Call	0	Local	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.0 Max: 0.0 Avg: 0.0	Min: 0.00 Max: 0.00 Avg: 0.00	Min: 0.00 Max: 0.00 Avg: 0.00
			Remote	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.0 Max: 0.0 Avg: 0.0	Min: 0.00 Max: 0.00 Avg: 0.00	Min: 0.00 Max: 0.00 Avg: 0.00
	Relay conn	0	Local	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.0 Max: 0.0 Avg: 0.0	Min: 0.00 Max: 0.00 Avg: 0.00	Min: 0.00 Max: 0.00 Avg: 0.00
			Remote	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.0 Max: 0.0 Avg: 0.0	Min: 0.00 Max: 0.00 Avg: 0.00	Min: 0.00 Max: 0.00 Avg: 0.00
0.0.0.0	Call	0	Local	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.0 Max: 0.0 Avg: 0.0	Min: 0.00 Max: 0.00 Avg: 0.00	Min: 0.00 Max: 0.00 Avg: 0.00
			Remote	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.0 Max: 0.0 Avg: 0.0	Min: 0.00 Max: 0.00 Avg: 0.00	Min: 0.00 Max: 0.00 Avg: 0.00
	Relay conn	0	Local	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.0 Max: 0.0 Avg: 0.0	Min: 0.00 Max: 0.00 Avg: 0.00	Min: 0.00 Max: 0.00 Avg: 0.00
			Remote	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.000 Max: 0.000 Avg: 0.000	Min: 0.0 Max: 0.0 Avg: 0.0	Min: 0.00 Max: 0.00 Avg: 0.00	Min: 0.00 Max: 0.00 Avg: 0.00

PARAMETERS	DESCRIPTION
BASE STATION NAME	Base IP address and base station name from management settings
TYPE	Call: Relay conn:
CALL COUNT	Count the number of calls
LOCAL/REMOTE SIDE	Local: Remote:
JITTER[MS]	Measures how the RTP packets are received, the lower the Jitter is the better
ROUND TRIP LATENCY [MS]	Measures the time it takes for RTP packets to reach it destination.
PACKET LOSS [%]	Percentages of packets lost.
R-VALUE	A way to measure call quality, from 0-120
MOS-VALUE	**MOS** measures subjective call quality for a call. MOS scores range from 1 for unacceptable, to 5 for excellent. VOIP calls often are in the 3.5 to 4.2 range See table above.

USER SATISFACTION LEVEL	MOS	R-Factor
MAXIMUM USING G.711	4.4	93
VERY SATISFIED	4.3-5.0	90-100
SATISFIED	4.0-4.3	80-90
SOME USERS SATISFIED	3.6-4.0	70-80
MANY USERS DISSATISFIED	3.1-3.6	60-70
NEARLY ALL USERS DISSATISFIED	2.6-3.1	50-60
NOT RECOMMENDED	1.0-2.6	Less than 50

5.17 Generic Statistics

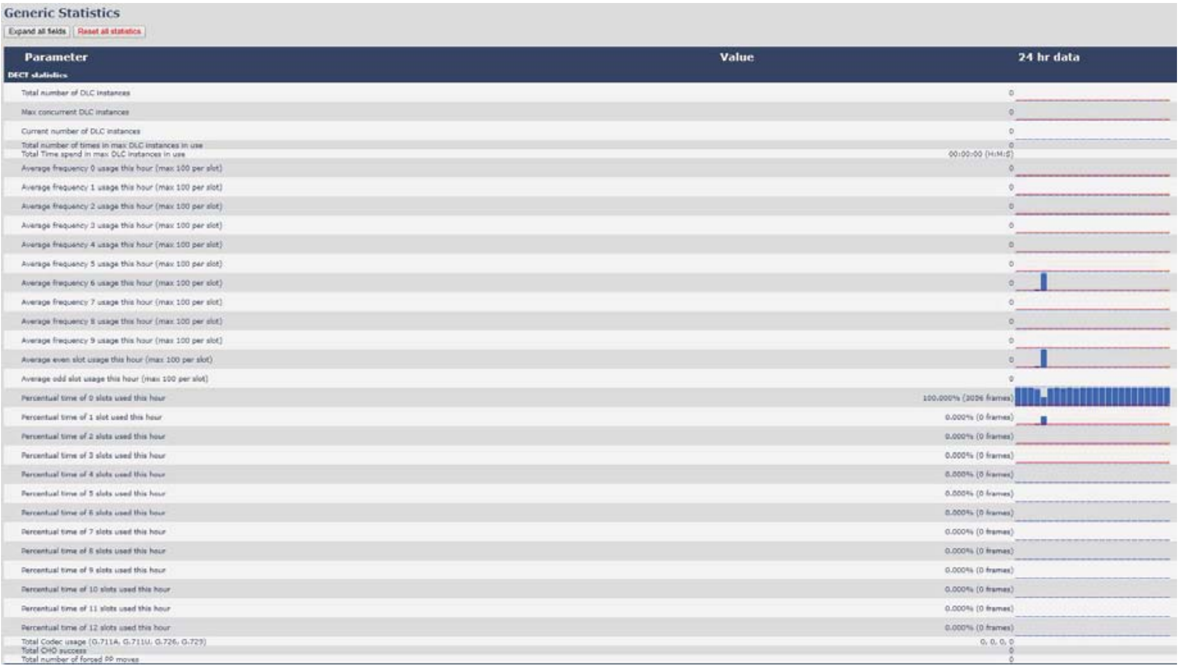
The statistic feature is divided into five sections, which can be accessed from any base.

1. DECT Statistics
2. DECT Synchronization statistics
3. RTP Statistics
4. IP Stack Statistics
5. System Statistics

By pressing the “Expand all fields” you can see statistics hour by hour and by pressing the “Reset all statistics” button all data in the full system is cleared.

PARAMETER	DEFAULT VALUES	DESCRIPTION
PARAMETER	Vary	Headline of the different statistics
VALUE	Vary	Vary for point to point
24 HR DATA	Vary	Data from the last 24 hours

Screenshot:


Generic Statistics

Expand all fields | Reset all statistics

Parameter	Value	24 hr data
DECT statistics		
Total number of DLC instances	0	
Max concurrent DLC instances	0	
Current number of DLC instances	0	
Total number of times in max DLC instances in use	0	
Total Time spend in max DLC instances in use	00:00:00 (H:M:S)	
Average frequency 0 usage this hour (max 100 per slot)	0	
Average frequency 1 usage this hour (max 100 per slot)	0	
Average frequency 2 usage this hour (max 100 per slot)	0	
Average frequency 3 usage this hour (max 100 per slot)	0	
Average frequency 4 usage this hour (max 100 per slot)	0	
Average frequency 5 usage this hour (max 100 per slot)	0	
Average frequency 6 usage this hour (max 100 per slot)	0	
Average frequency 7 usage this hour (max 100 per slot)	0	
Average frequency 8 usage this hour (max 100 per slot)	0	
Average frequency 9 usage this hour (max 100 per slot)	0	
Average even slot usage this hour (max 100 per slot)	0	
Average odd slot usage this hour (max 100 per slot)	0	
Percentual time of 0 slots used this hour	100.000% (2036 frames)	
Percentual time of 1 slot used this hour	0.000% (0 frames)	
Percentual time of 2 slots used this hour	0.000% (0 frames)	
Percentual time of 3 slots used this hour	0.000% (0 frames)	
Percentual time of 4 slots used this hour	0.000% (0 frames)	
Percentual time of 5 slots used this hour	0.000% (0 frames)	
Percentual time of 6 slots used this hour	0.000% (0 frames)	
Percentual time of 7 slots used this hour	0.000% (0 frames)	
Percentual time of 8 slots used this hour	0.000% (0 frames)	
Percentual time of 9 slots used this hour	0.000% (0 frames)	
Percentual time of 10 slots used this hour	0.000% (0 frames)	
Percentual time of 11 slots used this hour	0.000% (0 frames)	
Percentual time of 12 slots used this hour	0.000% (0 frames)	
Total Codec usage (G.711A, G.711U, G.726, G.729)	0, 0, 0, 0	
Total CHO success	0	
Total number of forced PP moves	0	

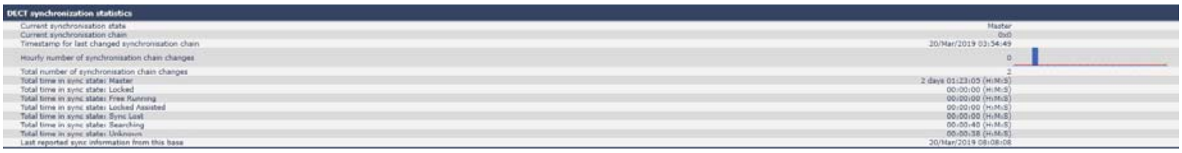
PARAMETERS	DESCRIPTION
TOTAL NUMBER OF DLC INSTANCE	The lifetime total count of instantiated DLC instances.
MAX CONCURRENT DLC INSTANCES	The lifetime highest concurrent count of instantiated DLC instances.
CURRENT NUMBER OF DLC INSTANCES	The current count of instantiate DLC instances.
TOTAL NUMBER OF TIMES IN MAX DLC INSTANCES IN USE	The number of times we reach the currently highest count of DLC instances.

TOTAL TIME SPEND IN MAX DLC INSTANCES IN USE	The time we have spent in the highest concurrent number of instantiated DLC instances.
AVERAGE FREQUENCY X USAGE THIS HOUR (MAX 100 PER SLOT)	The average use of frequency number X. The value is 100 if the frequency is fully used by a slot in the measured time frame.
AVERAGE EVEN SLOT USAGE THIS HOUR (MAX 100 PER SLOT)	The average use of even numbered slots.
AVERAGE ODD SLOT USAGE THIS HOUR (MAX 100 PER SLOT)	The average use of odd numbered slots.
PERCENTAGE TIME OF X SLOTS USED THIS HOUR	The percentual time that X number of DECT slots are used during the given hour (compared to other slot counts).
TOTAL CODEC USAGE (G.711A, G.711U, G.726, G.729)	This shows what codec, that have been used. The number of times we instantiate RTP stream using either codec.
TOTAL CHO SUCCESS	The number of times connection handover is successfully made.
Total number of forced PP moves	The lifetime total count that this base forces PP moves.

5.17.1 DECT Synchronization Statistics

DECT Synchronization statistics is related to this base station only.

Screenshot:



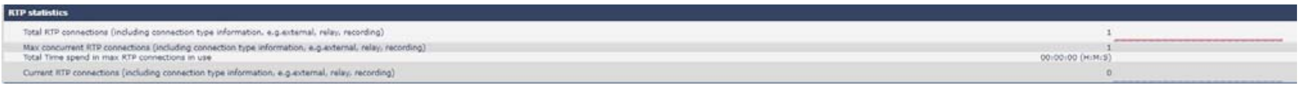
DECT synchronization statistics	
Current synchronisation state	Master
Current synchronisation chain	0x0
Timestamp for last changed synchronisation chain	20/Mar/2019 03:54:49
Hourly number of synchronisation chain changes	0
Total number of synchronisation chain changes	2
Total time in sync state: Master	2 days 01:23:05 (H:M:S)
Total time in sync state: Locked	00:00:00 (H:M:S)
Total time in sync state: Free Running	00:00:00 (H:M:S)
Total time in sync state: Locked Assisted	00:00:00 (H:M:S)
Total time in sync state: Sync Lost	00:00:00 (H:M:S)
Total time in sync state: Searching	00:00:40 (H:M:S)
Total time in sync state: Unknown	00:00:38 (H:M:S)
Last reported sync information from this base	20/Mar/2019 08:08:08

PARAMETERS	DESCRIPTION
CURRENT SYNCHRONISATION STATE	The current DECT sync state (e.g. Master, Searching, Free Running, etc).
CURRENT SYNCHRONISATION CHAIN	The current DECT sync source Fp Id of this base.
TIMESTAMP FOR LAST CHANGED SYNCHRONISATION CHAIN	Timestamp of the last time this base changed DECT sync source.
HOURLY NUMBER OF SYNCHRONISATION CHAIN CHANGES	The number of times this base changed DECT sync source in the current hour.
TOTAL NUMBER OF SYNCHRONISATION CHAIN CHANGES	The lifetime total count of times this base changed DECT sync source.
TIME IN SYNCHRONISATION STATE: MASTER	Time this hour where this base station has had the state Master
TIME IN SYNCHRONISATION STATE: LOCKED	Time this hour where this base station has had the state Locked
TIME IN SYNCHRONISATION STATE: FREE RUNNING	Time this hour where this base station has had the state Alien Free Running
TIME IN SYNCHRONISATION STATE: LOCKED ASSISTED	Time this hour where this base station has been in lock assisted
TIME IN SYNCHRONISATION STATE: SYNC LOST	Time this hour where this base station has not been in Sync
TIME IN SYNCHRONISATION STATE: SEARCHING	Time this hour where this base has been searching for its sync source
TIME IN SYNCHRONISATION STATE: UNKNOWN	Time this hour where this base station has not been in unknown state

5.17.2 RTP Statistics

RTP statistics are related to this base station only.

Screenshot:

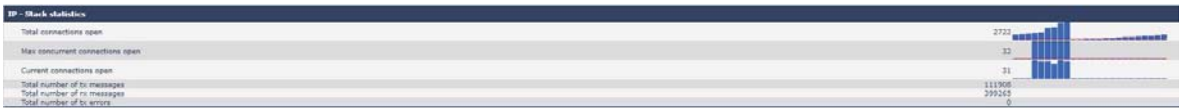


PARAMETERS	DESCRIPTION
TOTAL RTP CONNECTIONS (INCLUDING CONNECTION TYPE INFORMATION, E.G. EXTERNAL, RELAY, RECORDING)	The lifetime total count of instantiated RTP streams.
MAX CONCURRENT RTP CONNECTIONS (INCLUDING CONNECTION TYPE INFORMATION, E.G. EXTERNAL, RELAY, RECORDING)	The lifetime highest concurrent count of instantiated RTP streams.
TOTAL TIME SPEND IN MAX RTP CONNECTIONS IN USE	The time we have spent in the highest concurrent count of instantiated RTP streams.
CURRENT RTP CONNECTIONS (INCLUDING CONNECTION TYPE INFORMATION, E.G. EXTERNAL, RELAY, RECORDING)	The current count of instantiated RTP streams.

5.17.3 IP - Stack statistics

IP - Stack statistics is related to this base station only.

Screenshot:

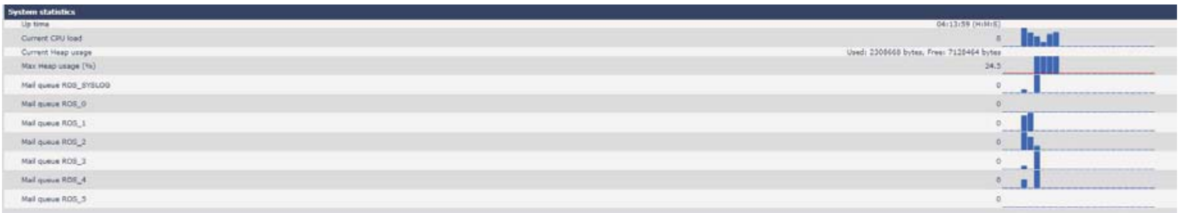


PARAMETERS	DESCRIPTION
TOTAL CONNECTIONS OPEN	The lifetime total count of used sockets.
MAX CONCURRENT CONNECTIONS OPEN	The lifetime highest concurrent count of used sockets.
CURRENT CONNECTIONS OPEN	The current count of used sockets.
TOTAL NUMBER OF TX MESSAGES	The lifetime total count of transmitted IP packets.
TOTAL NUMBER OF RX MESSAGES	The lifetime total count of received IP packets.
TOTAL NUMBER OF TX ERRORS	The lifetime total count of errors occurred during IP packet transmission.

5.17.4 System Statistics

System Statistics is related to this base station only.

Screenshot:



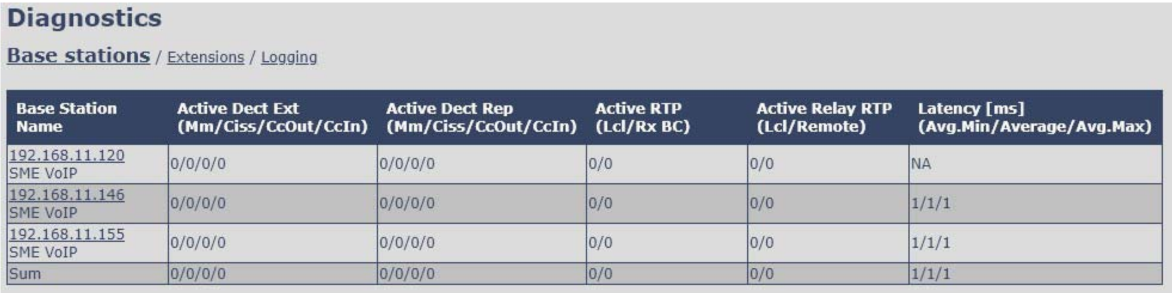
PARAMETERS	DESCRIPTION
UP TIME	The time the base has been running consecutively.
CURRENT CPU LOAD	The current load percentage of CPU. This is refreshed once every 5 seconds.
CURRENT HEAP USAGE	The current use of heap in Bytes.
MAX HEAP USAGE (%)	The peak usage of heap in percentage.
MAIL QUEUE ROS_SYSLOG	Size of internal mail queue for syslog.
MAIL QUEUE ROS_X	Size of internal mail queue.

5.18 Diagnostics

This page provides information about the Ethernet connection to each base station and Extension.

5.18.1 Base Stations

Screenshot



Diagnostics

Base stations / Extensions / Logging

Base Station Name	Active Dect Ext (Mm/Ciss/CcOut/CcIn)	Active Dect Rep (Mm/Ciss/CcOut/CcIn)	Active RTP (Lcl/Rx BC)	Active Relay RTP (Lcl/Remote)	Latency [ms] (Avg.Min/Average/Avg.Max)
192.168.11.120 SME VoIP	0/0/0/0	0/0/0/0	0/0	0/0	NA
192.168.11.146 SME VoIP	0/0/0/0	0/0/0/0	0/0	0/0	1/1/1
192.168.11.155 SME VoIP	0/0/0/0	0/0/0/0	0/0	0/0	1/1/1
Sum	0/0/0/0	0/0/0/0	0/0	0/0	1/1/1

PARAMETERS	DESCRIPTION
BASE STATION NAME	Base IP address and base station name from management settings
ACTIVE DECT EXT (MM/CISS/CCOUT/CCIN)	Number of active DECT MAC connections to extensions in the different base stations. Types of connection is (mm/Ciss/CcOut/CcIn)
ACTIVE DECT REP (MM/CISS/CCOUT/CCIN)	Number of active DECT MAC connections to repeaters in the different base stations. Types of connection is (mm/Ciss/CcOut/CcIn)
ACTIVE RTP (LCL/RX BC)	Number of active RTP Streams used. Types of stream (Local RTP stream/Broadcast Receive RTP stream)
ACTIVE RELAY RTP (LCL/REMOTE)	Number of active RTP Relay Streams used. Types of stream (Local RTP Relay stream/Remote RTP Relay stream)
LATENCY [MS] (AVG.MIN/AVERAGE/AVG.MAX)	Ping latency between base station performed by base index 0. Average Minimum delay/Average/Average Maximum delay)

5.18.2 Extensions

Screenshot

Diagnostics

Base stations / Extensions

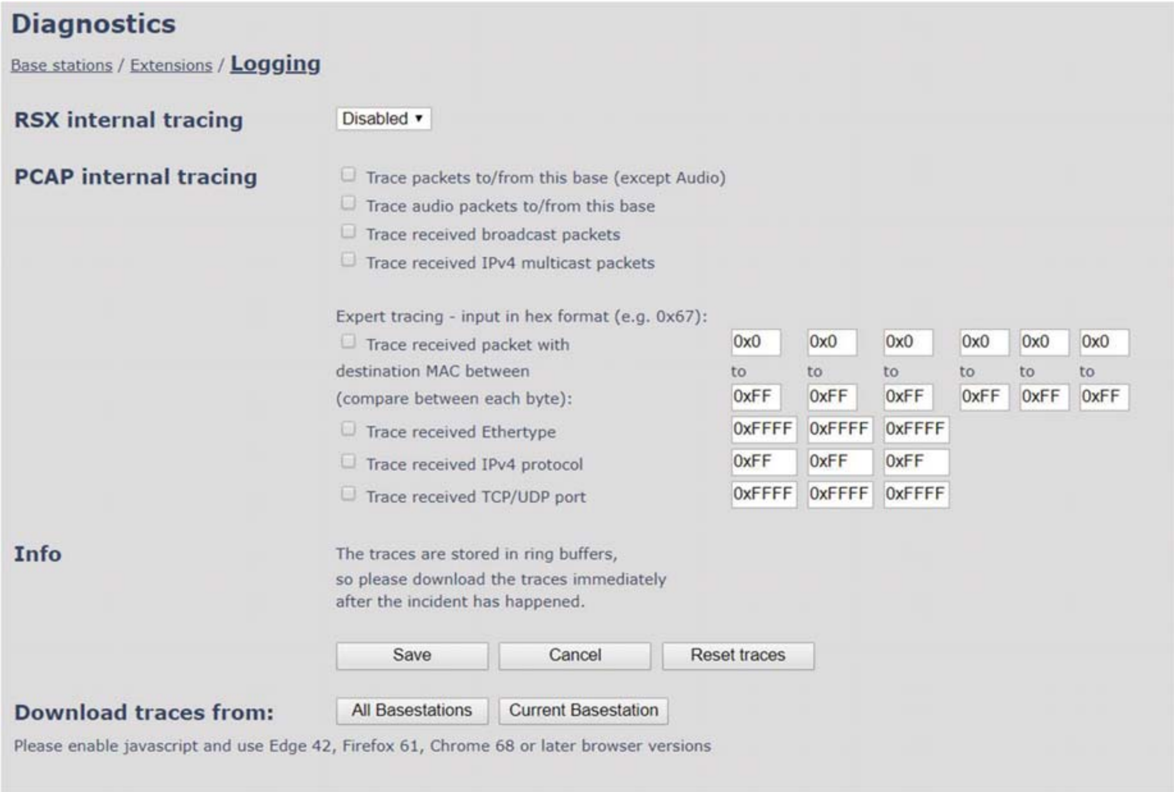
Idx	No of HS restarts	Last HS restart (dd/mm/yyyy hh:mm:ss)
1	0	01/01/1970 00:00:00

PARAMETERS	DESCRIPTION
IDX	Extension Index number
NO OF HS RESTARTS	Number of times that the Handset has restarted
LAST HS RESTART (DD/MM/YYYY HH:MM:SS)	Date and time of the last time the Handset has restarted

5.18.3 Logging

The Diagnostics/Logging page allows you to collect system diagnostics information into a zip file.

Screenshot



PARAMETERS	DESCRIPTION
RSX INTERNAL TRACING	Enable/Disable. Only RTX engineers can debug the traces
PCAP INTERNAL TRACING	
TRACING PACKETS TO/FROM THIS BASE (EXCEPT AUDIO)	If selected, all Ethernet packets sent to/from the base station's MAC address are traced. Broadcast packets sent from the base are also being traced.
TRACE AUDIO PACKETS TO/FROM THIS BASE	If selected, RTP streams to/from the BS are traced. Audio packets are filtered by the port number used for RTP packets which is set on the web page
TRACE RECEIVED BROADCAST PACKETS	If selected, all broadcast packets received by the BS are traced.
TRACE RECEIVED PACKET WITH DESTINATION MAC BETWEEN	If selected, each byte of the received destination MAC is checked if it is in the trace range
TRACE RECEIVED ETHERTYPE	If selected, the user can select 3 received Ethertypes to trace
TRACE RECEIVED IPV4 PROTOCOL	If selected, the user can select 3 received IPv4 protocols to trace
TRACE RECEIVED TCP/UDP PORT	If selected, the user can select 3 received TCP/UDP ports to trace.
INFO	

DOWNLOAD TRACES FROM	Choose from which base stations to download the traces – all of them or just the current one

The following information is added to the zip file.
1: RSX trace (Good practice is to enable RSX internal tracing)
2: Syslog(s)
3: SIPLOG
4: Statistics
5: Home/Status page (HTML format)
6: Config file(s)
7: Error reason (entered by the user)
8: Requested BS(s) – information about what base stations is in the trace)

5.19 Configuration

This page provides non-editable information showing the native format of entire SME VoIP 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:

- Using the SME VoIP Configuration interface to make changes. Each page of the web interface is a template for which the user can customize settings in the configuration file.
- Retrieving the relevant configuration file from the TFTP and modify and enter new changes. This should be done with an expert network administrator.
- Navigate to the settings page of the VoIP SME Configuration 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.

An example of contents of settings is as follows:

```
~RELEASE=BEATUS_FP_V0400_B0001
~System Mode=51/51
%GMT_TIME_ZONE%:0x06
%COUNTRY_VARIANT_ID%:0x12
%COUNTRY_REGION_ID%:0x00
%TIMEZONE_BY_COUNTRY_REGION%:0x01
%DST_BY_COUNTRY_REGION%:0x01
%DST_ENABLE%:0x02
%DST_FIXED_DAY_ENABLE%:0x00
%DST_START_MONTH%:0x03
%DST_START_DATE%:0x00
………
```

For detailed description on how to use provisioning please see Provisioning HOW-TO guide. Link is found in Appendix.

5.20 Sys log

This page shows live feed of system level messages of the current base station. The messages the administrator sees here depend 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.

A sample of debug logs is as follows:

0101000013 [N](01):DHCP Enabled
0101000013 [N](01):IP Address: 192.168.10.101
0101000013 [N](01):Gateway Address: 192.168.10.254
0101000013 [N](01):Subnet Mask: 255.255.255.0
0101000013 [N](01):TFTP boot server not set by DHCP. Using Static.
0101000013 [N](01):DHCP Discover completed
0101000013 [N](01):Time Server: 192.168.10.11
0101000013 [N](01):Boot server: 10.10.104.63 path: Config/ Type: TFTP
0101000013 [N](01):RemCfg: Download request of Config/00087b077cd9.cfg from 10.10.104.63 using TFTP
0101000014 [N](01):accept called from task 7
0101000014 [N](01):TrelAccept success [4]. Listening on port 10010
0101000019 [N](01):RemCfg: Download request of Config/00087b077cd9.cfg from 10.10.104.63 using TFTP
0101000019 [W](01):Load of Config/00087b077cd9.cfg from 10.10.104.63 failed

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

5.21 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 is saved in the TFTP server as **<MAC_Address><Time_Stamp>SIP.log**
These logs are saved in 2 blocks of 17Kbytes. When a specific SIP log is fully dumped to one block, the next SIP logs are dumped to the other blocks.

An example of SIP logs is shown below:

.....
Sent to udp:192.168.10.10:5080 at 12/11/2010 11:56:42 (791 bytes)
REGISTER sip:192.168.10.10:5080 SIP/2.0
Via: SIP/2.0/UDP 192.168.10.101:5063;branch=z9hG4bKrlga4nkuhimpnj4.qx
Max-Forwards: 70
From: <sip:Ext003@192.168.10.10:5080>;tag=3o5l314
To: <sip:Ext003@192.168.10.10:5080>
Call-ID: p9st.zzrfff66.ah8
CSeq: 6562 REGISTER
Contact: <sip:Ext003@192.168.10.101:5063>
Allow: INVITE, CANCEL, BYE, ACK, REGISTER, OPTIONS, REFER, SUBSCRIBE, NOTIFY, MESSAGE, INFO, PRACK
Expires: 120
User-Agent: Generic-DPV-001-A-XX(Generic_SIPEXT2MLUA_v1)
Content-Type: application/X-Generic_SIPEXT2MLv1
Content-Length: 251
.....

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

Appendix – How-To setup a Dual-Cell System

This chapter we describe how to setup a dual-cell system, add and synchronize one or two base stations to the network.

NOTE: It is possible to have RTX8660 and RTX8663 in the same chain.

Adding Base stations

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

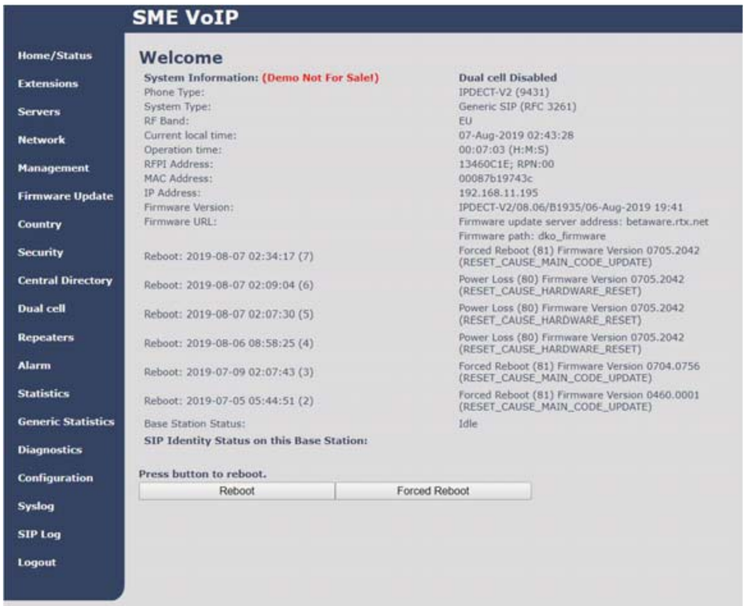
STEP 1:
Connect the Base station to a private network via standard Ethernet cable.

STEP 2:
Use one of the two methods to determine the base station IP address (see chapter 3.5 for more details).
Use the IP find menu in the handset (Menu * 4 7 *) to determine the IP address of the base station by matching the MAC address on the back of the base station with the MAC address list on the handset. If not, use the second method by typing the ipdect address I the browser, followed by the MAC address of the Base station.

STEP 3:
Open a browser on the computer and type in the IP address of the base. Press "Enter" to access the base Login to the base station. The default input for Username/Password is: admin/admin.

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

Screenshot

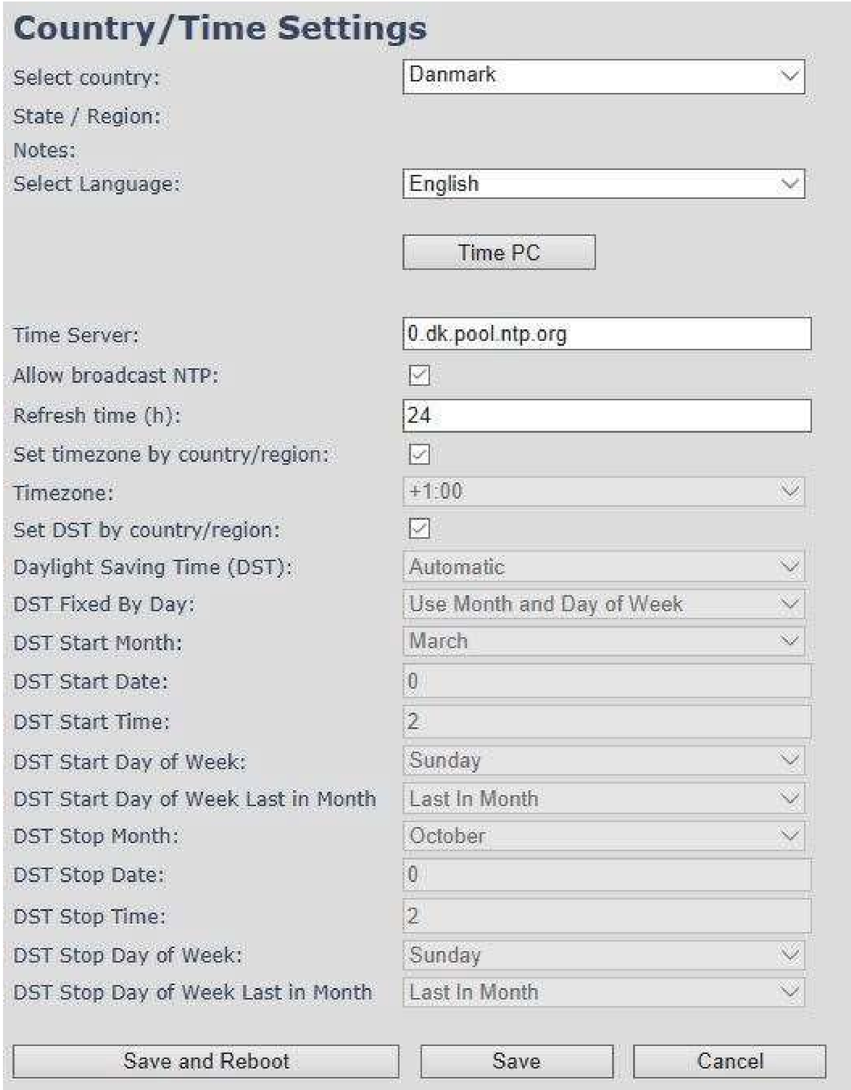


Country and Time Server Setup

STEP 4:
Navigate to the Country page and configure its country and time settings.
Use the PC time feature or enter the relevant NTP server address and press the **Save and Reboot** button. Make sure there is contact to the "Time server" otherwise the Dual-cell feature will not work.

You can verify whether the Time server is reachable by rebooting the base station and verifying that the correct Time Server IP address is still in place.

Screenshot



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 to a SIP server vendor on how to setup SIP servers.

a. Click the link "**Server"** at the left-hand column of home page. This is the place where you can add your SIP server for base station use.
b. Next, from the Server page, click on the **Add Server** URL and enter the relevant SIP server information (an example is shown below).
c. 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. Click **Save**.

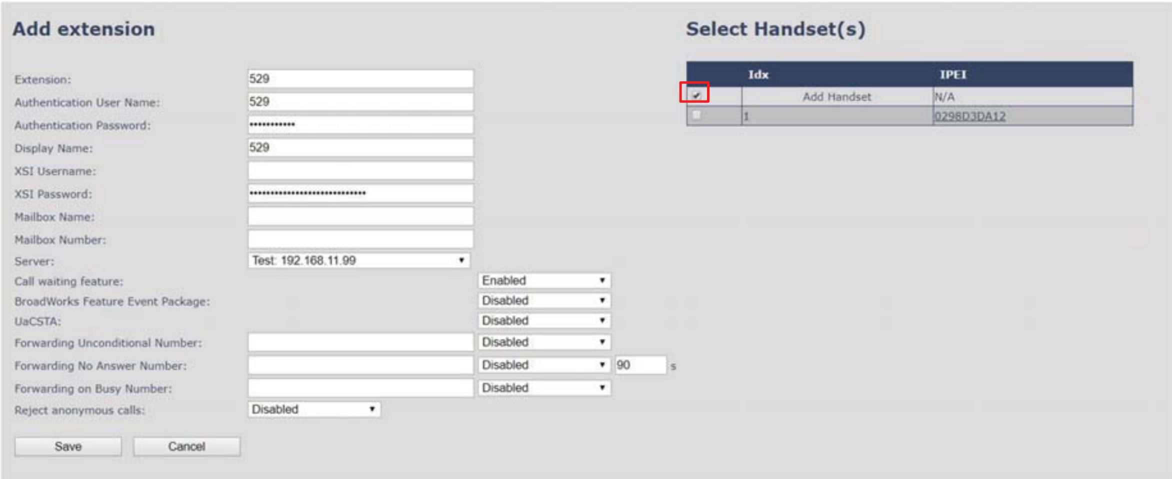
Screenshot

Add an extension and handset

STEP 6:

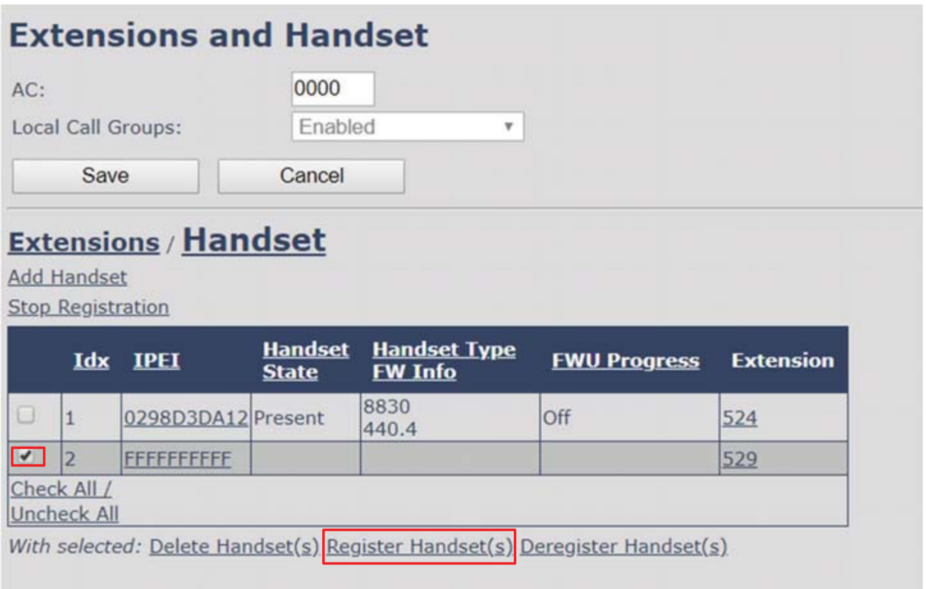
Add an extension before you move to the Dual Cell page. Go to Extensions – Add Extension.
Fill in the extension data and check the checkbox for adding a new handset. If you wish to replace an already existing handset – check the box with the relevant IPEI number of the handset. Press Save.

Screenshot



You will now see the extension on the extension page. Usually you do not need to fully register the extension, but since the handset is checked in the above guide, the next step is to add the extension. Click on the "Handset" link and check the box of the handset that is not registered and select "Register handset". Thereafter, go to the main menu of the **handset** and go to Connectivity – Register – type the password of 0000 and after a minute, the handset should be registered. For more details, please go to Handset guide..

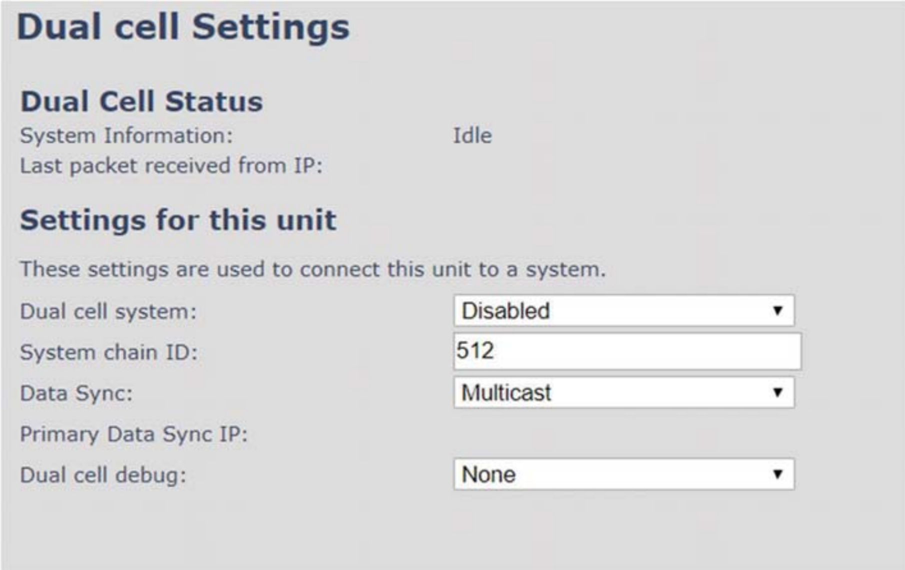
Screenshot



STEP 7:

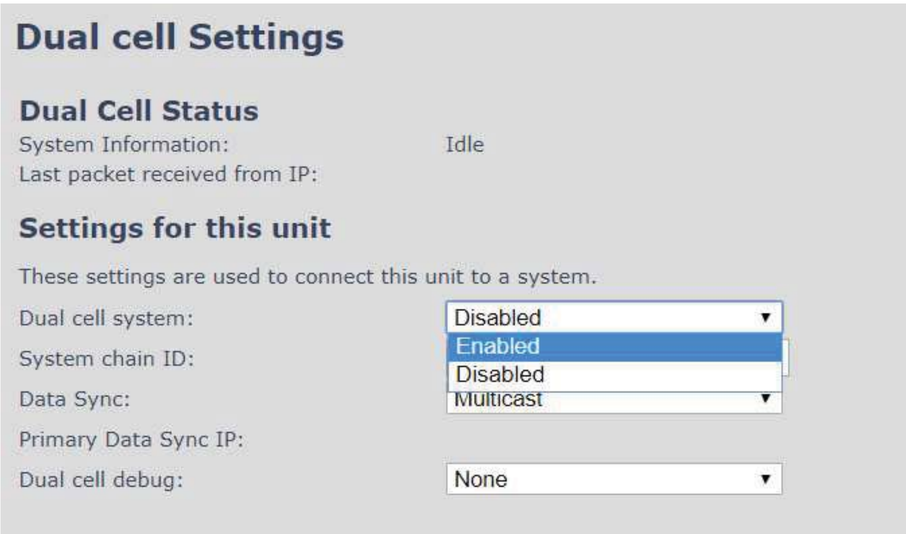
Click on Dual-cell URL link in the SME VoIP Configuration to view the current Dual cell settings
status of the current base station. Brand new base stations have **Dual-cell system** feature disabled by default

Screenshot



STEP 8:
Next, the system administrator needs to create and Enable Dual Settings profile for the current base station. On the **Dual-cell settings** Page, choose **Enable** option from the drop-down menu of the **Dual-cell system** parameter. Enable the **Dual-cell debug** option if the system administrator wants some Dual-cell related logs to be catalogued by the system.

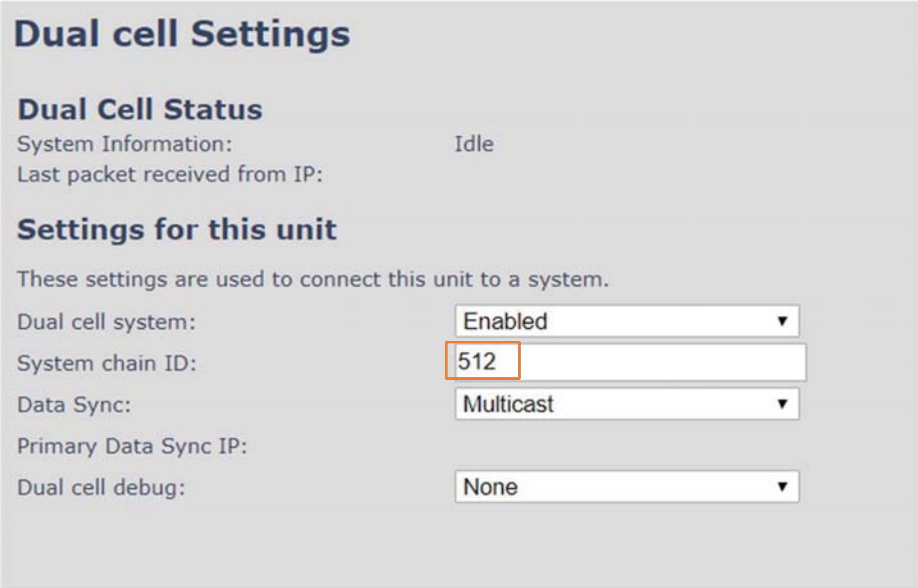
Screenshot



STEP 9:
On the same **Dual-cell Settings** page > Enter the relevant values for **System chain ID** 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**.

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

Screenshot



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

Screenshot

NOTE: That after you save the entries, the System information changes status to "Unchained Allowed to Join as Primary"

NOTE: The Dual-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 4**.

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

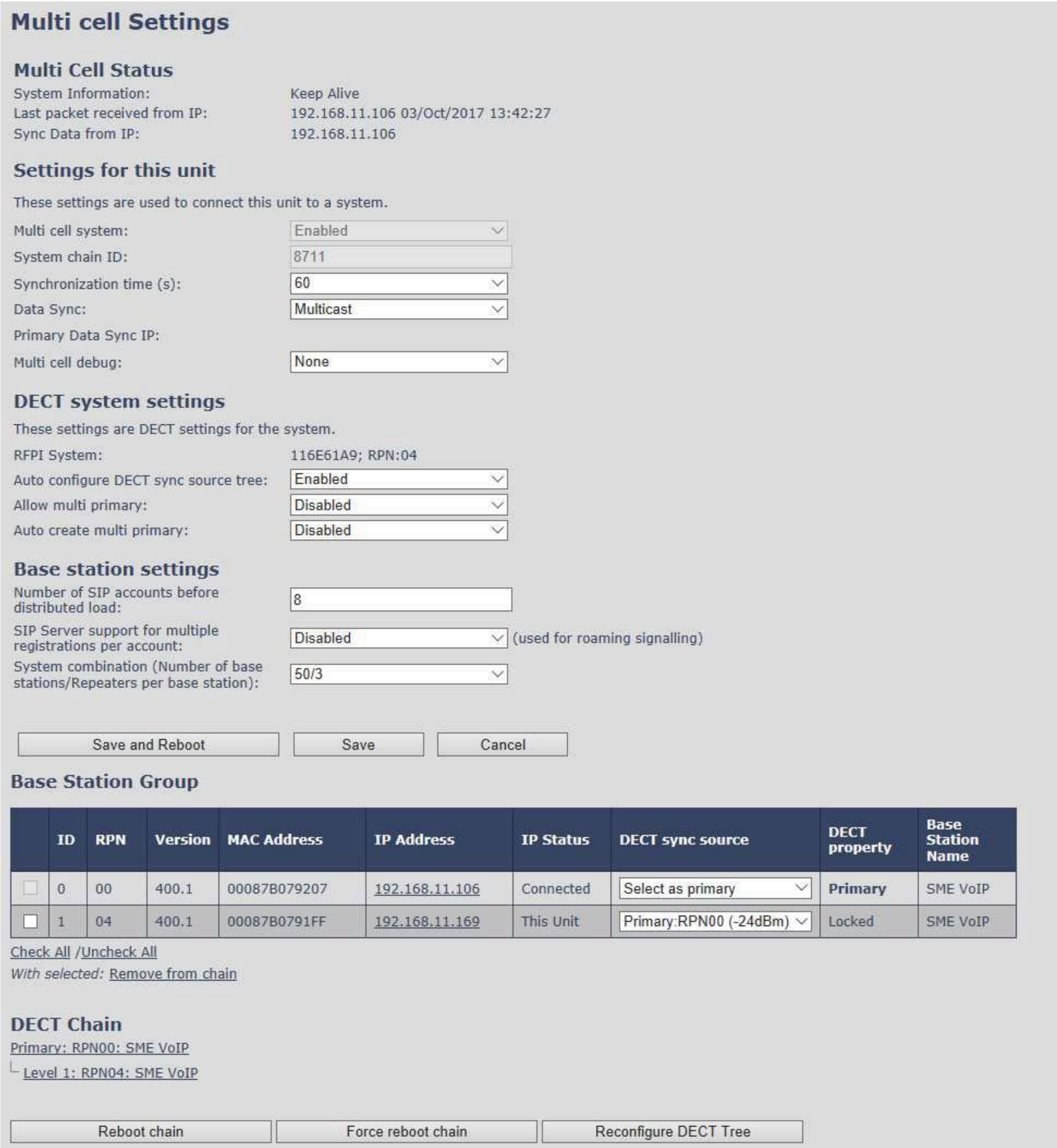
STEP 10:
Logon to the base station that you want to connect to the Dual-cell system.

STEP 11:
Navigate to the Dual-cell page and "Enable" Dual-cell system and enter the Chain ID that you used on the first base Station.

STEP 12:
Press Save and Reboot

IMPORTANT: It takes up to 5 minutes (synchronization time) to add a new base station to a Dua-cell System.

Screenshot



Appendix - Adding Extensions

This section describes how to register the wireless handset to a Dual-cell system.

NOTE: Minimum one server must be registered to the base (system), otherwise a handset cannot be registered to the system. Please see chapter 0.

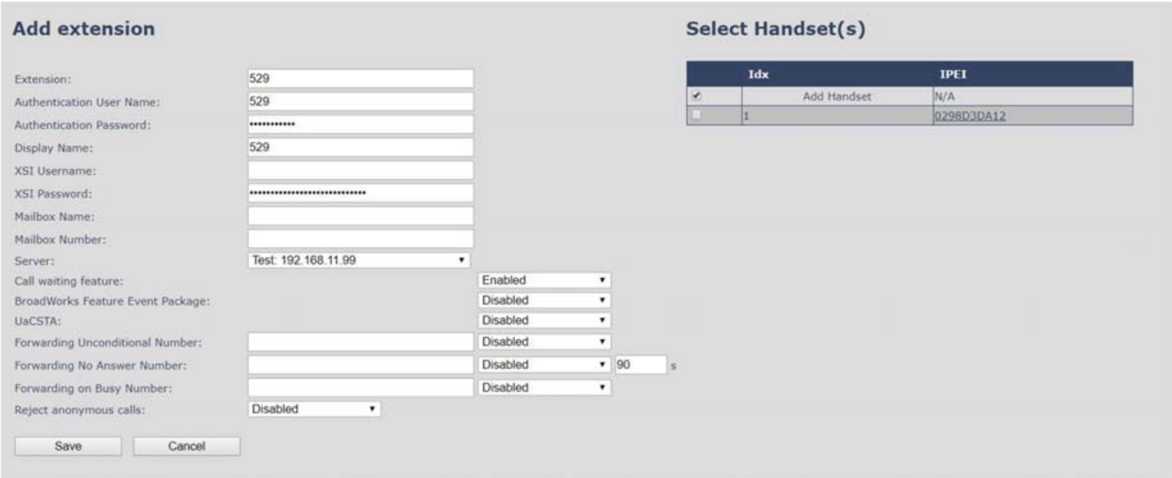
STEP 1:

Login to a base station.

STEP 2:
'Select "Extensions" URL and click "Add extension" link

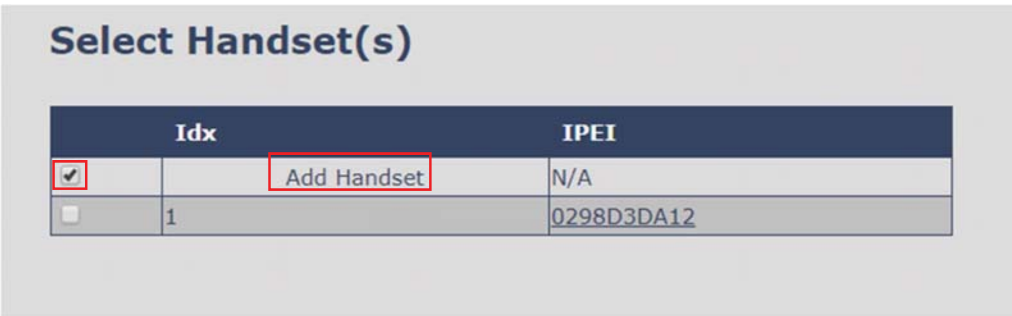
STEP 3:
Fill out the form and click "Save". In the example below, we add the extension "529" and this SIP account got the same number as "Authentication User Name", "Password" and "Display Name".

Screenshot



STEP 4:
On the right-hand side there is a "Select Handset" table. In order to activate the registration of a handset to the current extension, check the box on the "Add Handset" parameter and click Save

Screenshot



STEP 5:
On the "Extensions and Handset" menu click the "Handset" link for registering a handset. Afterwards, check the box on the extension you wish to add the handset and click "Register handset(s)". The registration will be open for 5 min.

STEP 6:
To start the registration procedure on the handset, go to the "Connectivity" menu and select "Register". Select an "Empty" parameter and type in the PIN code of "0000". After a while the handset is registered, and the idle display is shown.

STEP 6:
To check if the handset has been registered, go to the "Extensions and Handset" menu and verify that the unique IPEI of the handset is displayed in the "IPEI" column.

NOTE: 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) is not displayed immediately on the web page.

Screenshot

STEP 7:
Verify the SIP registration by SIP "State" in left of the "IPEI".

NOTE: The web page must be manually updated by pressing "F5" to see that the handset is SIP registered; otherwise the handset SIP state is not displayed immediately on the web page.

Repeat **STEP 2-7** for each handset you want to register.

Appendix - Firmware Upgrade Procedure

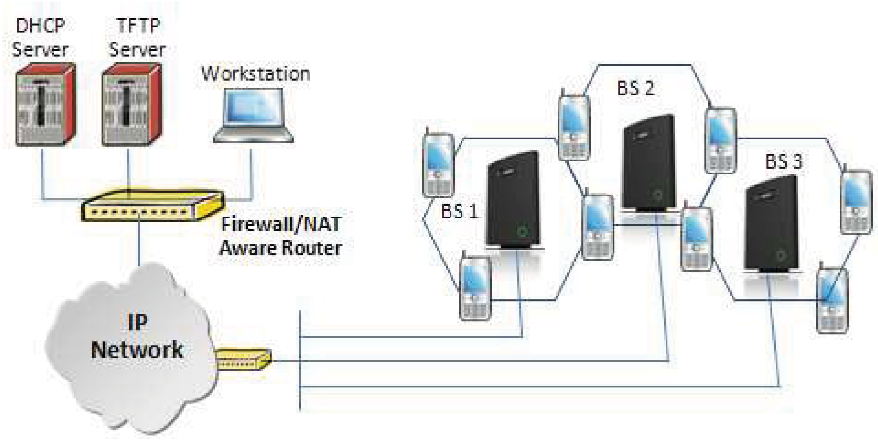
This step-by-step chapter describes how to upgrade or downgrade base station(s) and/or handset(s) / repeater (s) to the relevant firmware provided by RTX.

Network Dimensioning

In principle, several hardware and software components should be available or be satisfied before base station/handset update can be possible.

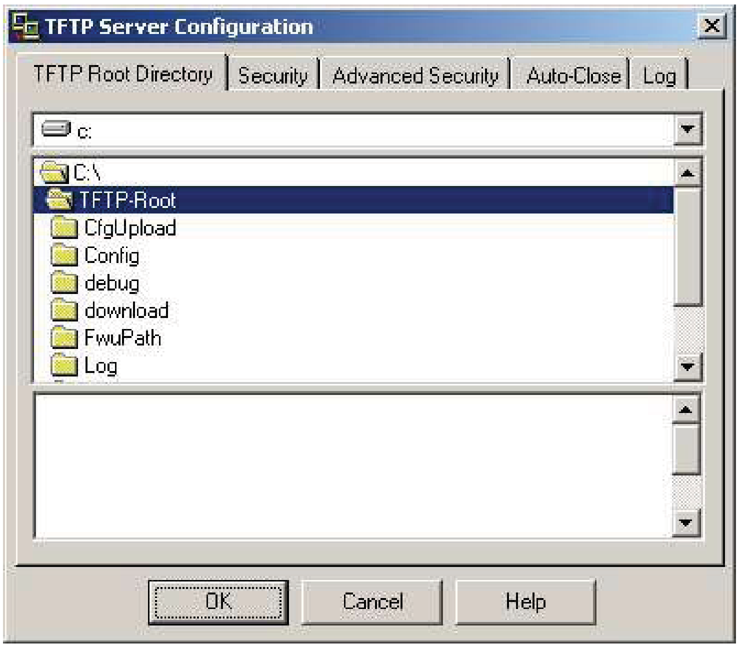
The minimum hardware and software components that are required to be able update via TFTP include the following (but not limited to):

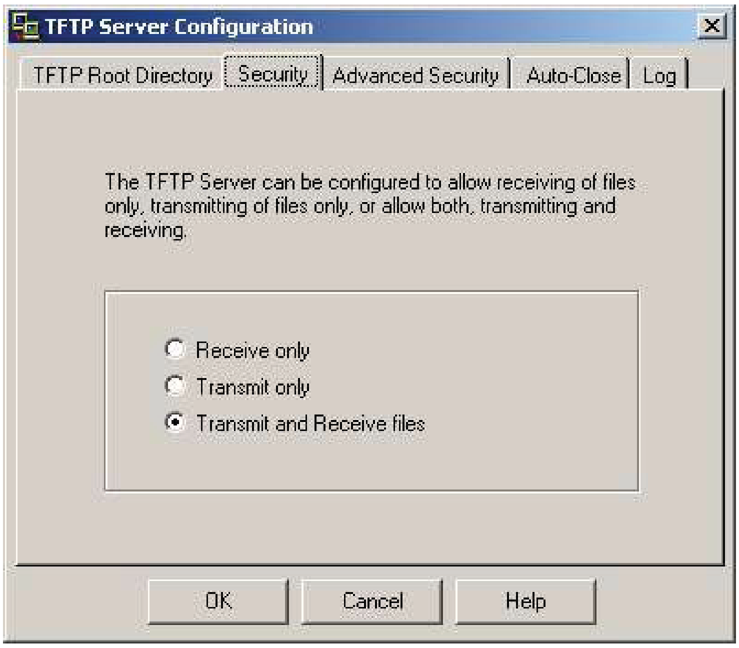
- Handsets
- Base stations
- TFTP Server (Several Windows and Linux applications are available)
- DHCP Server (Several Windows and Linux applications are available)
- Workstation (e.g. Normal terminal or PC)
- Any standard browser (e.g. Firefox)
- Public/Private Network



TFTP Configuration

This section illustrates TFTP Server configuration using “SolarWinds” vendor TFTP Server. Create the following relevant folders as shown in the snap shots and choose defaults settings for the remaining options and save.





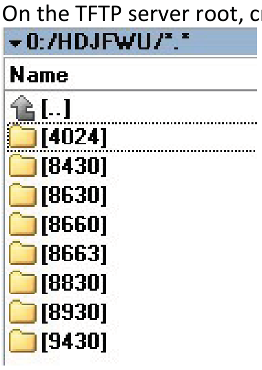
NOTE: If TFTP server timeout settings are too short firmware upgrade might not complete. Recommended time out setting is more than 3 seconds.

Create Firmware Directories

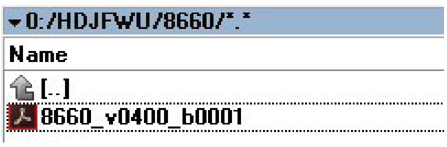
The admin from the service provider's side must create the relevant firmware directory in the server where both old and new firmware(s) can be placed in it. (See the STEP above)

Base:

On the TFTP server root, create directory's as in screenshot.



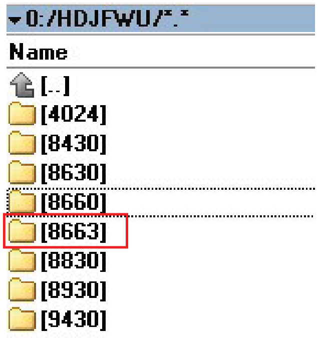
Copy Base station firmware to the named directory.



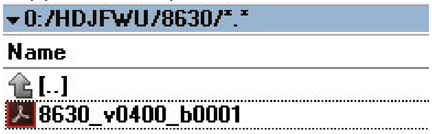
IMPORTANT: The **8663** directory name cannot be changed.

Handsets/Repeaters:

On the TFTP server root, create directory “8430” or “8630” or “8830” or “8930” or “4024” depending on type.



Copy handset/repeater firmware to the named directory of each model.

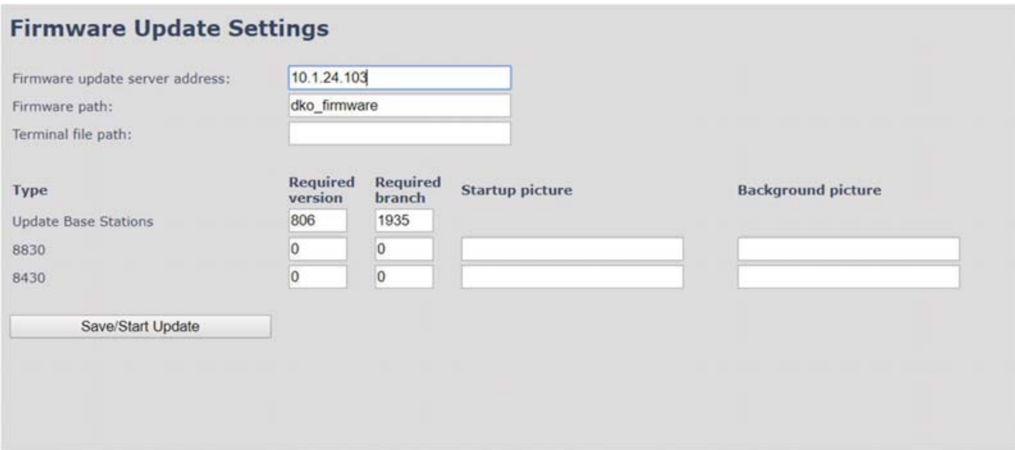


IMPORTANT: The **8430, 8630,8830 and 8930** directory names cannot be changed.

Handset Firmware Update Settings

Scroll down and Click on Firmware Update URL link in the SME VoIP Configuration Interface to view the Firmware Update Settings page.

Screenshot



Type IP address and firmware path followed by save.

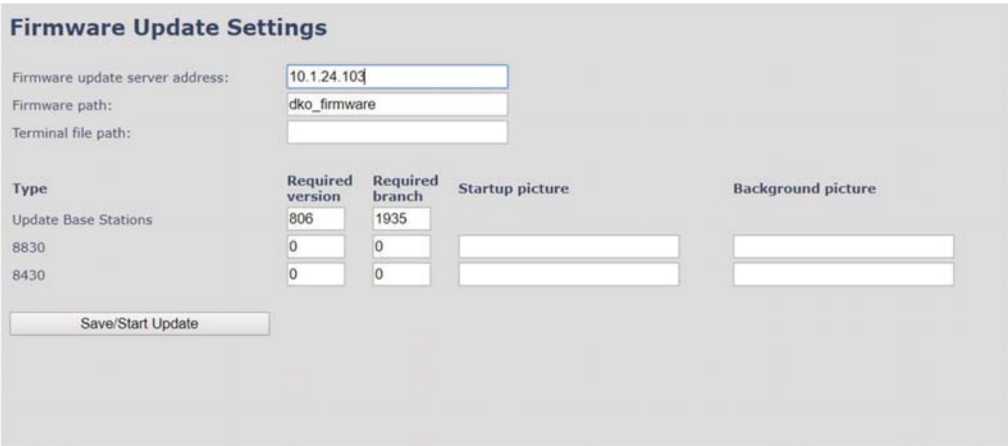
For Http download the firmware update server settings must be entered as follows:

Screenshot

Handset(s) and Repeater Firmware Upgrade

On the **Firmware Update Settings** page enter the relevant handset/repeater firmware for each type and Branch name (e.g. 440 for v440 for Required Version) and (e.g.01 for Branch 01 for Required Branch) to upgrade or downgrade > press **Save** button to initialize the process of updating all handsets.

Screenshot



NOTE: To disable handset/repeater firmware process type version 0 in the required version field, followed by the save button. It is recommended to use version 0 after all units are upgraded.

NOTE: For handset TFTP/HTTP download only one handset type can be downloaded at the same time. In case two handset models are defined for fwu at the same time fwu will fail.

5.21.1 Monitor handset firmware upgrade

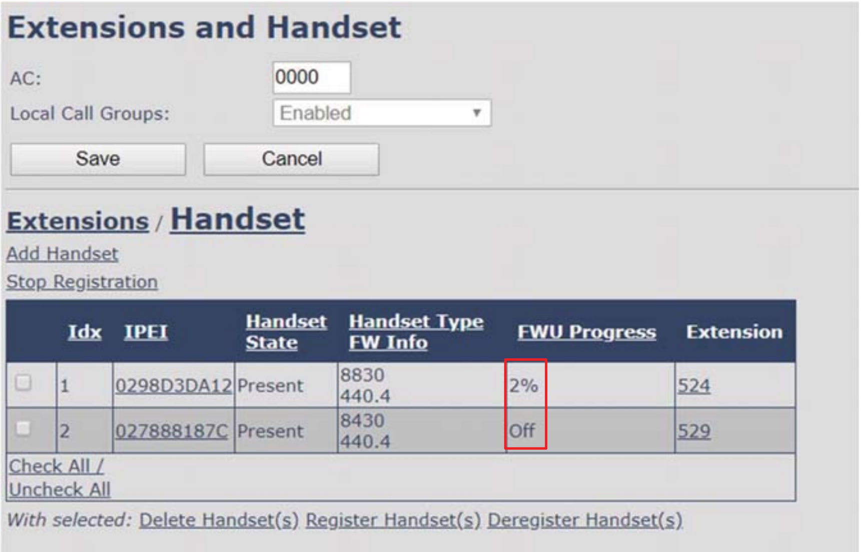
Handset firmware upgrade status is monitored on the handset extensions page, FWU Process Colum.

If the status says “Off” it means that the Required Version and Branch is set to “0” as it should be unless you’re in process of updating/downgrading the firmware.

The firmware Upgrade/Downgrade process has 6 states:

- Initializing
- In progress (% from 0-100)
- Verifying (% 0-100)
- Waiting for charger (The handset must be placed in charger and NOT removed until it reboots)
- Complete
- Off

Screenshot



Handset firmware update time from start to complete takes 20- 40 minutes.

Monitor Repeater firmware upgrade

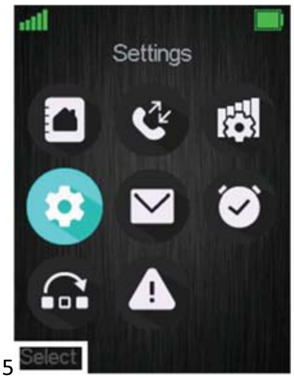
Repeater firmware upgrade status is monitored on the Repeater page, right column.

Repeater firmware upgrade time from start to complete takes minimum 20 minutes.

Verification of Firmware Upgrade

The firmware upgrade is confirmed by the FWU Progress status in the FWU Colum on the handset extension list or repeater list. The "FWU info" column contains the software version and the "FWU Progress" column contains the status. In case status is "Complete", the unit is firmware upgraded.

Alternatively, the handset firmware can be verified from the Handset **Menu** by selecting **Settings** > **Status.** This menu will list information regarding Base station and Handset firmware versions.

5 

Base Station(s) Firmware Upgrade

On the **Firmware Update** Page Base stations are updated in the same way as handsets and other extensions.

After entering Required Version and Required Branch 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 behavior 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 after the firmware update procedure starts.

Base firmware confirmation

Base station firmware version status in a dual-cell environment can be seen in the dual-cell base station group overview page, column 4 (Version).

Screenshot

Base Station Group

	ID	RPN	Version	MAC Address	IP Address	IP Status	DECT sync source	DECT property	Base Station Name
☐	0	00	400.1	00087B079207	192.168.11.106	This Unit	Select as primary	**Primary**	SME VoIP
☐	1	04	400.1	00087B0791FF	192.168.11.169	Connected	Primary:RPN00 (-26dBm)	Locked	SME VoIP

Check All /Uncheck All

With selected: Remove from chain

Verification of Firmware Upgrade

If the firmware Upgrade/Downgrade does not start, you can check the syslog to see if the path is right.

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

[FWU Downloading File tftp://10.1.24.103/FwuPath/8663/8663_v0440_b0001.fwu]
[Base FWU started]
[Base FWU ended with exit code 2101 (NE_FILE_TRANSFER_EOF): End of file]

This is the path when the base station expects to find the firmware: tftp://10.1.24.103/FwuPath/8663/8663_v0440_b0001.fwu

Check if the firmware file is in the correct directory.

Appendix – Multiline Feature

This section describes how to register the wireless handset to a system with active multiline feature.

One handset will be able to support up to 4 lines (4 different SIP accounts) ... A handset only supports 2 call appearances.
The limitation of maximum 1000 terminals in the system is maintained, and the maximum number of SIP registrations, one base station can handle, is maintained.
With 4 lines pr. terminal maximum number of terminals registered in a system are 250.
With 1-line pr. terminal maximum number of terminals registered in a system are 1000.
Still the limitation of 30 SIP accounts registered pr. base is maintained.
With 4 lines (SIP accounts) pr. terminal maximum number of terminals registered pr. base is 7.
The 4 SIP accounts pr. terminal follow the location of the terminal similar.
With multiline feature enabled 200 contacts in contact list is possible.

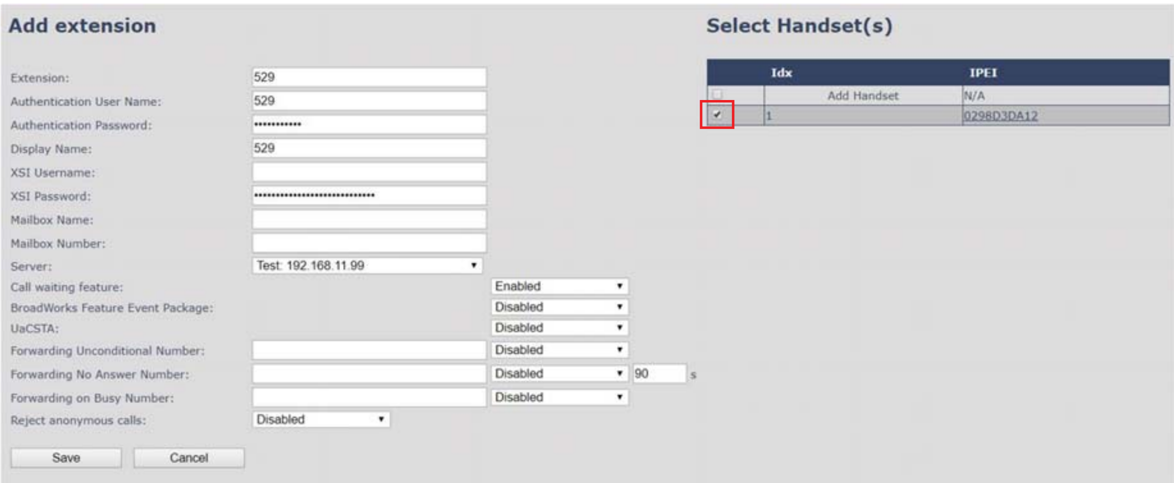
How to setup Multiline.

Step 1:

Register handset as described in chapter 7 (Appendix Adding Extensions).

Step 2:

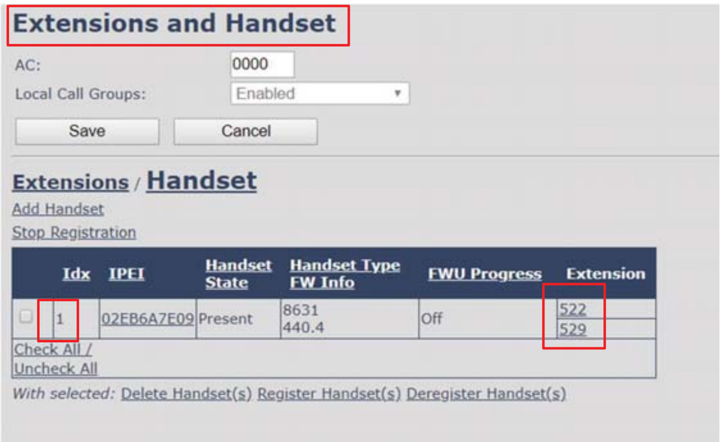
Add a multiline to a handset by creating a new extension but instead for “New Handset” select the existing handset that you want to add the multiline to. (in this case Handset Idx 1)



Step 3:

The extension will now show in the extension list with a new Idx , but the same IPEI, whereas on the handset list, the Idx will be the same and the extension column will show the available extensions for the current handset.

NB: the handset must be rebooted for the changes to take effect.



The Extension will now have two numbers 522 and 529.
When making call the user can chose which line to call from. Simply enter the number to call and press line.
Select the desired line and press the green “Off-hook” button to place the call from this line.

Appendix - Functionality Overview

So far, we have setup our SME VoIP system. Next, in this chapter we list what features and functionalities are available in the system. The SME VOIP system supports all traditional and advanced features of most telephony networks. In addition, 3rd party components handle features like voice mail, call forward, conference calls, etc. A brief description of SME VOIP network functionalities is:

- **Outgoing/incoming voice call management:** The SME VOIP system can provide multiple priority user classes. Further, up to 3 repeaters can be linked to a Base-station.
- **Internal handover**: User locations are reported to SIP Server to provide differentiated services and tariff management. Within a DECT traffic area, established calls can seamlessly be handover between Base-stations using connection handover procedures.

- **Security:** The RTX SME VOIP system also supports robust security functionalities for Base-stations. Most security[2] functionalities are intrinsically woven into the SME VOIP network structure so that network connections can be encrypted, and terminal authentication can be performed.

Gateway Interface

CONNECTOR INTERFACES	
POWER	**Version 1:** Connector: Ethernet PoE (Ethernet adaptor for normal power) IEEE 802.3af: Power class 2 (3.84 – 6.49W) DC plug: 5VDC 2A **Version 2:** Connector: Ethernet PoE (Ethernet adaptor for normal power) IEEE 802.3af: Power class 2 (3.84 – 6.49W)
LAN INTERFACE	Standard : 10BASE-T(IEEE 802.3 100Mbps) Connector: RJ45 8/8
INTERNET PROTOCOL:	• IPv4 • IPv6
KEYS	
	1 x Reset key
LED INDICATOR	
	One Status LED (red, green, orange)
RF	
FREQUENCY BANDS	1880 – 1895 MHz (Taiwan) 1880 – 1900 MHz (EMEA, AUS) 1910 – 1920 MHz (Brazil) 1910 – 1930 MHz (LATAM, Chile) 1920 – 1930 MHz (USA, Canada) These are software settings and need to be set when packed in factory.
OUTPUT POWER	250 mW (EMEA, Taiwan, Brazil, LATAM) 160 mW (Chile, Australia) 140 mW (Canada, USA)
SENSITIVITY	-92 dBm
ANTENNA	Two antennas for diversity
SOFTWARE UPGRADE	
DOWNLOADABLE	Remote firmware update HTTP/HTTPS/TFTP

[2] With active security with authentication 4 channels are supported

Detail Feature List

CODECs	
G.711 A-LAW & U-LAW	Yes/Yes
G.722	Yes
G.726	Yes, 32 Kbps
G.729	A/AB (including VAD) – maximum 4 simultaneously call. **Note**: Only with additional module, this is an extra option that requires a board connector mounted in Gateway. Per default not mounted.
SIP	
RFC2327	SDP: Session Description Protocol
RFC2396	Uniform Resource Identifiers (URI): Generic Syntax
RFC2833	In-Band DTMF/Out of band DTMF support
RFC2976	The SIP INFO method
RFC3261	SIP 2.0
RFC3262	Reliability of Provisional Responses in the Session Initiation Protocol (PRACK)
RFC3263	Locating SIP Servers (DNS SRV, redundant server support)
RFC2543	Session Initiation Protocol (HOLD Option)
RFC3264	Offer/Answer Model with SDP
RFC3265	Specific Event Notification
RCF3326	The Reason Header Field for the Session Initiation Protocol
RFC3311	The Session Initiation Protocol UPDATE Method
RFC3325	P-Asserted Identity
RFC3420	Internet Media Type message/sipfrag
RFC3326	The Reason Header Field for the Session Initiation Protocol (SIP)
RFC3489	STUN
RFC3515	REFER: Call Transfer
RFC3550	RTP: A Transport Protocol for Real-Time Application
RFC3581	Rport
RFC3665	Basic Call Flow Examples
RFC3842	Message Waiting Indication
RFC3891	Replace header support
RFC3892	The Session Initiation Protocol (SIP) Referred-By Mechanism
RFC3960	Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)
RFC4475	Session Initiation Protocol (SIP) Torture Test Messages
SIPS	Secure SIP
IN-BAND DTMF	RFC2833
SRTP	With authentication 16 calls incl. relays are supported.
WEB SERVER	
	Embedded web server HTTP
OTHER FEATURES	
BOOT TIME	Max 60 seconds
QUALITY OF SERVICE	Type of Service (ToS) including DiffServ Tagging, and QoS per IEEE 802.1p/q
IP QUALITY	Warning – Network outage, VoIP service outage
	Adaptive Jitter Buffer support
AUTOMATIC DST	Yes
TONE SCHEME	Tone Scheme is based on CADENCE configuration of the following tones: • Dial Tone • Outside Dial Tone • Prompt Tone • Busy Tone • Reorder Tone • Off Hook Warning Tone • Ring Back Tone

	• Call Waiting Tone • Confirm Tone • MWI Dial Tone • CFwd Dial Tone • Holding Tone • Conference Tone • Secure Call Indication Tone • Page Tone • Mute Tone • Unmute Tone • System Beep • Call Pickup Tone
SUPPORT FOR ROOT CA CERTIFICATE DOWNLOAD	Yes (but PKI deployment/enrollment is not supported)
SHARE NUMBERING	Yes (same as RTX MultiLine feature)
*CODES	Supported through provisioning
VOIP CALLER PIN AND ASSOCIATED DIAL PLAN	Yes
ZERO TOUCH INSTALLATION	The 2nd base station in a dual cell setup must support automatic installation and not require any web-interface installation.
ETHERNET FEATURES	
IPV4	Yes
IPV6	Hardware ready, software not included
VLAN	VLAN (802.1p/q)
DHCP SUPPORT	Yes
STATIC IP	Yes
TLS 1.2	For secure connections (SCA-256)
TFTP	For configuration download.
HTTP	For configuration download.
ENCRYPTED TFTP CONFIG FILES	Yes (AES 128 and 256 key)
HTTP CLIENT	For secure configuration download
HTTPS	Yes, for secure configuration download (Digest authentication using MD5, SHA128, SHA256)
TCP/IP/UDP	Yes/Yes/Yes
SNTP	For internet clock synchronization
DHCP OPTION	66, 160, 159, 150, 60, 43, 125
DNS SERVER	Yes
LANSYNC IEEE1588	No
TOS SUPPORT	SIP TOS and RTP TOS should be supported
NAT TRAVERSAL	Device should be able to function normally behind the firewall
DNS SRV	Device should follow DNS SRV priorities, timeout and A-Rec
TR069	Device must support TR069
REGISTRATION FAILOVER AND FALLBACK	In case of SIP registration server failover, device should be able to register to alternate server
DECT	
DECT CAP	Connectionless handover
CAT-IQ V1.0	Yes
DECT ULE	Yes
ROOT CA	Support for Root CA Certificate Download A new field will be added in the provisioning tab to upload/add new root CA. Upload protocols: http, https, tftp
POWER SUPPLY FEATURES	
LED INDICATOR	No

COLORS	N/A
SEPARATE ADAPTOR	Yes
SWITCH MODE ADAPTOR	Yes, EUP II approved
POWER SPEC	100-240 VAC 50-60Hz 5V2A
MULTI-PLUG ADAPTOR	No
GENERAL TELEPHONY	
HANDSET SUPPORT	10 simultaneous NB calls supported/cell. Total 10 simultaneous call supported in a single cell configuration. Total 20 simultaneous call supported in a dual cell configuration
VOIP ACCOUNTS	20 VoIP accounts
SIMULTANEOUS CALLS	4 Wideband calls (g.722). 10 narrowband calls (PCMA, PCMU, G.726) pr base station.
CALL FEATURES	Codec Negotiation
	Codec Switching
	Auto Echo Cancellation (AEC)
	Missed call notification
	Voice message waiting notification
	Date and Time synchronization
	Parallel calls
	Common parallel call procedures
	Call transfer unannounced
	Call transfer announced
	Call back on Busy
	Conference
	Call Waiting (including Call Waiting Caller ID)
	Calling line identity restriction
	Outgoing call
	Call Toggle
	Incoming call
	Line identification
	Multiple Lines
	Multiple calls
	Call identification
	Calling Name Identification Presentation (CNIP)
	Calling Line Identification Presentation (CLIP)
	Caller ID Blocking (hiding the caller ID if call is private)
	Selective/Anonymous Call Rejection
	Call Hold
	List of registered handsets
	Hot line and Warm Line Calling
	Distinctive Ringing - Calling and Called Number
	Advanced Inbound and Outbound Call Routing
	Independent Configurable Dial Plans – (1 per port)
	Music on Hold
PHONE BOOK	Common Phonebook: Broadsoft Directory LDAP, XML or csv file load
CONTACT LIST ENTRIES	Up to 3000 (depends on size of the entries)
CALL DEFLECTION	Yes
DO NOT DISTURB	Yes
CALL FORWARD UNCONDITIONAL	Yes
CALL FORWARD NO ANSWER	Yes
CALL FORWARD BUSY	Yes
EMERGENCY CALL	Yes

FCC Warning

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications to this equipment not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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

For Handset

SAR tests are conducted using standard operating positions accepted by the FCC with device transmitting at its highest certifed power level in all tested frequency bands, although the SAR is determined at the highest certified power level, the actual SAR level of the device while operating can be well below the maximum value. Before a new model device is an available for sale to the public, it must be tested and certified to the FCC that it does not exceed the exposure limit established by the FCC, tests for each device are performed in positions and locations as required by the FCC. For body worn operation, this model device has been tested and meets the FCC RF exposure guidelines when used with an accessory designated for this product or when used with an accessory that contains no metal.

For Base

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator& your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter located or operating in conjunction with any other antenna or transmitter.

ISEDC Warning

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.

2. This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil est compatible avec la licence de l’Innovation, la Science et le développement conomique du Canada à l’exemption des normes RSS. Le fonctionnement est sujet aux deux (2) conditions suivantes :

(1) Cet appareil peut ne pas causer de l’interférence, et

(2) Cet appareil doit accepter l’interférence, incluant de l’interférence qui peut causer un mauvais fonctionnement de cet appareil.

For Handset

SAR tests are conducted using standard operating positions accepted by the ISEDC with device transmitting at its highest certifed power level in all tested frequency bands, although the SAR is determined at the highest certified power level, the actual SAR level of the device while operating can be well below the maximum value. Before a new model device is an available for sale to the public, it must be tested and certified to the ISEDC that it does not exceed the exposure limit established by the ISEDC, tests for each device are performed in positions and locations as required by the ISEDC. For body worn operation, this model device has been tested and meets the ISEDC RF exposure guidelines when used with an accessory designated for this product or when used with an accessory that contains no metal.

For Base

This equipment complies with ISEDC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator& your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter located or operating in conjunction with any other antenna or transmitter.

Pour le combiné

Les tests SAR sont faits en utilisant les normes de positions d’opération acceptées par l’ISEDC avec les appareils émettant les plus hauts niveaux de puissance certifiés sur toutes les bandes de fréquences, même si le SAR est déterminé d’être du plus haut niveau de puissance certifié, le niveau SAR actuel de l’appareil peut être sous la valeur maximale de fonctionnement. Avant qu’un nouveau modèle d’appareil ne soit disponible pour la vente au public, celui-ci doit être soumis à des tests de certification par l’ISEDC lesquels n’excèdent aucunement la limite d’exposition issue par l’ISEDC, lesquels sont des tests effectués sur chaque appareil dans des positions et endroits requis par l’ISEDC. Pour l’usure de construction de ce modèle d’appareil, celui-ci a été testé et rencontre les lignes directrices émises par l’ISEDC RF pour l’exposition, lorsqu’il est utilisé avec un accessoire conçu pour ce produit ou utilisé avec un accessoire qui ne contient aucun métal.

Pour la base

Cet équipement est conforme avec les limites d’exposition à la radiation de l’ISEDC émises dans un environnement contrôlé. Cet équipement devrait être installé et fonctionnel avec un minimum de distance entre le radiateur et votre corps d’au moins 20 cm. Ce transmetteur ne doit pas être co-situé près d’une autre antenne ou en conjonction avec un autre transmetteur.

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareille numérique de classe B est conforme aux normes canadiennes ICES-003.