Spectralink IP-DECT Servers

Installation and Configuration Guide

Spectralink IP-DECT Server 200/400/6500
Virtual IP-DECT Server One

722-0210-000 Rev: A
November 2020

Copyright Notice

Notice

Spectralink Corporation has prepared this document for use by Spectralink personnel and customers. The drawings and specifications contained herein are the property of Spectralink and shall be neither reproduced in whole or in part without the prior written approval of Spectralink, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Spectralink reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Spectralink to determine whether any such changes have been made.

NO REPRESENTATION OR OTHER AFFIRMATION OF FACT CONTAINED IN THIS DOCUMENT INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, RESPONSE-TIME PERFORMANCE, SUITABILITY FOR USE, OR PERFORMANCE OF PRODUCTS DESCRIBED HEREIN SHALL BE DEEMED TO BE A WARRANTY BY SPECTRALINK FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF SPECTRALINK WHATSOEVER.

Warranty

The Product Warranty and Software License and Warranty and other support documents are available at http://support.spectralink.com/.

Contact Information

US Location
+1 800-775-5330

Spectralink Corporation
2560 55th Street
Boulder, CO 80301
USA

info@spectralink.com

Denmark Location
+45 7560 2850

Spectralink Europe ApS
Bygholm Soepark 21 E Stuen
8700 Horsens
Denmark

infoemea@spectralink.com

UK Location
+44 (0) 20 3284 1536

Spectralink Europe UK
329 Bracknell, Doncastle Road
Bracknell, Berkshire, RG12 8PE
United Kingdom

infoemea@spectralink.com

Contents

Chapter 1: About This Guide

This guide is intended for qualified technicians who will install, configure and maintain the Spectralink IP-DECT Server 200/400/6500 and Spectralink Virtual IP-DECT Server One solution. To qualify to install the Spectralink IP-DECT Server 200/400/6500 and Spectralink Virtual IP-DECT Server One solution, you must have successfully completed the Spectralink IP-DECT Server 200/400/6500 and Spectralink Virtual IP-DECT Server One technical training. The guide provides all the necessary information for successful installation and maintenance of the wireless solutions.

This includes the installation and configuration of:

- Spectralink IP-DECT Server 200/400/6500
- Spectralink Virtual IP-DECT Server One
- Spectralink DECT Media Resource (only Spectralink IP-DECT Server 6500 and Spectralink Virtual IP-DECT Server One)
- Spectralink Virtual IP-DECT Media Resource (only Spectralink Virtual IP-DECT Server One)
- Spectralink IP-DECT Base Station (only Spectralink IP-DECT Server 400/6500 and Spectralink Virtual IP-DECT Server One)
- Spectralink DECT Repeater

The guide also provides you with information about:

- Web-based Administration Page of the Spectralink IP-DECT Server 200/400/6500, Spectralink Virtual IP-DECT Server One, Spectralink DECT Media Resource, Spectralink Virtual IP-DECT Media Resource, and Spectralink IP-DECT Base Station.

Important Information Before You Begin

This guide assumes the following:

- that users have a working knowledge of the call handler's operations
- that the call handler is installed, initialized and is working correctly
- that you have a working knowledge of deployment in general
- that you have a running VMware vSphere solution or ESXi host and solid knowledge of deploying OVA files and managing virtual machines on VMware vSphere/ESXi (only if using the Spectralink Virtual IP-DECT Server One and Spectralink Virtual IP-DECT Media Resources)
- that a site survey has been conducted and that the installer has access to these plans

Note:

The site survey should determine the number of handsets, base stations and repeaters needed, and where to place them. The site survey should also determine how many RF channels are needed.

Related Documentation

All Spectralink documents are available at http://support.spectralink.com/products including Safety and Handling information and Regulatory information.

Contact your Spectralink support representative if you need more information.

Subject	*Documentation*
Spectralink DECT Handset	For more information about the handset, refer to the user guide for the model being deployed.
Site Survey Function in Handset	For more information about the site survey function in handset, refer to the online guide.
Synchronization and Deployment	For more information about synchronization and deployment, refer to the refer to the online guide.
Provisioning	For more information about the redirection service, refer to the online guide.
Installation	For more information about IP-DECT Server Installation, refer to the online guide for the model server you are installing.
Handset and Repeater Management Tool	For more information about handset and repeater management using the Handset and Repeater Management Tool, refer to the online guide.
VMware vSphere/ESXi	Navigate to the VMware documentation site for more information about OVA files and managing virtual machined on VMware vSphere/ESXi.
Release Notes	Document that describes software changes, bug fixes, outstanding issues, and hardware compatibility considerations for new software releases. Available online--refer to the online guide.
Spectralink DECT Training material	In order to gain access to the Spectralink training material, you must attend training and become Spectralink Certified Specialist. Contact your Spectralink support representative for more information.

Terminology and Acronyms

The table below refers to common terms and acronyms that are related to the Spectralink IP-DECT solutions.

Term	*Definition*
AC	Authentication Code
AEC	Acoustic Echo Canceller
ARI	Access Rights Identity–Wireless identity of the Spectralink
BHCA	Busy Hour Call Attempts
CLI	Command Line Interface
COTA	(Handset) Configuration Over The Air
CTI	Computer Telephony Integration (for CUCM)
CUCM	Cisco Unified Communications Manager

Term	*Definition*
dB	Decibels (deciBells)
DECT	Digital Enhanced Cordless Telecommunications
Deployment	The act of locating the mounting location and installing base stations and repeaters. System performance is dependent on the deployment made–and, therefore, the survey performed.
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
e.i.r.p.	Equivalent Isotropic Radiated Power
Erlang	The erlang is a dimensionless unit that is used in telephony as a measure of offered load or carried load on service providing elements such as telephone circuits or telephone switching equipment.
FP	Fixed Part
GAP	Generic Access Profile
Handover	A process initiated by the handset in which the traffic channel carrying an active conversation is passed from one base station to another.
HW PCS	Hardware Product Change Status–Hardware edition
IGMPv3	Internet Group Management Protocol version 3
IP	Internet Protocol
IPEI	International Portable Equipment Identity–Serial number of the handset
IWU	Inter Working Unit
LAL	Location Area Level
LAN	Local Area Network
LAN synchronization	Method for synchronizing IP-DECT base stations over LAN
LED	Light Emitting Diode
Li-ion	Lithium-ion
MAC	Media Access Control–hardware address of a device connected to a network
Media channel	A network connection used to carry communication between the base station and the media resource, and between the media resource and an external endpoint.
MTU	Maximum Translation Unit
MWI	Message Waiting Indication
Ni-MH	Nickel -Metal Hydride
NTP	Network Time Protocol
OVA	Open Virtualization Application
OVF	Open Virtualization Format
OAM REST API	Operation and Administration Management Representational State Transfer Application Programming Interface
PBX	Private Branch eXchange
PCS	Product Change Status (Edition)
PIE	Product Initial Edition
PoE	Power over Ethernet
PP	Portable Parts–wireless handset
PTP	Precision Time Protocol (IEEE-1588v2)
QoS	Quality of Service

Term	*Definition*
Q Value	Signal Quality Factor value. An expression of the bit failure rate in the communication between the handset and a base station. The value has a max. of 64, equal to no bit errors measured.
Radio synchronization (OTA)	Method for synchronizing IP-DECT base stations over radio (Over The Air/OTA)
RF	Radio Frequency
RFP	Radio Fixed Part–base station
RPN	Radio Part Number–base station number
RSSI	Received Signal Strength Indicator
RSSI Value	Radio Signal Strength Indication value. A relative expression for the signal strength of a base station as measured by the handset at a given location.
RTP	Real-time Transport Protocol
SfB	Skype for Business
SIP	Session Initiated Protocol
Site survey	A site survey comprises the act of locating the best places for base stations by measuring RSSI levels with DECT handsets. Complete survey consists of measuring with multiple base stations, combining RSSI and Q value reading in real surroundings.
Spectralink IP-DECT Server	Spectralink IP-DECT Server 200/400/6500
Spectralink Virtual IP-DECT Server One	Spectralink Virtual IP-DECT Server One
SRPS	Spectralink Redirection and Provisioning Service
SRTP	Secure Real-time Transport Protocol
SUOTA	Software Update Over The Air
SW PCS	Software Product Change Status–Software edition
Synchronization Over the Air (OTA)	Method for synchronizing IP-DECT base stations over Air (radio)
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
Traffic channel	A traffic channel is used to carry communication between the handset and the base station or repeater.
TTL	Time To Live
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
UUID	Universally Unique Identifier
VoIP	Voice over Internet Protocol
WLAN	Wireless Local Area Network
WRFP	Wireless Radio Fixed Part–Wireless Repeater

Chapter 2: About DECT

DECT stands for Digital Enhanced Cordless Telecommunications.

DECT is the standard for short-range cordless communications developed by the European Telecommunications Standards Institute (ETSI): ETSI EN 300 175-1.

DECT is used in all countries in Europe and in most of Asia, Australia, South America and North America.

DECT is a low power technology and can be used in radio sensitive environments. Both handsets and base stations have an average power output of 10mW, but can deliver a burst power output of 250mW.

Note:

The entire Spectralink 7000 Portfolio is built on DECT technology.

DECT Frequency Bands

The following frequency bands are dedicated to DECT:

- EMEA, Australia & New Zealand: 1G8: 1880–1900 MHz
- South America (SAM): 1G9: 1910–1930 MHz
- USA & Canada: 1G9: 1920–1930 MHz (DECT 6.0)

Note:

Because DECT has its own dedicated frequency band, it is not subject to interference from other radio transmitters such as GSM phOne, Bluetooth, microwave ovens and widely used Wi-Fi equipment.

Chapter 3: Spectralink IP-DECT/Virtual IP-DECT Server One Solution

Types of Servers

Following types of servers are available:

- Spectralink IP-DECT Server 200
- Spectralink IP-DECT Server 400
- Spectralink IP-DECT Server 6500
- Spectralink Virtual IP-DECT Server One

Note:

Besides the Spectralink IP-DECT/Virtual IP-DECT Server One solutions, a Spectralink DECT Server solution is also available. The Spectralink DECT Server solution is out of the scope of this Installation and Configuration Guide but see Spectralink Server Solution Overview and Comparison.

Spectralink IP-DECT Server 200

- a single cell system (one built-in base station in the server) supporting SIP lines only.
- designed with connector for External Antenna.
- Up to 3 additional Spectralink DECT Repeaters can be added to the Spectralink IP-DECT Server 200.
- supports up to 12 registered handsets and 6 simultaneous calls.
- The DECT radius of coverage is up to 600 meters/2000 feet with a handset in free sight.
- The DECT radius of coverage can vary significantly if obstacles block the signal, for example in buildings with many rooms, hallways, walls and floors. The radius coverage is typically around 30 meters/100 feet in office environments. Coverage

should always be verified to ensure optimal location of the Spectralink IP-DECT Server 200 before it is permanently installed.

Spectralink IP-DECT Server 400

- As a basic edition the Spectralink IP-DECT Server 400 is a single cell system (one built-in base station in the server) supporting SIP lines only.
- The Spectralink IP-DECT Server 400 is designed with connector for External Antenna.
- Additional Spectralink IP-DECT Base Stations can be added to the Spectralink IP-DECT Server 400 to enable multi-cell functionality and to expand the covered area.

Note:

A license is required to enable the multi-cell function. For more information, see Licenses for Spectralink IP-DECT Server 400/6500.

- All Spectralink IP-DECT Base Station models can be used. Up to 9 additional Spectralink IP-DECT Base Stations can be added to the Spectralink IP-DECT Server 400 system and up to 3 additional Spectralink DECT Repeaters can be added to each Spectralink IP-DECT Base Station. This results in up to 30 Spectralink DECT Repeaters if all Spectralink IP-DECT Base Stations are registered.
- The Spectralink IP-DECT Server 400 without any licenses supports up to 12 registered handsets and 6 simultaneous calls.
- The DECT radius of coverage is up to 600 meters/2000 feet with a handset in free sight.

Spectralink IP-DECT Server 6500

- The Spectralink IP-DECT Server 6500 controls the wireless infrastructure. It manages Spectralink DECT Media Resources, Spectralink IP-DECT Base Stations and the IP interface to the call handler.
- The communication protocol between the Spectralink IP-DECT Server 6500 and the call handler is a SIP line interface.
- A Spectralink IP-DECT Server 6500 is installed directly on the LAN and must be managed as part of the corporate network.
- The Spectralink IP-DECT Server 6500 is a multi-cell solution in a 19” cabinet. It is shipped from the factory as a Spectralink IP-DECT Server 6500 with one Ethernet port and 32 on-board traffic channels, which allows for up to 32 full duplex simultaneous media streams (RTP streams) depending on the codec being used. There is no radio part in the Spectralink IP-DECT Server 6500. This means that at least one Spectralink IP-DECT Base Station must be part of the Spectralink IP-DECT Server 6500 solution.

Note:

The Spectralink IP-DECT Server 6500 is extremely scalable and is very easy to scale in order to meet customer demands. If it is upgraded to its full potential via licenses, it supports up to 4096 registered handsets, up to 1024 Spectralink IP-DECT Base Stations and with a maximum of 32 Spectralink DECT Media Resources, it supports up to 1024 simultaneous calls. For more information, see Licenses for Spectralink IP-DECT Server 400/6500.

Spectralink Virtual IP-DECT Server One

- The Spectralink Virtual IP-DECT Server One controls the wireless infrastructure. It manages external Spectralink Virtual IP-DECT Media Resources, Spectralink DECT Media Resources, Spectralink IP-DECT Base Stations and the IP interface to the call handler.
- The communication protocol between the Spectralink Virtual IP-DECT Server One and the call handler is a SIP line interface.
- A Spectralink Virtual IP-DECT Server One is deployed on VMware and must be managed as part of the corporate network.
- The Spectralink Virtual IP-DECT Server One is a multi-cell solution, that is distributed as an Open Virtual Appliance (OVA) file. The OVA file is easily deployed on a VMware vSphere infrastructure or directly on an ESXi host. Future updates can be applied directly in the web-based Administration Page of the Spectralink Virtual IP-DECT Server One using a new OVA file.
- When initially deployed, the Spectralink Virtual IP-DECT Server One includes a demo mode license with these features available:
    - Residential ARI
    - 4 users
    - 4 simultaneous calls
    - 4 base stations
    - Skype for Business interoperability
    - Redundancy feature
    - LAN Sync
    - Enhanced Provisioning
    - Handset sharing
    - OAM REST API

For more information about deploying the OVA file of a Spectralink Virtual IP-DECT Server One, see Deploying Spectralink Virtual IP-DECT Server One and Spectralink Virtual IP-DECT Media Resource on VMware ESXi.

Mandatory Base License ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License

To activate the Spectralink Virtual IP-DECT Server One, a Mandatory Base License ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License must be obtained and loaded.

The Mandatory Base License ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License is created with the following information:

- UUID (Universally Unique Identifier)
- New ARI
- Number of allowed users: 150
- Number of media channels: 32
- Number of allowed base stations: 64

At least one Spectralink IP-DECT Base Station must be part of the Spectralink Virtual IP-DECT Server One solution to ensure the presence of a radio part. The Spectralink Virtual IP-DECT Server One has an internal media resource with 32 media channels after the Mandatory Base License ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License has been loaded. Additional users, numbers of allowed base stations and media channels can then be increased by installing corresponding licenses.

Note:

The Spectralink Virtual IP-DECT Server One is extremely scalable and is very easy to scale in order to meet customer demands. If it is upgraded to its full potential via licenses, it supports up to 4096 registered handsets, up to 2048 Spectralink IP-DECT Base Stations and with a maximum of 16 Spectralink Virtual IP-DECT Media Resources (each with up to 64 channels), it supports up to 1024 simultaneous calls. For more information, see Licenses for Spectralink Virtual IP-DECT Server One.

The Spectralink Virtual IP-DECT Server One uses Security (TLS, SRTP) as default.

Note:

The Spectralink Virtual IP-DECT Server One can use both the external Spectralink DECT Media Resources (requires acquisition of a cabinet) and the Spectralink Virtual IP-DECT Media Resources.

Base Stations License

With the Mandatory Base License ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License installed, the number of allowed base stations can be increased by installing a Base Stations License.

The Base Stations License comes in the following variants:

- 16 base stations
- 64 base stations
- 256 base stations

- 1024 base stations

These Base Stations Licenses can be stacked up to a maximum of 2048 allowed base stations. For more information, see Licenses for Spectralink Virtual IP-DECT Server One.

32 Media Channels | Virtual IP-DECT Server One License

With the Mandatory Base License ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License installed, the number of allowed media channels in the Spectralink Virtual IP-DECT Server One can be increased by installing a 32 Media Channels | Virtual IP-DECT Server One License (64 media channels in total).

Besides the internal media resource, Spectralink Virtual IP-DECT Media Resources can also be deployed from the same OVA file used for the Spectralink Virtual IP-DECT Server One, and then loaded with 32 Media Channels | Virtual IP-DECT Server One Licenses.

Using Spectralink Virtual IP-DECT Media Resources can increase the capacity tremendously, as you can create up to 16 Spectralink Virtual IP-DECT Media Resources with two 32 Media Channels | Virtual IP-DECT Server One Licenses each. For more information about Spectralink Virtual IP-DECT Media Resources, see Spectralink Virtual IP-DECT Media Resource and Deploying Spectralink Virtual IP-DECT Server One and Spectralink Virtual IP-DECT Media Resource on VMware ESXi. For more information about licenses, see Licenses for Spectralink Virtual IP-DECT Server One.

Other Solution Components

In addition to the Spectralink IP-DECT/Virtual IP-DECT Server One, a Spectralink IP-DECT/Virtual IP-DECT Server One configuration can include a number of the following components:

- Spectralink DECT Media Resources (only Spectralink IP-DECT Server 6500 and Spectralink Virtual IP-DECT Server One)
- Spectralink Virtual IP-DECT Media Resources (only Spectralink Virtual IP-DECT Server One One)
- Spectralink IP-DECT Base Stations (only Spectralink IP-DECT Server 400/6500 and Spectralink Virtual IP-DECT Server One)
- Spectralink DECT Repeaters
- Spectralink External Antennas (only Spectralink IP-DECT Server 200/400 and Spectralink IP-DECT Base Station)

To handle the calls in the solution a call handler (IP-PBX SIP) is used.

Note:

For more information about system compatibility, see Product Compatibility.

For configuration overview, see Total Configuration Overview.

Spectralink DECT Media Resource

The Spectralink DECT Media Resource can be used with Spectralink IP-DECT Server 6500 and Spectralink Virtual IP-DECT Server One.

The Spectralink DECT Media Resource performs media conversion between the call handler and the Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One and is the media termination point for incoming and outgoing calls.

If used with Spectralink IP-DECT Server 6500: The Spectralink DECT Media Resource is a print board that is placed within the same cabinet next to the Spectralink IP-DECT Server 6500 board. Up to 2 Spectralink DECT Media Resources can be placed in the same cabinet that houses the Spectralink IP-DECT Server 6500 board. If more media resources are needed, it is necessary to acquisition a media resource cabinet. The media resource cabinet comes with one media resource print board and the possibility of installing up to two more media resource print boards.

If used with Spectralink Virtual IP-DECT Server One: Acquisition of a media resource cabinet is required. The media resource cabinet comes with one media resource print board and the possibility of installing up to two more media resource print boards. Each Spectralink Virtual IP-DECT Server One contains 32 built in media channels if the Mandatory Base License ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License is installed. The Spectralink Virtual IP-DECT Server One supports a total of 1024 media channels – up to 31 media resource print boards (11 cabinets in total).

Each Spectralink DECT Media Resource adds 32 media channels. The maximum number of simultaneous calls for a fully loaded system is 1024 calls at the same time. Depending on codec choice, the number of media channels per Media Resource card can vary from 12 - 32.

G.726 allows for 32 duplex traffic channels as this codec requires no processing and is routed directly to the Spectralink IP-DECT Base Station. Other codecs such as G.711 or G.729 must be converted to G.726 before routed further on to the Spectralink IP-DECT Base Station and this affects the total number of available media channels on the Spectralink DECT Media Resource, lowering the number of media channels down to 12 if all calls utilize the G.729 codec.

The Spectralink DECT Media Resource connects directly with the LAN and must operate in conjunction with the Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One. If using sites, the Spectralink DECT Media Resources can be placed at different locations.

The Spectralink DECT Media Resource contains no radio parts. It ships from the factory configured for DHCP. Should it enter an unrecoverable state, it can be reset to factory default settings when the reset button is pressed and held for more than 5 seconds.

Spectralink Virtual IP-DECT Media Resource

The Spectralink Virtual IP-DECT Media Resource is distributed in the same Open Virtual Appliance (OVA) file as the Spectralink Virtual IP-DECT Server One. The OVA file is easily deployed on a VMware vSphere infrastructure or directly on an ESXi host. The Spectralink Virtual IP-DECT Media Resource is connected to the Spectralink Virtual IP-DECT Server One using UPnP or by manually entering the IP address or host name of the server through the web-based Administration Page or using OAM REST API.

The Spectralink Virtual IP-DECT Media Resource performs media conversion between the call handler and the Spectralink Virtual IP-DECT Server One and is the media termination point for incoming and outgoing calls.

When deployed and connected, the Spectralink Virtual IP-DECT Media Resource can be loaded with 32 Media Channels | Virtual IP-DECT Server One Licenses. Using Spectralink Virtual IP-DECT Media Resources can increase the capacity tremendously, as you can deploy up to 16 Spectralink Virtual IP-DECT Media Resources with two 32 Media Channels | Virtual IP-DECT Server One Licenses each (a total of 64 media channels on each virtual external media resource). The Spectralink Virtual IP-DECT Server One itself can have an extra 32 Media Channels | Virtual IP-DECT Server One License installed as well (64 media channels in total on the server).

The Spectralink Virtual IP-DECT Media Resource performs media conversion between the call handler and the Spectralink Virtual IP-DECT Server One and is the media termination point for incoming and outgoing calls.

Each Spectralink Virtual IP-DECT Server One contains 32 built in media channels if the Mandatory Base Licence ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License is installed. Spectralink Virtual IP-DECT Server One supports a total of 16 Spectralink Virtual IP-DECT Media Resources. The Spectralink Virtual IP-DECT Server One supports a total of 1024 (16 x 64) media channels.

Each Spectralink Virtual IP-DECT Media Resource adds 32 voice channels. The maximum number of simultaneous calls for a fully loaded system is 1024 calls at the same time.

For more information about licenses and Spectralink Virtual IP-DECT Media Resources, see Licenses for Spectralink Virtual IP-DECT Server One and Deploying Spectralink Virtual IP-DECT Server One and Spectralink Virtual IP-DECT Media Resource on VMware ESXi.

Spectralink IP-DECT Base Station

The Spectralink IP-DECT Base Station is to be used with Spectralink IP-DECT Server 400/6500, Spectralink Virtual IP-DECT Server One and Spectralink DECT Server 2500/8000.

The Spectralink IP-DECT Base Station is designed with two internal antennas and supports antenna diversity.

The Spectralink IP-DECT Base Station is designed with connector for External Antenna.

The Spectralink IP-DECT Base Station is also able to carry out a handover between the RF channels under the same Spectralink IP-DECT Base Station, and handles up to 12 (depending on synchronization configuration) DECT traffic channels simultaneously.

The Spectralink IP-DECT Base Station is able to frame synchronize with other Spectralink IP-DECT Base Stations under the same server.

The Spectralink IP-DECT Base Station can be powered over ethernet (PoE/802.3af) or by a separate power supply (available separately).

The DECT radius of coverage is up to 600 meters/2000 feet with a handset in free sight.

Spectralink DECT Repeater

The Spectralink DECT Repeater is a building block to be used to extend the coverage area in a wireless Spectralink DECT solution. The repeater does not increase the number of traffic channels, however, it provides a larger physical spreading of the traffic channels and

thereby increases the coverage area established with the Spectralink IP-DECT/Digital DECT Base Stations/Spectralink IP-DECT Servers 200/400.

Note:

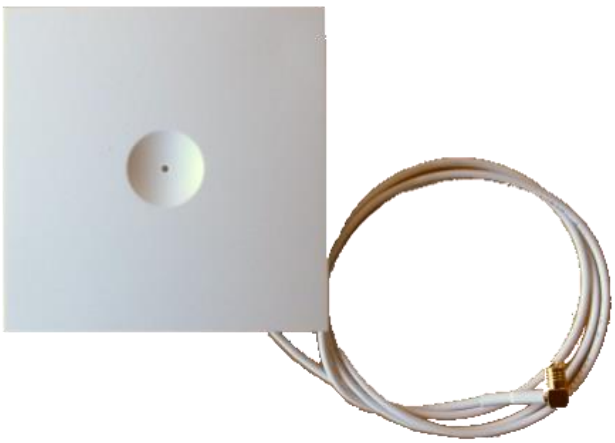
Both the Spectralink IP-DECT Server 200 and Spectralink IP-DECT Server 400 are Spectralink IP-DECT Servers with a built-in Spectralink IP-DECT Base Station.

The repeaters are mainly used in areas with limited traffic. The Spectralink DECT Repeater is available with either 2 or 4 traffic channels. It is wireless and does not need physical connection to the Spectralink IP-DECT/Virtual IP-DECT Server One, making it very easy to install. The repeaters can be supplied with an external antenna making it possible to create radio coverage in a remote area without cabling to the rest of the installation.

The base station/server 200/400 can support up to 3 repeaters.

External Antenna

Spectralink IP-DECT Base Stations, Spectralink IP-DECT Server 200/400 and Spectralink DECT Repeaters can be equipped with an external antenna using a specially designed connection cable between the external antenna and the host.



The external antenna is highly directional and used with Spectralink IP-DECT Base Stations or the Spectralink IP-DECT Server 200/400 for added coverage in complex environments or to link up with remote areas. External antennas can also be used with Spectralink DECT Repeaters to link up with remote areas where wiring between the server and base station is difficult or impossible.

Note:

When used with a Spectralink IP-DECT Server 200/400 or Spectralink IP-DECT Base Station, the external antenna always use the same channel as the host and provides full coverage for handsets.

When used with a Spectralink DECT Repeater, the external antenna always use a channel different from the host and only provides a link to the main coverage area–no speech coverage.

The range of the host (on base station and server) is reduced when the external antenna is connected.

For more information about using the external antenna to add coverage in complex environments or to link up with remote areas, see Using Spectralink IP-DECT Server 200/400 and Spectralink IP-DECT Base Station with External Antenna.

For more information about using the repeater with external antenna, see Using the Spectralink DECT Repeater with External Antenna.

System Capacity Overview

Below you will find an overview of the system capacity of the Spectralink IP-DECT/Virtual IP-DECT Server One and Spectralink DECT Media Resources/Spectralink Virtual IP-DECT Media Resources:

System Capacity – Servers

Description	*Server 200*	*Server 400*	*Server 6500*	*Virtual Server One*
IP-DECT Servers	1	1	2 *	2 *
Media Resources	N/A	N/A	32 print boards	16 ****
Protocol supported	SIP	SIP	SIP	SIP
Max number of simultaneous SIP calls	6	Up to 24 **	1024 ** Up to 12 per Radio Base Station 32 media channels per Media Resource	1024 ** Up to 12 per Radio Base Station 64 media channels per Media Resource
Codecs supported	G.711A, G.711µ, G.726, G.729	G.711A, G.711µ, G.726, G.729	G.711A, G.711µ, G.726, G.729	G.711A, G.711µ, G.726, G.729
Max number of subscribed DECT handsets	12	60 **	4096 ***	4096
Max number of IP-DECT Base Stations	N/A	9 **	1024	2048
Repeaters per base station	0	3	3	3
Repeaters per server	3	3	0	0

*) Two Spectralink IP-DECT Server 6500s/Spectralink Virtual IP-DECT Server One for redundancy. License required.

**) License required.

***) License required. Skype for Business only supports up to 1500 users.

****) Installations of the Spectralink Virtual IP-DECT Media Resource (each with two 32 Media Channels | Virtual IP-DECT Server One Licenses)

System Capacity–Media Resources

Spectralink DECT Media Resource

Item	*IP-DECT Server 6500 – Maximum Quantity*	*Virtual IP-DECT Server One – Maximum Quantity*
Media Resources	32 print boards	32 print boards
Protocol supported	SIP	SIP
Simultaneous calls	32 (depending on used codec)*	32 (depending on used codec)*
Codecs supported	G.711A, G.711µ, G.726, G.729	G.711A, G.711µ, G.726, G.729

*) The available number of channels on a Spectralink DECT Media Resource depends on the codec type of the active calls. Calls utilizing the G.726 codec uses approximately 2% of the available resources, calls utilizing the G.711 codec uses approximately 3%, and calls utilizing the G.729 codec uses approximately 8%. E.g.: With 5 active G.729 calls and 10 active G.711 calls, the total resource utilization will be approximately 70%.

Recommendations

If configuring a system with Spectralink DECT Media Resources or Spectralink Virtual IP-DECT Media Resources, Spectralink recommends disabling the internal media resource of the Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One when:

- The system handles more than 20 simultaneous calls.
- There are more than 500 users (200 users if using Lync/Skype for Business).

For more information, see Configuring Media Resource Settings.

Spectralink Virtual IP-DECT Media Resource

Item	*Virtual IP-DECT Server One – Maximum Quantity*
Media Resources	16 *
Protocol supported	SIP
Simultaneous calls	64
Codecs supported	G.711A, G.711µ, G.726, G.729

*) Installations of the Spectralink Virtual IP-DECT Media Resource (each with two 32 Media Channels | Virtual IP-DECT Server One Licenses)

Spectralink Server Solution Overview and Comparison

Product Overview

WS (Wireless Server): IP-DECT Server 6500 / 400*) / 200*) Virtual IP-DECT Server One DECT Server 8000 / 2500		
RFP (Radio Fix Part): IP-DECT base station and DECT base station **). Radio devices controlled by the Server	IP-DECT base station Sync over air (1 ch) or sync over LAN Up to 1 speech channels 	DECT base station Sync via cable 4 or 8 speech channels 
WRFP (Wireless Radio Fix Part): DECT repeater. Autonomous radio device used for added coverage	DECT repeater works with all radio devices  2 or 4 speech/link channels	
EA (External Antenna): *)** Used with RFP, WRFP or IP-DECT Server 200/400 for added coverage or to link remote locations	Works with IP-DECT Server 200/400, IP-DECT base stations and RFP 6 DECT base stations 	
PP (Portable Part): The Spectralink 7000 Portfolio Handsets		

*) The Spectralink IP-DECT Server 200/400 has a built-in radio which acts like a Spectralink IP-DECT Base Station with up to 12 traffic channels.

**) Spectralink Digital DECT Base Stations are available in the following editions: RFP4 and RFP5 (4 traffic channels) and RFP6 (4 or 8 traffic channels).

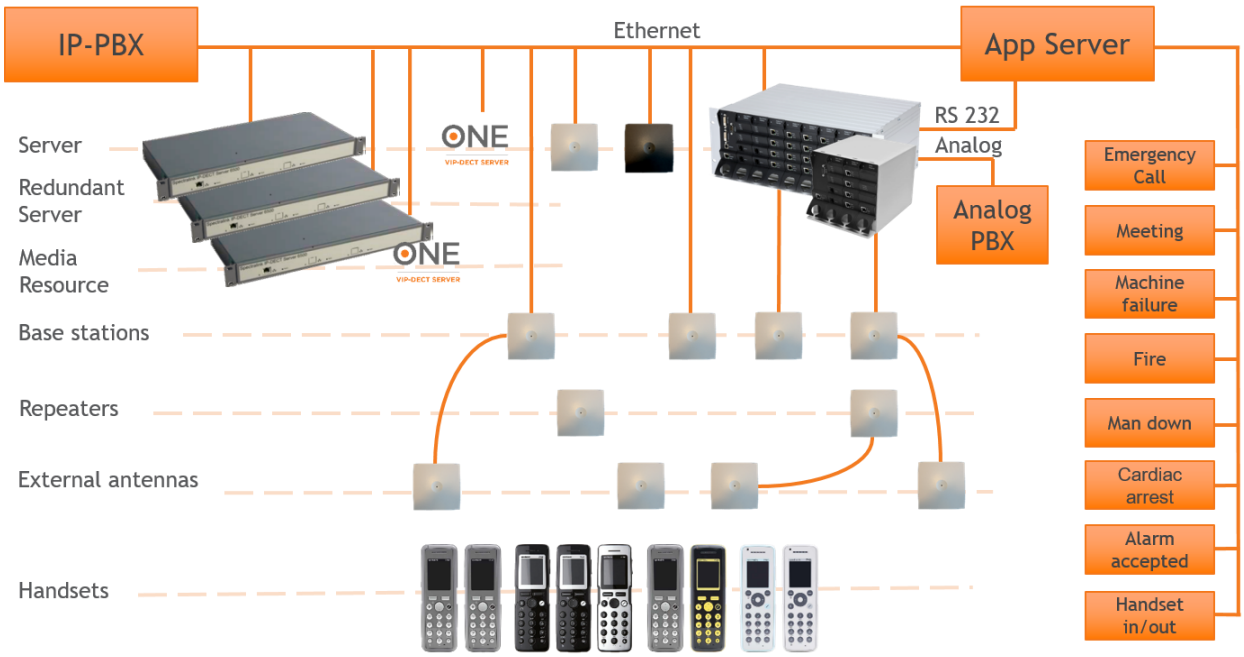
***) The external antenna is highly directional and used with RFP6 Spectralink Digital DECT Base Stations and Spectralink IP-DECT Base Stations or the Spectralink IP-DECT Server 200/400 for added coverage in complex environments or to link up with remote areas. External antennas can also be used with Spectralink DECT Repeaters to link up with remote areas where wiring between the server and base station is difficult or impossible.

For a comparison of Spectralink Servers, and Spectralink Base Stations, see Server Comparison Matrix and Base Station Comparison Matrix.

Spectralink Handset Portfolio Overview

For more information about the handsets, see the relevant Handset User Guides.

Total Configuration Overview



Server Comparison Matrix

The illustration below shows a Spectralink 7000 Portfolio Infrastructure/Spectralink Server comparison matrix.


Server	200 VoIP	400 VoIP	6500 VoIP	One VoIP	2500 Analog	2500 VoIP	8000 Analog	8000 VoIP
Market	SOHO	Small Business	Medium to large business	Large enterprise	SMB	SMB	Medium to large business	Medium to large business
PBX Integration	IP (SIP)	IP (SIP)	IP (SIP)	IP (SIP)	Analog	IP (SIP)	Analog	IP (SIP)
Simultaneous calls	6	Up to 24	1024	1024	32	32	1008	1024
DECT base stations	-	-	-	-	16/8 *)	16/8 *)	504/252 *)	512/256 *)
IP-DECT base stations	Itself **)	Itself **) +9	1024	2048	1024	1024	1024	1024
Repeaters	3	3	3 per base station	3 per base station	3 per base station	3 per base station	3 per base station	3 per base station
Ext. antenna ***)	✓	✓	✓	✓	✓	✓	✓	✓
Handsets (subscription)	12	60	4096	4096	32	150 ‘’’’)	1008	4096

Server	200 VoIP	400 VoIP	6500 VoIP	One VoIP	2500 Analog	2500 VoIP	8000 Analog	8000 VoIP
Increased functionality with license based features	✓	✓	✓	✓	✓	✓	✓	✓
Skype for Business support	✓	✓	✓	✓	-	✓	-	✓
Cisco support	✓	✓	✓	✓	-	✓	-	✓
Security (SRTP/TLS)	✓	✓	✓	✓	✓	✓	✓	✓
Redundancy	-	-	✓	✓	-	-	-	-
Handset sharing	-	✓	✓	✓	✓	✓	✓	✓
G.726, G.711 a-law & u-law	✓	✓	✓	✓	-	✓	-	✓
G.729	✓	✓	✓	✓	-	-	-	-
SUOTA *) All handsets 	✓	✓	✓	✓	✓	✓	✓	✓

*) 4 channel/8 channel Spectralink Digital DECT Base Station.

**) The Spectralink IP-DECT Server 200/400 has a built-in radio which acts like a Spectralink IP-DECT Base Station with up to 12 traffic channels.

***) External antenna can only be used with Spectralink IP-DECT Server 200/400, RFP 6 Spectralink Digital DECT Base Stations, Spectralink IP-DECT Base Stations and Spectralink DECT Repeaters.

****) Recommended limitation is 150 subscribed Spectralink DECT Handsets, but more handsets can be subscribed.

Base Station Comparison Matrix

The illustration below shows a Spectralink Base Station comparison matrix. In the comparison matrix you see the currently most used Spectralink base stations and the difference between them.

Only the Spectralink IP-DECT Base Station and the RFP6 Spectralink Digital DECT Base Station are in production. All other base stations seen here are no longer in production, but are still widely used in the field.

Note:

The Spectralink Digital DECT Base Stations are not relevant to the Spectralink IP-DECT/Virtual IP-DECT Server One.

Base station	KIRK IP base station 12	IP-DECT base station	DECT base station (RFP4)	DECT base station (RFP5)	DECT base station (RFP6)
Connector type	RJ45	RJ45	RJ11	RJ11	RJ45
10/100Mb RJ45 PoE *)	✓	✓			
Separate Power		✓			
Phantom powered over twisted pair			✓	✓	✓
Tx power	100/250 mW	100/250 mW	100/250 mW	100/250 mW	100/250 mW
Cable type	UTP CAT5	UTP CAT5	UTP CAT5	UTP CAT5	UTP CAT5
Cable length	100m/328ft	100m/328ft	2 km (1,2 mi)	2 km (1,2 mi)	2 km (1,2 mi)
IP-DECT Server support (6500 / 400)	✓	✓			
DECT Server support (8000 / 2500)	✓	✓	✓	✓	✓
Time slot structure	Full slot	Full slot	Blind slot (Odd/Even)	Blind slot (Odd/Even)	Full slot

Base station	KIRK base station 12	IP-DECT base station	DECT base station (RFP4)	DECT base station (RFP5)	DECT base station (RFP6)
Use with repeaters	✓	✓	✓	✓	✓
Ext. Antenna support		✓			✓
Speech channels	11	11	4	4	4 or 8 *)
Synchronization	Over the air	Over the air	Via cable	Via cable	Via cable
LAN synchronization		✓			
Administration	Browser via Server or directly	Browser via Server or directly	Browser via Server	Browser via Server	Browser via Server
Codec	G.726	G.726	G.726	G.726	G.726
Mounting	Vertically	N/A	Vertically	Vertically	N/A

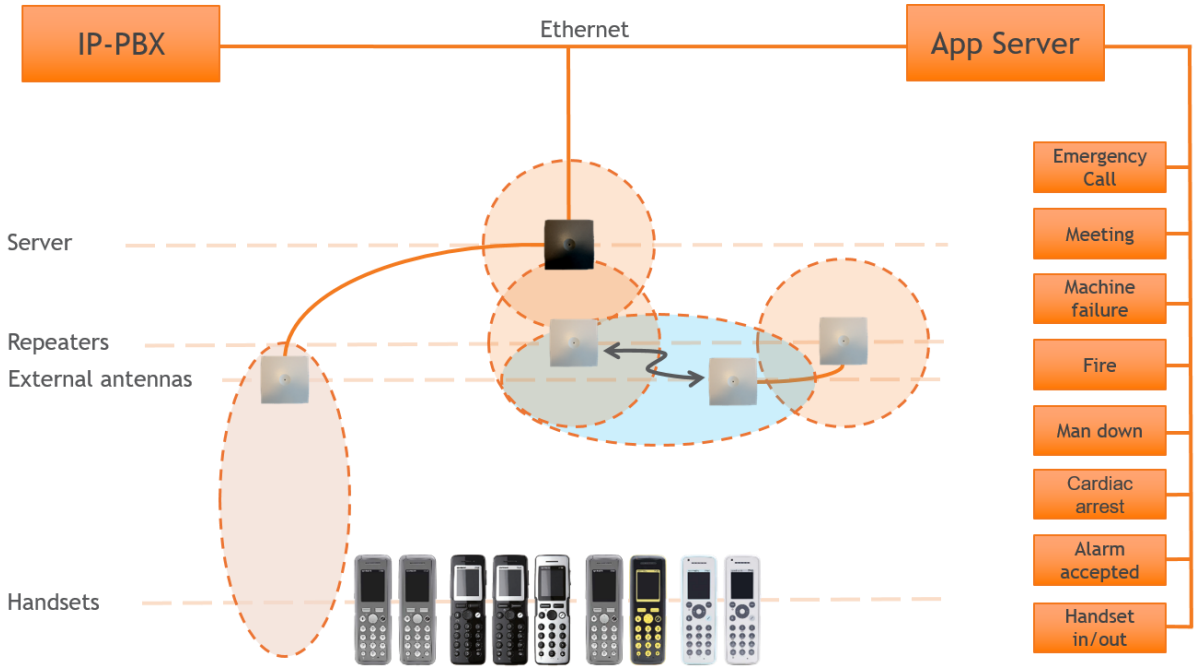
*) The Spectralink Digital DECT Base Station with 8 channels requires two sets of twisted pairs.

Note:

You can use LAN synchronization for Spectralink IP-DECT Base Station instead of Radio synchronization (Over The Air). This requires installation of a LAN Synchronization License.

Configuration Overview-Spectralink IP-DECT Server 200

The Spectralink IP-DECT Server 200 is typically configured as illustrated below:



The Spectralink IP-DECT Server 200 connects with Ethernet as well as the IP-PBX and third-party application server.

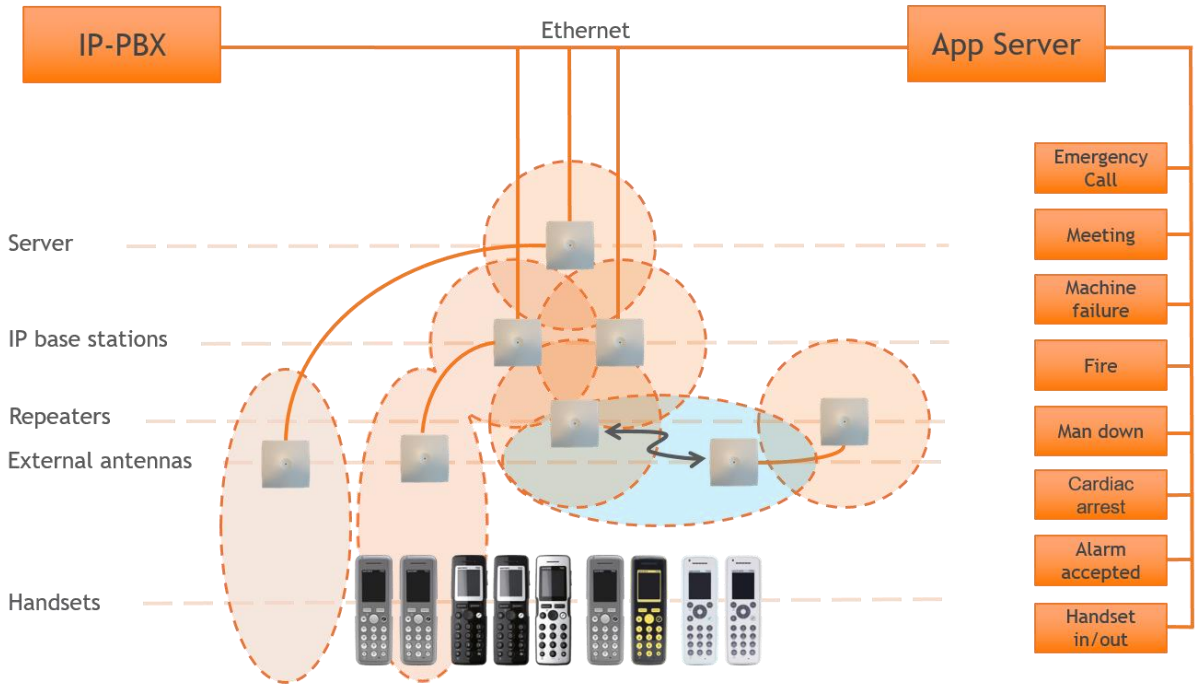
Optional wireless repeaters can be used to extend the coverage of the Spectralink IP-DECT Server 200. External directional antennas are also optional and can be used with the Spectralink IP-DECT Server 200 in physically complex environments which are challenging to cover with the built-in base station or repeaters.

External antennas can also be used to create long distance coverage to bridge two locations belonging to the same DECT system. Spectralink DECT Repeaters can make use of external antennas as well and create a link from a remote location to the main coverage area. There is no speech coverage in the linking area which is symbolized by the light blue color.

All Spectralink 7000 Handsets are supported. The Spectralink IP-DECT Server 200 itself connects with the LAN via the ethernet interface, and an optional third-party application can communicate over LAN with the Spectralink IP-DECT Server 200.

Configuration Overview-Spectralink IP-DECT Server 400

The Spectralink IP-DECT Server 400 is typically configured as illustrated below:



The Spectralink IP-DECT Server 400 connects with Ethernet as well as the IP-PBX and third-party application server. The optional Spectralink IP-DECT Base Stations are controlled by the Spectralink IP-DECT Server 400.

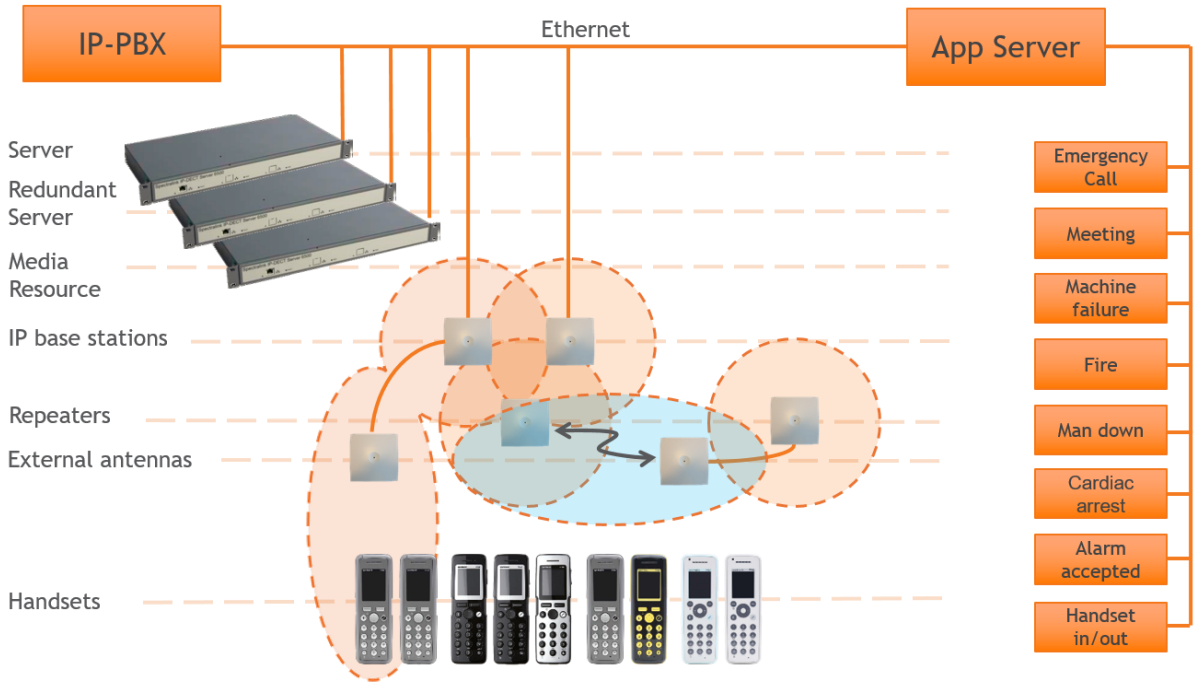
Optional wireless repeaters can be used to extend the coverage of the Spectralink IP-DECT Base Stations or the Spectralink IP-DECT Server 400 itself. External directional antennas are also optional and can be used with Spectralink IP-DECT Base Stations or the Spectralink IP-DECT Server 400 itself in physically complex environments which are challenging to cover with base stations or repeaters.

External antennas can also be used to create long distance coverage to bridge two locations belonging to the same DECT system. Spectralink DECT Repeaters can make use of external antennas as well and create a link from a remote location to the main coverage area. There is no speech coverage in the linking area which is symbolized by the light blue color.

All Spectralink 7000 Handsets are supported.

Configuration Overview-Spectralink IP-DECT Server 6500

The Spectralink IP-DECT Server 6500 is typically configured as illustrated below:



The Spectralink IP-DECT Base Stations connect with the Ethernet as well as the IP-PBX and third-party application server. The Spectralink IP-DECT Base Stations are controlled by the Spectralink IP-DECT Server 6500.

Optional wireless Spectralink DECT Repeaters can be used to extend the coverage of the Spectralink IP-DECT Base Stations. External antennas are also optional and can be used with Spectralink IP-DECT Base Stations in physically complex environments which are challenging to cover with base stations or repeaters.

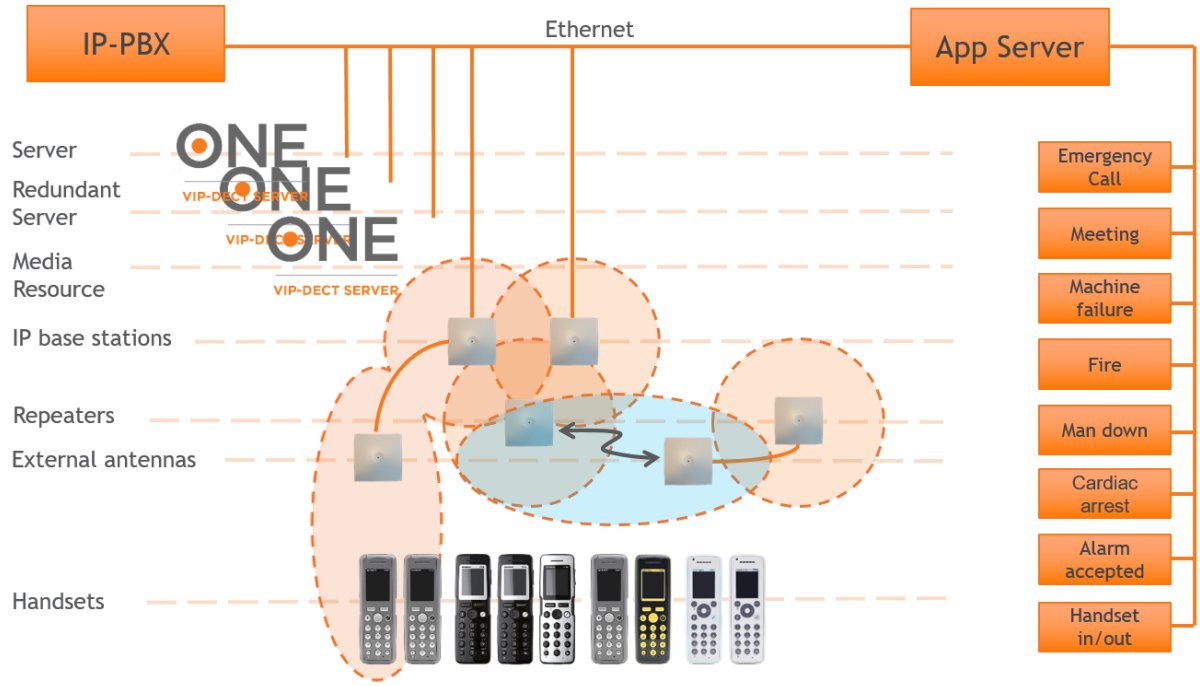
External antennas can also be used to create long distance coverage to bridge two locations belonging to the same DECT system. Spectralink DECT Repeaters can make use of external antennas as well and create a link from a remote location to the main coverage area. There is no speech coverage in the linking area which is symbolized by the light blue color.

All Spectralink 7000 Handsets are supported. The Spectralink IP-DECT Server 6500 itself connects with the LAN via the ethernet interface and an optional third-party application can communicate over LAN with the Spectralink IP-DECT Server 6500.

An optional Spectralink DECT Media Resource and Redundancy Spectralink IP-DECT Server 6500 can be added to the network in order to increase speech resources or share system load and maximize uptime.

Configuration Overview-Spectralink Virtual IP-DECT Server One

The Spectralink Virtual IP-DECT Server One is typically configured as illustrated below:



The Spectralink IP-DECT Base Stations connect with the Ethernet as well as the IP-PBX and third-party application server. The Spectralink IP-DECT Base Stations are controlled by the Spectralink Virtual IP-DECT Server One.

Optional wireless Spectralink DECT Repeaters can be used to extend the coverage of the Spectralink IP-DECT Base Stations. External antennas are also optional and can be used with Spectralink IP-DECT Base Stations in physically complex environments which are challenging to cover with base stations or repeaters.

External antennas can also be used to create long distance coverage to bridge two locations belonging to the same DECT system. Spectralink DECT Repeaters can make use of external antennas as well and create a link from a remote location to the main coverage area. There is no speech coverage in the linking area which is symbolized by the light blue color.

All Spectralink 7000 Handsets are supported. The Spectralink Virtual IP-DECT Server One itself connects with the LAN via the ethernet interface and an optional third-party application can communicate over LAN with the Spectralink Virtual IP-DECT Server One.

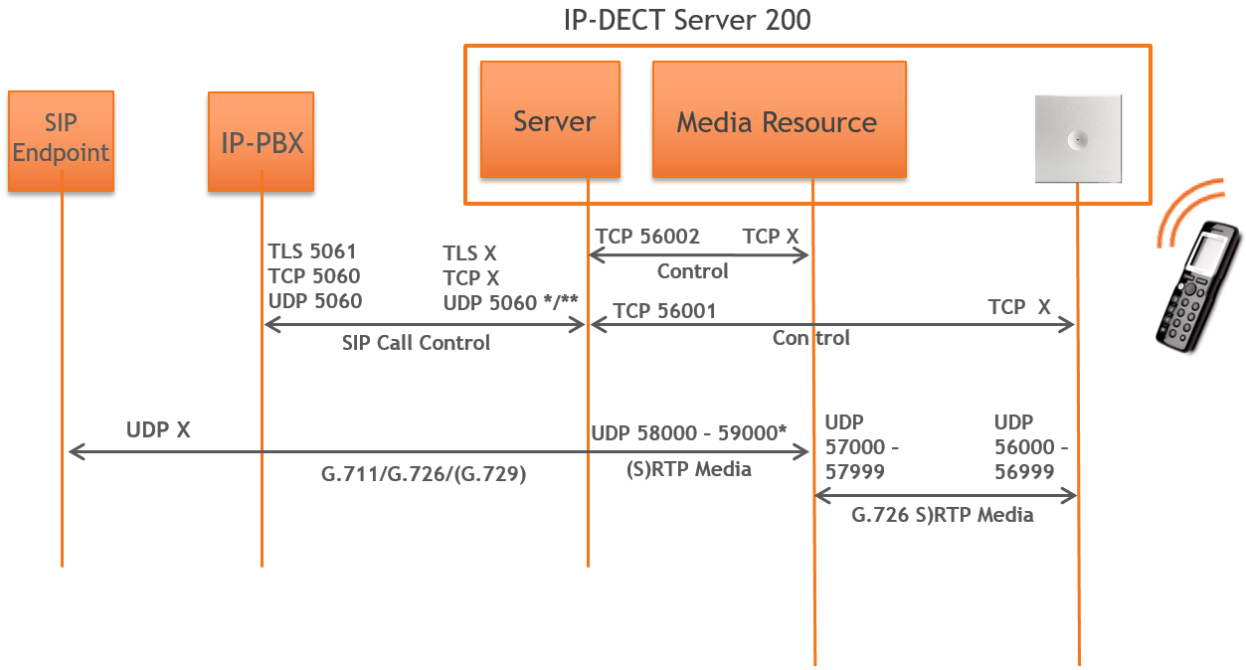
Optional Spectralink Virtual IP-DECT Media Resources (or optional Spectralink DECT Media Resources) and an optional Redundancy Spectralink Virtual IP-DECT Server One can be added to the network in order to increase speech resources or share system load and maximize uptime.

Communication Ports-Spectralink IP-DECT Server 200

The Spectralink IP-DECT Server utilizes a number of different protocols and ports on the network (see illustration below).

These ports MUST not be blocked by firewalls or other network equipment.

Example of protocols and ports for a Spectralink IP-DECT Server 200:



*) Default configurable

**) If SIP per port registration is checked = 5060 + X (Number of SIP Registrations)

Spectralink IP-DECT Server 200 system can utilize the following protocols: HTTP/HTTPS, FTP/TFTP, UPnP, MSF (TCP port 56003), syslog (UDP port 514), NTP, LDAP and SNMP.

Tip:

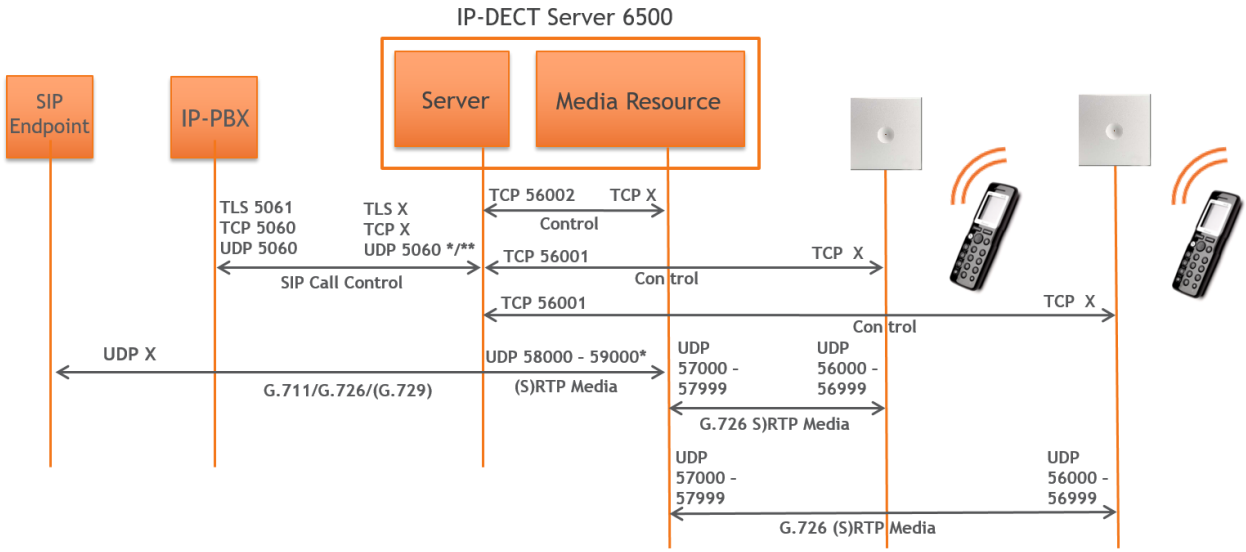
Use the communication port illustration as a reference when configuring your network for a Spectralink IP-DECT Server 200 solution.

Communication Ports-Spectralink IP-DECT Server 400/6500

The Spectralink IP-DECT Server utilizes a number of different protocols and ports on the network (see illustration below).

These ports MUST not be blocked by firewalls or other network equipment.

Example of protocols and ports for a Spectralink IP-DECT Server 6500:



*) Default configurable

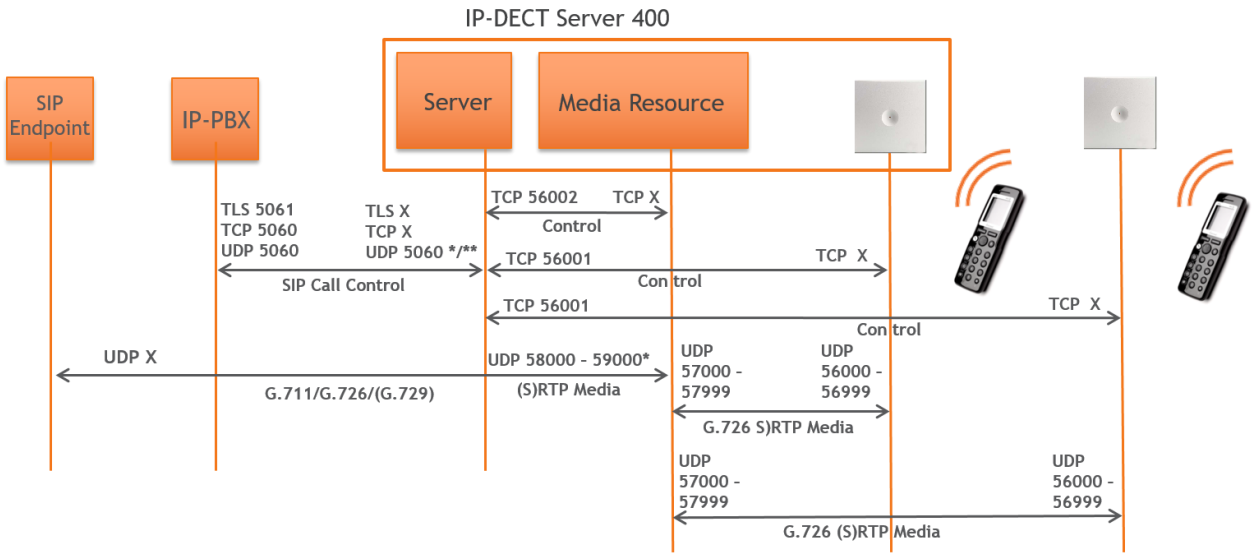
**) If SIP per port registration is checked = 5060 + X (Number of SIP Registrations)

Spectralink IP-DECT Server 6500 system can utilize the following protocols:HTTP/HTTPS, FTP/TFTP, UPnP, MSF (TCP port 56003), syslog (UDP port 514), NTP, LDAP and SNMP.

Tip:

Use the communication port illustration as a reference when configuring your network for a Spectralink IP-DECT Server 6500 solution.

Example of protocols and ports for a Spectralink IP-DECT Server 400:



*) Default configurable

**) If SIP per port registration is checked = 5060 + X (Number of SIP Registrations)

Spectralink IP-DECT Server 400 system can utilize the following protocols: HTTP/HTTPS, FTP/TFTP, UPnP, MSF (TCP port 56003), syslog (UDP port 514), NTP, LDAP and SNMP.

Tip:

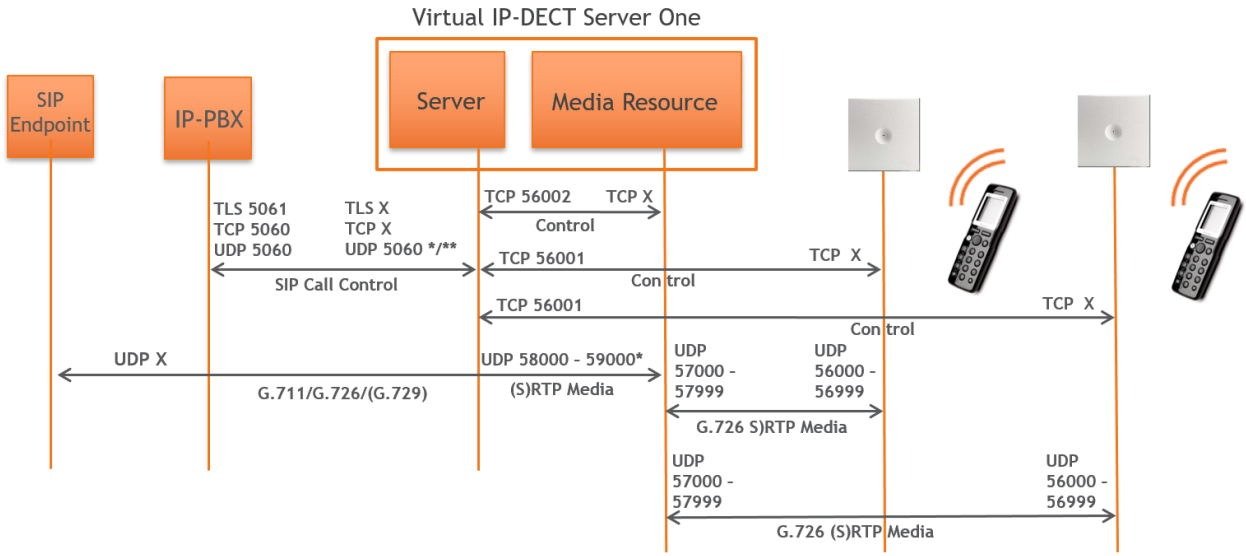
Use the communication port illustration as a reference when configuring your network for a Spectralink IP-DECT Server 400 solution.

Communication Ports-Spectralink Virtual IP-DECT Server One

The Spectralink IP-DECT Server utilizes a number of different protocols and ports on the network (see illustration below).

These ports MUST not be blocked by firewalls or other network equipment.

Example of protocols and ports for a Spectralink Virtual IP-DECT Server One:



*) Default configurable

**) If SIP per port registration is checked = 5060 + X (Number of SIP Registrations)

Spectralink IP-DECT Server 6500 system can utilize the following protocols: HTTP/HTTPS, FTP/TFTP, UPnP, MSF (TCP port 56003), syslog (UDP port 514), NTP, LDAP and SNMP.

Tip:

Use the communication port illustration as a reference when configuring your network for a Spectralink Virtual IP-DECT Server One solution.

Service Codes-Spectralink IP-DECT/Virtual IP-DECT Server One

You can access the Spectralink IP-DECT/Virtual IP-DECT Server One in operation using a handset.

Use any handset and enter ***999* followed by a 2-digit code for the information you wish to retrieve, and then press off-hook.

Access basic information such as:

- IP address - enter ***999*00
- MAC address - enter ***999*01 (not relevant to Spectralink Virtual IP-DECT Server One)
- Server firmware ***999*02

Note:

If UPnP is enabled, all Spectralink IP-DECT/Virtual IP-DECT Server One can be identified on the network by their serial number/UUID. For more information, see Discovering Spectralink IP-DECT/Virtual IP-DECT Components on the Network.

The serial number can be found on the label on every Spectralink IP-DECT/Virtual IP-DECT Server One. For more information, see Identifying ARI on Spectralink IP-DECT/Virtual IP-DECT Server One.

Chapter 4: Licenses

Licenses can be purchased to enable additional features on the Spectralink IP-DECT Server 200/400/6500 and Spectralink Virtual IP-DECT Server One. Some of the licenses are specific to the servers, some are common.

The following tables provide information about:

- Licenses for Spectralink IP-DECT Server 200
- Licenses for Spectralink IP-DECT Server 400/6500
- Licenses for Spectralink Virtual IP-DECT Server One

For more information about obtaining and loading licenses, see Ordering Licenses and Loading Licenses.

Licenses for Spectralink IP-DECT Server 200

Licenses	*Description*	*Server 200*
Lync/SfB + Security (TLS, SRTP) | IP-DECT Server 200 (14075511)	Allows for integration with Microsoft Skype for Business and additional features. Includes Software Security Package (TLS + SRTP). Note: The Software Security Package is not needed on servers running PCS 20A_ or newer as security from R1-2020 is available without license.	✓
Lync/SfB + Security (TLS, SRTP) 3 Users | IP-DECT Server 200 (14232830)	Allows for integration with Microsoft Skype for Business and additional features. Includes Software Security Package (TLS + SRTP). Allows for up to 3 users. Note: The Software Security Package is not needed on servers running PCS 20A_ or newer as security from R1-2020 is available without license.	✓
Security (TLS, SRTP) | IP-DECT Server 200 (14075281)	Enables SRTP (Secure Real-time Transport Protocol) and TLS. Note: This license is not needed on servers running PCS 20A_ or newer as security from R1-2020 is available without license.	✓
Software Assurance 1 Year 12 Users | IP-DECT Server 200 (14232800)	Allows for server and handset firmware update. Note: Required from Q4-2018 to be able to update firmware.	✓
Software Assurance 3 Years 12 Users | IP-DECT Server 200 (14232801)	Allows for server and handset firmware update. Note: Required from Q4-2018 to be able to update firmware.	✓
Software Assurance 5 Years 12 Users | IP-DECT Server 200 (14232842)	Allows for server and handset firmware update. Note: Required from Q4-2018 to be able to update firmware.	✓

Licenses	*Description*	*Server 200*
OAM-REST-API | IP-DECT Server 200 (14232835)	Allows for enabling of OAM REST API.	✓

Licenses for Spectralink IP-DECT Server 400/6500

Licenses	*Description*	*Server 400*	*Server 6500*
12 Channels + 24 Users | IPDECT Server 400 (14075500)	Allows for additional 24 users. Increases the number of channels in air enabled from 6 to 12.	✓	-
12 Channels + 24 Users + Multi-cell | IP-DECT Server 400 (14075560)	Allows: Additional 24 users. Up to 9 additional base stations. Increases the number of channels in air enabled from 6 to 12.	✓	-
Multi-cell, Max voice channels, 48 Users | IP-DECT Server 400 (14232839)	Allows: Additional 48 users Up to 9 additional base stations. Increase the number of media channels from 6 to 24.	✓	-
Lync/SfB + Security (TLS, SRTP) | IP-DECT Server 400 (14075510)	Allows for up to 12 users and 6 media channels in air. Includes Software Security Package (TLS + SRTP). **Note**: The Software Security Package is not needed on servers running PCS 20A_ or newer as security from R1-2020 is available without license.	✓	-
Lync/SfB + Security (TLS, SRTP) 6 Users | IP-DECT Server 400 (14232838)	Allows for integration with Microsoft Skype for Business and additional features. Includes Software Security Package (TLS + SRTP). Allows for additional 6 users. **Note**: The Software Security Package is not needed on servers running PCS 20A_ or newer as security from R1-2020 is available without license.	✓	-
Multi-cell | IP-DECT Server 400 (14075520)	Allows: Up to 9 additional base stations. Increases the number of channels in air enabled from 6 to 12.	✓	-
LAN Sync | IP-DECT Server 400 (14075600)	Allows base stations to be synchronized over LAN.	✓	-

Licenses	*Description*	*Server 400*	*Server 6500*
Cisco Unified CM (Advanced Features) | IP-DECT Server 400 (14075490)	Allows for tighter integration with the Cisco Unified Communications Manager and additional features.	✓	-
CTI | IP-DECT Server 400 (14232868)	Allows for Computer Telephony Integration (CTI) when having the Cisco Unified CM (Advanced Features) | IPDECT Server 400 license installed as well.	✓	-
Lync/SfB + Security (TLS, SRTP) | IP-DECT Server 6000/6500 (14075270)	Allows for integration with Microsoft Skype for Business and additional features. Includes Software Security Package (TLS + SRTP). **Note**: The Software Security Package is not needed on servers running PCS 20A_ or newer as security from R1-2020 is available without license.	-	✓
LAN Sync | IP-DECT Server 6500 (14075610)	Allows base stations to be synchronized over LAN.	-	✓
Security (TLS, SRTP) | IPDECT/DECT Servers 400/6000/6500/2500/8000 (14075280)	Enables SRTP (Secure Realtime Transport Protocol) and TLS. **Note**: This license is not needed on servers running PCS 20A_ or newer as security from R1-2020 is available without license.	✓	✓
Handset Sharing | IPDECT/DECT Servers 400/6500/2500/8000 (14075460)	Allows handsets to be shared among numbers and vice versa.	✓	✓
Frequency Swap | IPDECT/DECT Servers 400/6500/2500/8000 (14075620)	Allows the active radio frequency to be changed in accordance to geographical locations. **Note**: Besides the Frequency Swap License, a special Spectralink DECT Handset 7212 (part no. 02610004) with a special configuration (and compliance to be compatible with frequency swap) is also required.	✓	✓
Cisco Unified CM (Advanced Features) | IP-DECT Server 6500 (14075495)	Allows for tighter integration with the Cisco Unified Communications Manager and additional features.	-	✓
CTI | IP-DECT Server 6500 (14232869)	Allows for Computer Telephony Integration (CTI) when having the Cisco Unified CM (Advanced Features) | IPDECT Server 6500 license installed as well.	-	✓

Licenses	*Description*	*Server 400*	*Server 6500*
Automatic Alarm Call | IP-DECT/DECT Servers 300/400/2500/6000/6500/8000 (14075450)	Allows the use of alarm key, with tear-off and/or motion sensors. The Automatic Alarm Call license can trigger an alarm. There are 4 alarm triggers available depending on the type of Spectralink DECT Handset being used: ○ man down ○ running ○ tear-off ○ alarm button	✓	✓
Redundancy Backup | IPDECT Server 6000/6500 (14075260)	Allows adding a backup server to a system.	-	✓
Redundancy Master | IP-DECT Server 6000/6500 (14075250)	Allows adding a backup server to a system.	-	✓
150 Users | IP-DECT Server 6000/6500 (14075210)	Allows for up to 150 users.	-	✓
500 Users | IP-DECT Server 6000/6500 (14075220)	Allows for up to 500 users.	-	✓
1500 Users | IP-DECT Server 6000/6500 (14075230)	Allows for up to 1500 users.	-	✓
4096 Users | IP-DECT Server 6000/6500 (14075240)	Allows for up to 4096 users. **Note**: Skype for Business only supports up to 1500 users.	-	✓
Lync/SfB + Security (TLS, SRTP) | IP-DECT Server 6000/6500 (14075270)	Allows for integration with Microsoft Skype for Business and additional features. Includes Software Security Package (TLS + SRTP). **Note**: The Software Security Package is not needed on servers running PCS 20A_ or newer as security from R1-2020 is available without license.	-	✓
Enhanced Provisioning | IP-DECT Server 400 (14075701)	Allows for provisioning of firmware for: ○ IP-DECT base stations ○ Handsets Allows for provisioning of Handset Configuration.	✓	-

Licenses	*Description*	*Server 400*	*Server 6500*
Enhanced Provisioning | IP-DECT Server 6500 (14075700)	Allows for provisioning of firmware for: ○ IP-DECT base stations ○ Media resources ○ Handsets Allows for provisioning of Handset Configuration.	-	✓
Software Assurance 1 Year 12 Users | IP-DECT Server 400 (14232802)	Allows for base station, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	✓	-
Software Assurance 3 Years 12 Users | IP-DECT Server 400 (14232803)	Allows for base station, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	✓	-
Software Assurance 5 Years 12 Users | IP-DECT Server 400 (14232843)	Allows for base station, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	✓	-
Software Assurance 1 Year 24 Users | IP-DECT Server 400 (14232804)	Allows for base station, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	✓	-
Software Assurance 3 Years 24 Users | IP-DECT Server 400 (14232805)	Allows for base station, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	✓	-
Software Assurance 5 Years 24 Users | IP-DECT Server 400 (14232844)	Allows for base station, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	✓	-
Software Assurance 1 Year 60 Users | IP-DECT Server 400 (14232840)	Allows for base station, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	✓	-
Software Assurance 3 Year 60 Users | IP-DECT Server 400 (14232841)	Allows for base station, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	✓	-
Software Assurance 5 Year 60 Users | IP-DECT Server 400 (14232845)	Allows for base station, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	✓	-
Software Assurance 1 Year 30 Users | IP-DECT Server 6500 (14232806)	Allows for base station, media resource, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	-	✓
Software Assurance 3 Years 30 Users | IP-DECT Server 6500 (14232807)	Allows for base station, media resource, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	-	✓

Licenses	*Description*	*Server 400*	*Server 6500*
Software Assurance 5 Years 30 Users | IP-DECT Server 6500 (14232846)	Allows for base station, media resource, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	-	✓
Software Assurance 1 Year 150 Users | IP-DECT Server 6500 (14232808)	Allows for base station, media resource, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	-	✓
Software Assurance 3 Years 150 Users | IP-DECT Server 6500 (14232809)	Allows for base station, media resource, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	-	✓
Software Assurance 5 Years 150 Users | IP-DECT Server 6500 (14232847)	Allows for base station, media resource, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	-	✓
Software Assurance 1 Year 500 Users | IP-DECT Server 6500 (14232810)	Allows for base station, media resource, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	-	✓
Software Assurance 3 Years 500 Users | IP-DECT Server 6500 (14232811)	Allows for base station, media resource, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	-	✓
Software Assurance 5 Years 500 Users | IP-DECT Server 6500 (14232848)	Allows for base station, media resource, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	-	✓
Software Assurance 1 Year 1500 Users | IP-DECT Server 6500 (14232812)	Allows for base station, media resource, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	-	✓
Software Assurance 3 Years 1500 Users | IP-DECT Server 6500 (14232813)	Allows for base station, media resource, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	-	✓
Software Assurance 5 Years 1500 Users | IP-DECT Server 6500 (14232849)	Allows for base station, media resource, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	-	✓
Software Assurance 1 Year MAX Users | IP-DECT Server 6500 (14232814)	Allows for base station, media resource, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	-	✓

Licenses	*Description*	*Server 400*	*Server 6500*
Software Assurance 3 Years MAX Users | IP-DECT Server 6500 (14232815)	Allows for base station, media resource, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	-	✓
Software Assurance 5 Years MAX Users | IP-DECT Server 6500 (14232850)	Allows for base station, media resource, server and handset firmware update. **Note**: Required from Q4-2018 to be able to update firmware.	-	✓
OAM-REST-API | IP-DECT Server 400 (14232836)	Allows for enabling of OAM REST API.	✓	-
OAM-REST-API | IP-DECT Server 6500 (14232837)	Allows for enabling of OAM REST API.	-	✓

Licenses for Spectralink Virtual IP-DECT Server One

Licenses	*Description*	*Virtual Server*
Mandatory Base Licence ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One (14233244)	Allows for multi-cell ARI and basic capacity.	✓
30 Users | Virtual IP-DECT Server One (14233200)	Allows for up to 30 users.	✓
150 Users | Virtual IP-DECT Server One (14233201)	Allows for up to 150 users.	✓
500 Users | Virtual IP-DECT Server One (14233202)	Allows for up to 500 users.	✓
1500 Users | Virtual IP-DECT Server One (14233203)	Allows for up to 1500 users.	✓
4096 Users | Virtual IP-DECT Server One (14233204)	Allows for up to 4096 users. Note: Skype for Business only supports up to 1500 users.	✓
Lync/SfB 1 Year | Virtual IP-DECT Server One (14233252)	Allows for integration with Microsoft Skype for Business and additional features.	✓
Handset Sharing 1 Year | Virtual IP-DECT Server One (14233253)	Allows handsets to be shared among numbers and vice versa.	✓
Enhanced Provisioning 1 Year | Virtual IP-DECT Server One (14233250)	Allows for provisioning of firmware for: ○ IP-DECT base stations ○ Media resources ○ Handsets Allows for provisioning of Handset Configuration.	✓
OAM-REST-API 1 Year | Virtual IP-DECT Server One (14233249)	Allows for enabling of OAM REST API.	✓

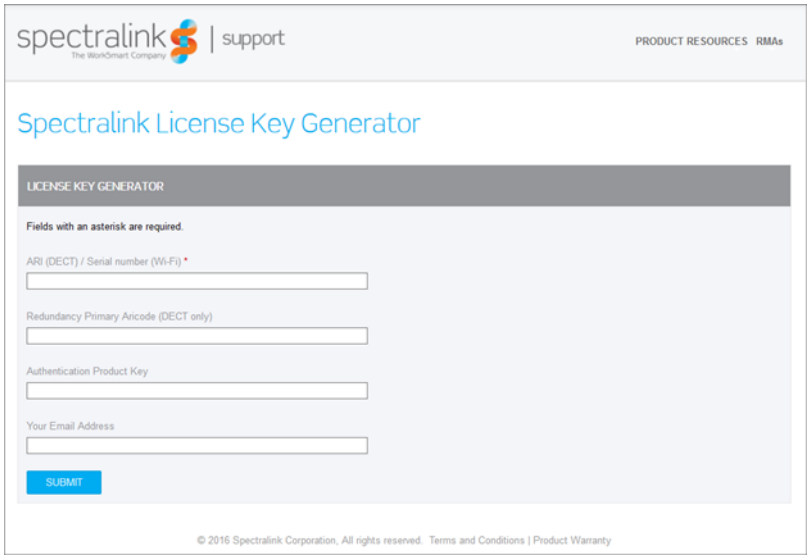
Licenses	*Description*	*Virtual Server*
Frequency Swap | Virtual IP-DECT Server One (14233248)	Allows the active radio frequency to be changed in accordance with geographical locations. **Note**: Besides the Frequency Swap License, a special Spectralink DECT Handset 7212 (part no. 02610004) with a special configuration (and compliance to be compatible with frequency swap) is also required.	✓
COTA | VIP-DECT Server One 14233242:	Allows for Handset Configuration Over The Air	✓
Enhanced Provisioning | Virtual IP-DECT Server One 14233254 :	Allows for provisioning of firmware for: IP-DECT base stations ○ Media resources ○ Handsets ○ Allows for provisioning of Handset Configuration.	✓
Cisco Unified CM Advanced Features | Virtual IP-DECT Server One 14233255	Allows for tighter integration with the Cisco Unified Communications Manager and additional features.	✓
Lync/SfB | Virtual IP-DECT Server One 4233256	Allows for integration with Microsoft Skype for Business and additional features.	✓
Handset Sharing | Virtual IP-DECT Server One 14233257	Allows handsets to be shared among numbers and vice versa.	✓
Automatic Alarm Call | Virtual IP-DECT Server One 14233269	Allows the use of alarm key, with tear-off and/or motion sensors. The Automatic Alarm Call license can trigger an alarm. There are 4 alarm triggers available depending on the type of Spectralink DECT Handset being used: ○ man down ○ running ○ tear-off ○ alarm button	✓
Redundancy Master | Virtual IP-DECT Server One (14233246)	Allows adding a backup server to a system.	✓
Redundancy Backup | Virtual IP-DECT Server One (14233247)	Allows adding a backup server to a system.	✓
LAN Sync | Virtual IP-DECT Server One (14233245)	Allows base stations to be synchronized over LAN.	✓
32 Media Channels | Virtual IP-DECT Server One (14233270)	Allows for additional 32 media resource channels.	✓
16 Base Stations | Virtual IP-DECT Server One (14233233)	Allows for additional 16 base stations.	✓
64 Base Stations | Virtual IP-DECT Server One (14233234)	Allows for additional 64 base stations.	✓

Licenses	*Description*	*Virtual Server*
256 Base Stations | Virtual IP-DECT Server One (14233235)	Allows for additional 256 base stations.	✓
1024 Base Stations | Virtual IP-DECT Server One (14233236)	Allows for additional 1024 base stations.	✓
Software Assurance 1 Year 30 Users | Virtual IP-DECT Server One (14233211)	Allows for server and handset firmware update.	✓
Software Assurance 3 Years 30 Users | Virtual IP-DECT Server One (14233212)	Allows for server and handset firmware update.	✓
Software Assurance 1 Year 150 Users | Virtual IP-DECT Server One (14233213)	Allows for server and handset firmware update.	✓
Software Assurance 3 Years 150 Users | Virtual IP-DECT Server One (14233214)	Allows for server and handset firmware update.	✓
Software Assurance 1 Year 500 Users | Virtual IP-DECT Server One (14233215)	Allows for server and handset firmware update.	✓
Software Assurance 3 Years 500 Users | Virtual IP-DECT Server One (14233216)	Allows for server and handset firmware update.	✓
Software Assurance 1 Year 1500 Users | Virtual IP-DECT Server One (14233217)	Allows for server and handset firmware update.	✓
Software Assurance 3 Years 1500 Users | Virtual IP-DECT Server One (14233218)	Allows for server and handset firmware update.	✓
Software Assurance 1 Year 4096 Users | Virtual IP-DECT Server One (14233219)	Allows for server and handset firmware update.	✓
Software Assurance 3 Years 4096 Users | Virtual IP-DECT Server One (14233220)	Allows for server and handset firmware update.	✓

Ordering Licenses

To Order Licenses for Spectralink IP-DECT Servers

1. Send your Purchase Order (PO) including the software part number and the number of licenses needed to Spectralink Order Management via (EMEA and APAC) **emeaom@spectralink.com** or (NALA) **nalaom@spectralink.com** .
2. When your order is processed, Order Management will send you an email including an Authentication Product Key for your software license.
3. To activate your software license, use the License Key Generator available at **http://support.spectralink.com/keycode** .



Note:

Once a software license is generated, this is locked to the specified ARI code, and cannot be changed.

To Order Licenses for Spectralink Virtual IP-DECT Server One

1. Send your Purchase Order (PO) including the Server ID (UUID) and the number of licenses needed to Spectralink Order Management via (EMEA and APAC) **emeaom@spectralink.com** or (NALA) **nalaom@spectralink.com** .
2. When your order is processed, Order Management will send you an email including a license key for the relevant software license.

Loading Licenses

1. Click **Administration**, and then click **License**.
2. Copy the provided license key from your email, paste it in the License field, and then click **Load**.
3. Reboot the server to activate the license.

Loaded licenses can be seen on the web-based Administration Page> **Administration**> **Licenses**> **Loaded licenses**.

For information about deleting a license and retrieving a license being deleted by mistake, see Deleting Licenses.

Chapter 5: Installation Requirements

Safety and Handling information is available online at **http://support.spectralink.com/products**.

All Spectralink documents are available at **http://support.spectralink.com/products**.

Requirements for Spectralink IP-DECT Server 200/400

The Spectralink IP-DECT Server 200/400 is a combined Spectralink IP-DECT Base Station and server.

For more information about requirements, see Requirements for Spectralink IP-DECT Base Station and Spectralink DECT Repeater.

Requirements for Spectralink IP-DECT Server 6500 and Spectralink DECT Media Resource

Environmental Requirements

The installation area must:

- be clean, free of traffic and excess dust, dry, and well ventilated
- be within the temperature ranges of 10°C and 40°C/50°F and 104°F
- be between 20% and 80% non-condensing relative humidity

Note:

The installation area must be of sufficient height from the floor to prevent water damage. 1U rack space in a 19" cabinet or respective space on the wall when mounting the Spectralink IP-DECT Server 6500 in vertical position on a wall.

For more information about installing the Spectralink IP-DECT Server 6500 and Spectralink DECT Media Resource, see Installing Spectralink IP-DECT Server 6500 and Spectralink DECT Media Resource.

Requirements for Spectralink Virtual IP-DECT Server One and Spectralink Virtual IP-DECT Media Resource

Software Requirements

The following is required to run the Spectralink Virtual IP-DECT Server One/Spectralink Virtual IP-DECT Media Resource:

- OS: Windows 10 or newer
- VMware ESXi 6.5+ host
- 1 GB memory
- 16 GB disk (can be thinly provisioned)
- 1 GHz CPU
- Intel Sandy Bridge or newer CPU architecture

For more information about deploying the Spectralink Virtual IP-DECT Server One and Spectralink Virtual IP-DECT Media Resource, see Deploying Spectralink Virtual IP-DECT Server One and Spectralink Virtual IP-DECT Media Resource on VMware ESXi.

Requirements for Spectralink IP-DECT Base Station and Spectralink DECT Repeater

Note:

The Spectralink IP-DECT Server 200/400 is a combined Spectralink IP-DECT Base Station and server. Therefore, the below mentioned requirements also apply to the Spectralink IP-DECT Server 200/400.

Environmental Requirements

- Do not install a device near metal objects and steel constructions.
- Do not position devices in ducts, plenums or hollow spaces used to transport environmental air except where the duct, plenum or hollow space is created by a suspended ceiling having lay-in panels.
- Do not position devices behind furniture.
- The installation area must be clean, free of traffic and excess dust, dry, and well ventilated.
- The installation area must be within the temperature ranges of 10°C and 40°C/50°F and 104°F.
- The installation area must be between 20% and 80% non-condensing relative humidity.
- For best RF coverage, the device must be mounted vertically on walls.

Power Requirements

The Spectralink IP-DECT Base Station uses:

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

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

Use an 8V-DC power supply when using a port without PoE.

For more information about installing the Spectralink IP-DECT Base Station and Spectralink DECT Repeater, see Installing Spectralink IP-DECT Base Station and Installing Spectralink DECT Repeater.

Note:

For more information about installing the Spectralink IP-DECT Server 200, see Installing Spectralink IP-DECT Server 200.

For more information about installing the Spectralink IP-DECT Server 400, see Installing Spectralink IP-DECT Server 400 and Installing Spectralink IP-DECT Base Station.

Requirements for Spectralink DECT Handset

For more information about the handset, refer to the user guide available online at **http://support.spectralink.com/products**.

Requirements for Handset and Repeater Management Tool

Software Requirements

The following is required to run the Handset and Repeater Management Tool:

- OS: Windows 10 or newer

Chapter 6: Installation Prerequisites

Note:

Ensure that a site survey and deployment have been conducted and that the installer has access to these plans before proceeding any further. For more information about deployment, see the Synchronization and Deployment Guide for the Spectralink IP-DECT Server 400/6500/Spectralink Virtual IP-DECT Server One or the IP-DECT Server 200 Deployment and Installation Guide depending on your installation.

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

- ARI for the Spectralink IP-DECT/Virtual IP-DECT Server One:

  For more information, see Identifying ARI on Spectralink IP-DECT/Virtual IP-DECT Server One.

- Serial numbers for handsets:

  For more information, see Identifying IPEI on Spectralink Handset.

- AC (Authentication Codes):

  The AC is a customer-defined optional subscription pin code of a maximum of eight digits for the individual handset. The AC can be used when connecting the handset to the server.

- Repeaters:

  Mark each repeater with the number of the related base station (or Spectralink IP-DECT Server 200/400). This way you can easily configure the system on site.

- Handsets:

  To use the handsets, you must first install the radio infrastructure, e.g. base stations and repeaters to transmit and receive radio signals to and from the handsets. There are no direct connections between the handset and the system.

- Charging battery:

  When charging the handset battery for the first time, leave the handset in the charger for 14 to 16 hours to ensure that the battery is fully charged and the handset ready for use. For more information about the handset, refer to the user guide available online at http://support.spectralink.com/products.

Chapter 7: About ARI and IPEI Identification

All Spectralink DECT Handsets and all Spectralink IP-DECT/Virtual IP-DECT Server One have unique identification numbers.

This is needed in order for:

- The handsets to know which Spectralink IP-DECT/Virtual IP-DECT Server One installation they belong to.
- The Spectralink IP-DECT/Virtual IP-DECT Server One to know which handsets that are subscribed to it.

A handset uses an International Portable Equipment Identifier, also called IPEI number, for handset identification and subscription to a Spectralink IP-DECT/Virtual IP-DECT Server One.

A Spectralink IP-DECT/Virtual IP-DECT Server One uses an Access Right Identity number, also called ARI number, for server identification.

When an IPEI number of a handset is linked to a Spectralink IP-DECT/Virtual IP-DECT Server One, the handset is subscribed. There is a record in the Spectralink IP-DECT/Virtual IP-DECT Server One holding information about all the handsets being subscribed to it. This record is subdivided into User profiles, often referred to as just a User. Each User must hold information about extension number, the handset's IPEI number, and its registration credentials for the PBX. This information is used to link the subscribed handset to the PBX which is the same as a line registration. A Users profile holds subscription data and registration data. For more information, see Registering Users and Subscribing Spectralink DECT Handsets.

Identifying IPEI on Spectralink Handset

You can identify the unique IPEI number on a handset in two ways:

- From the handset: **Menu**> **Status**> **General**
- From label by removing the battery cover and battery

For more information about the handset, refer to the user guide available online at **http://support.spectralink.com/products**.

Identifying ARI on Spectralink IP-DECT/Virtual IP-DECT Server One

You can identify the unique ARI number on the server in the following ways:

- Spectralink IP-DECT Server 6500: See label on the bottom of the server.

- Spectralink IP-DECT Server 200/400: See label on the rear side of the server.
- Spectralink IP-DECT Server 200/400/6500 and Spectralink Virtual IP-DECT Server One: From the web-based Administration Page> **Status**> **Wireless Server**.

Note:

The Spectralink Virtual IP-DECT Server One runs in demo mode with a residential ARI until a Mandatory Base License ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License is installed.

The Mandatory Base License ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License contains the ARI, that must be used for further deployment of the Spectralink Virtual IP-DECT Server One solution.

Chapter 8: Installing Spectralink IP-DECT Server 200

Below you will find information about installing the server.

Note:

Before you install the equipment, ensure that a site planner defines the location of the server.

Before you begin the installation, determine the position of the server for best coverage. The average coverage within buildings is 75 meters/245 feet.

The coverage depends on the construction of the building, architecture, and the choice of building materials.

Power Requirements for the Spectralink IP-DECT Server 200

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

Use a standard PoE adapter or a PoE-enabled port on an ethernet switch adhering to PoE 802.3af when connecting the Spectralink IP-DECT Server 200 to a PoE power source.

Use an 8V-DC power supply when using a port without PoE.

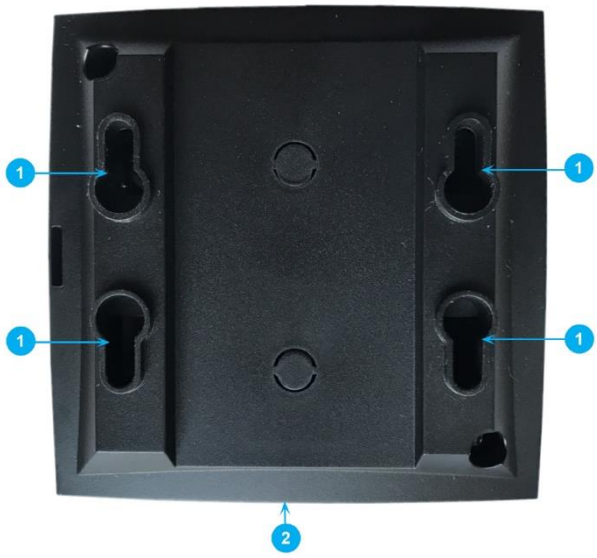
Spectralink IP-DECT Server 200 Appearance and Components

Below you will find a description of the Spectralink IP-DECT Server 200 appearance and components:

Spectralink IP-DECT Server200 – bottom

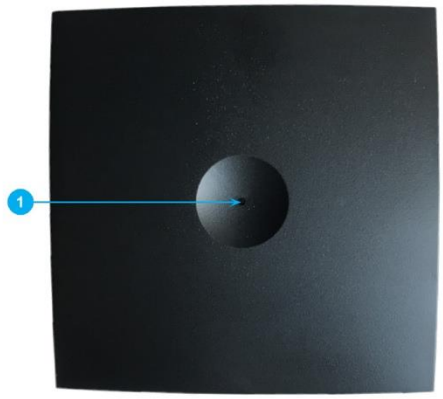
1. Reset button
2. DC
3. LINK/Activity Indicator
4. ETH port (power supply by PoE)

Spectralink IP-DECT Server200 – rear



1. Holes for wall mounted screws
2. Connection to LAN

Spectralink IP-DECT Server 200 – front



1. LED

Spectralink IP-DECT Server 200 LED Indicators

Below you will find information about LED indicators on the server.

Front Cover

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

LED Indicator	*Meaning*
Steady green	OK and idle.
Slow green flashing	OK and active voice call.
Fast green flashing	Busy (all channels are in use).
Steady red	Reset/shutdown in progress.
Steady red for 5 seconds followed by fast red flashing	Reset to factory settings.
Red flashing	Error or rebooting

LAN Port on Face Plate

LED Indicator	*Meaning*
LINK Indicator - yellow	Link layer software has established connection.
LINK Indicator - green flashing	Activity

Spectralink IP-DECT Server 200 Reset Button

You can restart or reset the Spectralink IP-DECT Server 200 by pressing the Reset button on the bottom of face plate of the server.

The following table contains a description of the different actions that take place when pressing the Reset button.

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

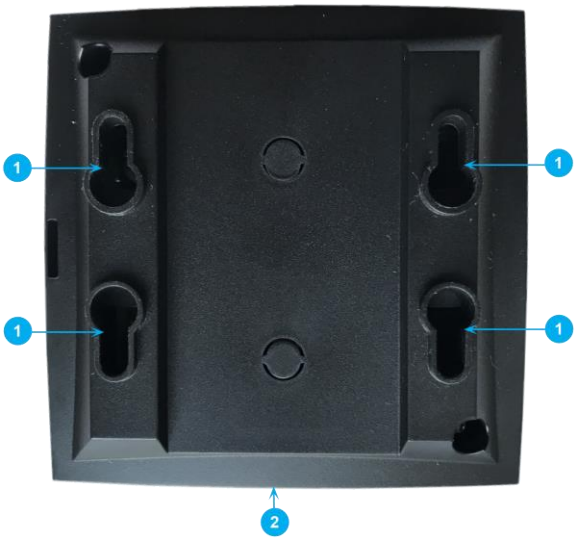
Wall-Mount and Power on the Spectralink IP-DECT Server 200

For best RF coverage, the Spectralink IP-DECT Server 200 must be mounted vertically on walls.

1 Mount the Spectralink IP-DECT Server 200 on the wall using the anchors and screws accompanying the product. For more information, see Measurements and Mounting Template.

Note:

When you place the Spectralink IP-DECT Server 200 on the screws, ensure that the screws do not touch the printed circuit board.



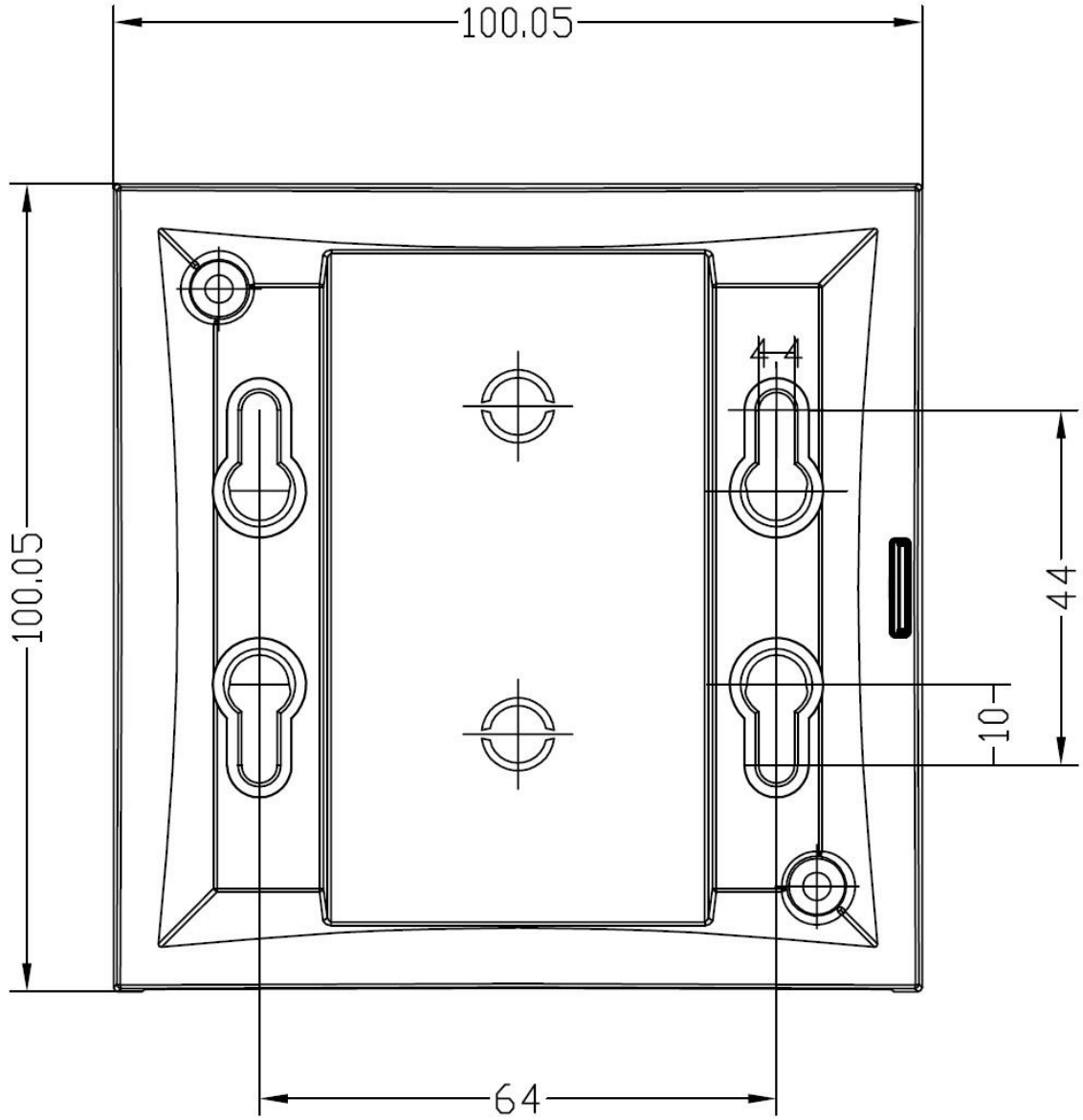
1. Holes for wall mounted screws
2. RJ45 port

2 Connect the RJ45 plug to the ethernet connector at the bottom of the Spectralink IP-DECT Server 200.

3 After installing the Spectralink IP-DECT Server 200 you need to power it up.

Measurements and Mounting Template

Measurements in Millimeters



Mounting Template

Note:

For correct measurement, ensure that this page is printed as either **Actual size** or **Scale 100 %** (**Print** dialog box) on an A4 size paper before using the mounting template below.


64 mm

Chapter 9: Installing Spectralink IP-DECT Server 400

The Spectralink IP-DECT Server 400 is a combined Spectralink IP-DECT Base Station and server.

For more information about appearance and components, Reset Button and mounting, see Installing Spectralink IP-DECT Base Station.

Note:

Before you install the equipment, ensure that a site planner defines the locations of the server.

Chapter 10: Installing Spectralink IP-DECT Server 6500 and Spectralink DECT Media Resource

Below you will find information about the appearance and components of the:

- Spectralink IP-DECT Server 6500/Spectralink DECT Media Resource

The section also provides information about resetting the Spectralink IP-DECT Server/Spectralink DECT Media Resource hardware using the Reset button.

Note:

The installation of a Spectralink DECT Media Resource with the Spectralink IP-DECT Server 6500 is optional. Installation of a media resource will increase the number of simultaneous voice calls supported by a stand-alone server.

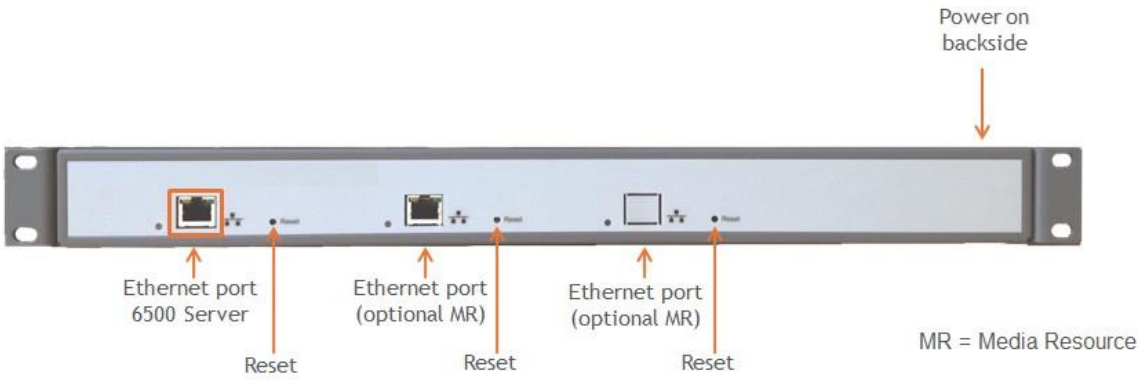
The Spectralink IP-DECT Server 6500 comes with one built-in media resource.

Note:

Before you install the equipment, ensure that a site planner defines the locations of the Spectralink IP-DECT Server 6500 and Spectralink DECT Media Resources.

Server Appearance and Components

Below you will find a description of the Spectralink IP-DECT Server 6500 appearance and components:



Spectralink IP-DECT Server 6500 and Media Resource LED Indicators

Below you will find information about LED indicators on the Spectralink IP-DECT Server 6500 and Spectralink DECT Media Resource.

Front Faceplate

The Spectralink IP-DECT Server 6500/Spectralink DECT Media Resource front cover has one indicator describing the faults and failures of the device. The indicator is off when the Spectralink IP- DECT Server 6500/Spectralink DECT Media Resource is not powered. The LED flashes when the Spectralink IP-DECT Server 6500/Spectralink DECT Media Resource initializes. The indicator is on when the Spectralink IP-DECT Server 6500/Spectralink DECT Media Resource is operating.

LED Indicator	Meaning
Steady green	OK and idle.
Slow green flashing	OK and active voice call.
Fast green flashing	Active, in operation with the maximum active connections (busy).
Slow red flashing	Missing media resource or base station (if it is a media resource: missing connection to Spectralink IP-DECT Server 6500).
Fast red flashing	Error
Steady red	Reset/shutdown in progress.
Steady red for 5 seconds followed by fast red flashing	Reset to factory settings.

Front LAN Port

LED Indicator	*Meaning*
LINK Indicator - yellow	Link layer software has established connection.
LINK Indicator - green flashing	Activity

Spectralink IP-DECT Server 6500 and Media Resource Reset Button

You can restart or reset the Spectralink IP-DECT Server 6500/Spectralink DECT Media Resource by pressing the Reset button on the front of the server/media resource.

Resetting or Restarting the Spectralink IP-DECT Server and Spectralink DECT Media Resource

Below you will find information about Reset button actions that can take place when you press the Reset button.

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

Mounting in a Rack

The Spectralink IP-DECT Server 6500/Spectralink DECT Media Resource is mountable in a rack.

1 Mount the two wings with the screws. If you are mounting the Spectralink IP-DECT Server 6500 on a wall, twist the wings 90° degrees.

2 Mount the cabinet in the 19" rack or on the wall.

Note:

Screws and nuts/rawl plugs are not supplied.

3 Connect the RJ45 ethernet plug to the front of the cabinet.

All Spectralink IP-DECT Server 6500s and Spectralink DECT Media Resources must be connected to a switch port.

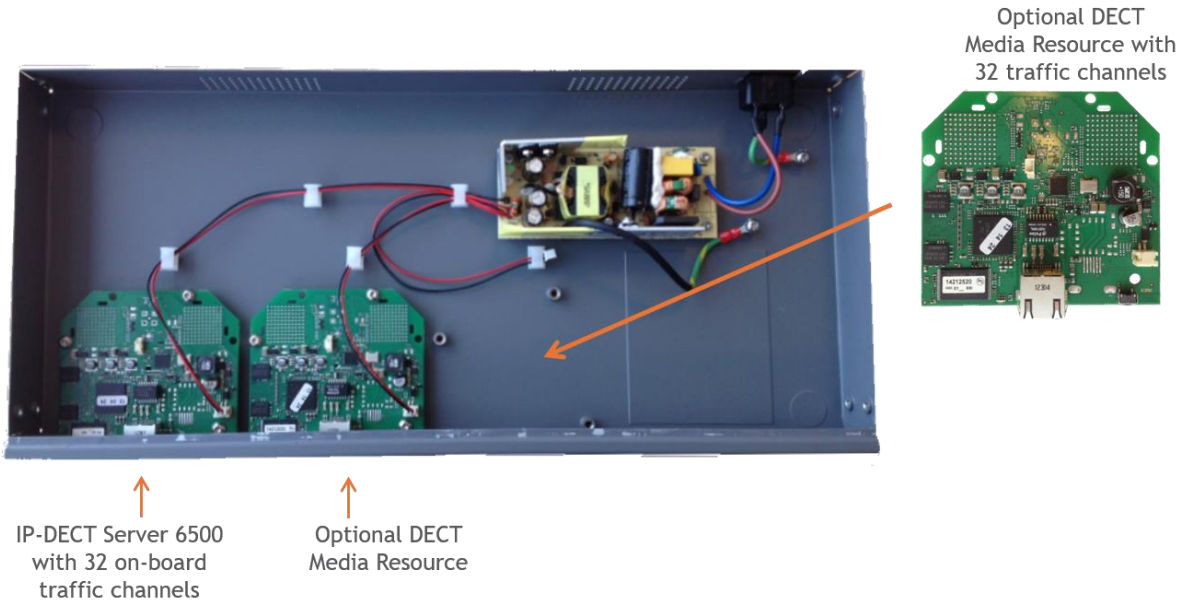
Installed Spectralink DECT Media Resources must have their own switchport.

4 Connect the power on the back of the cabinet.

Adding Additional Spectralink DECT Media Resources

The Spectralink IP-DECT Server 6500 can be upgraded with up to two additional Spectralink DECT Media Resources to increase speech capacity. Each Spectralink DECT Media Resource provides 32 media channels and is purchased separately.

Below is an image of the Spectralink IP-DECT Server 6500 cabinet. The Spectralink IP-DECT Server 6500 itself resides to the far left, which is standard, and the two optional Spectralink DECT Media Resources reside in the middle and to the far right.



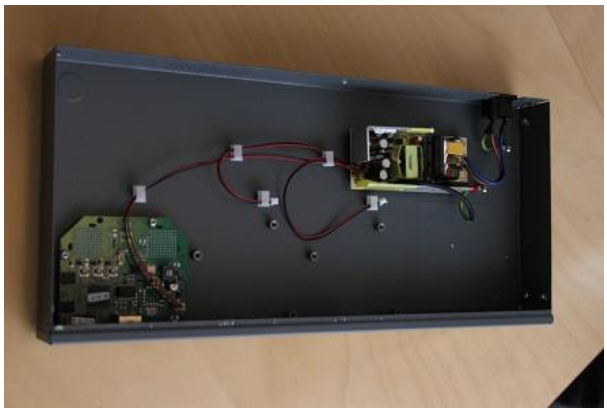
Note:

You can have cabinets with Spectralink DECT Media Resources only.

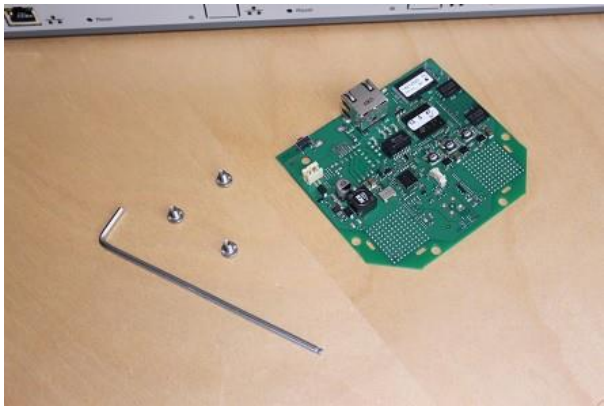
If Spectralink DECT Media Resources are used in conjunction with a Spectralink Virtual IP-DECT Server One, acquisition of a cabinet is required. The media resource cabinet comes with one media resource print board and the possibility of installing up to two more media resource print boards. Each Spectralink Virtual IP-DECT Server One contains 32 built in media channels if the Mandatory Base License ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License is installed. The Spectralink Virtual IP-DECT Server One supports a total of 1024 media channels - up to 31 media resource print boards (11 cabinets in total).

How to Add a Spectralink DECT Media Resource

1 Remove the top cover from the cabinet.



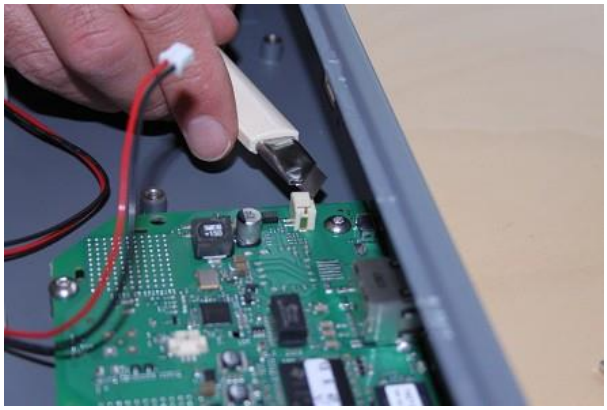
2 Unpack the media resource board.

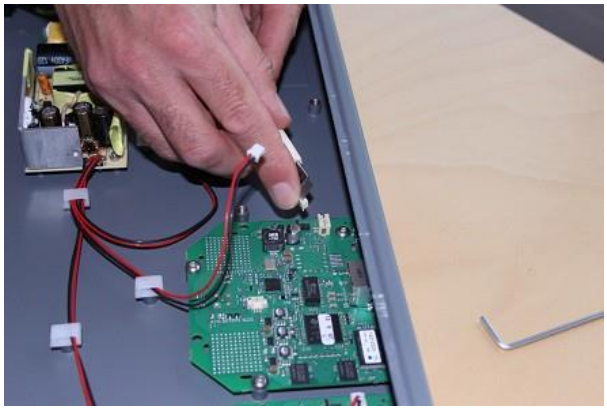


3 Cut a hole for the RJ45 network connector in the front foil of the cabinet.

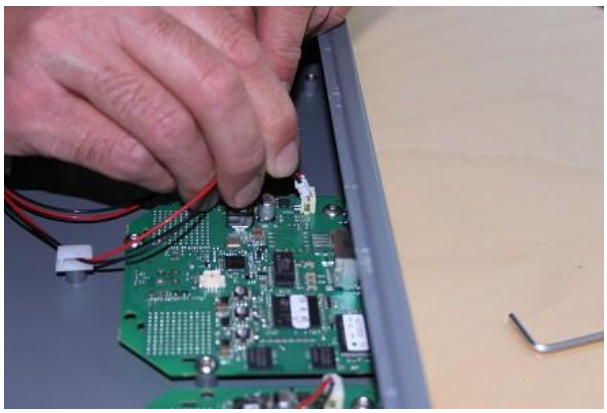
4 Mount the media resource board in the cabinet with three screws.

5 Prepare the media resource power connector.





6 Connect the power cable to the media resource power connector.



7 Close the cabinet again.

Chapter 11: Deploying Spectralink Virtual IP-DECT Server One and Spectralink Virtual IP-DECT Media Resource on VMware ESXi

Below you will find information about deploying the following virtual machines:

- Spectralink Virtual IP-DECT Server One
- Spectralink Virtual IP-DECT Media Resource

The Spectralink Virtual IP-DECT Server One is a multi-cell solution, that is distributed as an Open Virtual Appliance (OVA) file. The Spectralink Virtual IP-DECT Media Resource is distributed in the

same Open Virtual Appliance (OVA) file as the Spectralink Virtual IP-DECT Server One.The OVA file is easily deployed on a VMware vSphere infrastructure or directly on an ESXi host. Future updates can be applied directly in the web-based Administration Page of the Spectralink Virtual IP-DECT Server One/Spectralink Virtual IP-DECT Media Resource using a new OVA file.

Note:

It is assumed, that users have a running VMware vSphere solution or ESXi host and a solid knowledge of handling and deploying OVA files. For more information about VMware vSphere and OVA files, see VMware documentation.

Note:

Creation of a Spectralink Virtual IP-DECT Media Resource with the Spectralink Virtual IP-DECT Server One is optional. A media resource will increase the number of simultaneous voice calls supported by a stand-alone server.

The Spectralink Virtual IP-DECT Server One with the Mandatory Base License ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License installed will itself provide 32 internal media channels.

The Spectralink DECT Media Resource can also be used with the Spectralink Virtual IP-DECT Server One. For more information about installment, see Installing Spectralink IP-DECT Server 6500 and Spectralink DECT Media Resource.

Deploying a Spectralink Virtual IP-DECT Server One (or Spectralink Virtual IP-DECT Media Resource)

1. Download the OVA file of the Spectralink Virtual IP-DECT Server One from **http://support.spectralink.com/products**.
2. Deploy the OVA file using the VMware vSphere / ESXi management interface. When deployed and powered up, the vSphere / ESXi virtual machine summary will show the IP address and hostname of the Spectralink Virtual IP-DECT Server One.
3. During the deployment of the ova file, the installer will have the option to continue the installation as a IP-DECT Server One or a Media Resource. Continue as IP-DECT Server One is business as usual.
4. (Conditional) If deploying as a Media Resource.

   Starting as Media Resource enables the setup to continue as a Media Resource with no internal media channels installed. The "Server licensed Media Resource" must be configured as usual (pointing to an IP-DECT Server One). On the IP-DECT Server One web GUI the new "Server licensed Media Resource" will show up as a shared Media Resource. The internal media resource in the server and all connected "Server licensed Media Resources" will share the number of media channels that is given from the server license.

   In a Redundancy setup the number of media channels should be the same in the primary and backup server. A "Server licensed Media Resource" can default handle up to 96 media channels (if license on server allows). This setting is depending on hardware performance on the computer that runs the virtual machines and which codecs are in use. Possible settings are 32, 64, 96 and 128 channels and can be configured from web GUI on the hosting server.

   Beside continuing as a “Server licensed Media Resource” during deployment of the .ova file, it is also possible to set Admin password and some network settings.
5. Optionally (only relevant to ESXi 6.7 + hosts), upgrade the VM Compatibility to VM version 15 and set the Guest OS Version to **Other 4.x or later Linux (64-bit**) (in Settings> **VM Options**> **General Options**).
6. Use the IP address/hostname to log in to the Spectralink Virtual IP-DECT Server One using a browser. Change of password is required.

   When initially deployed, the Spectralink Virtual IP-DECT Server One includes a demo mode license with these features available:

   - Residential ARI
   - 4 users
   - 4 simultaneous calls
   - 4 base stations
   - Skype for Business interoperability
   - Redundancy feature

- LAN Sync
- Enhanced Provisioning
- Handset sharing
- OAM REST API

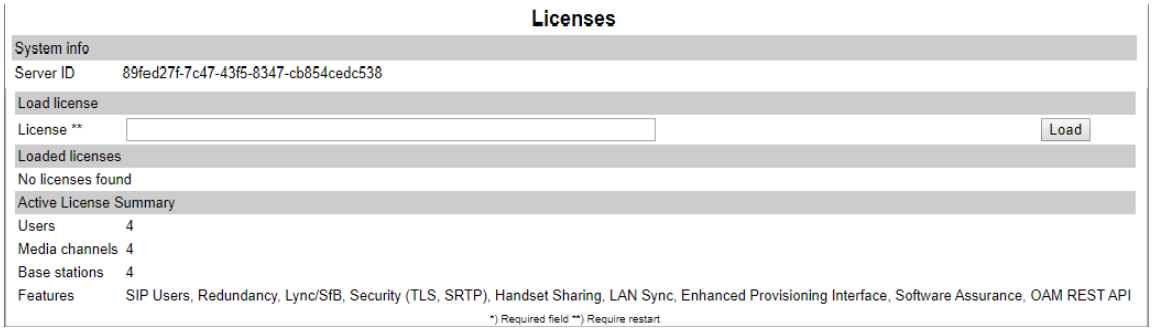
Note:

The Spectralink Virtual IP-DECT Server One runs in demo mode with a residential ARI until a Mandatory Base License ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License is installed.

The Mandatory Base License ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License contains the ARI, that must be used for further deployment of the Spectralink Virtual IP-DECT Server One solution.

7 To be able to order licenses for the virtual machine, note the Server ID (UUID).

- Click **Administration**, and then click **License**.



- Under **System Info**, note the Server ID.

Note:

Server ID (UUID) must be used to order further licenses.

If the virtual machine is to run as a Spectralink Virtual IP-DECT Server One, you must order the Mandatory Base License ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License, which also provides you with an ARI.

If the virtual machine is to run as a Spectralink Virtual IP-DECT Media Resource (no ARI needed), you must order a 32 Media Channels | Virtual IP-DECT Server One License.

8 To order a license, you must use the Server ID (UUID), that you noted under Administration> License> Licenses.

The following licenses must be ordered:

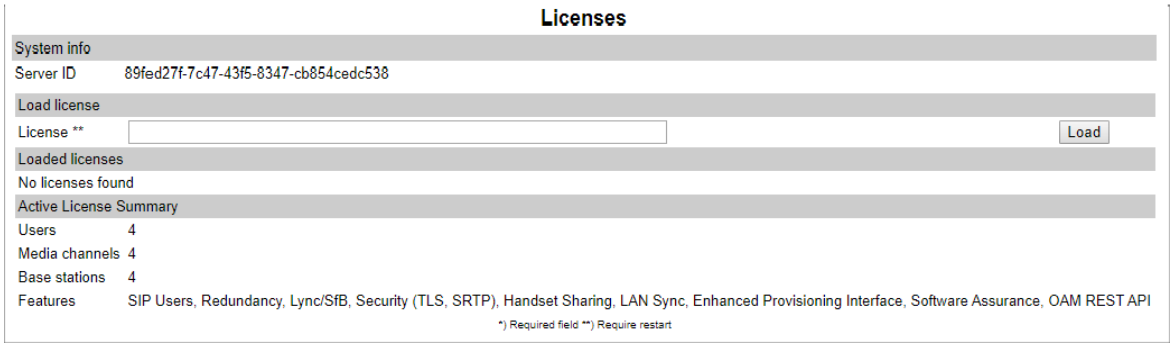
- If the virtual machine is to run as a Spectralink Virtual IP-DECT Server One, you must order the Mandatory Base License ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License, which also provides you with an ARI.

- If the virtual machine is to run as a Spectralink Virtual IP-DECT Media Resource (no ARI needed), you must order a 32 Media Channels | Virtual IP-DECT Server One License.

For more information about ordering a license and information about available licenses, see Ordering Licenses and Licenses for Spectralink Virtual IP-DECT Server One.

9 Upload the Mandatory Base License ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License (or 32 Media Channels | Virtual IP-DECT Server One) from the web-based Administration Page under **Administration**> **License**> **Licenses**.

For more information, see Loading Licenses.



Depending on the license uploaded, you have now created a Spectralink Virtual IP-DECT Server One or a Spectralink Virtual IP-DECT Media Resource. Continue with further configuration of the Spectralink Virtual IP-DECT Server One solution by installing other licenses, configuring the solution to meet your needs.

Example of a Spectralink Virtual IP-DECT Server One:

Example of a Spectralink Virtual IP-DECT Media Resource:

Licenses

System info	
Server ID	8984a0d9-e39a-4f64-84f0-ca4b1743e87b
Load license	
License **	Load
Loaded licenses	
Key	S0xWMwkQDOkJzCCrWnCIFAY7QlrQ+QIEskyLXQoBIAYBBgggsowfiMG5kcyaunhvdTW1JxYqgiyW8lUDtOzIwO4gNRo=
Users	0
Features	
Channels	32
Base stations	0
Expires	Delete**
Active License Summary	
Users	0
Media channels	32
Base stations	0
Features	

Note:

When first created, future updates can be applied directly in the web-based Administration Page of the Spectralink Virtual IP-DECT Server One or Spectralink Virtual IP-DECT Media Resource using a new OVA file.

Chapter 12: Installing Spectralink IP-DECT Base Station

Below you will find information about installing the base station.

Note:

Before you install the equipment, ensure that a site planner defines the location of the base stations.

Before you begin the installation, determine the position of the base station for best coverage. The average coverage within buildings is 30 meters/100 feet.

The coverage depends on the construction of the building, architecture, and the choice of building materials.

Power Requirements for the Base Station

The Spectralink IP-DECT Base Station uses:

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

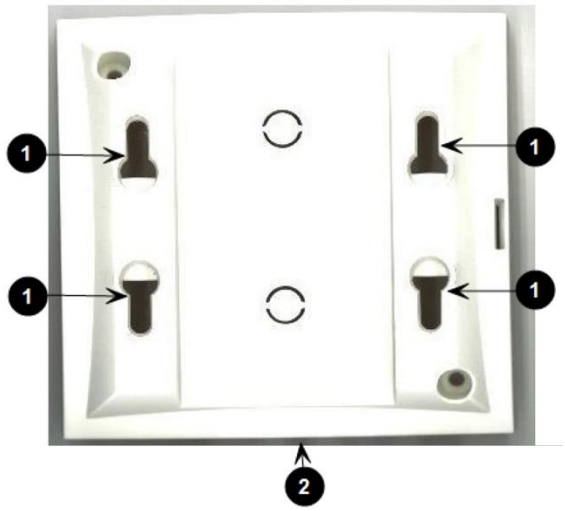
Use a standard PoE adapter or a PoE-enabled port on a switch adhering to PoE 802.3af when connecting the base station to a PoE power source.

Use an 8V-DC power supply when using a port without PoE.

Base Station Appearance and Components

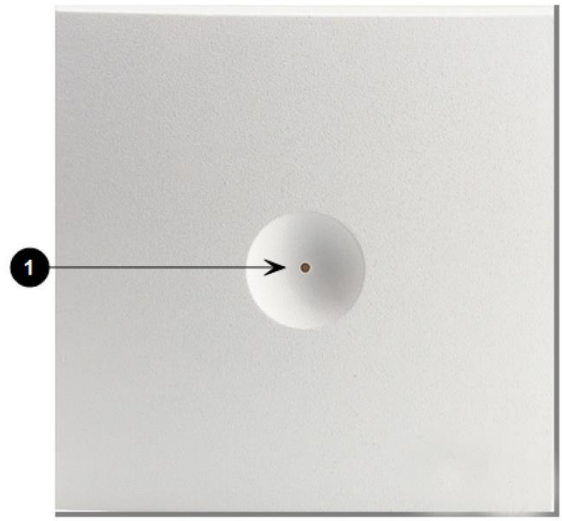
Below you will find a description of the base station appearance and components:

Spectralink IP-DECT Base Station – rear



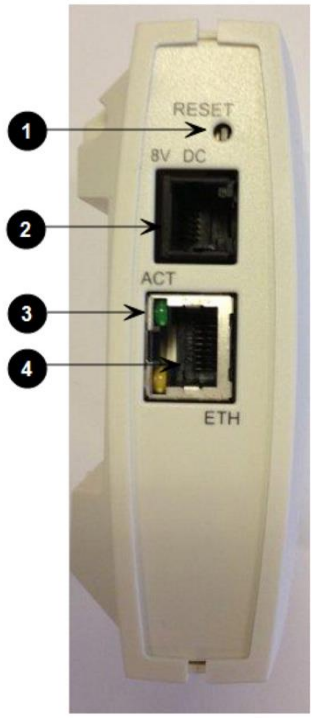
1. Holes for wall mounted screws
2. Connection to LAN

IP-DECT Base Station – front



1. LED

IP-DECT Base Station



1. Reset button
2. DC
3. LINK/Activity Indicator
4. ETH port (power supply by PoE)

Base Station LED Indicators

Below you will find information about LED indicators on the base station.

Front Cover

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

LED Indicator	*Meaning*
Steady green	OK and idle.
Slow green flashing	OK and active voice call.
Fast green flashing	Busy (all channels are in use).
Slow red flashing	No server connection.
Fast red flashing	No sync over air possible, or sync master is not available, or other error.
Steady red	Reset/shutdown in progress.
Steady red for 5 seconds followed by fast red flashing	Reset to factory settings.

LAN Port on Face Plate

LED Indicator	*Meaning*
LINK Indicator - yellow	Link layer software has established connection.
LINK Indicator - green flashing	Activity

Base Station Reset Button

You can restart or reset the base station by pressing the Reset button on the bottom of face plate of the base station.

The following table contains a description of the different actions that take place when pressing the Reset button.

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

Mounting the Base Station

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

The base stations are designed to only be mounted on the wall at least 2,40 m (8ft) off the ground but no higher than 6 m (20ft). The connectors can be pointed either up or down. The base stations should not be flush mounted to the ceiling as it would affect signal propagation. If ceiling mounting is a requirement, the base stations could be drop mounted from the ceiling in the same orientation (i.e., vertical) and height (no higher than 6 m (20ft) from ground as described for wall mounting. If mounting base stations higher than 6 m (20ft) off the ground, coverage directly underneath the base station will be impacted.

Wall Mounted (Vertical) Installation RF Coverage

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

Caution:

The base station must not be installed at any angle other than vertical.

Do not mount the base station on soft surfaced walls such as those covered with canvas, metal or sponge-like materials.

How to Wall Mount the Spectralink IP-DECT Base Station

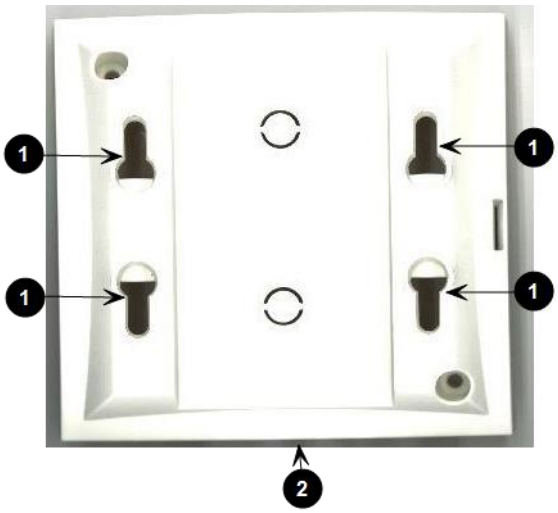
The base station must be mounted vertically on the wall for best coverage.

1. Use a twisted pair cable, cat. 5e or higher between the base station and the network switch.

2 Mount the base station onto the wall using the screws accompanying the base station. For more information, see Measurements and Mounting Template.

Note:

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



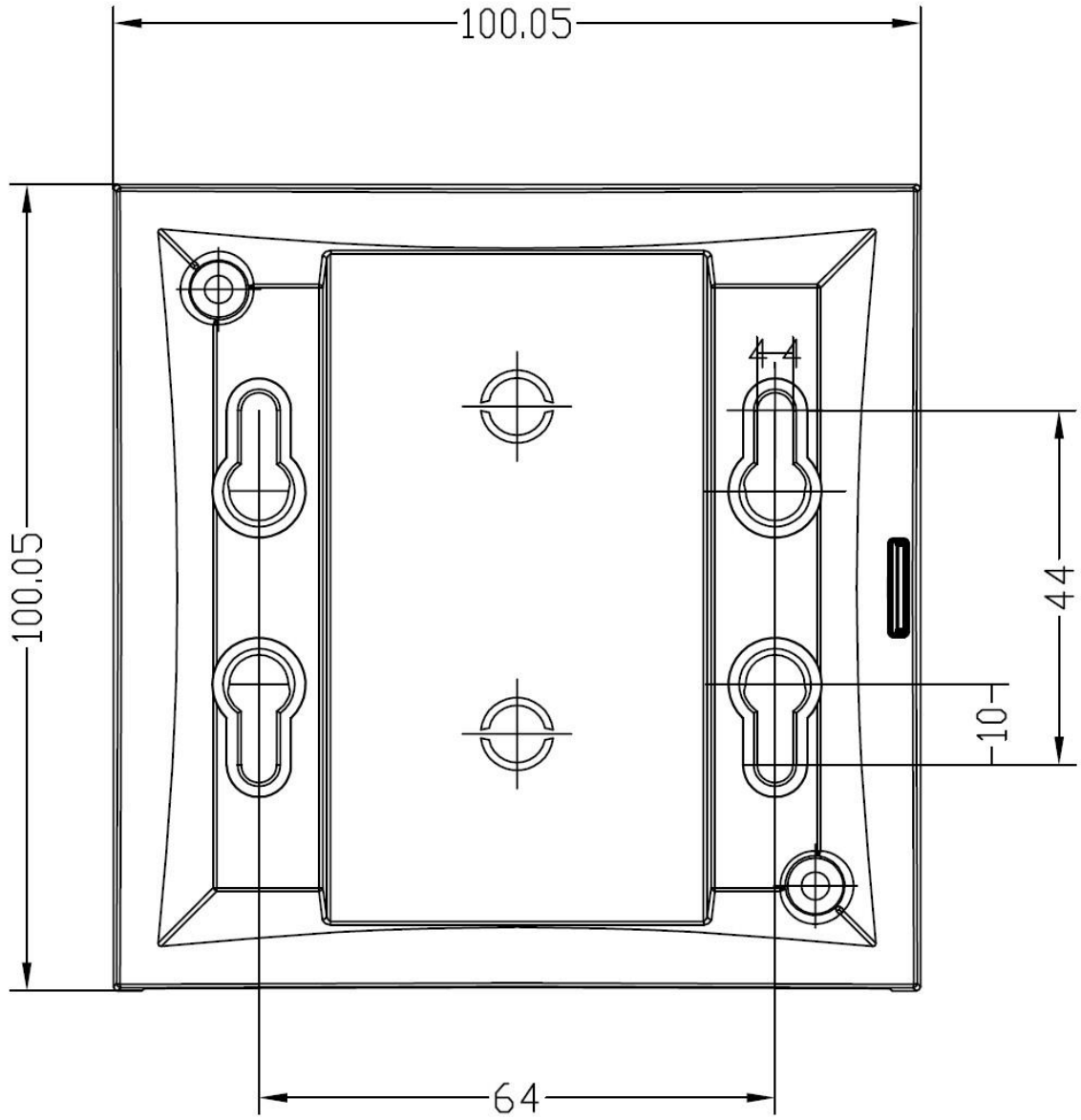
1. Holes for wall mounted screws
2. RJ45 port

3 Connect the network cable to the RJ45 port.

4 After installing the base station you need to power it up. For more information, see Installing Spectralink IP-DECT Base Station.

Measurements and Mounting Template

Measurements in Millimeters



Mounting Template

Note:

For correct measurement, ensure that this page is printed as either **Actual size** or **Scale 100 %** (**Print** dialog box) on an A4 size paper before using the mounting template below.


64 mm

Chapter 13: Installing Spectralink DECT Repeater

This section describes the Spectralink DECT Repeater and how to unpack and install it. Installing repeaters requires a software installation as well as a hardware installation.

Note:

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

The coverage depends on the construction of the building and the choice of building materials.

The repeater does not add channels. It only adds additional coverage area.

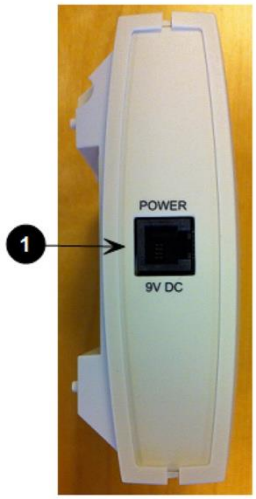
For installations, the following items should be present in every box containing a Spectralink DECT Repeater:

- Spectralink DECT Repeater
- Mounting template
- Two mounting screws and anchors

Repeater Appearance and Components

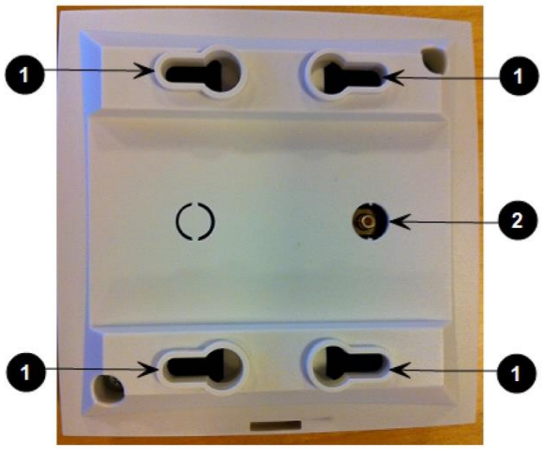
Below you will find a description of the repeater appearance and components:

DECT Repeater – bottom



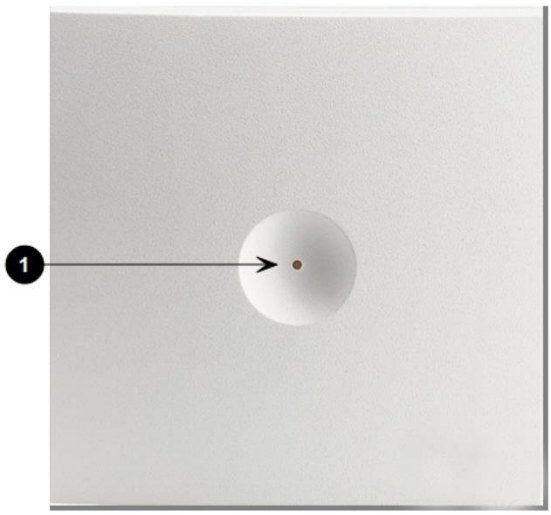
1. RJ9 port

DECT Repeater – rear



1. Holes for wall mounted screws
2. External antenna connector

DECT Repeater – front



1. LED

Repeater LED Indicators

Below you will find information about LED indicators on the repeater.

Front Cover

LED Indicator	*Meaning*
Indicator Off	The repeater is not powered.
Flashing	Repeater has been powered, sync has still not been established.

LED Indicator	*Meaning*
Steady green	The repeater is powered and sync is established.
Short flash	A handset connects or makes handover to the repeater.

Site Installation Considerations

Before you begin the installation, determine the position of the repeater for best coverage. The coverage depends on the construction of the building and the choice of building materials.

The repeater can be registered on the system under the following circumstances.

- When placed within the coverage area of a base station/server 200/400.
- When placed within the coverage area of an already-installed repeater.
- When placed outside the coverage area of a base station or repeater using an external antenna.

Note:

The repeater does not add channels. It only adds additional coverage area.

Environmental Considerations

- Do not install a device near metal objects and steel constructions.
- Do not position devices in ducts, plenums or hollow spaces used to transport environmental air except where the duct, plenum or hollow space is created by a suspended ceiling having lay-in panels.
- Do not position devices behind furniture.
- The installation area must be clean, free of traffic and excess dust, dry, and well ventilated.
- The installation area must be within the temperature ranges of 10°C and 40°C/50°F and 104°F.
- The installation area must be between 20% and 80% non-condensing relative humidity.
- For best RF coverage, the device must be mounted vertically on walls.

How to Wall Mount the Repeater

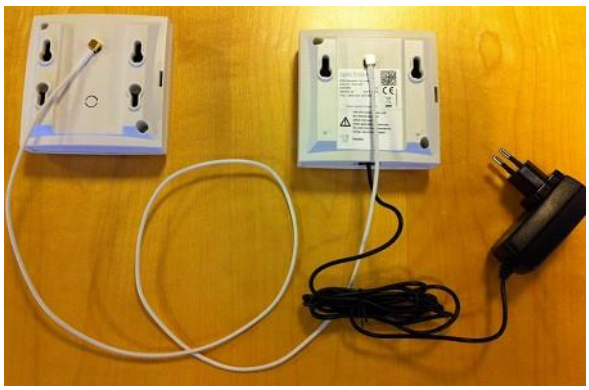
For best RF coverage, the device must be mounted vertically on walls.

Caution:

The repeater and external antenna is to be fixed-mounted on indoor permanent structures providing a separation distance of at least 20 cm/8 inches from all persons during normal operation and must not be co-located or operating in conjunction with any other antenna or repeater. The maximum radiated output power is 1W e.i.r.p.

1 Connect the power supply cable to the RJ9 port on the bottom of the repeater.

For repeaters with external antenna, connect the external antenna cable to the antenna connector on the rear side of the repeater and in the same way on the external antenna.

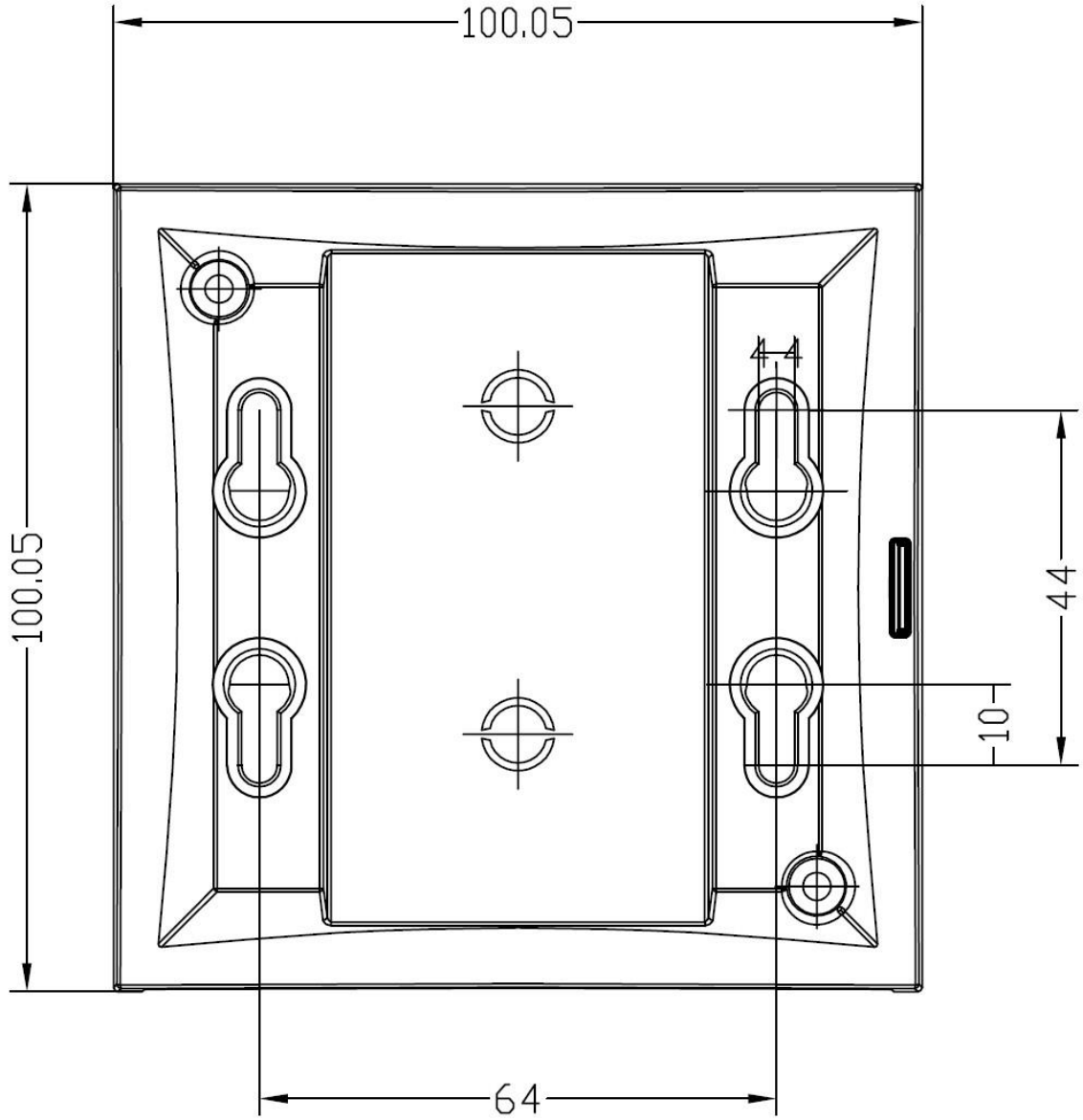


Mount the repeater on the wall using the anchors and screws accompanying the product. For more information, see Measurements and Mounting Template.

2 After installing the repeater you need to power it up. The power supply for the repeater is 9VDC, 350mA.

Measurements and Mounting Template

Measurements in Millimeters



Mounting Template

Note:

For correct measurement, ensure that this page is printed as either **Actual size** or **Scale 100 %** (**Print** dialog box) on an A4 size paper before using the mounting template below.

Programming a Spectralink DECT Repeater with the Repeater Programming Kit

Content of the Spectralink Repeater Programming Kit

The Repeater Programming Kit (Part no. 02509210) consists of:

- Splitter
- Programming tool with RJ-Connector
- USB cable

Set up of the Hardware for Repeater Programming

Spectralink recommends that you carry out the set up in the following order:

1. Unplug the repeater power supply and insert the splitter into the power socket of the repeater.
2. Connect the repeater power supply (small one - RJ9) to the splitter and the mains.
3. Wait until the LED flashes (starts with solid red - goes to flashing red after 3 sec.)
4. Connect the programming plug (RJ11) to the splitter.
5. Connect the USB cable to the programming tool.

6 Download the Handset and Repeater Management Tool from **http://support.spectralink.com/** and install it on your computer.

The repeater is now ready for programming via the Handset and Repeater Management Tool.

Programming the Spectralink DECT Repeater with the Handset and Repeater Management Tool

The Handset and Repeater Management Tool is the tool you access from your desktop and use for repeater programming, handset management and software download to the handset.

The Handset and Repeater Management Tool identifies the type of repeater, and with this software you can program the Spectralink DECT Repeater to connect to the Spectralink DECT Radio Infrastructure solutions.

For more information about programming the repeater with the Handset and Repeater Management Tool, refer to the Handset and Repeater Management Tool User Guide.

Note:

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

Numbering of Base Stations/Server 200/400 and Repeaters in a Normal Configuration

Note:

Repeater and base station/server RPNs must not be the same. Also, in a situation where common overlap is present between the actual units, a repeater cannot have an RPN that is similar to that of a base station/server or another repeater. If this occurs, handover between the different units is not possible.

First Repeater

- RPN of base station/server 200/400 + 64
- Base to synchronize on: RPN of base station/server

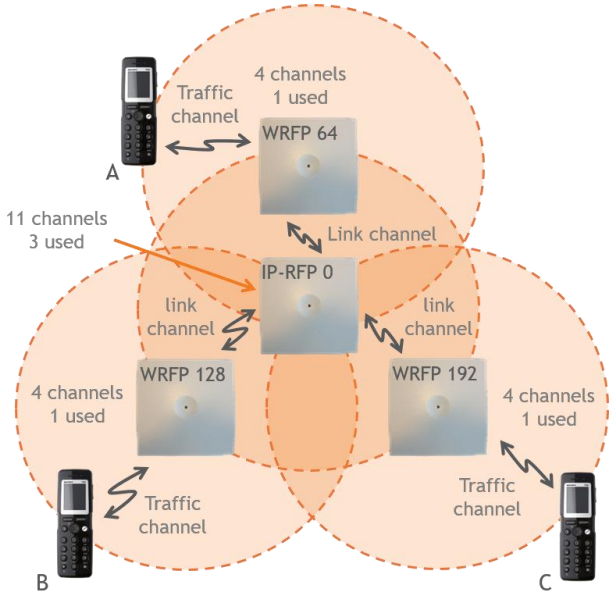
Second Repeater

- RPN of base station/server 200/400 + 128
- Base to synchronize on: RPN of base station/server

Third Repeater

- RPN of base station/server 200/400 + 192
- Base to synchronize on: RPN of base station/server

Below is an example of base station and repeater numbering in a normal configuration.



Numbering of Repeaters in a Repeater Daisy Chain Configuration

First Repeater in Chain

- RPN of base station/server 200/400 + 64
- Base to synchronize on: RPN of base station/server

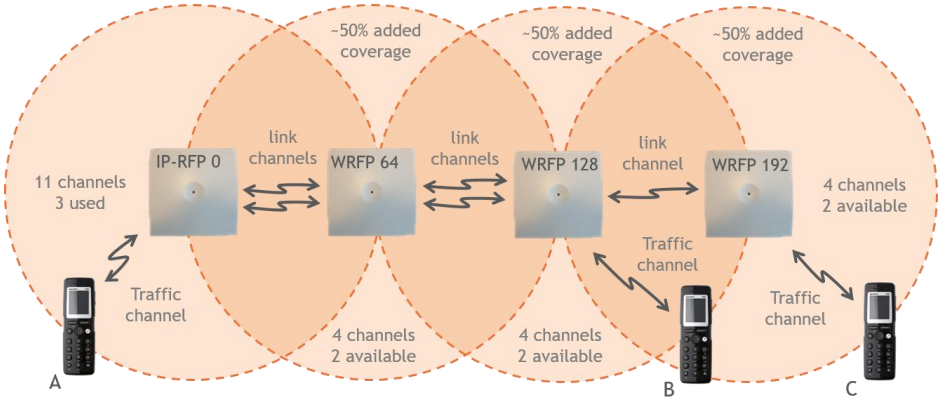
Second Repeater in Chain

- RPN of base station/server 200/400 + 128
- Base to synchronize on: RPN of previous repeater

Third Repeater in Chain

- RPN base station/server 200/400 + 192
- Base to synchronize on: RPN of previous repeater

Below is an example of repeater numbering in a daisy chain configuration.



Using the Spectralink DECT Repeater with External Antenna

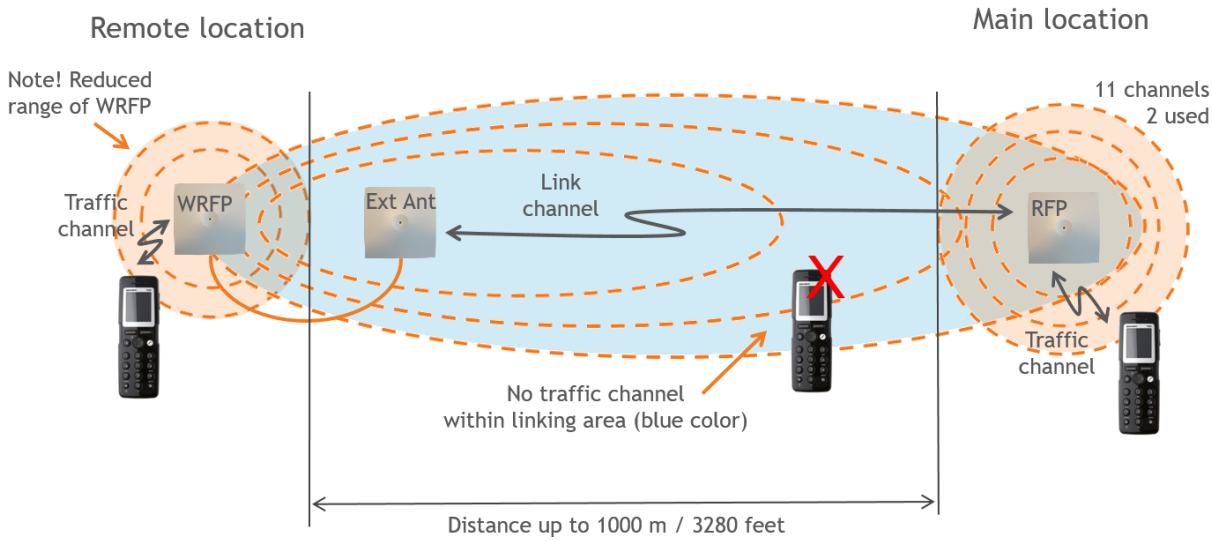
If coverage is needed in a remote area, synchronization can be established between the main system and a repeater by use of an external antenna. The external antenna establishes a radio link between the main system and a Spectralink DECT Repeater.

Note:

Only the Spectralink external antenna (part no. 02319507 - including 1 m connection cable) is approved along with the Spectralink DECT Repeater. The external antenna is delivered with a 1 m connection cable. The connection cable is also available in 7.5 m (part no. 14002706).

The Spectralink DECT Repeater is automatically configured to the external antenna when connected.

Below is an example of using a Spectralink DECT Repeater with external antenna.



A repeater is placed at a remote location and a base station is placed at the main location. They are too far away to allow the repeater to extend the coverage of the base station. Therefore, an external antenna can be used to establish a connection between the two end points. As the external antenna is a high gain directional antenna, it must point towards the base station you want to link with.

The radio link way must be stable and free of moving objects. The RSSI level of the main system at the Spectralink DECT Repeater placed remotely must not be lower than 75.

Note:

Inside the area named "radio link" there is no radio coverage for handsets.

If a situation occurs where the primary synchronization for some reason breaks down, the Spectralink DECT Repeater will obtain synchronization on the alternative synchronization source.

Alternative Synchronization Ways

The Spectralink DECT Repeater with or without external antenna, 4 channels, can be programmed to obtain synchronization on two radio units (base station, wireless server 200/400 or repeater).

Note:

The primary synchronization source has priority; the alternative synchronization source is only in use as long as the primary synchronization source is down.

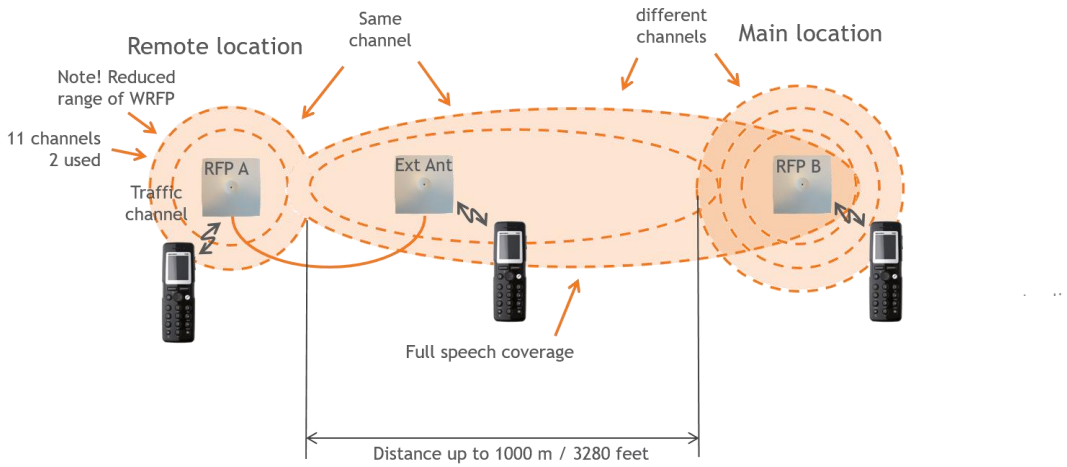
Chapter 14: Using Spectralink IP-DECT Server 200/400 and Spectralink IP-DECT Base Station with External Antenna

Note:

Only the Spectralink external antenna (part no. 02319507) is approved along with the Spectralink IP-DECT Server 200/400 and Spectralink IP-DECT Base Station. The external antenna is delivered with a 1 m connection cable. The connection cable is also available in 7.5 m (part no. 14002706).

The devices are automatically configured to the external antenna when connected.

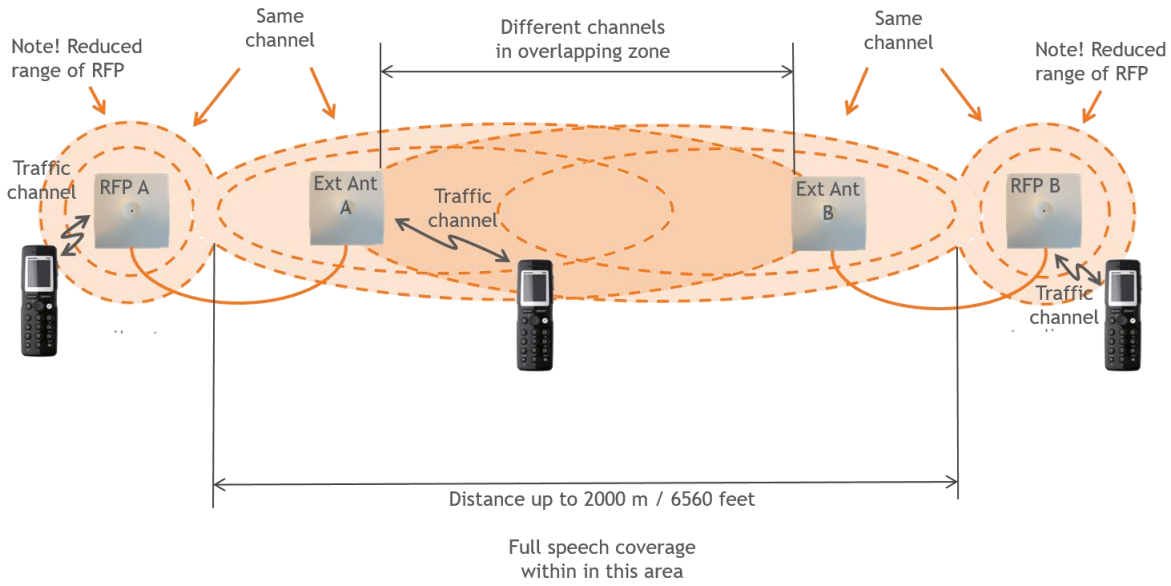
First example (see illustration below) is an example of using a Spectralink IP-DECT Base Station with external antenna.



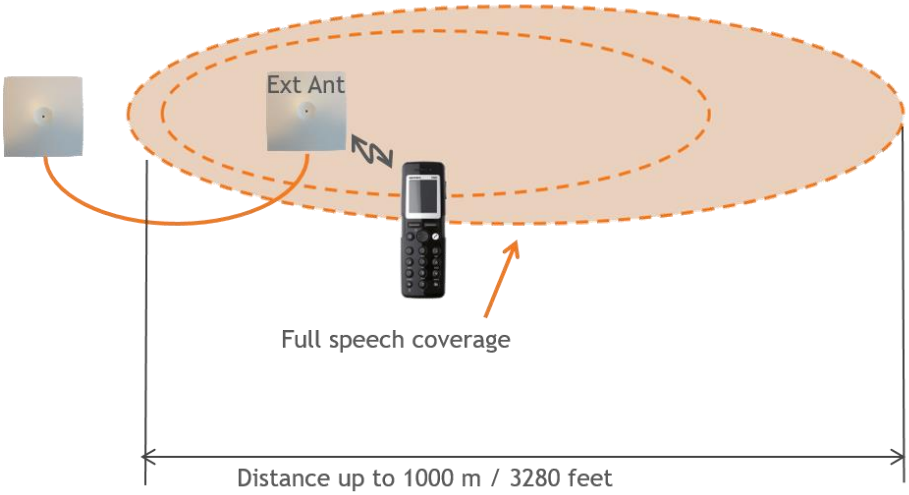
*) see separate documentation on USB stick

The 2 base stations are too far apart to maintain full speech coverage between them. An external antenna can be used on either side to create an overlap which allows for full speech coverage anywhere between the two base stations. Note that the range of RFP A is reduced when connected with an external antenna. RFP A and the external antenna also operates on the same channel as opposed to a repeater which always operates on a channel that is different from its host.

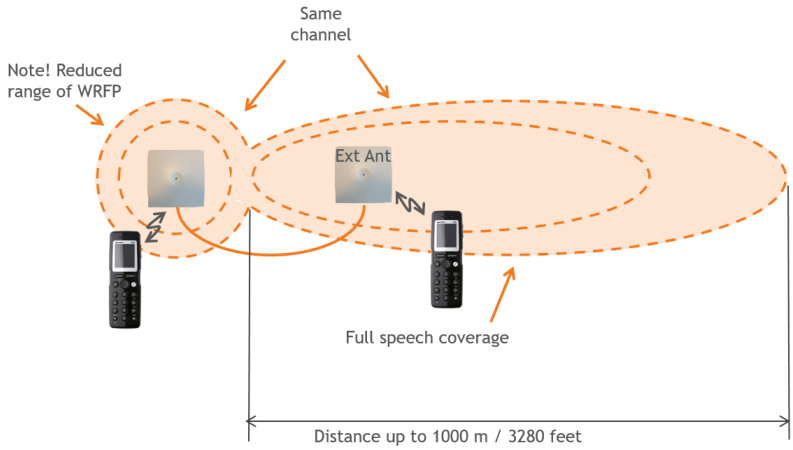
Second example (see illustration below) is an example of using Spectralink IP-DECT Base Stations, both having external antennas. This scenario allows for coverage over very long distances.



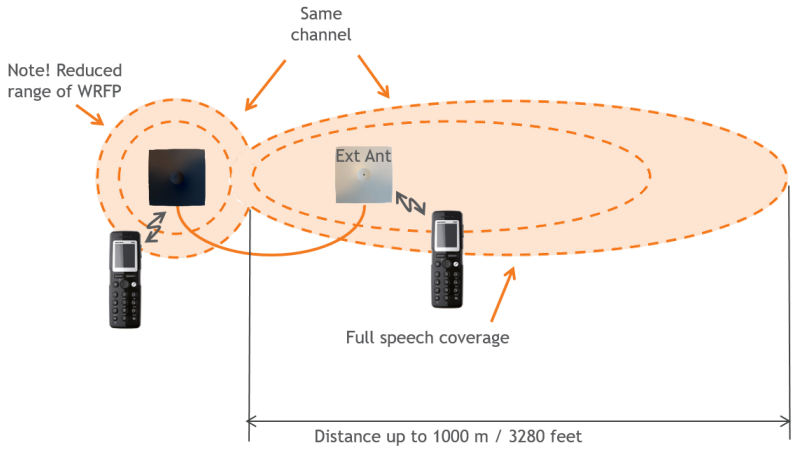
Third example (see illustration below) is an example of using external antenna only on a Spectralink IP-DECT Base Station or Spectralink IP-DECT Server 400 with built-in antenna turned off (requires Multi-cell | IP-DECT Server 400 License on the Spectralink IP-DECT Server 400).



Fourth example (see illustration below) is an example of using a Spectralink IP-DECT Server 400 (single cell solution) with external antenna.



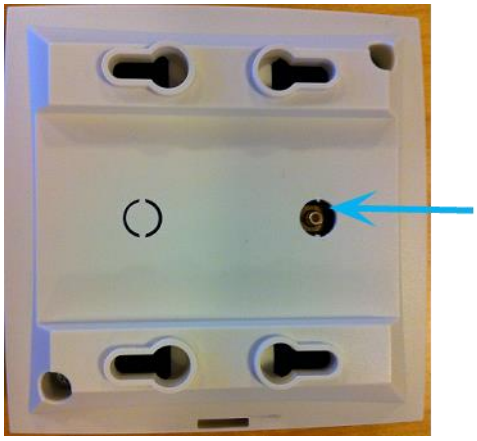
Fifth example (see illustration below) is an example of using a Spectralink IP-DECT Server 200 with external antenna.



How to Connect External Antenna to Device

Connect the external antenna cable to the antenna connector on the rear side of the Spectralink IP-DECT Base Stations and Spectralink IP-DECT Server 200/400 and in the same way on the external antenna.

Below is an illustration of the antenna connector. Use a screwdriver to remove the plastic carefully.



Below are illustrations of a Spectralink IP-DECT Server 200 and Spectralink IP-DECT Server 400 with external antenna.

Chapter 15: Configuration Steps Overview

Below is an overview of the steps to follow in order to configure the Spectralink IP-DECT/Virtual IP-DECT Server One solution after having installed all system components and completed all pre-configuration tasks.

After following these steps, you will be able to make calls between handsets:

1. Power up the Spectralink IP-DECT/Virtual IP-DECT Server One and Spectralink DECT Media Resource/Spectralink Virtual IP-DECT Media Resource (if used).
2. Change the IP address of the Spectralink IP-DECT/Virtual IP-DECT Server One.

   For more information, see Configuring Network Settings.
3. Power up the Spectralink IP-DECT Base Station.

Note:

Not relevant to the Spectralink IP-DECT Server 200.

4. Change the IP address of the Spectralink IP-DECT Base Station.

   For more information, see Configuring Network Settings.

Note:

Not relevant to the Spectralink IP-DECT Server 200.

5. Configure the Spectralink IP-DECT Base Station with the address of the Spectralink IP-DECT/Virtual IP-DECT Server One.

   For more information, see Assigning the Server Address.

Note:

Not relevant to the Spectralink IP-DECT Server 200.

6. SIP registration–configure the settings for the IP-PBX (**Configuration**> **SIP**). Remember to reboot the server.

   For more information, see Configuring SIP and IP-PBX Settings.
7. Register/create users and enter values for username, authentication user and authentication password (depending on PBX type).

   For more information, see Handset Management.
8. Subscribe handset.

   For more information, see Registering Users and Subscribing Handsets.

Note:

The above-mentioned configuration steps are only the minimum steps for configuring a system and being able to make calls between two handsets.

Depending on your solution, configuration of media resources, sites, redundancy server, handset sharing, phone book, MSF messaging and handset can also be part of further configuration.

For more information, see:

- Configuring Media Resource Settings
- Configuring Sites (and Zone)
- Configuration of Handset Sharing
- Configuring Company Phone Book/Directory
- Messaging Over MSF
- Managing Handset Configuration and Configuration Groups

Chapter 16: Configuring the Servers

This section provides you with information on basic network configuration of the following solutions:

- Spectralink IP-DECT Server 200/400/6500
- Spectralink Virtual IP-DECT Server One
- Spectralink DECT Media Resource
- Spectralink Virtual IP-DECT Media Resource
- web-based Administration Page

Note:

Configuration of Spectralink DECT Media Resources and Sites is not relevant to the Spectralink IP-DECT Server 200/400.

Configuration of Spectralink IP-DECT Base Stations is not relevant to the Spectralink IP- DECT Server 200.

Configuration of Spectralink Virtual IP-DECT Media Resources is only relevant to the Spectralink Virtual IP-DECT Server One.

The web-based Administration Page is used to configure the different components of the Spectralink IP-DECT/Virtual IP-DECT Server One solution.

Basic network settings can be obtained the following ways:

From a DHCP server

Using DHCP the device requests and obtains an available IP address from a DHCP server. The device also obtains other parameters such as the default gateway, subnet mask, DNS server, Time server and other IP parameters from the DHCP server.

Entered manually through web-based Administration Page> Configuration> General> General Configuration page.

Using manual network configuration, the IP-addresses and other networking parameters are entered manually through the web-based Administration Page.

Recommended Network Configuration

When configuring a Spectralink IP-DECT/Virtual IP-DECT Server One solution, Spectralink recommends doing it the following way:

- Spectralink IP-DECT Server 400/6500 or Spectralink Virtual IP-DECT Server One using static IP address

  This is to avoid sudden change of the IP address which would temporarily affect all base stations and thus the entire installation.

- Spectralink IP-DECT Server 200 using static IP address

- Spectralink DECT Media Resources or Spectralink Virtual IP-DECT Media Resources using static IP address

  Like with the servers, this is to avoid sudden change of the IP address.

- Spectralink IP-DECT Base Stations using DHCP

  This makes it easy to manage many base stations without having to keep track of many IP addresses.

Note:

When the base stations are set up to DHCP, you can use UPnP to discover all the Wireless devices on the local network. In Windows Explorer the devices will appear under **Network** and **Other Devices** as “<device name>-<Serial number/UUID> “ (e.g. KWS6500- 8442621, MR6500-84532341 and IP-DECT-89fed27f-7c47-43f5-8347-cb854cedc538).

Note:

Spectralink IP-DECT Base Stations, Spectralink DECT Media Resources and Spectralink Virtual IP-DECT Media Resources can be managed from the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One.

If the Spectralink IP-DECT/Virtual IP-DECT Server One solution is configured as recommended above, you can assign options to the DHCP server making it extremely easy to configure all media resources and base stations. If the Spectralink IP-DECT/Virtual IP-DECT Server One is configured using DHCP, it is necessary to assign a reservation for the device on the DHCP server.

Assigning DHCP Server Options

Note:

Not relevant to the Spectralink IP-DECT Server 200.

This section provides you with information on basic network configuration of the Spectralink IP-DECT Server 400/6500 and Spectralink Virtual IP-DECT Server One solution and the web-based Administration Page.

You can provide information about the static IP address of Spectralink IP-DECT Server 400/6500 and Spectralink Virtual IP-DECT Server One in the DHCP server through DHCP options. When defining the IP address of the Spectralink IP-DECT/Virtual IP-DECT Server One in the DHCP server, all media resources and Spectralink IP-DECT Base Stations are configured automatically.

The media resources and Spectralink IP-DECT Base Stations will include a Vendor Class Identifier option (60) with the value KIRK.IP6000 and a request for the Vendor Specific Information option (43) in the initial DHCP Discover request.

In the DHCP offer message, it will then expect the address of the Spectralink IP-DECT/Virtual IP-DECT Server One location in the Vendor Specific Information option (43), sub-option 43 encapsulated as a string type parameter.

On a Windows Server 2012 DHCP Management Console, the following steps will configure the correct DHCP option for a Spectralink IP-DECT Server 6500:

1. Right-click **IPv4/IPv6**, and click **Define Vendor Classes**....
2. Add a class new class:
   - Display name: **IP-DECT**
   - Description: **Spectralink IP-DECT**
   - ASCII: **KIRK.IP6000** (case sensitive)
3. Right-click **IPv4/IPv6**, and click **Set Predefined Options**....
4. Add a new option in the **IP-DECT** class:
   - Name: **IP-DECT Server**
   - Type: **String**
   - Code: **43**
   - Description: IP address of the IP-DECT Server
5. Right-click **Server Options**, and click **Configure Options**.
6. Under **Advanced**, add option 43 in the **Spectralink IP-DECT** vendor class, and set the value to the IP address of the Spectralink IP-DECT Server 6500.

Using the Powershell, following commands will configure the correct DHCP options for a Spectralink IP-DECT Server with the IP address 192.168.1.10:

```
netsh dhcp server add class IP-DECT "Spectralink IP-DECT"

netsh dchp server add optiondef 43 "IP-DECT Server" string 0
vendor- r=IP- DECT comment="IP address of the IP-DECT Server"

netsh dhcp server set optionvalue 43 string vendor=IP-
DECT "192.168.1.10"
```

On an ISC DHCP server, the following configuration file fragment will be the correct DHCP options for a Spectralink IP-DECT Server with the IP address 192.168.1.10:

```
option space ipdect code width 1 length width
1; option ipdect.server code 43 = text;
option vendor-ipdect code 43 = encapsulate
ipdect; class "vendor-classes" {
 match option vendor-class-identifier;
}
subclass "vendor-classes"
 "KIRK.IP6000" { vendor-option-space
 ipdect;
option ipdect.server "192.168.1.10";
```

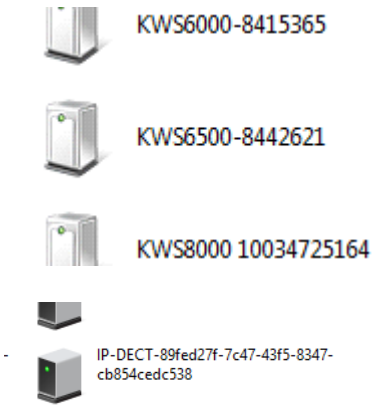
Discovering Spectralink IP-DECT/Virtual IP-DECT Components on the Network

If the DHCP server on the local network supports dynamic DNS updates, the Spectralink IP-DECT/Virtual IP-DECT Server One and Spectralink IP-DECT Base Stations can be located on the network with the hostname configured under **Configuration**> **General**> **General** page, or with the hostname ipdect-<serial number/UUID> if no hostname is configured.

Alternatively, they can be discovered using UPnP (using e.g. Windows Explorer):

- The Spectralink IP-DECT Server 6500 will appear under **Network** and **Other Devices** as e.g."KWS6500 -<Serial number>", e.g. KWS6500-8442621.
- The Spectralink Virtual IP-DECT Server One will appear under **Network** and **Other Devices** as e.g. "IP-DECT-<UUID>", e.g. IP-DECT-89fed27f-7c47-43f5-8347-cb854cedc538.

Below are examples of using UPnP to discover Spectralink IP-DECT Server 6500 or Spectralink Virtual IP-DECT Server One.



Double-click the icon to access the web-based Administration Page of the relevant server.

Assigning DHCP Server Reservations

If the Spectralink IP-DECT/Virtual IP-DECT Server One and Spectralink DECT Media Resource/Spectralink Virtual IP-DECT Media Resource is configured using DHCP, it is necessary to assign a reservation for the device on the DHCP server. For more information about this feature, contact your network administrator.

Accessing the Web-Based Administration Page

The Spectralink IP-DECT/Virtual IP-DECT Server One, Spectralink DECT Media Resources, Spectralink Virtual IP-DECT Media Resources and Spectralink IP-DECT Base Stations have their own web-based Administration Page.

You can access the web-based Administration Page through a standard web browser by entering the IP address discovered by UPnP, along with the username and password.

For more information, see Discovering Spectralink IP-DECT/Virtual IP-DECT Components on the Network.

Note:

If no IP address is received from the DHCP server, the server automatically falls back to IP address 192.168.0.1

Note:

For security reasons, you can disable the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One/Spectralink IP-DECT Base Station, so that it cannot be accessed from a browser. For more information about enabling/disabling the web-based Administration Page, see Disabling Web-Based Administration Page.

Password

The Spectralink IP-DECT/Virtual IP-DECT Server One, Spectralink DECT Media Resources, Spectralink Virtual IP-DECT Media Resources and Spectralink IP-DECT Base Stations are delivered with a default username and password.

- Default username of the system is: **admin**
- Default password of the system is: **admin**

Note:

After five successive failed login attempts, the web-based Administration Page will be locked for the next five minutes.

After being idle for 20 minutes, the user is automatically logged out of the web-based Administration Page.

Click **Logout** to logout manually from the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One.

Note:

It is strongly recommended that you change the default password. You will be prompted to change the password when logging on to the system the first time. For more information, see

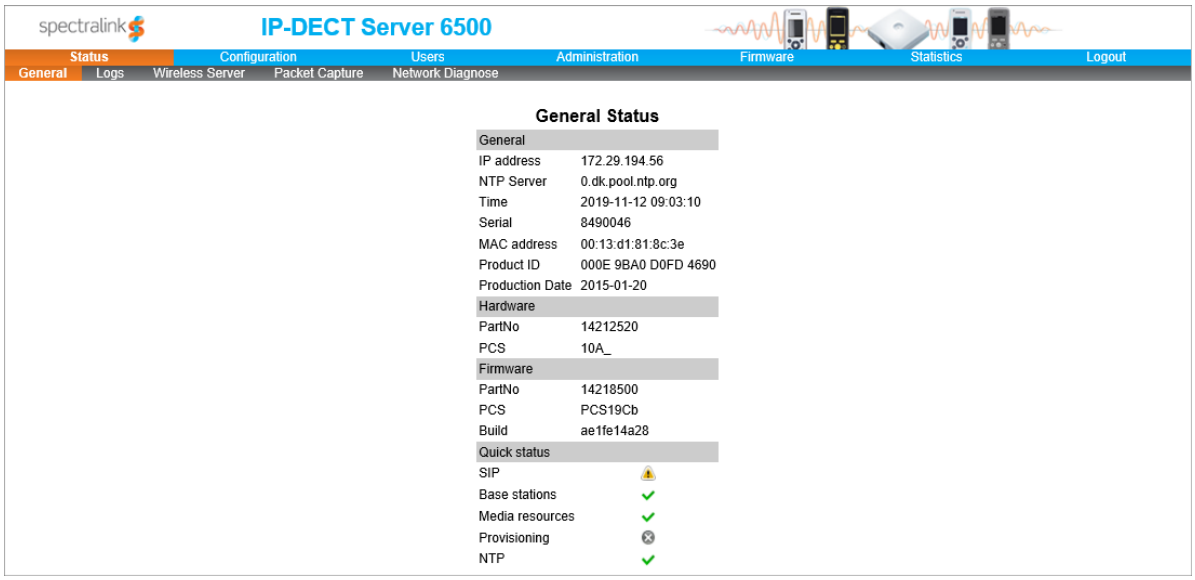
About the Main Page of the Web-Based Administration Page

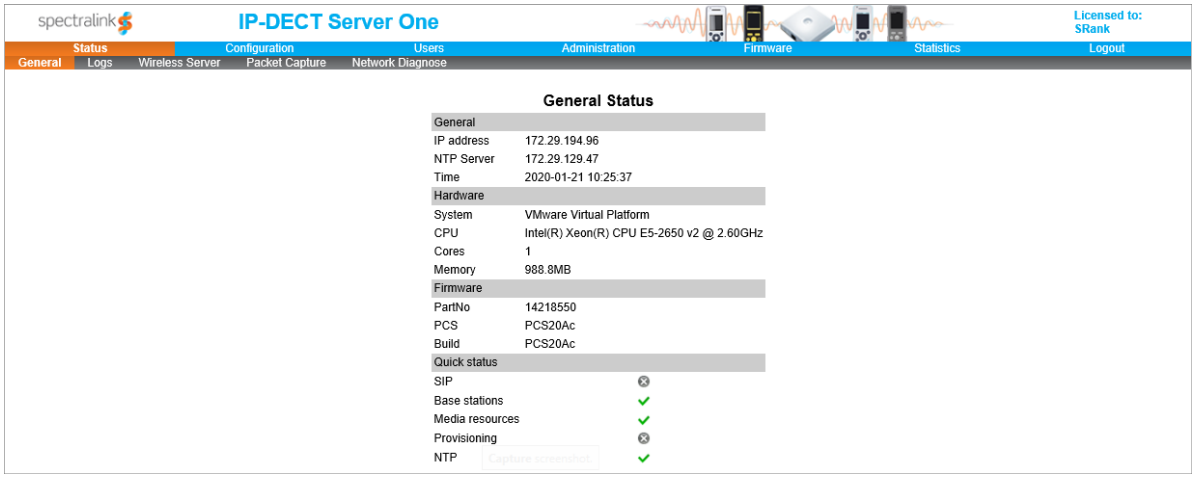
The main page of the web-based Administration Page for the Spectralink IP-DECT/Virtual IP-DECT Server One, Spectralink DECT Media Resource, Spectralink Virtual IP-DECT Media Resource and Spectralink IP-DECT Base Station consists of menus and submenus.

First you click a menu, and then you click one of the submenus to display the relevant page.

Spectralink IP-DECT/Virtual IP-DECT Server One

The web-based Administration Page is used to configure the different solution components of the Spectralink IP-DECT/Virtual IP-DECT Server One. For an overview and description of parameters on the different pages, see Parameter Overview.

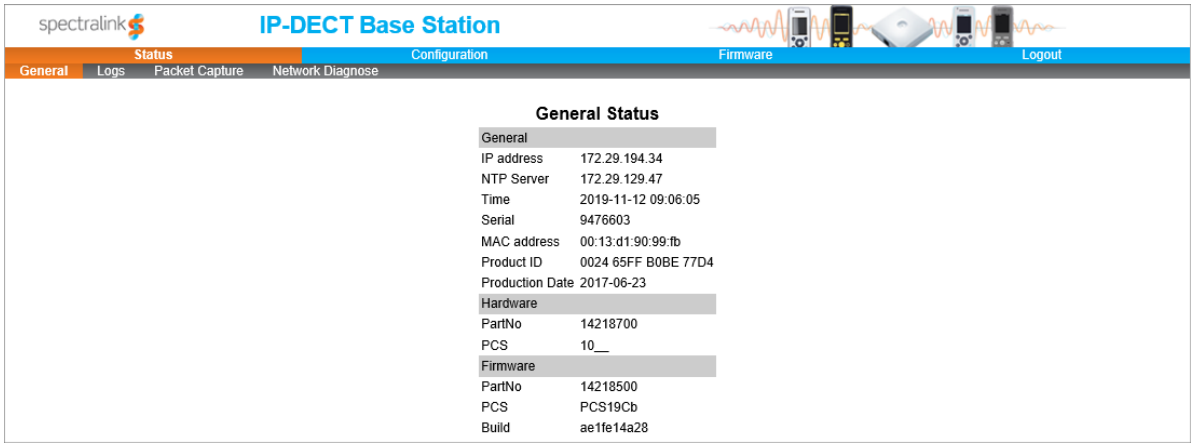




Spectralink IP-DECT Base Station

The web-based Administration Page of the Spectralink IP-DECT Base Station can be used in the following situations:

- Configuration–to specify to which Spectralink IP-DECT/Virtual IP-DECT Server One the Spectralink IP-DECT Base Station should connect.
- Status Information
- Firmware update



Spectralink DECT Media Resource/Spectralink Virtual IP-DECT Media Resource

The web-based Administration Page of the Spectralink DECT Media Resource/Spectralink Virtual IP-DECT Media Resource can be used in the following situations:

- Configuration–to specify to which Spectralink IP-DECT/Virtual IP-DECT Server One the Spectralink DECT Media Resource/Spectralink Virtual IP-DECT Media Resource should connect.

Note:

The Spectralink Virtual IP-DECT Media Resource is only relevant to Spectralink Virtual IP-DECT Server One.

- Status Information
- Firmware update

Configuring Network Settings

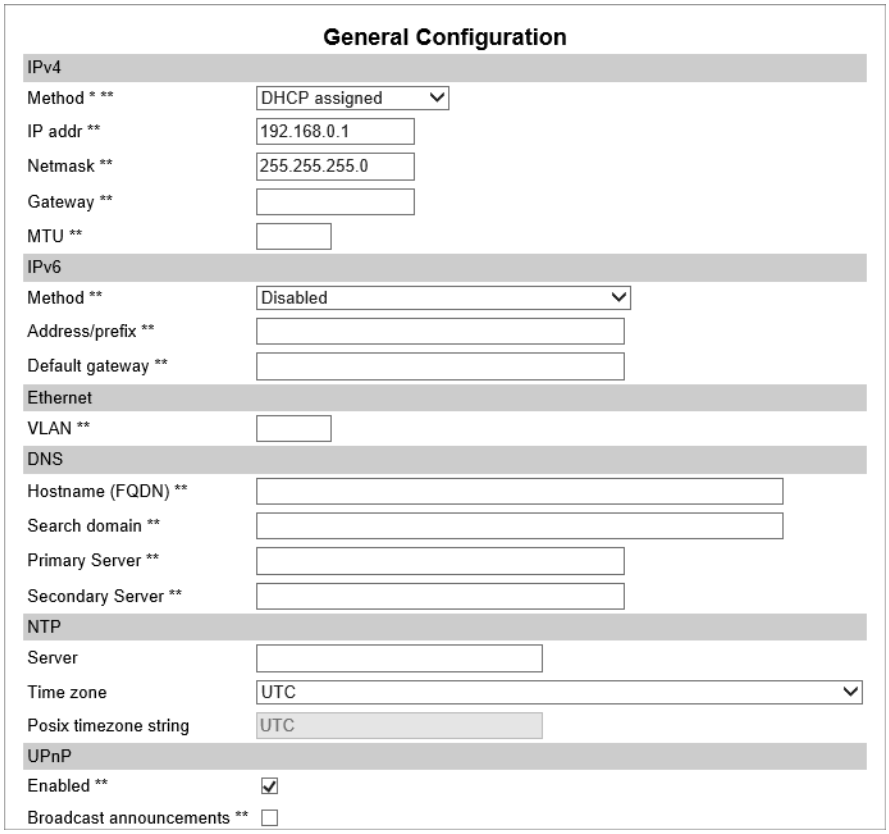
Through the web-based Administration Page of the server, you can configure the network for the Spectralink IP-DECT/Virtual IP-DECT Server One components using a static IP address or a dynamic IP address (DHCP). For more information, see Recommended Network Configuration.

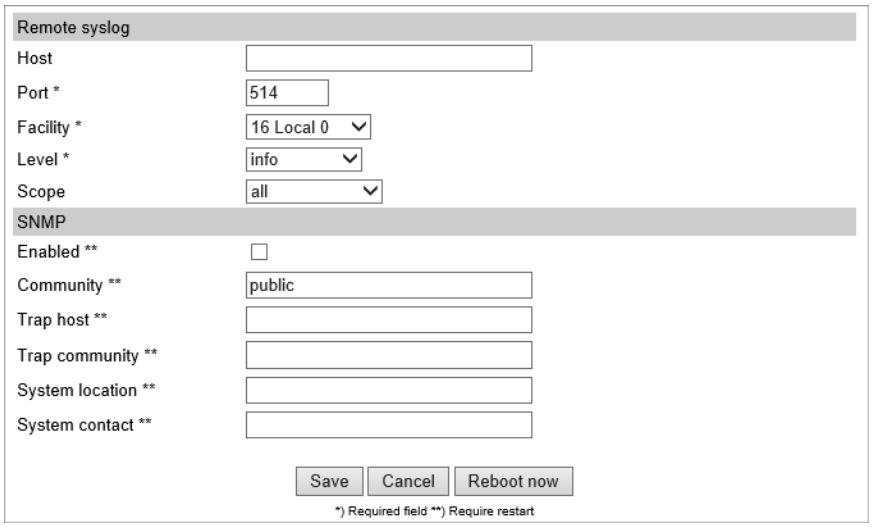
Note:

As the Spectralink IP-DECT/Virtual IP-DECT Server One is a critical part of the SIP infrastructure, it is highly recommended that you do not use DHCP.

Using a static IP address for the Spectralink IP-DECT/Virtual IP-DECT Server One is the preferred method. If the device is configured using a static IP address, you can assign options to the DHCP server making it extremely easy to configure all base stations.

It is also possible to configure Simple Network Management Protocol (SNMP) or configure for use of Advanced Mobile Intelligence for Enterprises (AMiE).





To Configure a Dynamic IP address

Spectralink recommends using a dynamic IP address (DHCP) for base stations.

To configure network settings (dynamic IP address) for the base stations from the web-based Administration Page:

1. Click **Configuration**, and then click **General**.
2. On the **General Configuration** page, enter the following data:

Field	*Setting*
General Configuration–Pv4	
Method	Select DHCP **assigned**. **Note**: Selecting DHCP, all other network settings are provided automatically.

3 Click **Save**.

To Configure a Static IP Address and Other Network Settings

It is highly recommended to use a static IP address for the server and media resource/Spectralink Virtual IP-DECT Media Resource.

To configure IP address, DNS and NTP settings for the server and media resource from the web-based Administration Page:

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

2 On the **General Configuration** page, enter the following data:

Field	*Setting*
General Configuration–IPv4	
Method	Default value: DHCP assigned (dynamic IP address) Select **Use Static IP Address** to configure a static IP address. **Note**: When using a static IP address, it is also necessary to configure other network settings below such as DNS and NTP settings. For more information, see Recommended Network Configuration.
IP addr	Enter the IP address of the Spectralink IP-DECT/Virtual IP-DECT Server One.
Netmask	Enter a new network mask. Contact your system administrator for more information.
Gateway	Enter the IP address of the default gateway. The default gateway serves as an access point to another network. Contact your system administrator for more information.
MTU (Maximum Translation Unit) (Optional)	Enter the size of the largest packet, that your network protocol can transmit.
General Configuration–Ipv6	
Method (Optional)	Default value: Disabled If not using IPv4, select **Static** to set the following settings manually: IPv6 address, Subnet Prefix Length, Default Gateway, Primary DNS Server, and Secondary DNS Server. Other possible settings are: • **Stateless Address Autoconfiguration (SLAAC)**: An IPv6 address is automatically generated based on the prefix being advertised on the connected network. • **Statefull (DHCPv6)**: IPv6 address, DNS servers and DNS search list will be obtained from router.
Address/prefix (Optional)	You can enter a prefix (Static IPv6 address with an optional prefix length). Address and prefix length must be separated by: /
Default gateway (Optional)	Enter IP address of the default gateway. The default gateway serves as an access point to another network.

Field	*Setting*
General Configuration–Ethernet	
VLAN (Optional)	You can enter the VLAN Identifier (VID) according to IEEE 802.1Q specifying the VLAN to which the device belongs. **Note**: If this setting is used, network access from outside the VLAN is no longer possible. The Spectralink IP-DECT/Virtual IP-DECT Server One supports 4094 different VLANs. Possible values: 1-4094
General Configuration–DNS (Domain Name System)	
Hostname (FQDN) (Optional)	The hostname (Fully Qualified Domain Name) will be inserted into the SIP Contact and via headers. The hostname will also be published via DHCP, and if the network infrastructure supports it, the device will be reachable via this hostname. E.g. Example.spectralink.com
Search Domain (Optional)	Domain name used for resolving host names without a domain.
Primary Server (Optional)	Enter the IP address of the Primary DNS server.
Secondary Server (Optional)	Enter the IP address of the Secondary DNS server.
General Configuration–NTP (Network Time Protocol)	
Server (Optional)	Enter the IP address of the NTP server from which the system will obtain the current time.
Time zone (Optional)	Select the wanted time zone. The time zone include daylight saving times.
Posix timezone string (Optional)	Customized time zone setting. The string must be in POSIX time zone format.
General Configuration–UPnP	
Enabled (Optional)	Enabled by default. If enabled, the device is UPnP discoverable. UPnP is an acronym for Universal Plug and Play. If the IP address of the device is unknown (e.g. forgotten or DHCP-assigned), UPnP can be used to easily identify the IP address of the device. **Note**: If **My Network Places** in Windows is setup to show icons for networked UPnP devices, every Spectralink IP-DECT/Virtual IP-DECT Server One, Media resource and Base station will be present in **My Network Places**.
Broadcast announcements (Optional)	Specifies if UPnP announcements are broadcasted. If enabled, the device broadcasts announcements automatically.
General Configuration–Remote syslog	
Host (Optional)	Enter the host or IP address of the remote syslog server. If specified, messages will be sent to the server.
Port	Server port used for remote syslog. Default value: 514
Facility	Remote syslog facilities used for log messages. Default value: Local 0 Refer to RFC5424.
Level	Log level to send via syslog. Possible values: **emergency**, **critical**, **error**, **warning**, **notice**, **info** or **debug**. Default value: Info
Scope (Optional)	Scope of syslog settings.

Field	*Setting*
	If set to **all**, the settings will override any local settings on e.g. connected base stations. If set to **server only**, these settings will only apply to the server. If set to **server and mr**, these settings will only apply to the server and media resource. Default value: all
General Configuration–SNMP	
Enabled (Optional)	If enabled, access to the SNMP is allowed, and the server will respond to SNMP requests.
Community (Optional)	SNMP Community name (public). The server will respond to requests from a manager in this community.
Trap host (Optional)	Address of SNMP trap host to which SNMP traps are sent.
Trap community (Optional)	SNMP trap Community name used for sending traps.
System location (Optional)	Information about the physical location of this host. E.g. telephone closet, 3rd floor
System contact (Optional)	The textual identification of the contact person for this host, together with information about how to contact them.

3 Click **Save**.

Simple Network Management Protocol (SNMP)

The Spectralink IP-DECT product portfolio support the Simple Network Management Protocol (SNMP) version 2c for monitoring system health and performance.

A number of general MIBs are supported by Spectralink IP-DECT/Virtual IP-DECT Server One, Spectralink DECT Media Resources, Spectralink Virtual IP-DECT Media Resources and Spectralink IP-DECT Base Stations. These provide general information e.g. uptime, number of received/transmitted udp datagrams etc.

The following MIBs are implemented on the DECT devices:

- IF
- IP
- IP-FORWARD
- TCP
- EtherLike l SNMPv2 l IPV6
- UDP

In addition to the general information mentioned above, specific Spectralink DECT information is available on the Spectralink IP-DECT/Virtual IP-DECT Server One only. This information is defined in a SPECTRALINK-IPDECT MIB, which includes the following groups of information:

- dectGeneralInfoGroup

  Objects which provide general information about the IP-DECT/Virtual IP-DECT Server One.

- dectGeneralStatisticsGroup

Objects which provide general statistics about the IP-DECT/Virtual IP-DECT Server One.

- dectUserInfoGroup

  Objects which provide information about users on the IP-DECT/Virtual IP-DECT Server One.

- dectRfpInfoGroup

  Objects which provide information about base stations (RFP) configured on the IP-DECT/Virtual IP-DECT Server One.

- dectMediaResourceInfoGroup

  Objects which provide information about media resources configured on the IP-DECT/Virtual IP-DECT Server One.

- dectNotificationsGroup

  Notifications that are generated by the IP-DECT/Virtual IP-DECT Server One.

SNMP along with the associated Management Information Base (MIB), encourage trap-directed notification. The SPECTRALINK-IPDECT MIB includes a number of traps, also called notifications. One example of a notification is "Connection to a base station is lost", another example is "Base station lost DECT synchronization". Please refer to the SPECTRALINK-IPDECT MIB document (available at http://support.spectralink.com/products) for more details on the information available via SNMP.

To Configure SNMP Settings

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

2 On the **General Configuration** page, enter the following data:

Field	*Setting*
General Configuration–SNMP	
Enabled (Optional)	If enabled, access to the SNMP is allowed, and the server will respond to SNMP requests.
Community (Optional)	SNMP Community name (public). The server will respond to requests from a manager in this community.
Trap host (Optional)	Address of SNMP trap host to which SNMP traps are sent.
Trap community (Optional)	SNMP trap Community name used for sending traps.
System location (Optional)	Information about the physical location of this host. E.g. telephone closet, 3rd floor
System contact (Optional)	The textual identification of the contact person for this host, together with information about how to contact them.

3 Click **Save**.

Advanced Mobile Intelligence for Enterprises (AMiE)

The IP-DECT Servers are now able to connect and communicate with AMiE for IP-DECT (Advanced Mobile Intelligence for Enterprises). AMiE is a Centralized Administration and

Performance Monitoring platform for IP-DECT that monitors and administers and configures all your Spectralink IP- DECT/Virtual IP-DECT Server One in the cloud.

You must acquire a license for AMiE and registration of your servers on AMiE.

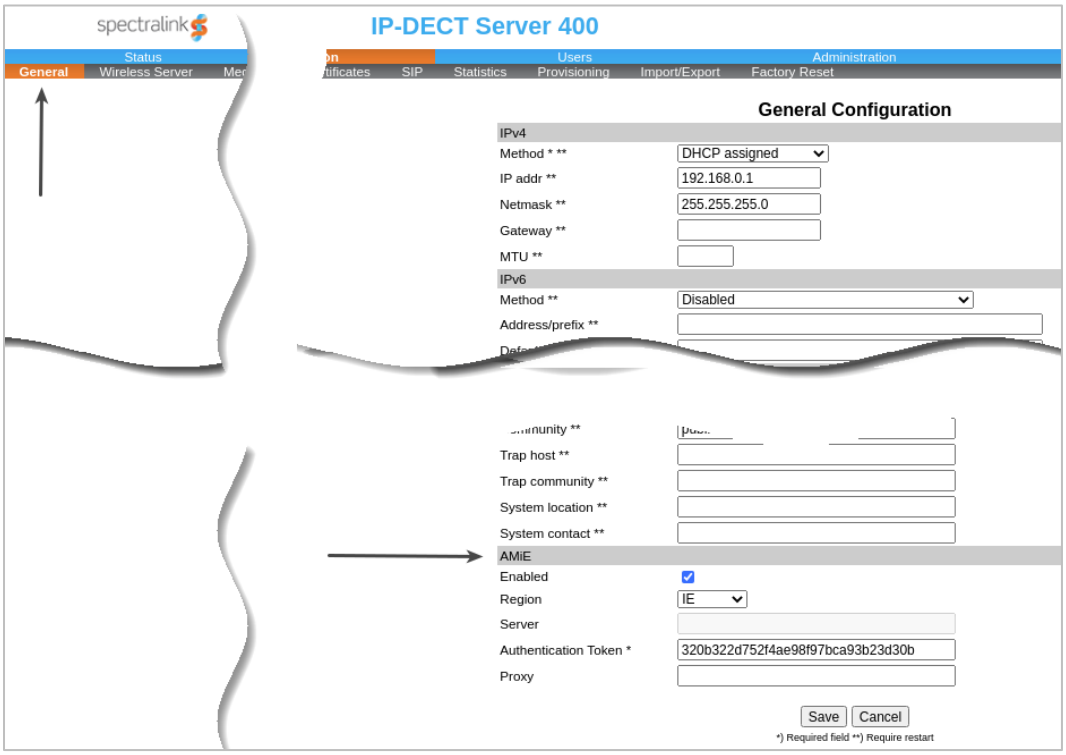
Before being able to connect an IP-DECT Server to AMiE, the IP-DECT Server must be registered in AMiE. Once the IP-DECT Server is registered within AMiE, the connection can be configured from AMiE> Configuration> General, under the category.

Admin Tip

AMiE support for IP-DECT Servers is NOT backward compatible. Servers must be installed with firmware version 2020R3 or newer to connect to AMiE.

To Configure AMiE Settings

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



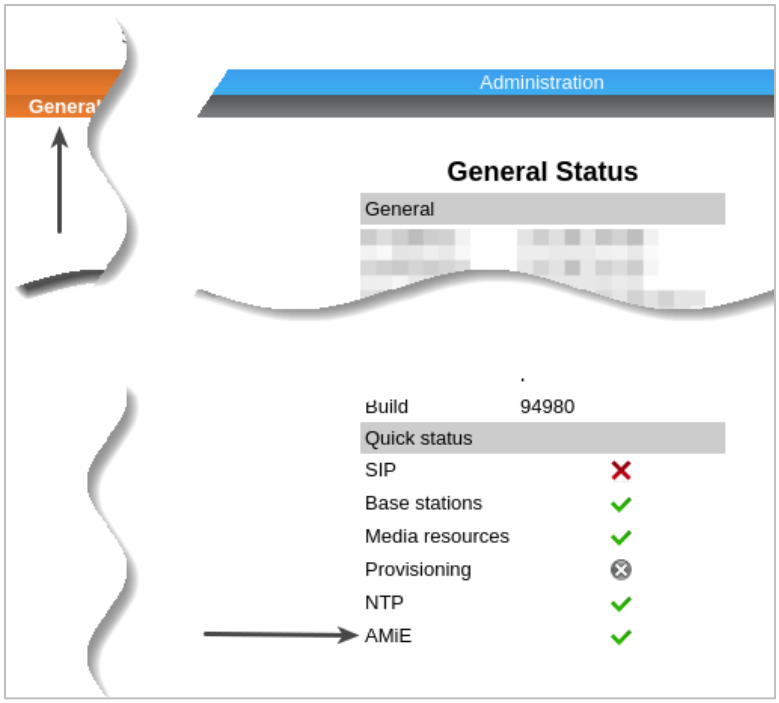
2 On the **General Configuration** page, enter the following data:

Field	*Setting*
General Configuration–AMiE	
Enabled, (Optional)	If enabled, you can establish connection to AMiE (if an AMiE License is acquired and the server is registered on AMiE).
Region, (Optional)	AMiE regions to connect to. The values available depends on the registration information defined for the server in AMiE. Possible values: **DE**, **UK**, **US**, **Custom** Default value: DE
Server, (Optional)	AMiE custom server name.

Field	*Setting*
	Note: The field **Region** must be set to **Custom** to be able to define a custom server name.
Authentication, Token	Enter token to be used to authenticating to AMiE. The authentication token is defined in AMiE when registering the server, and it must be used to configure the server for AMiE integration. Contact your system administrator for more information.
Proxy, (Optional)	You can use a HTTP proxy when connecting to AMiE.

3 Click Save

4 Once the connection between AMiE and the IP-DECT Server has been established, a green checkmark with the text "AMiE" can be found under Status> General> Quick Status.



Note: Getting started with AMiE

For more information on AMiE and how to get started, please see: https://www.spectralink.com/products/mobile-device-management-intelligence/amie/

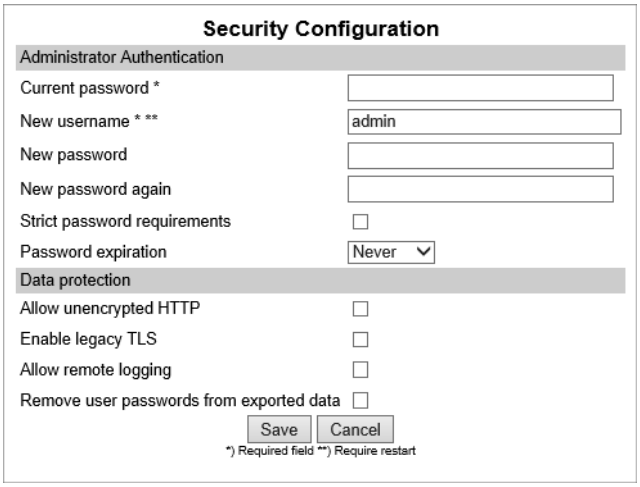
Configuring Security Settings and Changing System Password

Spectralink recommends changing the password for the devices. To change the password and other security settings from the web-based Administration Page of the different devices (server, base stations and media resources):

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

2 On the **Security Configuration** page, enter the following data:

Field	*Setting*
Security Configuration–Administrator Authentication	
Current password	Enter the current password.
New username	Enter a new username. **Note**: Requires a reboot of the server.
New password (Optional)	Enter a new password.
New password again (Optional)	Enter the new password again to confirm.
Strict password requirements (Optional)	If enabling strict password requirements, the device can be configured to enforce certain security rules and naming conventions. For more information, see Strict Password Requirements. **Note**: Once enabled, this setting can only be disabled by a factory reset (Configuration> Factory Reset) that will remove all configuration and user data.
Password expiration (Optional)	Select when you want the password to expire. Possible values: **Never**, **30 days** or **90 days**. Default value: **Never** **Note**: Once enabled, this setting can only be disabled by a factory reset (**Configuration**> **Factory Reset**) that will remove all configuration and user data.
Security Configuration–Data protection	
Allow unencrypted HTTP (Optional)	HTTPS is forced by default. If enabled, HTTP support is supported instead of HTTPS. **Note**: Enabling unencrypted HTTP can cause passwords and other sensitive data to be transmitted in clear text on the network.
Enable legacy TLS (Optional)	If enabled, TLS versions 1.0 and 1.1, certificates signed with the SHA-1 algorithm and CBC based ciphers are supported. **Note**: Enabling legacy TLS is required for security and interoperability with some older browsers and call handing platforms.
Allow remote logging (Optional)	If enabled, remote logging is allowed. Remote logging allows for Spectralink debug tools to extract debug information from the unit.
Remove user passwords from exported data (Optional)	If enabled, users passwords are prevented from being included when data are exported from the Spectralink IPDECT/ Virtual IP-DECT Server One, e.g. when exporting the user list to XML files or CSV files. **Note**: Enabling this will exclude the user database from full system backups. **Note**: Once enabled, this setting can only be disabled by a factory reset (**Configuration**> **Factory Reset**) that will remove all configuration and user data.



3 Click **Save**.

4 Click **OK** to confirm.

5 Click **Reboot now** or **Reboot when idle**, if you have changed the username.

Note:

For security reasons, you can disable the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One/Spectralink IP-DECT Base Station, so that it cannot be accessed from a browser.

For more information, see Disabling Web-Based Administration Page.

Strict Password Requirements

When using strict password requirements, the password of the web-based Administration Page must meet the following requirements:

- Minimum length of 8 characters
- Must contain characters from at least two of the following classes: upper case letters, lower case letters, numbers and special characters
- Must not be simple or dictionary-based words
- Must be different from the last three passwords
- Must not contain more than two successive identical characters

Configuring SIP and IP-PBX Settings

You can configure general SIP settings, authentication information, DTMF signaling, message waiting indication and media for the IP-PBX through the web-based Administration Page.

This section describes how to configure general SIP settings and register for SIP.

For more information about IP-PBX specific settings, see the relevant Interoperability Guides.

To Configure SIP Settings

To configure SIP settings from the web-based Administration Page:

1. Click **Configuration**, and then click **SIP**.
2. On the **SIP Configuration** page, enter the following data:

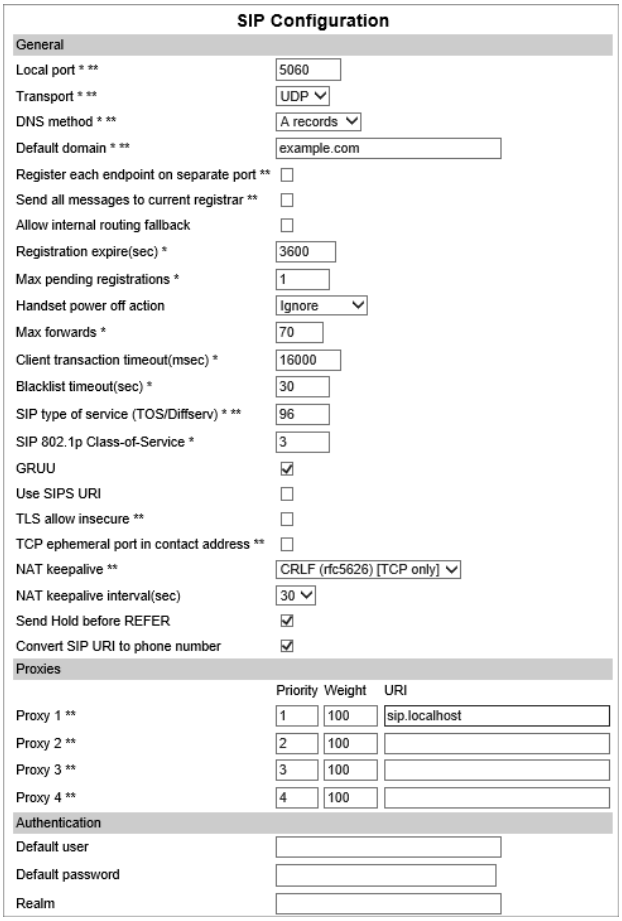
Field	*Setting*
SIP Configuration–General	
Local port	Enter the local port number. The local port is the port on which the Spectralink IPDECT/Virtual IP-DECT Server One listens for incoming SIPsignalling. The default local port number is 5060.
Transport	Transport mechanism used for SIP messages. Possible values: **UDP**, **TCP** or **TLS**. **Note**: If TLS is used as SIP Transport Method, it is necessary to import host certificate and CA certificates into the server. For more information, see Configuring Certificates.
DNS method	Used for looking up the destination of SIP messages. Possible values: **A records** or **DNS SRV**.
Default domain	Used for SIP registration. Enter the name of the domain. **Note**: If no user specific domain is configured under a specific user, the handsets registered on the Spectralink IP-DECT/Virtual IP-DECT Server One will use the default domain as the domain part of the SIP URI; e.g. John Doe <sip:1234@example.org> If only one SIP PBX is used and no domain is available, enter the IP address of PBX here.
Register each endpoint on separate port (Optional)	If enabled, separate local ports for each endpoint are used, instead of the global local port.
Send all messages to current registrar (Optional)	If enabled, all non-REGISTER requests to the current registrar will be sent, when more proxies are available.
Allow internal routing fallback	**Allow internal routing fallback** must be enabled if secondary username is defined. See Configuration–SIP.
Registration expire(sec)	The maximum time between re-registrations. The registrar can signal a shorter time-out. Default value: 3600 sec
Max pending registrations	The maximum amount of pending SIP registrations allowed. The setting can range from 1 to 100 simultaneous SIP registrations. Default value: 1 To increase SIP registration speed, you can increase the value for faster registration handling (system dependent).
Handset power off action (Optional)	Action performed when a handset is turned off. Possible values: **Ignore** or **De-register**. If **De-register** is selected, the handset will de-register when turned off. Default value: Ignore
Max forwards	The maximum number of proxies outgoing messages are allowed to traverse. Default value: 70

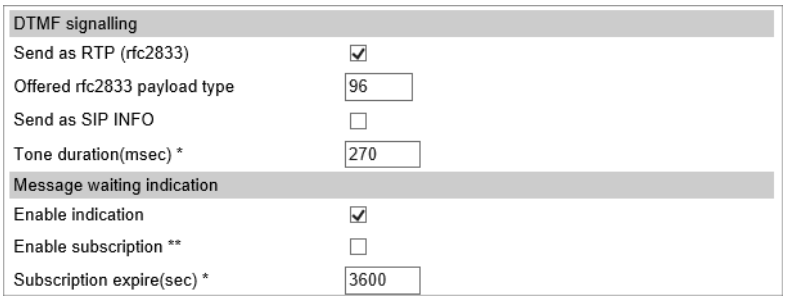
Field	*Setting*
Client transaction timeout (msec)	Controls timer B and F as specified in RFC 3261. Increase this to eliminate time out errors or decrease it to reduce fail over time. Default value: 16000 msec
Blacklist timeout (sec)	Controls the timeout duration for a SIP server to be blacklisted, after losing connection to the server. After leaving the blacklist, the server will reattempt to establish connection. The setting can be set in the range of 5 sec to 600 sec. Default value: 30 sec **Note**: Instead of being a strict timeout, the timeout is considered loose. This means that the setting guarantees that at least the specified time will elapse before trying to reconnect. Thus, more time may elapse, depending on the activeness of the server, as the timeout is checked at given server SIP activities.
SIP type of service (TOS/Diffserv)	TOS/Diffserv used for SIP signaling. Entered in decimal. Default value: 96 (AF–Assured Forwarding)
SIP 802.1p Class-of-Service	This is the 802.1p PCP and must be between 0 and 7. The setting requires VLAN tagging. Default value: 3
GRUU (Optional)	If enabled, Globally Routable User Agent URIs are supported. Default value: Enabled
Use SIPS URI (Optional)	Normally, SIP communication on a TLS connection uses the SIPS: URI scheme. Disabling this option causes the Wireless Server to use the SIP: URI scheme with a transport=tls parameter for TLS connections. Default value: Disabled
TLS allow insecure (Optional)	By default, UDP and TCP transports are disabled when TLS transport is the default. If this setting is enabled, UDP and TCP are allowed as fallback if TLS fails. Default value: Disabled
TCP ephemeral port in contact address (Optional)	If enabled, the TCP ephemeral port (the local TCP port of the outgoing connection) to the contact header, used in outgoing SIP messages, is added.
NAT keepalive (Optional)	If enabled, the Spectralink IP-DECT/Virtual IP-DECT Server One sends UDP packets periodically to ensure that NAT translation continues. If not enabled, the port may be closed down for security reasons (as a consequence call will be dropped or disrupted). Possible values: **Disabled**, **CRLF (rfc5626)** or **SIP OPTIONS (rfc3261)**. Default value: CRLF (RFC 5626) **Note**: **CRLF** is only used for TCP transport. **SIP OPTIONS** is used for both UDP and TCP transports. If using UDP transport, then NAT keepalive is disabled unless you select **SIP OPTIONS**.
NAT keepalive interval (sec) (Optional)	If NAT keepalive is enabled, specify the interval at which NAT keepalive packets must be sent. Possible values: **10**, **20** or **30** sec Default value: 30 sec
Send Hold before REFER (Optional)	If enabled, all calls are put on hold before initiating a call transfer using a REFER message. Some call control platforms require this to be disabled, otherwise the transfer target may stay on hold after a transfer has completed. Default value: Enabled

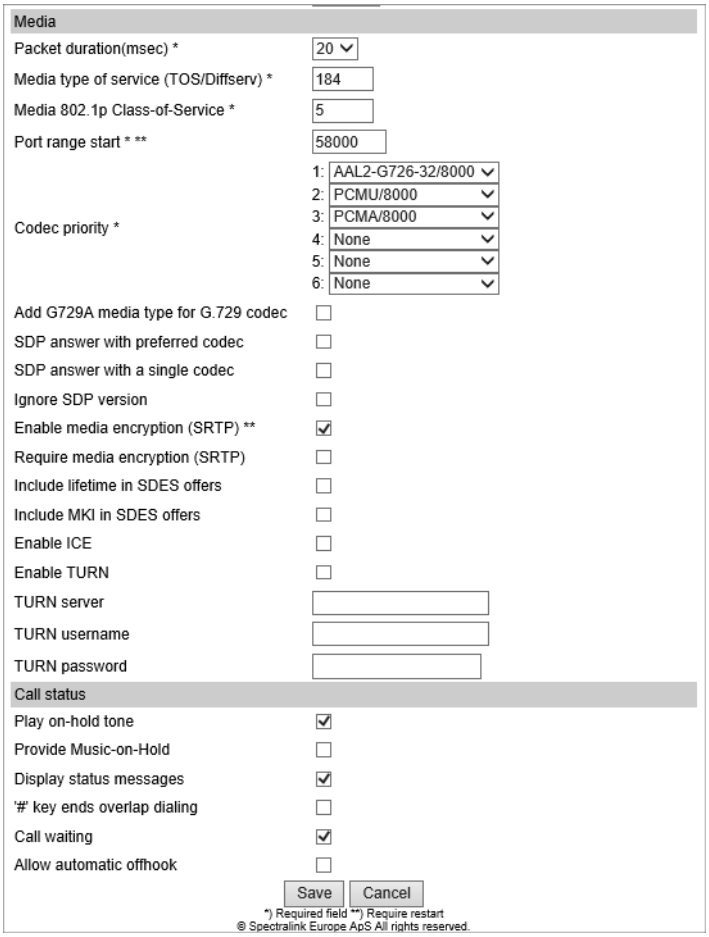
Field	*Setting*
Convert SIP URI to phone number (Optional)	If enabled, the Spectralink IP-DECT/Virtual IP-DECT Server One converts the callers SIP URI received from the PBX to a phone number, e.g. SIP:1234@example.com to “1234”. The phone number is then displayed in a DECT handset as the caller ID instead of the SIP URI. **Note**: Conversion of SIP URIs makes the Call back feature unusable for users on a different domain. Default value: Enabled
SIP Configuration–Proxies	
Proxies (Optional)	**Priority**: The priority for using this proxy. Possible Value 1-4. **Weight**: The weight for using this proxy if more proxies have the same priority. Possible value 1–65.000 higher weight gives priority. Default value: 100 **URI**: The URI or IP address of the proxy
SIP Configuration–Authentication	
Default user (Optional)	Default username used for SIP authentication. **Note**: If no handset specific authentication username/-password is configured, handsets registered on the Spectralink IP-DECT/Virtual IP-DECT Server One will use the default username/password.
Default password (Optional)	Enter password.
Realm (Optional)	The realm presented by the proxy when requesting authentication. If this field is non-empty, authentication passwords will be encrypted. **Note**: When the realm is changed, all stored SIP passwords will be invalid.
SIP Configuration–DTMF signaling	
Send as RTP (Optional)	If enabled, keypad signaling will be sent as RTP event codes.
Offered RFC2833 payload type (Optional)	Payload type for RFC2833 in SDP offers. Default value: 96
Send as SIP INFO (Optional)	If enabled, keypad signaling will be sent as SIP INFO messages.
Tone duration (msec)	Enter the time length of the tone in milliseconds. Default value: 270 msec
SIP Configuration–Message waiting indication	
Enable indication (Optional)	If enabled, MWI is displayed in the handset.
Enable subscription (Optional)	If enabled, you can subscribe to MWI indications from the SIP proxy.
Subscription expire (sec)	Enter the number of seconds before MWI subscription will be renewed. Default value: 3600 sec
SIP Configuration–Media	
Packet duration (msec)	Packet duration for transmitted RTP Packets. Possible values: **10**, **20** or **40** msec
Media type of service (TOS/Diffserv)	TOS/Diffserv used for RTP (Media) signaling entered in decimal. Default value: 184 (EF–Expedited Forwarding)
Media 802.1p Class-of-Service	This is the 802.1p PCP and must be between 0 and 7. The setting requires VLAN tagging. Default value: 5
Port range start	Port range start for local RTP ports.

Field	*Setting*
	Default value: 58000
Codec priority	Define the priorities of codecs. Possible values: **PCMU**, **PCMA**, **G.726** or **G.729**.
Add G729A media type for G.729 codec (Optional)	If enabled, the Spectralink IP-DECT/Virtual IP-DECT Server One will use G.729A/8000 as the media type for the G.729 codec in addition to the standard G.729/8000. This allows interoperability with endpoints that uses the incorrect G.729A/8000 value. Default value: Disabled
SDP answer with preferred codec (Optional)	Specifies if the media handling should ignore the remote SDP offer codec priorities.
SDP answer with a single codec (Optional)	Specifies if the media handling should provide only a single codec in SDP answers.
Ignore SDP version (Optional)	Ignore the version of the SDP received from remote endpoints.
Enable media encryption (SRTP) (Optional)	If enabled, external SRTP is supported and optional. It must be negotiated with the remote endpoint. Default value: Enabled **Note**: If not running PCS 20A_ or newer, this field is only visible if a Security (TLS, SRTP) License is loaded.
Require media encryption (SRTP) (Optional)	If enabled, the usage of SRTP is required and SRTP must be negotiated with the remote endpoint. If negotiation of SRTP with the remote endpoint is unsuccessful, call establishment is aborted. Default value: Disabled **Note**: If not running PCS 20A_ or newer, this field is only visible if a Security (TLS, SRTP) License is loaded.
Include lifetime in SDES offers (Optional)	Handles the RFC 4568 SRTP lifetime key parameter in SDP offers. Default value: Disabled **Note**: If not running PCS 20A_ or newer, this field is only visible if a Security (TLS, SRTP) License is loaded.
Include MKI in SDES offers (Optional)	Handles the RFC 4568 SRTP Master Key Index Parameter in SDP offers. Default value: Disabled **Note**: If not running PCS 20A_ or newer, this field is only visible if a Security (TLS, SRTP) License is loaded.
Enable ICE (Optional)	If enabled, support for Interactive Connectivity Establishment (ICE) (RFC 5245) is allowed.
Enable TURN (Optional)	If enabled, support for Traversal Using Relays around NAT (TURN) (RFC 5766) is allowed.
TURN server (Optional)	Enter TURN server address.
TURN username (Optional)	Enter TURN server username. If left blank, the per-user authentication username will be used.
TURN password (Optional)	Enter TURN password. If left blank, the per-user authentication password will be used.
SIP Configuration–Call status	
Play on-hold tone (Optional)	If enabled, on-hold tone is received in remote end when placed on hold. Note: This might conflict with Music-on-Hold.
Provide Music-on-Hold (Optional)	If enabled, Music-on-Hold is played for the remote end.
Display status messages (Optional)	If enabled, call status messages are received in the handset.

Field	*Setting*
'#' key ends overlap dialing (Optional)	If enabled, pressing the # key dials number in overlap dialing.
Call waiting (Optional)	If enabled, call waiting is supported.
Allow automatic offhook (optional)	If enabled, automatic offhook is allowed for intercom features.







3 Click **Save**.

Configuring Wireless Server Settings

You must configure the Spectralink IP-DECT/Virtual IP-DECT Server One to allow for subscription to be able to subscribe handsets. The Spectralink IP-DECT/Virtual IP-DECT Server One supports DECT Security Step A as default. Therefore, subscription is only allowed for 120 sec. after enabling subscription or until a subscription succeeds, unless the parameter Automatically disable subscription allowed is disabled.

For more information, see also DECT Security available from www.dect.org

Note:

The re-keying procedure that is part of the DECT Security Step A is defined in a way that makes it very sensitive to bit error on the radio link. As a consequence, enabling early encryption and re-keying increases the requirements of the DECT deployment and can cause issues with call quality and dropped connections.

On sites, where it is planned to enable DECT Security Step A, it is highly recommended that a site survey is performed with the early encryption and re-keying option set to required.

In a deployment with areas with signal quality issues (e.g. muted and/or dropped calls), enabling early encryption and re-keying can significantly increase the risk of losing an active call in those areas.

Note:

If encryption is enabled, Spectralink DECT Repeaters are not supported.

You must also configure the wireless server in regard to the desired paging method and required base station configuration. For more information, see Configuring Wireless Server Settings.

To Configure Wireless Server Settings

To configure Wireless Server settings from the web-based Administration Page:

1. Click **Configuration**, and then click **Wireless Server**.
2. On the **Wireless Server Configuration** page, enter the following data:

Field	*Setting*
Wireless Server Configuration–DECT	
Subscription allowed (Optional)	If enabled, you can subscribe new handsets to the system. **Note**: Subscription will be disallowed after 120 seconds or when a subscription succeeds. If more time is needed or more handsets must be subscribed, it is necessary to disable the parameter **Automatically disable subscription allowed** below.
Automatically disable subscription allowed (Optional)	If enabled, subscriptions will automatically be disallowed after 120 seconds or when a subscription succeeds. If disabled, subscriptions will be allowed until explicitly disabled. Default value: Enabled **Note**: This feature is part of DECT Security Step A.
Authenticate calls (Optional)	If enabled, each individual DECT call will be authenticated.
Encrypt voice/data (Optional)	Encryption of voice/data packets transmitted via DECT. Possible values: **Disabled**, **Enabled** or **Required**. Default value: Required **Note**: Repeaters do not support encryption. If set to **Required**, the call is ended when handover is established on the repeater.
Early encryption and re-keying (Optional)	If enabled, this enables encryption immediately after connection establishment and regular re-keying until connection termination. Possible values: **Disabled**, **Enabled** or **Required**. Default value: Disabled

Field	*Setting*
	Note: Enabling early encryption may increase connectivity problems in areas with poor coverage. **Note**: Only Spectralink Handsets with firmware PCS 18Da or newer support **Required**. **Note**: This feature is part of DECT Security Step A.
System access code (Optional)	System wide DECT access code. The access code is from 0–8 decimal digits. **Note**: Individual user access code (AC) has precedence over system access code.
Send date and time (Optional)	If enabled, date and time will be sent to the handsets when a call is terminated. Default value: Enabled
System TX power (Optional)	Used for controlling (reducing) the output power of all connected base stations supporting power control. Unless set to default, this will override any base station specific power setting. Default value: Default (250 mW) **Note**: You can define a TX power value for a specific base station (**Administration**> **Base Station**).
Frequency (Optional) (Only visible if Frequency Swap License is loaded)	Radio Region used for DECT communication with handsets. With the Frequency Swap License installed, you can perform frequency swap between handsets. Besides the Frequency Swap License, a special Spectralink DECT Handset 7212 (part no. 02610004) with a special configuration (and compliance to be compatible with frequency swap) is also required. Possible values: • **Europe** (EMEA, Australia & New Zealand) • **South America** • **USA** (USA & Canada) When the frequency of the base stations is changed, handsets lose the signal from the base stations. Then, after a while, the handsets will try to find base stations (with same ARI–System ID) on the other frequency band. The server must be restarted after changing frequency. **Note**: You can change the frequency setting in the server using OAM-REST API. For more information, see OAM REST API. For more information about frequency swap and the special Spectralink DECT Handset, see Frequency Swap Support.
Allow bearer handovers to repeaters (Optional) (Not relevant to the Spectralink IP-DECT Server 200/400)	If enabled, bearer handover to repeaters is allowed. If disabled, handovers between a repeater and base station must take place as connection handovers. Default value: Enabled **Note**: If Zone-based paging is used, then bearer handover is not allowed, and this setting is overruled. See Configuring Wireless Server Settings.
Wireless Server Configuration–Media resources (Not relevant to the Spectralink IPDECT Server 200/400)	
Allow new (Optional)	If enabled, new media resources are allowed to connect to the server. Default value: Enabled
Add new as active (Optional)	If enabled, new media resources will become active when added. Otherwise they must be activated manually under **Administration**> **Media Resource** > Media Resource page.

Field	*Setting*
	Default value: Disabled **Note**: This must be enabled if setting up a redundant system using internal media resource.
Require encryption (Optional)	If enabled, the connection between the media resource and the Spectralink IP-DECT/Virtual IPDECT Server is required to be encrypted. **Note**: Enabling this, will only allow media resources with firmware PCS 17Fa or newer to connect. Default value: Disabled If not enabled, the connection will be encrypted if the media resource supports encryption.
Wireless Server Configuration–Base stations (Not relevant to the Spectralink IPDECT Server 200)	
Allow new (Optional)	If enabled, new base stations are allowed to connect to the server. Default value: Enabled
Add new as active (Optional)	If enabled, new base stations will become active when added. Otherwise, they must be activated manually under **Administration**> **Base Station**> **Base Station** page. Default value: Disabled.
Require encryption (Optional)	If enabled, the connection between the base station and the Spectralink IP-DECT/Virtual IP-DECT Server One is required to be encrypted. **Note**: Enabling this, will only allow base stations with firmware PCS 17Fa or newer to connect. Default value: Disabled If not enabled, the connection will be encrypted if the base station supports encryption.
Media encryption (SRTP) (Optional)	If enabled, secure RTP for base station audio connections is used. Default value: Disabled **Note**: If not running PCS 20A_ or newer, this field is only visible if a Security (TLS, SRTP) License is loaded.
RFP port range start	Port range start for RFP local RTP ports. Default value: 57000 **Note**: You can change the value in case of conflicting ports.
Paging method (not relevant to Spectralink IP-DECT Server 200/400)	“Paging” is about incoming voice and messaging calls, where the Spectralink IP-DECT/Virtual IP-DECT Server One has to send out an announcement (through the relevant Spectralink IP-DECT Base Stations) asking the handset to choose a base station and start establishing a connection. Possible values: **Default**, **Multicast**, **Site-based paging**, **Zone-based paging**. Default value: Default If having more than 256 base stations connected on a site, default paging is not enough due to the amount of base stations. In this situation, if multicast signaling is supported, multicast is the preferred paging method. Other paging methods are site-based paging and zone-based paging. On a site with heavy voice/messaging load, Spectralink recommends using Zone-based paging instead of using multicast signaling. If **Multicast** is enabled, this will impose multicast support for the network. See Configuring Wireless Server Settings.

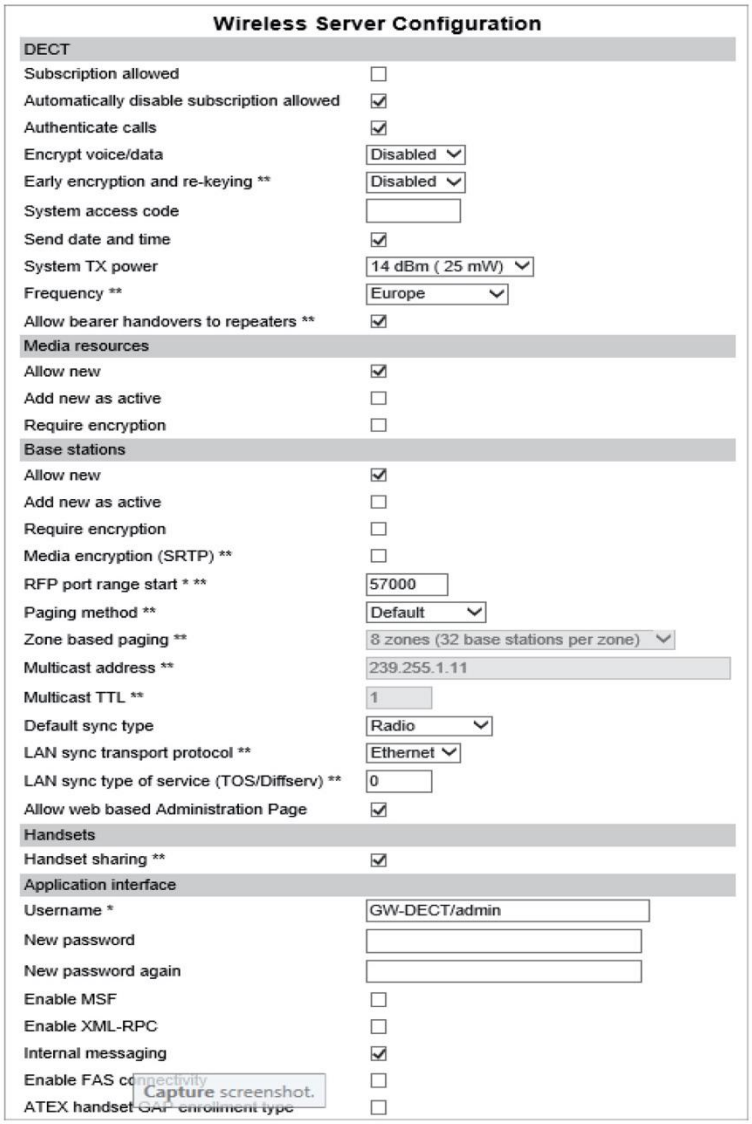
Field	*Setting*
	Note: For more information about deciding which paging method to use, see Spectralink IP-DECT Base Station Configuration Methods–Considerations. Please read the information carefully before continuing and ensure correct deployment of the base stations.
Zone-based paging (Optional)	Zone-based paging is used when grouping base stations into zone in site(s). Not using zone will be substantial in most average systems. **Note**: Zone based paging is built on the DECT Standard for Location Area Level (LAL). **Note**: The field Paging method must be set to Zone-based paging to be able to use zone-based paging. Possible values**: 8 Zone (32 base stations per zone)**, **16 Zone (16 base stations per zone)** or **32 Zone (8 base stations per zone)**. Default value: 8 Zone (32 base stations per zone). For more information about zone-based paging, see Configuring Wireless Server Settings. Please read the information carefully before continuing and ensure correct deployment of the base stations. **Caution**: Assigning RPN's are essential for using zone-based paging, as the RPN decides which zone the Spectralink IP-DECT Base Station will be part of. If changing zone size later on after having configured the base stations and assigned RPN's, then all configuration must be redone. Therefore, consider your system needs carefully before and when deploying. **Note**: Enabling **Zone-based paging** ensures automatic update of handset locations. For more information about configuration of sites and zone, see Configuring Sites (and Zone).
Multicast address (Optional)	Multicast address used for signaling. Default value: 239.255.1.11 Please refer to RFC 2365 and RFC 4291 for details. **Note**: Only used with multicast signaling as paging method.
Multicast TTL (Optional)	The TTL is used to limit the propagation of the multicast packets across routers. Default value: 1 **Note**: The TTL is configurable and you can change the value according to network topology. For more information, see vendor specific documentation. **Note**: Only used with multicast signaling as paging method.
Default sync type (Optional)	This setting controls the default sync type for new base stations connecting to the server. Possible values: **Free running**, **Radio** or **LAN**. **Note**: Selecting **Free running** will configure each base station as a sync master. For more information, see also Synchronization and Deployment Guide. Default value: Radio Note: Multicast address and Multicast TTL are hardcoded, when selecting **LAN**. For more information, see Using Multicast for LAN.
LAN sync transport protocol (Optional)	The protocol transport layer used by PTP for LAN sync. Possible values: **Ethernet**, **IPv4** or **IPv6**. For more information about using LAN synchronization, see LAN-Based Synchronization.

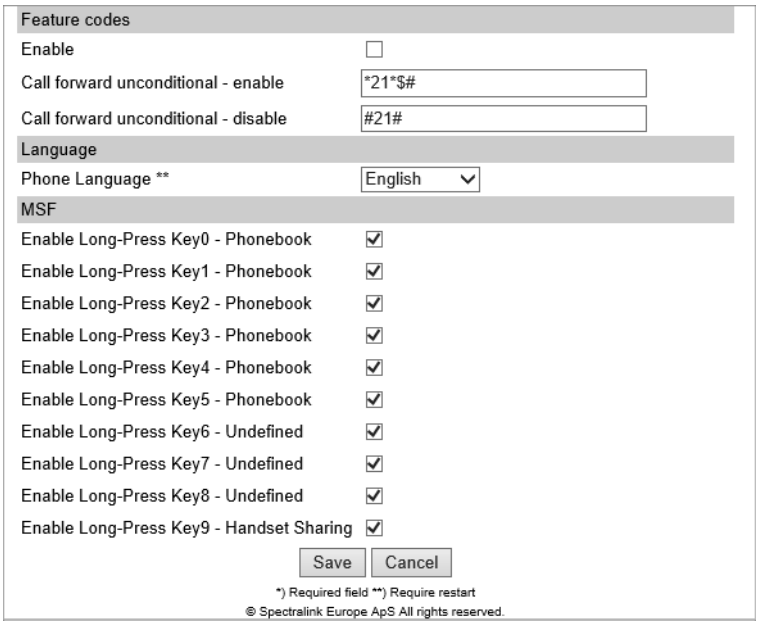
Field	*Setting*
LAN sync type of service (TOS/Diffserv) (Optional)	TOS/DiffServ values can be configured for PTP packets used for LAN sync. The values are entered in decimal. Network priority: Packets with higher TOS/DiffServ have higher priority on the network. 184 = critical (highest priority) 96 = flash 64 = immediate 32 = priority 0 = routine (lowest priority) Default value: 184 (Expedited Forwarding)

Allow web-based Administration Page (Optional)	If disabled, the web-based Administration Page (GUI) of all connected base stations will be disabled.
	Default value: Enabled
	Note: You can disable the web-based Administration Page directly in the configuration file by inserting the following:
	`<rfp>`
	`<allow_gui>false</allow_gui>`
	`</rfp>`
	Change "false" to "true" to enable it.
	For more information, see .

Wireless Server Configuration–Handsets (Not relevant to the Spectralink IP-DECT Server 200)	
Handset sharing (Optional)	Enabled by default when Handset Sharing License is loaded. Disable this, if handset sharing is not to be allowed. For more information about using handset sharing and configuring handset login, see Handset Sharing.
Handset login (Only visible if Lync/SfB + Security (TLS, SRTP) License is loaded)	If enabled, user credentials can be entered on the handset and no user configuration is required on the server. Use long key press 9 to login. (System dependent). For more information, see Configuring Handset Login and handset User Guides.
Wireless Server Configuration–Application interface	
Username	Enter username required to access the application interface. Max. length: 31 characters.
New password (Optional)	Enter password required to access the application interface. Max. length: 31 characters.
New password again (Optional)	Confirm password required to access the application interface.
Enable MSF (Optional)	If enabled, access to the MSF application interface is supported. Default value: Disabled
Enable XML-RPC (Optional)	If enabled, access to the XML-RPC application interface is supported. Default value: Disabled
Internal messaging (Optional)	If enabled, internal messaging to allow handset-to-handset messaging without an external application is supported.
Enable FAS connectivity (Optional) (System dependent and only relevant if using ATEX handset)	If enabled, connectivity to FAS is supported. Default value: Disabled
ATEX handset GAP enrollment type (Optional)	If enabled, GAP as enrollment type is used instead of DOIP enrollment type. Default value: Disabled

Field	*Setting*
(Only relevant if using ATEX handset)	
Wireless Server Configuration–Feature codes	
Enable (Optional)	If enabled, feature codes for controlling features from the handsets can be used.
Call forward unconditional–enable (Optional)	Enable call forward unconditional by dialing this code (***21***), followed by the desired extension ($ = extension) and #. E.g.: ***21*$#** **Note**: You can change the code *21* on the Spectralink IP-DECT/Virtual IP-DECT Server One to fit your standard. For more information, see the relevant documentation available at http://support. spectralink.com/.
Call forward unconditional–disable (Optional)	Disable call forward unconditional by dialing this code (**#21#**).
Wireless Server Configuration–Languages	
Phone Language (Optional)	Language of system messages displayed in handset. Select the desired language from the list.
Wireless Server Configuration–MSF	
Enable Long-Press Key0–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key1-Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key2–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key3–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key4–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key5–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key6–Undefined (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key7–Undefined (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for replacing handsets as an admin rights user. For more information about creating an admin rights user, see Registering Users and Subscribing Handsets. For more information about handset replacement, see Admin Rights User.
Enable Long-Press Key8–Undefined (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press.
Enable Long-Press Key9–Handset Sharing (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for handset sharing. For more information, see Handset Sharing and User Sign-in/Sign-out.


Wireless Server Configuration
DECT
Subscription allowed
Automatically disable subscription allowed
Authenticate calls
Encrypt voice/data
Disabled
Early encryption and re-keying **
Disabled
System access code
Send date and time
System TX power
14 dBm (25 mW)
Frequency **
Europe
Allow bearer handovers to repeaters **
Media resources
Allow new
Add new as active
Require encryption
Base stations
Allow new
Add new as active
Require encryption
Media encryption (SRTP) **
RFP port range start * **
57000
Paging method **
Default
Zone based paging **
8 zones (32 base stations per zone)
Multicast address **
239.255.1.11
Multicast TTL **
1
Default sync type
Radio
LAN sync transport protocol **
Ethernet
LAN sync type of service (TOS/Diffserv) **
0
Allow web based Administration Page
Handsets
Handset sharing **
Application interface
Username *
GW-DECT/admin
New password
New password again
Enable MSF
Enable XML-RPC
Internal messaging
Enable FAS connectivity
Capture screenshot.
ATEX handset GAP enrollment type


Feature codes
Enable
Call forward unconditional - enable
21$#
Call forward unconditional - disable
#21#
Language
Phone Language **
English
MSF
Enable Long-Press Key0 - Phonebook
Enable Long-Press Key1 - Phonebook
Enable Long-Press Key2 - Phonebook
Enable Long-Press Key3 - Phonebook
Enable Long-Press Key4 - Phonebook
Enable Long-Press Key5 - Phonebook
Enable Long-Press Key6 - Undefined
Enable Long-Press Key7 - Undefined
Enable Long-Press Key8 - Undefined
Enable Long-Press Key9 - Handset Sharing
Save
Cancel
*) Required field **) Require restart
© Spectralink Europe ApS All rights reserved.

3 Click **Save**.

Spectralink IP-DECT Base Station Configuration Methods–Considerations

Decisions regarding Spectralink IP-DECT Base Station configuration depend on many factors, e.g:

- system size
- traffic load
- base station density
- location(s)–and physical distance between locations (overlap issues)
- possible use of local media resources
- possible use of multicast signaling
- use of repeaters

To make the correct decisions, you must take into account both system capacity -- including calls (voice and MSF) -- and location(s). Also, to be considered, is the need for local media resources and possible use of multicast signaling. To help you decide how incoming calls must be handled, see Flowchart for Deciding Base Station Configuration. The flowchart refers to the options described below. The numbering of the options is equivalent to the most preferable paging method, starting with number 1.

Following options are available:

Paging Method	*Traffic Load Max. BHCA **	*Sites*	*Local Media Resource*	*Other Limitations*
1) Default	1000 incoming calls	Optional	Optional ***	Max. 256 base stations
2) Multicast	1000 incoming calls	Optional	Optional ***	WAN/LAN Connections
3) Site-based	1000 incoming calls per site	Mandatory	Optional	Max. 256 base stations per physical separated site
4) Zone-based ** (incl. Site-based)	1000 incoming calls per zone	Mandatory	Optional	No use of repeaters (bearer handover)

* BHCA = Busy Hour Call Attempts

** Zone-based paging is built on the DECT Standard for Location Area Level (LAL).

*** Local Media Resources require use of sites.

Note:

If having more than 256 base stations connected on a system, default paging is not enough due to the increased traffic load and higher density of base stations.

Spectralink

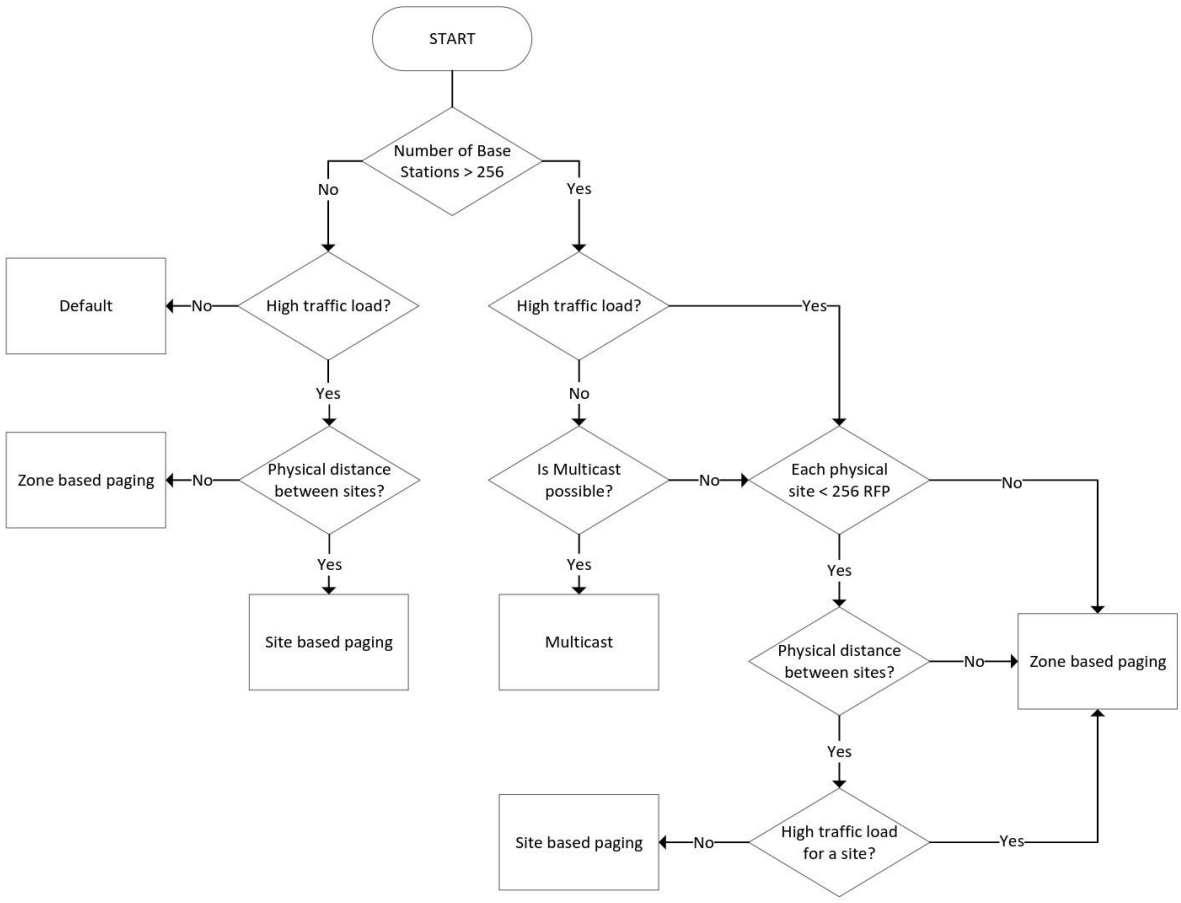
Spectralink recommends using zone-based paging on sites with heavy voice/messaging load.

Note:

The base stations installed on the different sites must not have any overlap with base stations from other sites -- therefore, the physical distance between locations is important. If overlap cannot be avoided, then it is necessary to use zone-based paging.

Flowchart for Deciding Base Station Configuration

Below is a decision tree with questions to answer to determine the best way to configure the Spectralink IP-DECT Base Stations. The flowchart refers to the options (paging methods). See LAN-Based Synchronization. The numbering of the options is equivalent to the most preferable paging method, starting with number 1. The higher the number, the higher the configuration complexity.



Using Default Paging

If having <= 256 base stations connected to a system, default paging is substantial to ensure as simple configuration as possible.

When using default paging, all Spectralink IP-DECT Base Stations are paged when an incoming call arrives.

Optionally, you can create sites when using default paging as well, e.g. if you have more locations and want to create an overview and be able to see which base station belongs to which site, and if using local media resources. All sites will be paged.

For more information about configuring sites and assigning base stations (RPN's) and media resources to sites, see Configuring Sites (and Zone).

Using Multicast Signaling for Paging

If having more than 256 base stations connected on a site, default paging is not enough due to the amount of base stations. In this situation, if multicast signaling is supported, multicast is the preferred paging method. For selecting multicast signaling as paging method, see Configuring Wireless Server Settings.

Optionally, you can create sites when using multicast signaling as well, e.g. if local media resources are needed (assuming no high traffic load).

- Multicast for more than 256 Spectralink IP-DECT Base Stations on a site is routable and configurable.
- TTL is default set to 1 but can be changed according to network topology.
- The multicast IP address is configurable, default value is 239.255.1.11

Note:

The multicast implementation for more than 256 Spectralink IP-DECT Base Stations on a site is designed for the scalability of large networks. Though multicast is the preferred paging method when using more than 256 Spectralink IP-DECT Base Stations on a site, it is also possible to use it on fewer Spectralink IP-DECT Base Stations.

A Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One with more than 256 Spectralink IP-DECT Base Stations does not always need to use Multicast signaling. Multicast signaling can be a problem in some WAN configurations.

When a Spectralink IP-DECT Base Station is connected to a switch port, it will announce itself by IGMPv3 (Internet Group Management Protocol). The Spectralink IP-DECT Base Station will then send a Membership report/Join group.

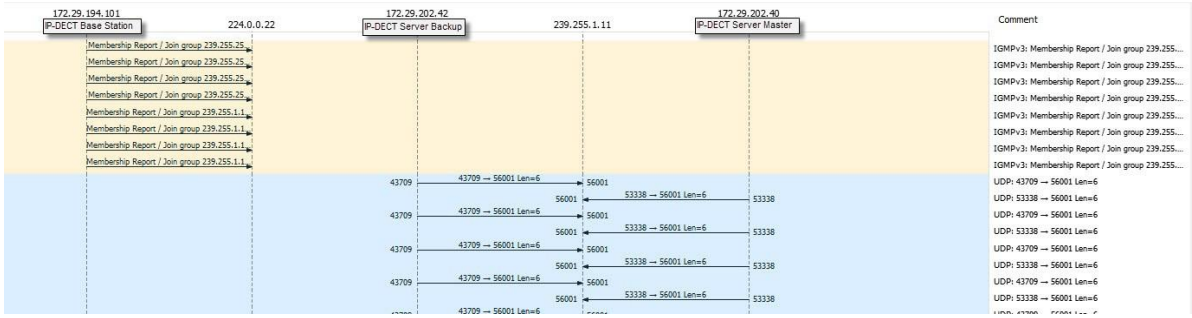
Note:

When using IGMP snooping for managing the multicast traffic in the network infrastructure, it may be required to have an IGMP querier running on the network for proper multicast operation. Please consult the network equipment documentation for more information.

Every 60 second, the Spectralink IP-DECT/Virtual IP-DECT Server One will send a keep alive signal IP- DECT Server -> 239.255.1.11:56001

If the system is redundant, the keep alive will be sent from the backup Spectralink IP-DECT/Virtual IP-DECT Server One as well.

The following image is from a Spectralink IP-DECT Base Station which is being connected to a switch (the traces is done by port mirroring the switch port):



The above image shows a situation with no incoming calls to handsets, but only the keep-alive signaling between server and base station.

When an incoming call is received in the Spectralink IP-DECT/Virtual IP-DECT Server One, the server will send a multicast packet. The multicast packet will contain the PP-ID of the handset. Each Spectralink IP-DECT Base Station will receive this multicast packet, and then send the page through the radio. If the handset is available on a given base, the handset will acknowledge the page. The Spectralink IP-DECT Base Station will then send a unicast message back to the Spectralink IP-DECT/Virtual IP-DECT Server One. Hereafter, the call setup will be transmitted between server and base station as unicast traffic.

Using Site-Based Paging

Spectralink IP-DECT Base Stations can use site-based paging in case you have defined two or more site(s) for your location. For selecting site-based paging as paging method, see Configuring Wireless Server Settings.

By default, the system will allocate a media channel on the media resource with the lowest load at the time a call is initiated. This can, however, lead to network traffic patterns that are not optimal in situations where base stations and media resource are located at different locations and/or in different networks.

To avoid this issue, you can create sites (i.e. a site for each location) and assign the base stations and media resources to them. When allocating a media channel, the system will then prioritize any media resources assigned to the same site as the base station handling the call, avoiding unnecessary RTP traffic over e.g. a WAN connection.

Though assigned to a site, the base stations are not forced to use that particular media resource only, it just takes priority over the other media resources in the system setup. If no media channels can be allocated on media resources in the local site, the system will attempt to allocate another media resource.

Note:

Using site-based paging, incoming calls are only sent to the site, where the handset was last active, which reduce the load on both Spectralink IP-DECT/Virtual IP-DECT Server One and WAN.

Note:

The base stations installed on the different sites must not have any overlap with base stations from other sites–therefore, the physical distance between locations is important. If overlap cannot be avoided, then it is necessary to use zone-based paging.

Using Zone-Based Paging

Note:

Repeaters cannot be used with zone-based paging. Replace existing repeaters with base stations, if any.

Only Spectralink DECT Handset 7202/7212, 7502, 7522/7532, 7622/7642 and 7722/7742 with firmware PCS 19K_ or newer support zone-based paging.

Only Spectralink IP-DECT/Virtual IP-DECT Server One with firmware PCS 19C_ or newer support zone-based paging.

Spectralink IP-DECT Base Stations will use zone-based paging in case you have designed zone for your site(s), defined base station numbers (RPN) and assigned RPN's to a zone. For selecting zone-based paging as paging method, see Configuring Wireless Server Settings.

Note:

Assigning RPN's are essential for using zone-based paging, as the RPN decides which zone the Spectralink IP-DECT Base Station will be part of.

Enabling **Zone-based paging** ensures automatic update of handset locations.

The advantage of dividing sites into zone is that instead of paging all base stations (all sites) when an incoming call arrives, the system can now just page the relevant zone where the handset was last registered. All handsets, that are turned on, can be located in the system. When moving the handset from one zone to another, a location registration occurs (the handset automatically sends a message to the server about position and zone).

Example of Defining Sites, Zone and Assigning Numbers to Base Stations

Limitations are maximum 1024 Spectralink IP-DECT Base Stations on a Spectralink IP-DECT Server 6500/maximum 2048 Spectralink IP-DECT Base Station on a Spectralink Virtual IP-DECT Server One, and maximum 256 Spectralink IP-DECT Base Stations on a site. The Spectralink IP- DECT/Virtual IP-DECT Server One can have up to 256 sites. The sites can have different numbers of base station connected–the total of base stations connected on the overall system cannot exceed the 1024/2048 though.

When defining a site, it is important to determine the maximum size of the location (max. amount of Spectralink IP-DECT Base Stations in each zone). The zone do not need to have the defined maximum amount of Spectralink IP-DECT Base Stations physically installed, but the assigned RPN's to a zone must match the zone size, and the physically installed Spectralink IP-DECT Base Stations have RPN's within that range. Also consider having

room for scaling the system with a couple of more base stations, if it turns out that more base stations are needed in one of the zone.

Zone can be designed for either 32, 16 or 8 Spectralink IP-DECT Base Stations. If one zone needs to contain> 16 base stations, all zone must be designed with 32, regardless that other zone only have < 16 base stations installed.

Caution:

If changing zone size later on after having configured the base stations and assigned RPN's, then all configuration must be redone. Therefore, consider your system needs carefully before and when deploying.

8 Zone (32 base stations per zone)

If defining 8 zone for a site with 256 base stations (selecting **8 Zone** (**32 base stations per zone**) in the Zone-based paging field), the numbering of base stations could be the following:

Site	*Zone*	*Max. Base Stations*	*RPN*
Site 1	Zone 1	32	0–31
	Zone 2	32	32–63
	Zone 3	32	64–95
	Zone 4	32	96–127
	Zone 5	32	128–159
	Zone 6	32	160–191
	Zone 7	32	192–223
	Zone 8	32	224–255

Note: The physical base station number in a zone can be less than 32, but the RPN assigned to it must be within the defined RPN range. If you move the base station to another zone, RPN must be changed accordingly.

16 Zone (16 base stations per zone)

If defining 16 zone for a site with 256 base stations (selecting **16 Zone** (**16 base stations per zone**) in the Zone-based paging field), the numbering of base stations could be the following:

Site	*Zone*	*Max. Base Stations*	*RPN*
Site 1	Zone 1	16	0–15
	Zone 2	16	16–31
	Zone 3	16	32–47
	Zone 4	16	48–63
	Zone 5	16	64–79
	Zone 6	16	80–95
	Zone 7	16	96–111
	Zone 8	16	112–127
	Zone 9	16	128–143
	Zone 10	16	144–159
	Zone 11	16	160–175

Site	*Zone*	*Max. Base Stations*	*RPN*
	Zone 12	16	176–191
	Zone 13	16	192–207
	Zone 14	16	208–223
	Zone 15	16	224–239
	Zone 16	16	240–255

Note: The physical base station number in a zone can be less than 16, but the RPN assigned to it must be within the defined RPN range. If you move the base station to another zone, RPN must be changed accordingly.

32 Zone (8 base stations per zone)

If defining 32 zone for a site with 256 base stations (selecting **32 Zone** (**8 base stations per zone**) in the Zone-based paging field), the numbering of base stations could be the following:

Site	*Zone*	*Max. Base Stations*	*RPN*
Site 1	Zone 1	8	0–7
	Zone 2	8	8–15
	Zone 3	8	16–23
	Zone 4	8	24–31
	Zone 5	8	32–39
	Zone 6	8	40–47
	Zone 7	8	48–55
	Zone 8	8	56–63
	Zone 9	8	64–71
	Zone 10	8	72–79
	Zone 11	8	80–87
	Zone 12	8	88–95
	Zone 13	8	96–103
	Zone 14	8	104–111
	Zone 15	8	112–119
	Zone 16	8	120–127
	Zone 17	8	128–135
	Zone 18	8	136–143
	Zone 19	8	144–151
	Zone 20	8	152–159
	Zone 21	8	160–167
	Zone 22	8	168–175
	Zone 23	8	176–183
	Zone 24	8	184–191
	Zone 25	8	192–199
	Zone 26	8	200–207
	Zone 27	8	208–215
	Zone 28	8	216–223
	Zone 29	8	224–231

Site	*Zone*	*Max. Base Stations*	*RPN*
	Zone 30	8	232–239
	Zone 31	8	240–247
	Zone 32	8	248–255

Note: The physical base station number in a zone can be less than 32, but the RPN assigned to it must be within the defined RPN range. If you move the base station to another zone, RPN must be changed accordingly.

For more information about configuring zone, sites and assigning base stations (RPN's) to zone, see Configuring Sites (and Zone)..

Configuring Media Resource Settings

Note:

Not relevant to the Spectralink IP-DECT Server 200/400.

To use the internal media resource, this must be enabled. To configure media resource settings from the web-based Administration Page:

1. Click **Configuration**, and then click **Media Resource**.
2. On the **Media Resource Configuration** page, enter the following data:

Field	*Setting*
Media Resource Configuration–Media resource	
Enable internal	If enabled, the internal media resource will start up and connect. If disabled, CPU power is increased. Additional media resource will take over then, if installed. Default value: Enabled **Note**: If configuring a system with Spectralink DECT Media Resources or Spectralink Virtual IP-DECT Media Resources, Spectralink recommends disabling the internal media resource of the Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One when: • The system handles more than 20 simultaneous calls. • There are more than 500 users (200 users if using Lync/ Skype for Business).

3. Click **Save**.

Configuring Certificates

To fully secure the communication between the Spectralink IP-DECT/Virtual IP-DECT Server One and other entities, a host key, a host certificate and a certificate authority (CA) certificate list must be present in the Spectralink IP-DECT/Virtual IP-DECT Server One.

The CA certificate list is used when utilizing these features:

- TLS as SIP transport
- Provisioning over HTTPS
- Secure LDAP (LDAPS) phone book
- PIN authentication with Lync/Skype for Business

A host key and certificate are required when utilizing these features:

- Authenticated HTTPS access to the web-based Administration Page
- Trusted server integration with Lync/Skype for Business
- TLS as SIP transport with Cisco Unified CM
- Client authentication with provisioning over HTTPS

The Spectralink IP-DECT/Virtual IP-DECT Server One is delivered with a CA certificate bundle with common public CA certificate. This means, that the Spectralink IP-DECT/Virtual IP-DECT Server One will accept certificates, for example, issued by Verisign out-of-the-box.

In addition to the CA bundle, the web-based Administration Page allows installation of a local CA certificate bundle. If the certificate is generated by a local authority (such as a service provider or the local IT department), you can import a certificate bundle in PEM-format (also known as base 64).

Furthermore, the Spectralink IP-DECT/Virtual IP-DECT Server One supports installing a host certificate that authenticates the identity of the Spectralink IP-DECT/Virtual IP-DECT Server One, e.g. when a browser accesses the web-based Administration Page.

Note:

- If no host certificate is installed on a Spectralink IP-DECT Server 200/400/6500, it will fall back to using the built-in device certificate signed by Spectralink.
- If no host certificate is installed on a Spectralink Virtual IP-DECT Server One, it will automatically generate a self-signed certificate.

The Spectralink IP-DECT/Virtual IP-DECT Server One supports three types of host keys and certificates:

- Locally generated key and self-signed certificate (not recommended)
- Locally generated key and certificate request signed by a CA
- Externally generated key and certificate

Host key and certificate generated externally can be in either a single PKCS#12 format file (.p12 or .pfx extension) or in two individually X.509 PEM formatted files. Both formats can optionally have password protection on the private key. For information on how to generate the key and certificate externally, please consult the documentation of the tools used.

To configure certificates, the following steps are necessary:

1 Create a host key

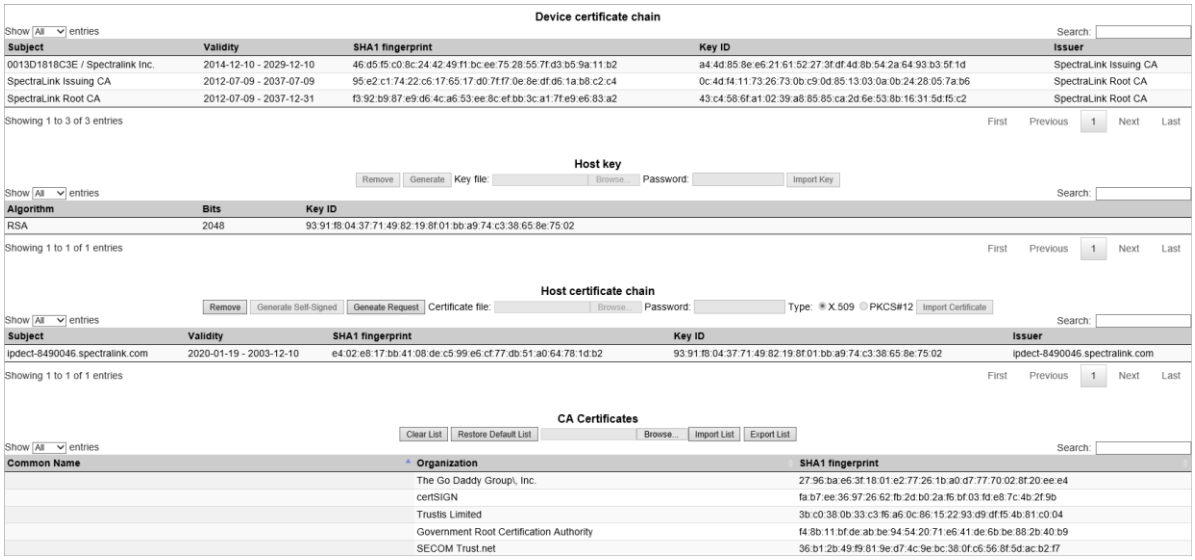
2 Create a host certificate signing request (CSR)

3 Download a root CA certificate (using e.g. Microsoft Active Directory Certificate Services)

4 Sign the host certificate with the CA certificate (using e.g. Microsoft Active Directory Certificate Services)

5 Import the host and CA certificate (+ reboot the server)

Some steps are carried out from the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One under **Configuration**> **Certificates**.



Below is a description of parameters and other important notes, that will be linked to from the different configuration steps.

Field	*Setting*
Certificates–Device certificate chain (Not relevant to Spectralink Virtual IP-DECT Server One)	
	Overview of device certificates. These are non-changeable. Examples of device certificates are: Device certificate, SpectraLink Issuing CA / Spectralink Inc. and SpectraLink Root CA / Spectralink Inc.
Key file	Click either **Generate** or **Browse** to find the relevant host key file (*.pem file). **Note**: Creating a new host key is not necessary when renewing a certificate. Click **Remove**, if you want to remove a host key. You must have removed the host certificate before removing the host key.
Password (Optional)	Enter a password.
	Click **Import Key**, if you want to import the host key.
Certificates–Host certificate chain	
Certificate file	Click Generate Request or Browse to find the relevant host certificate file (*.crt file). If generating a request, the host certificate signing request will be downloaded. **Note**: The generated certificate request will include CommonName and Subject Alternative Name fields containing the host name configured in Configuration> General page. If other fields a required, the host key and certificate must be generated using external tools.

Field	*Setting*
	Note: • If no host certificate is installed on a Spectralink IPDECT Server 200/400/6500, it will fall back to using the built-in device certificate signed by Spectralink. • If no host certificate is installed on a Spectralink Virtual IP-DECT Server One, it will automatically generate a self-signed certificate.
Password (Optional)	Enter a password.
Type	Select between the following certificate types; **X.509** or **PKCS#12**.
	Click **Import Certificate**, if you want to import the certificate. Click **Remove**, if you want to remove a certificate. **Note**: If a certificate already exists, it must be removed before you can import a new one.
Certificates–CA certificates	
	Click **Browse** to find the relevant CA certificate file (*.pem file). E.g. a custom list of CA certificate files. Click **Import List**, if you want to import the list. It is also possible to; remove all CA certificates (**Clear List**), restore default list of public CA certificates (**Restore Default List**), or export the list of CA certificates in PEM format (**Export List**).

Creating a Host Key

The following describes how to create a host key from the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One.

1. Click **Configuration**, and then click **Certificates**.
2. On the **Host key** page, under Key file, click **Generate** to generate a new key. See Configuration–Certificates for more information about Key files.

Note:

Creating a new host key is not necessary when renewing a certificate.

Creating a Host Certificate Signing Request (CSR)

The following describes how to create a host certificate signing request from the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One.

1. Click **Configuration**, and then click **Certificates**.
2. On the **Host certificate chain** page, under Certificate file, click **Generate Request** to send a generate request. See Configuration–Certificates for more information about Certificate files.
3. The host certificate signing request will be downloaded.

Note:

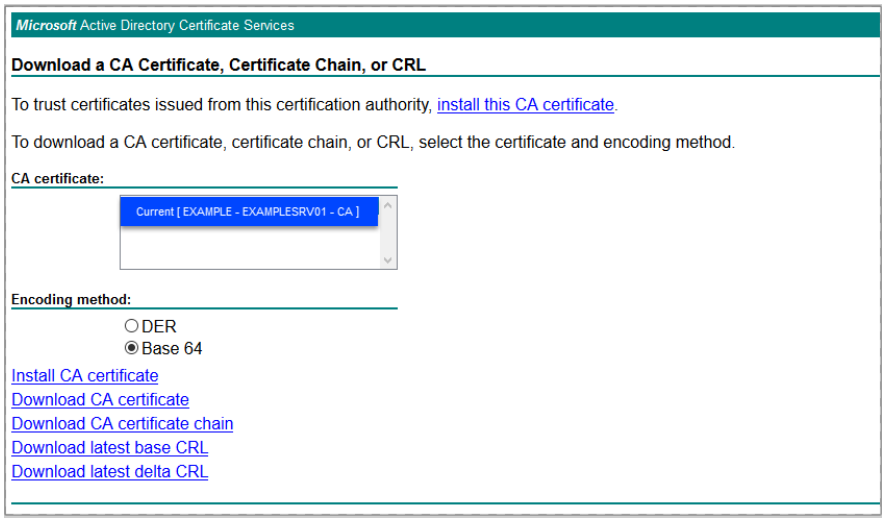
The generated certificate request will include CommonName and Subject Alternative Name fields containing the host name configured in **Configuration**> **General** page. If other fields a required, the host key and certificate must be generated using external tools.

Downloading a Root CA Certificate

If not using the public CA certificates provided with the Spectralink Virtual IP-DECT Server One, it is necessary to download and export a local CA certificate.

The following describes how to export the CA certificate from Microsoft Active Directory Certificate Services. If not using Microsoft Active Directory Certificate Services, please refer to the vendor documentation.

1. Open **Microsoft Active Directory Certificate Services** in your browser. E.g.: https://ca.example.org/certsrv/
2. Select **Download a CA certificate**.

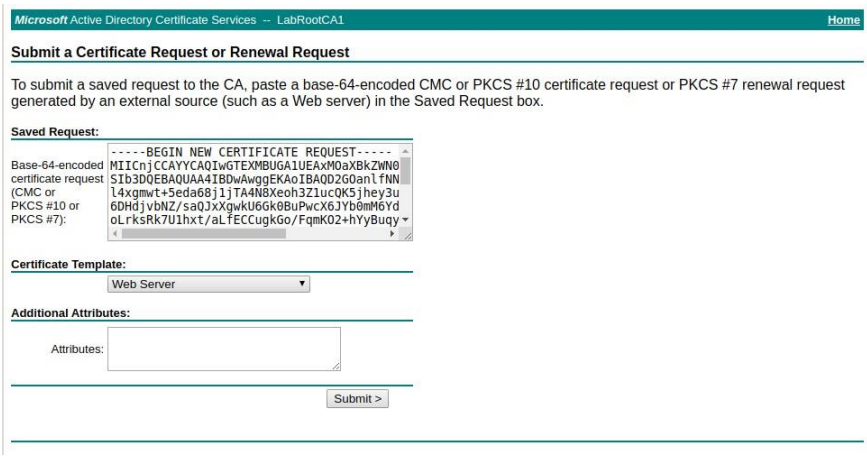


3. Select the current CA certificate.
4. Under **Encoding method**, select **Base 64**.
5. Click **Download CA certificate**.
6. The CA certificate is downloaded to your browser and will be used later in the configuration of the Spectralink IP-DECT/Virtual IP-DECT Server One.

Signing a Host Certificate with the CA Certificate

The following describes how to sign the host certificate from Microsoft Active Directory Certificate Services. If not using Microsoft Active Directory Certificate Services, please refer to the vendor documentation.

1. Open **Microsoft Active Directory Certificate Services** in your browser. E.g.: https://ca.example.org/certsrv/
2. Select **Request a certificate**.
3. Select **Advanced certificate request**.
4. Paste the content of the host certificate request file previously downloaded from the Spectralink IP-DECT/Virtual IP-DECT Server One into the **Saved Request** text box.
5. From the **Certificate Template** list, select **Web Server** or any applicable locally defined template.



6. Click **Submit**.
7. Select **Base 64 encoded**.
8. Click **Download certificate**.
9. The signed host certificate is downloaded to your browser and will be used later in the configuration of the Spectralink IP-DECT/Virtual IP-DECT Server One.

Importing the Host and CA Certificates

The following describes how to import host an CA certificates from the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One.

1. Click **Configuration**, and then click **Certificates**.
2. On the **CA Certificates** page, browse for/import the relevant signed host certificate file.
3. Reboot the server.

For more information about use of TLS and call handlers, see the relevant Interoperability Guides and Call handler documentation.

Configuring Sites (and Zone)

Note:

Not relevant to the Spectralink IP-DECT Server 200/400.

Configuration of sites in order to control assignment of base stations and media resources to specific sites and obtain maximum system performance is necessary when using:

- Default paging and local media resources
- Multicast and local media resources
- Site-based paging
- Zone-based paging
- Local media resources in general regardless of paging method
- Different locations or different networks

By default, the system will allocate a media channel on the media resource with the lowest load at the time a call is initiated. This can, however, lead to network traffic patterns that are not optimal in situations where base stations and media resource are located at different locations and/or in different networks.

To avoid this issue, you can create sites (i.e. a site for each location) and assign the base stations and media resources to them. When allocating a media channel, the system will then prioritize any media resources assigned to the same site as the base station handling the call, avoiding unnecessary RTP traffic over e.g. a WAN connection.

Though assigned to a site, the base stations are not forced to use that particular media resource only, it just takes priority over the other media resources in the system setup. If no media channels can be allocated on media resources in the local site, the system will attempt to allocate another media resource.

Dividing sites into zone is recommended on sites with heavy voice/messaging load. For more information, see. For more information about zone, see Using Zone-Based Paging. Please read the information carefully before continuing and ensure correct deployment of the base stations.

Note:

"Paging" is about incoming voice and messaging calls, where the Spectralink IP-DECT/Virtual IP-DECT Server One has to send out an announcement (through the relevant Spectralink IP-DECT Base Stations) asking the handset to choose a base station and start establishing a connection.

With 2019 release 2 of the Spectralink IP-DECT Server firmware (PCS 19Bc) site-based paging has been implemented, and in 2019 release 2 (and only this release), site-based paging is automatically used, when configuring minimum two sites.

With 2019 release 3 of Spectralink IP-DECT Server firmware (PCS 19C_) zone-based paging has been implemented and must be used on sites where multicast signaling, or site-based paging alone is not enough.

From 2019 release 3 you must select relevant paging method before continuing with the base station configuration, and site-based paging is not automatically used when minimum two sites are configured. If Multicast signaling is supported, this is the preferred method. For more information, see Spectralink IP-DECT Base Station Configuration Methods–Considerations.

Defining a Site for the Media Resource and Base Stations

Using sites, you must as minimum define two site entities. Also, remember to select the desired paging method when configuring the wireless server settings.

Note:

If the wireless server is configured to use zone-based paging, the sites are automatically assigned the desired zone. Default naming of zone are Zone 1, Zone 2, Zone 3 etc. You can rename the zone. For more information, see Renaming Zone.

For selecting zone-based paging as configuration method, see Configuring Wireless Server Settings.

1. Click **Administration**, and then click **Sites**.
2. On the **Sites** page, click **New**.
3. On the **New Site** page, enter the following data:

Field	*Setting*
New site–General	
Name	Enter a name for the site. E.g. Site A, Site B, Site C.

4. Click **Save**.

You can now assign the base stations and media resources to use the relevant sites.

Note:

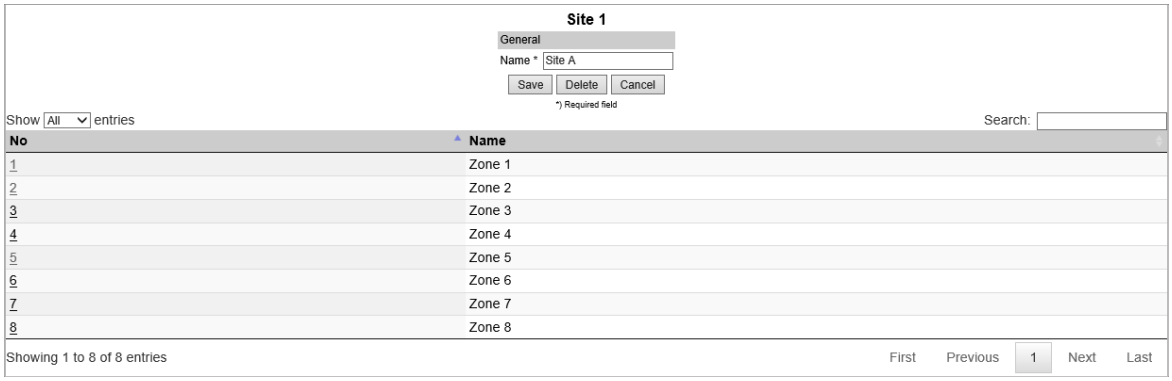
If using zone-based paging, assigning base stations and RPN's are essential, as the RPN decides which zone the Spectralink IP-DECT Base Station will be part of. For more information, see Example of Defining Sites, Zone and Assigning Numbers to Base Stations.

Renaming Zone

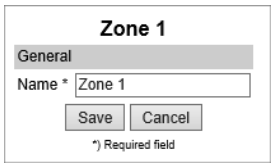
If the wireless server is configured to use zone-based paging, the sites are automatically assigned the desired zone. Default naming of zone are Zone 1, Zone 2, Zone 3 etc. You can rename the zone.

1. Click **Administration**, and then click **Sites**.
2. On the **Sites** page, click on the relevant site.

You can now see a list of all the zone of the selected site.



3. On the **Site** page, click on a zone, and then change the name.



4. Click **Save**.

Assigning Media Resources to Sites

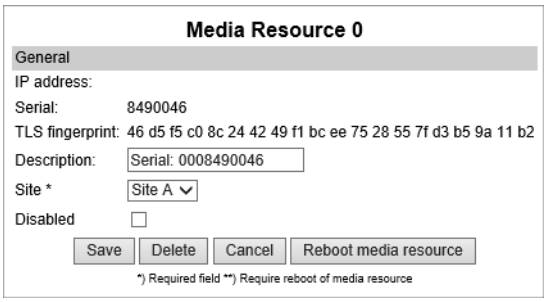
To avoid long delays on local calls, media resources can be allocated to the local sites. It is also possible to have a media resource, that is not assigned to a specific site, this media resource will then be used in case the other assigned media resource is fully allocated.

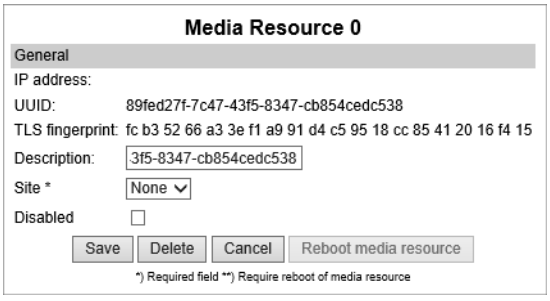
The devices can be both local and remote.

1. Click **Administration**, and then click **Media Resource**.
2. On the **Media Resources** page, click on the relevant media resource.

3 On the **Media Resource** page, under **General** in the **Site** field, select the desired site:

Field	*Setting*
Media Resource–General	
IP address (Read only)	Current IP address of the media resource. **Note**: If the field is empty, the media resource is an internal media resource.
Serial/UUID	Serial number of the Spectralink IP-DECT Server 6500 or UUID of the Spectralink Virtual IP-DECT Server One.
TLS fingerprint	The TLS fingerprint identifies the key associated with the certificate installed in the media resource. This can be used to verify the connected media resource by comparing the TLS fingerprint with the **Key ID** field of the Host Key (web-based Administration Page of the media resource> **Configuration**> **Certificates**> **Host key** page> **Key ID** column). E.g.: 46 d5 f5 c0 8c 24 42 49 f1 bc ee 75 28 55 7f d3 b5 9a 11 b2
Description (Optional)	Enter a description. Spectralink recommends using a description of the physical location.
Site	Default value: None You can define sites for devices that are located at the same location. To assign a site to the media resource, select the relevant site from the list. For information about defining sites, see Defining a Site for the Media Resource and Base Stations.
Disabled (Optional)	If enabled, the media resource will be disabled. **Note**: If **Add new as active** is enabled (**Configuration**> **Wireless Server**> **Media resources**), then this will be unset by default when adding a new media resource.





4 Click **Save**.

Assigning Base Stations to Sites

To make use of the created site entities, these must be assigned to the physical base stations. The devices can be both local and remote.

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

2 On the **Base Stations** page, click on the relevant base station.

Timesaver:

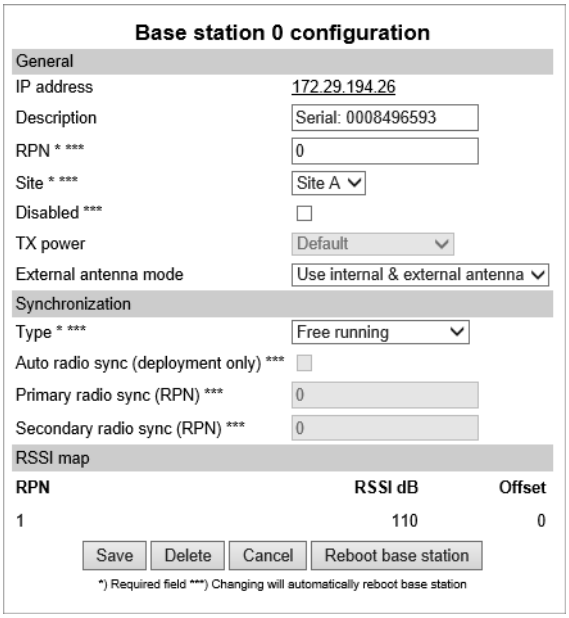
If you have many base stations that must be assigned to the same site, select all the relevant base stations, and then select the relevant site from the **Assign Site** list. When selected, click **OK** to confirm.

The base stations are automatically rebooted.

3 On the **Base Station** page, under **General** in the **Site** field, select the desired site:

Field	*Setting*
Base Station–General	
IP address (Read only)	Current IP address of the base station.
Description (Optional)	Enter a description. Spectralink recommends using a description of the physical location.
RPN	Radio Part Number of the base station. **Note**: If using zone-based paging, assigning base stations and RPN's are essential, as the RPN decides which zone the Spectralink IP-DECT Base Station will be part of. For more information, see Example of Defining Sites, Zone and Assigning Numbers to Base Stations. If using radio-based synchronization in connection with zone-based paging, RPN's must be assigned to the relevant zone before defining synchronization chain.
Site	Default value: None You can define sites for devices that are located at the same location. To assign a site to the base station, select the relevant site from the list. For information about defining sites, see Defining a Site for the Media Resource and Base Stations.
Disabled (Optional)	If enabled, the base station will be disabled. **Note**: If **Add new as active** is enabled (**Configuration**> **Wireless Server**> **Base stations**), then this will be unset by default when adding a new base station.
TX power (Optional)	Used for controlling the output power for this specific base station. Select another value from the list, if you need to change the output power. Default value: Default (250 mW). If Frequency is set to **USA**, the default value is 100 mW. **Note**: If a system TX power other than default is set for the whole system (**Configuration**> **Wireless Server**> **DECT**), that setting will override this setting.
External antenna mode (Optional)	Determines which antenna(s) are used when an external antenna is connected. Possible values: **Use Internal & external antenna**, **Use internal antenna only** or **Use external antenna only**. Default value: Use Internal & external antenna **Note**: This setting is ignored when no external antenna is connected.

Field	*Setting*
	Note: When using external antenna, the range is reduced by up to 50%.
Base Station–Synchronization	
Type	This setting controls the synchronization type used for the specific base station/DECT radio. Possible values: **Free running**, **Radio**, **LAN** or **Radio/LAN Gateway**. Select **Free running**, if you want to configure this base station as sync master. Otherwise select either **Radio**, **LAN** or **Radio/LAN Gateway**, depending on the synchronization method. Default value: Radio **Note**: Automatic configuration of radio synchronization is supported on systems running firmware PCS 20B_ or newer. For more information, see Automatic Configuration of Radio Synchronization. **Note**: To be able to select **LAN** or **Radio/LAN Gateway**, acquisition of a LAN Synchronization License is required. **Note**: System wide settings for synchronization are located under **Configuration**> **Wireless Server**> **Base stations**. For more information, see Synchronization and Deployment Guide.
Auto radio sync (deployment only) (Optional)	If enabled, the base station will be auto synchronized while deploying the system. **Note**: This must only be used while deploying the system.
Primary radio sync (RPN) (Optional)	RPN identifying the base station used for primary radio synchronization.
Secondary radio sync (RPN) (Optional)	RPN identifying the base station used for secondary radio synchronization.
Base Station–RSSI map (Only visible if more than one base station on the system)	
RPN/RSSI dB/Offset	Possible to see the RSSI values of the base stations the selected base station is synchronizing on (Primary sync/ Secondary (Alternative) sync). For more information about RSSI values, see Synchronization and Deployment Guide.



4 Click **Save**.

The base stations are automatically rebooted.

Assigning the Server Address

Note:

Not relevant to the Spectralink IP-DECT Server 200.

After installation, it is necessary to assign a server address to the Spectralink IP-DECT Base Station and Spectralink DECT Media Resource/Spectralink Virtual IP-DECT Media Resource through the web-based Administration Page using either dynamic IP address (DHCP) or static IP address.

Spectralink

The Spectralink IP-DECT Base Station is pre-configured to use DHCP.

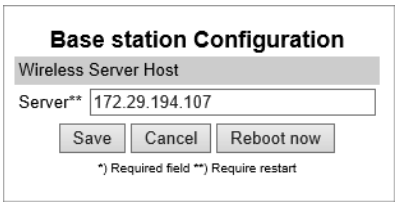
Spectralink recommends that you configure the base station using DHCP. When using DHCP, components should be discovered by UPnP. For more information, see Discovering Spectralink IP-DECT/Virtual IP-DECT Components on the Network.

Manually IP-DECT Server Address Configuration for Base Stations

To configure the server address manually through the web-based Administration Page of the base station:

1. Open a browser and enter the IP address of the base station.
2. Click **Configuration**, and then click **Base Station**.
3. On the **Base station Configuration** page, enter the following data:

Field	*Setting*
Base station Configuration–Wireless Server Host	
Server	Enter the address of the Spectralink IP-DECT/Virtual IP-DECT Server One that the base station must connect to.



4. Click **Save**.
5. Click **Reboot now** to enable the configuration changes.

Manually IP-DECT Server Address Configuration for Media Resources

Note:

Not relevant to the Spectralink IP-DECT Server 400.

To configure the IP-DECT server address manually through the web-based Administration Page of the media resource:

1. Open a browser, and enter the IP address of the media resource.
2. Click **Configuration**, and then click **Media Resource**.
3. On the **Media Resource Configuration** page, enter the following data:

Field	*Setting*
Base station Configuration–Wireless Server Host	
Server	Enter the address of the Spectralink IP-DECT/Virtual IP-DECT Server One that the base station must connect to.

4. Click **Save**.
5. Click **Reboot** to enable the configuration changes.

Chapter 17: Administration of Spectralink IP-DECT Base Stations

Note:

Not relevant to the Spectralink IP-DECT Server 200.

It is necessary to connect base stations to the system and configure synchronization for the Spectralink IP-DECT Base Stations.

In a multi-cell DECT system, the base station radios must be synchronized to each other to achieve the optimum handover experience, when handsets are moving around among the base stations.

The synchronization of the base stations can be determined using one -- or a combination -- of the following synchronization methods (sync. methods):

- Radio based synchronization
- Base stations that synchronize with each other via radio must be within radio coverage of each other.
- LAN-based synchronization (license required)

Note:

Synchronization via LAN and radio can be combined in the same DECT installation. Even when a base station is configured to synchronize via LAN, the base station transmits the signal required for synchronization via radio. Therefore, base stations synchronizing via radio can retrieve their synchronization signal from a base station synchronizing via LAN.

If configured as Radio/LAN Gateway, an IP-DECT Base Station will use an over-the-air synchronization as the source of synchronization and act as a LAN sync master. With this type you can add a LAN synchronized segment of IP-DECT Base Stations to an existing synchronization chain of base stations.

To get an overview or in case of troubleshooting, you can:

- Check the synchronization state of the base station. For more information, see Checking Sync State of Spectralink IP-DECT Base Station.
- Check LAN synchronization performance of the base station. For more information, see Checking LAN Sync Performance of Spectralink IP-DECT Base Station.
- Check for loops in the synchronization chain. For more information, see Checking for Loops.
- Check that base stations are assigned to the correct site. For more information, see Verifying Correct Base Station Assignment to Site.

- Change synchronization type of many/all base stations at the same time. For more information, see Bulk Changing Synchronization Type.

Using Multicast for LAN

Spectralink IP-DECT Base Stations uses IP multicast signaling when configured to use LAN-based synchronization.

Note:

Multicast for LAN has nothing to do with the paging method multicast.

LAN-Based Synchronization

- LAN Synchronization uses the PTP protocol.
- The PTP multicast is non-routable and TTL is static = 1.
- The multicast IP address is fixed and uses 224.0.1.129
- It is not possible to configure any of these parameters

When a Spectralink IP-DECT Base Station is connected to a switch port, it will announce itself by IGMPv3 (Internet Group Management Protocol). The Spectralink IP-DECT Base Station will then send a Membership report/Join group.

Connecting Base Station to System

Base stations can be connected to the system the following ways:

- Manually from the web-based Administration Page of the base station.

  For more information, see Manually IP-DECT Server Address Configuration for Base Stations".

- Automatically when using DHCP and UpNP (recommended).

  For more information, see Discovering Spectralink IP-DECT/Virtual IP-DECT Components on the Network.

Radio Based Synchronization

You define the synchronization chain (sync. chain) of the Spectralink IP-DECT Base Station through the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One. Radio synchronization can be done either manually or automatically.

Note:

Automatic configuration of radio synchronization is only supported on systems running firmware PCS 20B_ or newer.

Note:

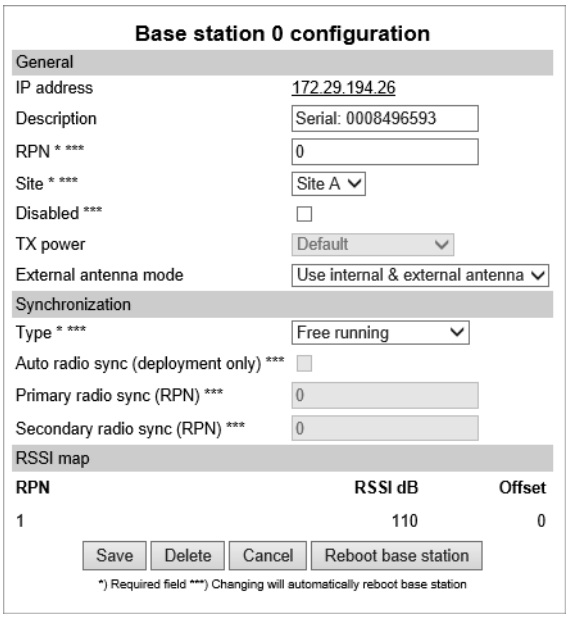
If using zone-based paging, RPN's must be assigned to the relevant zone before synchronization chain is defined.

Manual Configuration of Radio Synchronization

1. Click **Administration**, click **Base Station**, and then click on the relevant base station.
2. On the **Base station configuration** page, enter the following data:

Field	*Setting*
Base Station–General	
IP address (Read only)	Current IP address of the base station.
Description (Optional)	Enter a description. Spectralink recommends using a description of the physical location.
RPN	Radio Part Number of the base station. **Note**: If using zone-based paging, assigning base stations and RPN's are essential, as the RPN decides which zone the Spectralink IP-DECT Base Station will be part of. For more information, see Example of Defining Sites, Zone and Assigning Numbers to Base Stations. If using radio-based synchronization in connection with zone-based paging, RPN's must be assigned to the relevant zone before defining synchronization chain.
Site	Default value: None You can define sites for devices that are located at the same location. To assign a site to the base station, select the relevant site from the list. For information about defining sites, see Defining a Site for the Media Resource and Base Stations.
Disabled (Optional)	If enabled, the base station will be disabled. **Note**: If **Add new as active** is enabled (**Configuration**> **Wireless Server**> **Base stations**), then this will be unset by default when adding a new base station.
TX power (Optional)	Used for controlling the output power for this specific base station. Select another value from the list, if you need to change the output power. Default value: Default (250 mW). If Frequency is set to **USA**, the default value is 100 mW. **Note**: If a system TX power other than default is set for the whole system (**Configuration**> **Wireless Server**> **DECT**), that setting will override this setting.
External antenna mode (Optional)	Determines which antenna(s) are used when an external antenna is connected. Possible values: **Use Internal & external antenna**, **Use internal antenna only** or **Use external antenna only**. Default value: Use Internal & external antenna **Note**: This setting is ignored when no external antenna is connected. **Note**: When using external antenna, the range is reduced by up to 50%.
Base Station–Synchronization	
Type	This setting controls the synchronization type used for the specific base station/DECT radio. Possible values: **Free running**, **Radio**, **LAN** or **Radio/LAN Gateway**.

Field	*Setting*
	Select **Free running**, if you want to configure this base station as sync master. Otherwise select either **Radio**, **LAN** or **Radio/LAN Gateway**, depending on the synchronization method. Default value: Radio **Note**: Automatic configuration of radio synchronization is supported on systems running firmware PCS 20B_ or newer. For more information, see Automatic Configuration of Radio Synchronization. **Note**: To be able to select **LAN** or **Radio/LAN Gateway**, acquisition of a LAN Synchronization License is required. **Note**: System wide settings for synchronization are located under **Configuration**> **Wireless Server**> **Base stations**. For more information, see Synchronization and Deployment Guide.
Auto radio sync (deployment only) (Optional)	If enabled, the base station will be auto synchronized while deploying the system. **Note**: This must only be used while deploying the system.
Primary radio sync (RPN) (Optional)	RPN identifying the base station used for primary radio synchronization.
Secondary radio sync (RPN) (Optional)	RPN identifying the base station used for secondary radio synchronization.
Base Station–RSSI map (Only visible if more than one base station on the system)	
RPN/RSSI dB/Offset	Possible to see the RSSI values of the base stations the selected base station is synchronizing on (Primary sync/Secondary (Alternative) sync). For more information about RSSI values, see Synchronization and Deployment Guide.



3 Click **Save**.

4 Click **Reboot base station**.

Automatic Configuration of Radio Synchronization

For a coverage area with up to 256 base stations, you can perform automatic radio synchronization. If more than 256 base stations within the same coverage area, the radio synchronization must be configured manually. For more information, see Manual Configuration of Radio Synchronization.

When using automatic radio synchronization, the system measures and finds the base station with the highest signal strength (RSSI value) and best signal quality (Q value) to radio synchronize on.

Note:

Automatic configuration of radio synchronization is only supported on systems running firmware PCS 20B_ or newer. Both KIRK IP Base Stations and Spectralink IP-DECT Base Stations support automatic configuration of radio synchronization.

A site survey and deployment must have been conducted. For more information about deployment, see the Synchronization and Deployment Guide.

Be aware, that if using automatic synchronization of base stations, all current base station settings will be overwritten.

Automatic configuration of radio synchronization can only be used in a coverage area with a maximum of 256 base stations and only base stations with sync type Radio can be auto synchronized. More sites can be automatically radio synchronized simultaneously. If using different sites (with up to 256 base stations on each), the sites must be physically separated and not share coverage area.

For more information about configuring sites and assigning base stations to a site, see Configuring Sites (and Zone).

1 Click Administration, and then click Base Station.

Ensure that the base stations are deployed correctly and all have the synchronization type **Radio** before using automatic configuration. For more information, see Bulk Changing Synchronization Type.

2 On the **Base Stations** page, select the relevant group of base stations to be synchronized from the **AutoSync** list.

You can either select **All**, or (if using sites) select a specific site.

- If using sites, with only up to 256 base stations each, all base stations on all sites are automatically radio synchronized, when selecting **All**.

  For more information about configuring sites and assigning base stations to a site, see Configuring Sites (and Zone).

- If not using sites, all base stations (if maximum 256 base stations) within the coverage area are automatically radio synchronized, when selecting **All**.

When selected, click **OK** to confirm.

The system now starts measuring signal strength and signal quality of each base station (and signal strength/quality between base stations) to find the best synchronization

chain. The sync master is also automatically defined as a result of these measurements. Depending on system size, this can take a while (up to 15 minutes).

Caution:

Be aware, that if using automatic synchronization of base stations, all current base station settings will be overwritten. A backup of the Spectralink IP-DECT/Virtual IP-DECT Server One is always recommended, if you want to return to manually created synchronization chain.

Normal operation of the system in the selected coverage area is NOT possible, during auto synchronization, as all base stations will be offline during measurement.

Other coverage areas/sites will not be affected during the auto synchronization.

3 When the system has finished the automatic radio synchronization, the base stations are automatically rebooted.

The result of the measurement/synchronization and overview of each base station's sync source is displayed on the **Base Stations** page, under the **Sync Source** column. Clicking on a specific base station, you can see the RSSI values of the base stations that the selected base station is synchronizing on (**Administration**> **Base Station**> **Base stations**> **Base station configuration**> **RSSI map**). For more information about synchronization and RSSI values, see Synchronization and Deployment Guide.

LAN-Based Synchronization (License Required)

The LAN-based synchronization has several advantages over synchronization via the radio. The configuration is much simpler because no synchronization chains need to be configured and maintained. Furthermore, the system is self-healing as the system can handle if any base station is failing. Also using LAN-based synchronization, the system can be deployed with fewer base stations, as these are no longer required to be in the range of each other.

It may, however, not be the ideal solution in all cases. LAN-based synchronization requires that the base stations involved in a handover are on the same network segment and the network deployment meets a number of strict network quality criteria.

Precision Time Protocol Background

Precision Time Protocol version 2 (PTPv2) is used to synchronize the DECT radios via the LAN. PTPv2 is defined in the standard IEEE 1588-2008 and a brief introduction can be found here: http://en.wikipedia.org/wiki/Precision_Time_Protocol.

PTPv2 is based on a master-slave architecture, where the active master is automatically selected among the base stations. Each network segment will have one active master and the remaining base stations will be slaves. If the current master is failing a new one is automatically selected without disrupting the current synchronization state.

The PTPv2 datagrams are sent as multicast and transported via UDP on IPv4 or IPv6 or as raw Ethernet packets without IP.

The LAN-based synchronization is administrated centrally from the web-based Administration Page of the Spectralink IP-DECT Server. The synchronization itself, however, is handled autonomously by the base stations, and the server is not involved and hence does not need to be on the same network segment.

Configuration Settings through the Web-Based Administration Page

A few configuration settings on the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One are used to control base station synchronization via LAN.

To define system wide settings:

1. Click **Configuration**, and then click **Wireless Server**.
2. On the **Wireless Server configuration** page, under Base stations, set the desired synchronization options in Default sync type, LAN sync transport protocol and LAN sync type of service:

Field	*Setting*
Wireless Server Configuration–DECT	
Subscription allowed (Optional)	If enabled, you can subscribe new handsets to the system. **Note**: Subscription will be disallowed after 120 seconds or when a subscription succeeds. If more time is needed or more handsets must be subscribed, it is necessary to disable the parameter **Automatically disable subscription allowed** below.
Automatically disable subscription allowed (Optional)	If enabled, subscriptions will automatically be disallowed after 120 seconds or when a subscription succeeds. If disabled, subscriptions will be allowed until explicitly disabled. Default value: Enabled **Note**: This feature is part of DECT Security Step A.
Authenticate calls (Optional)	If enabled, each individual DECT call will be authenticated.
Encrypt voice/data (Optional)	Encryption of voice/data packets transmitted via DECT. Possible values: **Disabled**, **Enabled** or **Required**. Default value: Required **Note**: Repeaters do not support encryption. If set to **Required**, the call is ended when handover is established on the repeater.
Early encryption and re-keying (Optional)	If enabled, this enables encryption immediately after connection establishment and regular re-keying until connection termination. Possible values: **Disabled**, **Enabled** or **Required**. Default value: Disabled **Note**: Enabling early encryption may increase connectivity problems in areas with poor coverage. **Note**: Only Spectralink Handsets with firmware PCS 18Da or newer support **Required**. **Note**: This feature is part of DECT Security Step A.
System access code (Optional)	System wide DECT access code. The access code is from 0–8 decimal digits. **Note**: Individual user access code (AC) has precedence over system access code.
Send date and time (Optional)	If enabled, date and time will be sent to the handsets when a call is terminated. Default value: Enabled

Field	*Setting*
System TX power (Optional)	Used for controlling (reducing) the output power of all connected base stations supporting power control. Unless set to default, this will override any base station specific power setting. Default value: Default (250 mW) **Note**: You can define a TX power value for a specific base station (**Administration**> **Base Station**).
Frequency (Optional) (Only visible if Frequency Swap License is loaded)	Radio Region used for DECT communication with handsets. With the Frequency Swap License installed, you can perform frequency swap between handsets. Besides the Frequency Swap License, a special Spectralink DECT Handset 7212 (part no. 02610004) with a special configuration (and compliance to be compatible with frequency swap) is also required. Possible values: • **Europe** (EMEA, Australia & New Zealand) • **South America** • **USA** (USA & Canada) When the frequency of the base stations is changed, handsets lose the signal from the base stations. Then, after a while, the handsets will try to find base stations (with same ARI–System ID) on the other frequency band. The server must be restarted after changing frequency. **Note**: You can change the frequency setting in the server using OAM-REST API. For more information, see OAM REST API. For more information about frequency swap and the special Spectralink DECT Handset, see Frequency Swap Support.
Allow bearer handovers to repeaters(Optional) (Not relevant to the Spectralink IP-DECT Server 200/400)	If enabled, bearer handover to repeaters is allowed. If disabled, handovers between a repeater and base station must take place as connection handovers. Default value: Enabled **Note**: If Zone-based paging is used, then bearer handover is not allowed, and this setting is overruled.
Wireless Server Configuration–Media resources (Not relevant to the Spectralink IPDECT Server 200/400)	
Allow new (Optional)	If enabled, new media resources are allowed to connect to the server. Default value: Enabled
Add new as active (Optional)	If enabled, new media resources will become active when added. Otherwise they must be activated manually under **Administration**> **Media Resource**> **Media Resource** page. Default value: Disabled **Note**: This must be enabled if setting up a redundant system using internal media resource.
Require encryption (Optional)	If enabled, the connection between the media resource and the Spectralink IP-DECT/Virtual IP-DECT Server One is required to be encrypted. **Note**: Enabling this, will only allow media resources with firmware PCS 17Fa or newer to connect. Default value: Disabled If not enabled, the connection will be encrypted if the media resource supports encryption.
Wireless Server Configuration–Base stations (Not relevant to the Spectralink IP-DECT Server 200)	
Allow new (Optional)	If enabled, new base stations are allowed to connect to the server. Default value: Enabled

Field	*Setting*
Add new as active (Optional)	If enabled, new base stations will become active when added. Otherwise, they must be activated manually under **Administration**> **Base Station**> **Base Station** page. Default value: Disabled.
Require encryption (Optional)	If enabled, the connection between the base station and the Spectralink IP-DECT/Virtual IP-DECT Server One is required to be encrypted. **Note**: Enabling this, will only allow base stations with firmware PCS 17Fa or newer to connect. Default value: Disabled If not enabled, the connection will be encrypted if the base station supports encryption.
Media encryption (SRTP) (Optional)	If enabled, secure RTP for base station audio connections is used. Default value: Disabled **Note**: If not running PCS 20A_ or newer, this field is only visible if a Security (TLS, SRTP) License is loaded.
RFP port range start	Port range start for RFP local RTP ports. Default value: 57000 **Note**: You can change the value in case of conflicting ports.
Paging method (not relevant to Spectralink IP-DECT Server 200/400)	“Paging” is about incoming voice and messaging calls, where the Spectralink IP-DECT/Virtual IP-DECT Server One has to send out an announcement (through the relevant Spectralink IP-DECT Base Stations) asking the handset to choose a base station and start establishing a connection. Possible values: **Default**, **Multicast**, **Site-based paging**, **Zone-based paging**. Default value: Default If having more than 256 base stations connected on a site, default paging is not enough due to the amount of base stations. In this situation, if multicast signaling is supported, multicast is the preferred paging method. Other paging methods are site-based paging and zone-based paging. On a site with heavy voice/messaging load, Spectralink recommends using Zone-based paging instead of using multicast signaling. If **Multicast** is enabled, this will impose multicast support for the network. For more information, see Using Multicast Signaling for Paging. **Note**: For more information about deciding which paging method to use, see Spectralink IP-DECT Base Station Configuration Methods–Considerations. Please read the information carefully before continuing and ensure correct deployment of the base stations.
Zone-based paging (Optional)	Zone-based paging is used when grouping base stations into zone in site(s). Not using zone will be substantial in most average systems. **Note**: Zone-based paging is built on the DECT Standard for Location Area Level (LAL). **Note**: The field Paging method must be set to **Zone-based paging** to be able to use zone-based paging. Possible values: **8 Zone (32 base stations per zone)**, **16 Zone (16 base stations per zone)** or **32 Zone (8 base stations per zone)**. Default value: 8 Zone (32 base stations per zone). For more information about zone-based paging, see Spectralink IP-DECT Base Station Configuration Methods–Considerations. Please read the information carefully before continuing and ensure correct deployment of the base stations. **Caution**: Assigning RPN's are essential for using zone-based paging, as the RPN decides which zone the Spectralink IP-DECT Base Station will be part of. If changing zone size later on after having configured the base stations

Field	*Setting*
	and assigned RPN's, then all configuration must be redone. Therefore, consider your system needs carefully before and when deploying. **Note**: Enabling **Zone-based paging** ensures automatic update of handset locations. For more information about configuration of sites and zone, see Configuring Sites (and Zone).
Multicast address (Optional)	Multicast address used for signaling. Default value: 239.255.1.11 Please refer to RFC 2365 and RFC 4291 for details. **Note**: Only used with multicast signaling as paging method.
Multicast TTL (Optional)	The TTL is used to limit the propagation of the multicast packets across routers. Default value: 1 **Note**: The TTL is configurable and you can change the value according to network topology. For more information, see vendor specific documentation. **Note**: Only used with multicast signaling as paging method.
Default sync type (Optional)	This setting controls the default sync type for new base stations connecting to the server. Possible values: **Free running**, **Radio** or **LAN**. **Note**: Selecting **Free running** will configure each base station as a sync master. For more information, see also Synchronization and Deployment Guide. Default value: Radio **Note**: Multicast address and Multicast TTL are hardcoded, when selecting **LAN**. For more information, see Using Multicast for LAN.
LAN sync transport protocol (Optional)	The protocol transport layer used by PTP for LAN sync. Possible values: **Ethernet**, **IPv4** or **IPv6**. For more information about using LAN synchronization, see LAN-Based Synchronization.
LAN sync type of service (TOS/Diffserv) (Optional)	TOS/DiffServ values can be configured for PTP packets used for LAN sync. The values are entered in decimal. Network priority: Packets with higher TOS/DiffServ have higher priority on the network. 184 = critical (highest priority) 96 = flash 64 = immediate 32 = priority 0 = routine (lowest priority) Default value: 184 (Expedited Forwarding)

Allow web-based Administration Page (Optional)	If disabled, the web-based Administration Page (GUI) of all connected base stations will be disabled.
	Default value: Enabled
	Note: You can disable the web-based Administration Page directly in the configuration file by inserting the following:
	`<rfp>`
	`<allow_gui>false</allow_gui>`
	`</rfp>`
	Change "false" to "true" to enable it.
	For more information, see Disabling Web-Based Administration Page.

Wireless Server Configuration–Handsets (Not relevant to the Spectralink IP-DECT Server 200)	
Handset sharing (Optional)	Enabled by default when Handset Sharing License is loaded.

Field	*Setting*
	Disable this, if handset sharing is not to be allowed. For more information about using handset sharing and configuring handset login, see Handset Sharing.
Handset login (Only visible if Lync/SfB + Security (TLS, SRTP) License is loaded)	If enabled, user credentials can be entered on the handset and no user configuration is required on the server. Use long key press 9 to login. (System dependent). For more information, see Configuring Handset Login and Handset User Guides.
Wireless Server Configuration–**Application interface**	
Username	Enter username required to access the application interface. Max. length: 31 characters.
New password (Optional)	Enter password required to access the application interface. Max. length: 31 characters.
New password again (Optional)	Confirm password required to access the application interface.
Enable MSF (Optional)	If enabled, access to the MSF application interface is supported. Default value: Disabled
Enable XML-RPC (Optional)	If enabled, access to the XML-RPC application interface is supported. Default value: Disabled
Internal messaging (Optional)	If enabled, internal messaging to allow handset-to-handset messaging without an external application is supported.
Enable FAS connectivity (Optional) (System dependent and only relevant if using ATEX handset)	If enabled, connectivity to FAS is supported. Default value: Disabled
ATEX handset GAP enrollment type (Optional) (Only relevant if using ATEX handset)	If enabled, GAP as enrollment type is used instead of DOIP enrollment type. Default value: Disabled
Wireless Server Configuration–**Feature codes**	
Enable (Optional)	If enabled, feature codes for controlling features from the handsets can be used.
Call forward unconditional–enable (Optional)	Enable call forward unconditional by dialing this code (***21***), followed by the desired extension ($ = extension) and #. E.g.: ***21*$#** **Note**: You can change the code *21* on the Spectralink IP-DECT/Virtual IP-DECT Server One to fit your standard. For more information, see the relevant documentation available at http://support. spectralink.com/.
Call forward unconditional–disable (Optional)	Disable call forward unconditional by dialing this code (**#21#**).
Wireless Server Configuration–**Languages**	
Phone Language (Optional)	Language of system messages displayed in handset. Select the desired language from the list.
Wireless Server Configuration–**MSF**	
Enable Long-Press Key0–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key1-Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.

Field	*Setting*
Enable Long-Press Key2–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key3–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key4–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key5–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key6–Undefined (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press.
Enable Long-Press Key7–Undefined (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for replacing handsets as an admin rights user. For more information about creating an admin rights user, see Registering Users and Subscribing Handsets. For more information about handset replacement, see Admin Rights User.
Enable Long-Press Key8–Undefined (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press.
Enable Long-Press Key9–Handset Sharing (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for handset sharing. For more information, see Handset Sharing and User Sign-in/Sign-out.

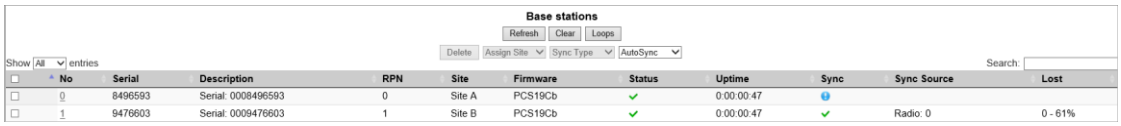
3 Click **Save**.

Checking Sync State of Spectralink IP-DECT Base Station

You can get information about the synchronization state (sync. state) of the base station–the uptime and to which radio unit it synchronizes on through the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One. This is useful when you want to get an overview of the base stations and in case of problem solving.

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

2 On the **Base Stations** page, check the sync. state of the base stations:



- If marked with : Free running (Sync Master)
- If marked with green: Synchronized (Primary Sync Master)
- If marked with : Searching (not in sync with any radio unit)
- If marked with : Unknown (not connected–base station removed from installation)

3 View RFP and RPN numbers.

Note:

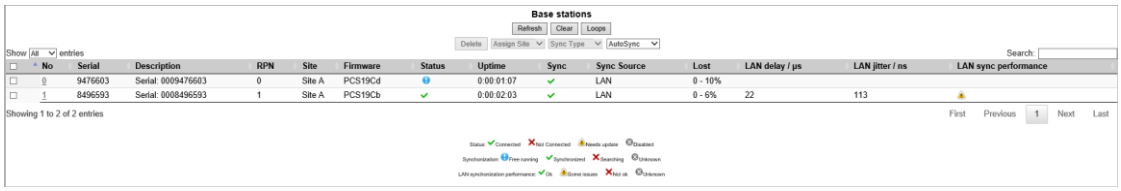
When you click a base station in the list, you can check the RSSI values of the base stations it is synchronizing on (Primary sync/Secondary (Alternative) sync). For more information about synchronization and RSSI values, see Synchronization and Deployment Guide.

Checking LAN Sync Performance of Spectralink IP-DECT Base Station

You can get information about the LAN synchronization performance of the base station -- and see the status of the individual IP-DECT base station LAN synchronization between the LAN sync master and slave sync base stations in the LAN segment -- through the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One. This is very useful, when you want to get a status and a full overview of the overall health and current performance of the LAN synchronization in the network.

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

2 On the **Base Stations** page, check the LAN sync performance of the base stations:



A status icon (–green, –yellow, –red or –grey) is shown under the **LAN sync performance** column, when all of the following conditions are true:

- A LAN Synchronization License is loaded
- **Status** column shows **Connected** icon
- **Sync** column does not show **Free running** icon (the base station is not the Sync Master)
- **Sync Source** column shows **LAN**

Note:

If some base stations never go green, then this could be an indication that your network is not LAN sync optimized, and if you cannot change the setup of the switches in questions, and get green indication on a base station, then you should consider switching the IP-DECT base station to radio synchronization, as this will give you better performance compared to having LAN sync base stations not running optimally.

There are three variables used, that determine which status colour icon is shown:

Variables determining status	Values and Status Colours
Jitter (Deviation in packets) Considered to be OK if it is 500 ns or less	✗: 1001 + ⚠: 501 to 1000 ✓: 0 to 500
Long Term Lucky Rate (Average over uptime of base station) Goes from 0 to 1.0 (0-100%)	✗: 0 – 0.49 ⚠: 0.5 to 0.79 ✓: From 0.8 to 1.0
Rate Correction (Frequency adjustment) Should be as close to zero as possible	✗: Higher than 4500 or less than -4500 ⚠: From 3000 to 4499 or -3000 to -4499 ✓: From -2999 to 2999
If any of the three variables goes from state green (best) to yellow (medium) to red (worst), it will overwrite the other conditions that have a better state.	

Description of status icon colours:

Status Colours	Variables
✗ - Red	• Jitter Jitter is too high (over 1000ns) for this base station and will most likely cause instability on LAN sync. Consider changing QoS on network or use radio synchronization method on base stations (Air). • Lucky Rate Critical packet queuing delays. Packets are experiencing large queuing delays, causing LAN sync not to run optimally. Check QoS on your network or use radio synchronization method on base stations (Air). • Rate Correction Base station frequency adjustment is higher than normal. Try changing Sync Master. It might also be an indication that the base station is defective and needs to be replaced. Contact Support for help on this!

Status Colours	Variables
 - Yellow	• Jitter Jitter is too high (max 500ns) for this base station and can cause instability on LAN sync. Consider changing QoS on network or use radio synchronization method on base stations (Air). • Lucky Rate Packets are experiencing queuing delays, causing LAN Sync to not run optimally. Check QoS on your network or use radio synchronization method on base stations (Air). • Rate AIR Correction Base station frequency adjustment is higher than normal. Try changing Sync Master. It might also be an indication that the base station is defective and needs to be replaced. Contact Support for help on this!
 - Green	• Jitter The LAN synchronization is OK. • Lucky Rate The LAN synchronization is OK. • Rate Correction The LAN synchronization is OK.
 - Grey	• Jitter State of the LAN synchronization is unknown. • Lucky Rate State of the LAN synchronization is unknown. • Rate Correction State of the LAN synchronization is unknown.

Checking for Loops

As part of troubleshooting you can check if loops have accidentally been created in the synchronization chain.

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

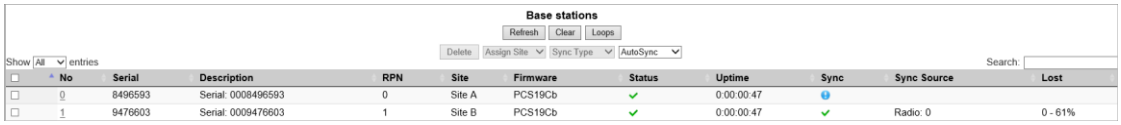
2 Click **Loops**.

If a synchronization loop is being detected, synchronization chain must be reconsidered.

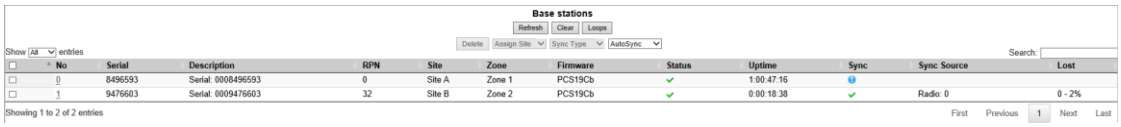
Verifying Correct Base Station Assignment to Site

If using sites, you can check which site a base station is assigned to.

1. Click **Administration**, and then click **Base Station**.
2. On the **Base Stations** page, check if the base station is assigned to the correct site.



If using zone-based paging, a column showing the zone is visible as well.



Bulk Changing Synchronization Type

You can bulk change the synchronization type of a group of base stations, e.g. from **LAN** to **Radio**. This is useful in case you experience problems with your network and LAN synchronization and must change all base stations to radio synchronization to obtain better performance.

Note:

Bulk change of synchronization type is only supported on systems with firmware PCS 20B_ or newer.

1. Click **Administration**, and then click **Base Station**.
2. On the **Base Stations** page, select all the relevant base stations, and then select the relevant synchronization type from the **Sync Type** list. When selected, click **OK** to confirm.

The base stations are automatically rebooted

Chapter 18: Registering Users and Subscribing Handsets

You must register a user and subscribe a handset before you can use it.

When registering users, you enter information about each user's settings (such as; IPEI, username (handset serial number), access code etc.) in the system database.

You can also register a user as an admin rights user with the ability to replace a handset. For more information about replacing a handset as an admin rights user, see Admin Rights User.

When subscribing handset, you subscribe a handset to a registered user with a matching IPEI.

Note:

If the user is not registered in the system database, subscription of the handset is not possible.

Registering a User

To register users, you use the web-based Administration Page of the server.

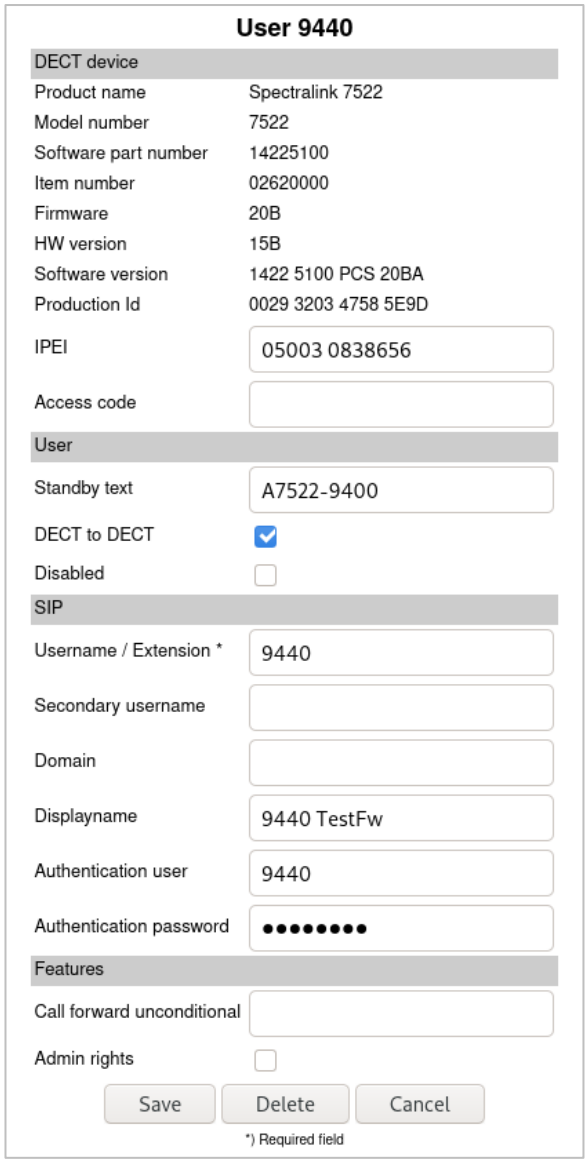
To Register/Create a New User

1. Click **Users**, and then click **List Users**.
2. Click **New** to create a new user.
3. On the **User** page, enter the following data:

Field	*Setting*
User–DECT device	
Product name	After registration of user and subscription of handset, this field will contain information about the handset product name. E.g. Spectralink 7532
Model number	After registration of user and subscription of handset, this field will contain information about the handset's technical model number. E.g. 7532
Software part number	After registration of user and subscription of handset, this field will contain information about the software part number. E.g. 14225100
Firmware	After registration of user and subscription of handset, this field will contain information about the firmware version. E.g. PCS 19K
IPEI (Optional)	If a specific handset is being subscribed for this user, enter the IPEI number of the actual handset (the IPEI number is readable from the label on the product).

Field	*Setting*
	If this is not the case, this field can be left empty and it will autofill when the handsets subscribe. **Note**: A SIP REGISTER will not be sent before there is an IPEI number present. **Note**: Programming of IPEI number into the system database is necessary to enable service to the handset. **Note**: If handset sharing is used, the IPEI label will be a link, that you can click on and link to a device. For more information, see Adding Devices to Server.
Access code (Optional)	Administrators can define a system wide or individual access code as extra wireless security during the subscription process. **Note**: Some 3rd party phOne may need an Access code to register to the Spectralink IP-DECT/Virtual IP-DECT Server One.
Configuration group (Optional)	If using handset configuration, enter the Group ID of the Configuration Group. For more information, see Managing Handset Configuration and Configuration Groups.
User–User	
PIN code (Optional) (Only visible if Handset Sharing License is loaded)	Enter a code in the PIN code field for added security to prevent other users from linking a handset with your user profile. The PIN code associates the user with a handset. For more information, see User Sign-in/Sign-out. See also Lync/Skype for Business Interoperability Guide.
Standby text (Optional)	Enter a standby text. **Note**: Disallowed characters: <>\" A standby text is a fixed label shown in the top left part of the screen on the DECT handset when in idle state. **Note**: This feature is only available if Spectralink DECT handsets are being used. If third-party DECT handsets are being subscribed, this feature is not supported.
DECT to DECT (Optional)	If selected, the user can only make call and receive call from other users that are subscribed to the same IP-DECT setup.
Disabled (Optional)	If enabled, the user is disabled. **Note**: A disabled user cannot make calls from the handset.
User–SIP	
Username/Extension	Must contain information used for SIP registration etc. E.g. the "user" in a SIP URI. **Note**: Allowed characters: a-z, A-Z, 0-9, -_.!~*'()&=+$,;?/
Secondary username (Optional)	Enter a Secondary username. **Note**: Allowed characters: a-z, A-Z, 0-9, -_.!~*'()&=+$,;?/ The Secondary username can be used to make voice calls, if the connection to the SIP PBX is lost. The Secondary username must be globally unique. In some PBXs there is a mapping between username and number (e.g. Username = hz2539jk, Number =1234). If the connection to the SIP PBX is lost, then you can make the mapping internally by defining a Secondary username. **Note**: The feature MUST be used with SIP setting **Allow internal routing fallback** enabled. For more information, see Configuring SIP and IP-PBX Settings.
Domain (Optional)	Enter the domain part of a SIP URI. **Note**: Allowed characters: a-z, A-Z, 0-9, .- E.g. example.org in John Doe<sip:1234@example.org> **Note**: If not configured, the default domain entered under SIP configuration will be used.
Displayname (Optional)	Enter the name of the user (e.g. caller ID).

Field	*Setting*
	Note: Disallowed characters: <>\" E.g. John Doe in John Doe<sip:1234@example.org> **Note**: If Cisco Unified CM (Advanced Features) License is loaded, the Cisco Unified CM will not use this, but it may ease the administration of users within the Spectralink IP-DECT Server.
Authentication user (Optional)	Enter the user ID of the end user. E.g. J**ohnDoe** or **5204**. **Note**: Disallowed characters: <>\" **Note**: The username will override the Default User field under SIP Configuration. Priority: 1. Authentication user set for individual users 2. Authentication user set in server SIP settings 3. Username set for individual users
Authentication password (Optional)	Enter the digest credential of the end user. **Note**: Disallowed characters: <>\" **Note**: The password will override the Default Password field under SIP Configuration.
User–Features	
Call forward unconditional (Optional)	A Call Forward Unconditional (an extension to forward calls to) can be added/removed via the web-based Administration Page. **Note**: Allowed characters: a-z, A-Z, 0-9, -_.!~*'()&=+$,;?/
Admin rights (Optional)	If enabled, the user becomes an admin rights user with the ability to replace a broken handset. For more information about replacing a handset as an admin rights user, see Admin Rights User.



4 Click **Save**.

Subscribing a Spectralink DECT Handset

Subscription of the Spectralink DECT Handset is performed from the menu in the handset.

Note:

You must configure the Spectralink IP-DECT/Virtual IP-DECT Server One to allow for subscription. If the system does not allow subscription, it is not possible to subscribe the handset. For more information, see Configuring Wireless Server Settings.

You subscribe a handset by creating a login (**Menu**> **Settings**> **Advanced**> **Login**> **Create Login: Search**).

For more information, see the relevant Handset User Guides.

Chapter 19: Admin Rights User

A user can be registered as an admin rights user with the ability to replace a handset. For more information, see Registering Users and Subscribing Handsets.

Note:

Only Spectralink DECT Handset 7202/7212, 7522/7532, 7622/7642 and 7722/7742 with firmware PCS 17H_ or newer support the admin rights user feature.

Only Spectralink IP-DECT/Virtual IP-DECT Server One with firmware PCS 20A_ or newer support the admin rights user feature.

If registered as an admin rights user, the handset replacement can be done from the admin rights user's handset in the **Settings**> **Advanced**> **Master handset** menu. If admin rights are given when handset is in use, the handset must be turned off/on again for the **Master handset** menu to appear. You must have access to both the handset to be replaced and new handset in order to do the replacement.

Note:

If you cannot access the feature on your handset, contact your system administrator.

To Replace a Handset

1. Ensure that you have the new handset charged and ready for use.
2. Identify the handset to be replaced. This information must be used when replacing the handset. A handset can be identified in the following ways:
   - Extension (numeric input)
   - Username (alphanumeric input)
   - Secondary username (numeric input)
   - IPEI
3. To invoke the admin rights user (master handset) feature though the menu of the handset, do the following:
   - Press **Menu** to enter main menu.
   - Scroll to **Settings**, and press **Select**.
   - Scroll to **Advanced**, and press **Select**.
   - Scroll to **Master handset**, and press **Select**.

Note:

The admin rights user (master handset) feature can also be invoked by long pressing the '7' key.

Long-press must be enabled in the handset in the **Settings**> **Advanced**> **Long Key** menu. For more information, see Handset User Guides.

Long-press must also be enabled on the server. For more information, see Configuration–Wireless Server.

4 When in the **Master handset** menu (**MSF Menu Select**), do the following to replace a handset:

- Scroll to **Replace handset**, and press **OK**.
- Scroll to either **Extension**, **Username**, **Sec. username** or IPEI, and press **OK**.
- Enter the relevant information for the handset to be replaced, and press **OK**.
- Enter the IPEI of the new handset.
- Press **OK** to replace handset.
- You now receive information about the AC code xxxxx (random generated), that must be used when subscribing the new handset.

  Subscription of the new handset is allowed for 4 minutes.

5 Subscribe the new handset:

- You subscribe a handset by creating a login (**Menu**> **Settings**> **Advanced**> **Login**> **Create Login: Search**).

  Use the AC code that was provided to you earlier in the Master handset menu.
- Press **OK** and subscribe the new handset.

Note:

If the subscription period times out, you can reenter the **Master handset** menu (**MSF Menu Select**), and do the following to allow subscription:

Scroll to **Allow Subs**, and press **OK**.

Within the next 4 minutes it is now possible to subscribe the new handset.

For more information, see the relevant Handset User Guides.

Chapter 20: Handset Management

Some handset management is performed using the web-based Administration Page of the server.

- Management of the handsets, firmware and users can be performed from **web-based Administration Page**> **Users**> **List Users**.

  For more information, see User List Information and Tasks to Perform from User List.

- Import and export of user data can be performed from **web-based Administration Page**> **Users**> **Import/Export**.

  For more information, see Import/Export of Users or Delete Users.

- Management of Handset Configuration Groups and specific configuration for handsets using Configuration Over The Air (COTA) can be performed from **web-based Administration Page**> **Users**> **Handset Configuration**.

Note:

Only Spectralink DECT Handset 7202/7212, 7502, 7522/7532, 7622/7642 and 7722/7742 with firmware PCS 19K_ or newer can be updated using Handset Configuration Over The Air.

Only Spectralink IP-DECT/Virtual IP-DECT Server One with firmware PCS 19C_ or newer support Handset Configuration Over The Air.

Handset Configuration Over The Air is not supported on redundant systems.

For more information, see Managing Handset Configuration and Configuration Groups.

Note:

Handset programming and firmware maintenance can be done using the Handset and Repeater Management Tool. The Handset and Repeater Management Tool can be downloaded from http://support.spectralink.com/products.

For more information, see Handset and Repeater Management Tool User Guide.

Handset firmware can also be updated through provisioning. For more information, see *Provisioning Guide*.

This section provides information about handset management such as:

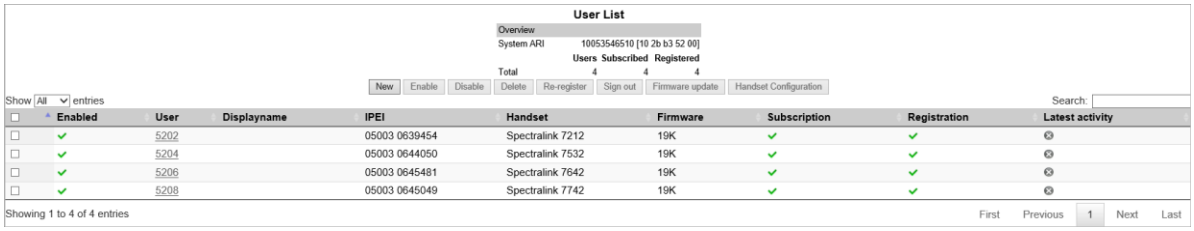
- Viewing handset/user configuration
- Searching for handset/user information
- Deregistering handsets (remove handset from the list)
- Changing user configurations
- Updating handset firmware

- Unsubscribing handsets (remove login)
- Importing handset registration data
- Using Handset Configuration Over The Air (COTA)

User List Information

From the **User List** page you can get an overview of the following:

- System ARI–the system the user is subscribed to.
- Enabled–if user/handset is enabled.
- User–SIP account username/extension
- Display name–name presenting the user in outgoing calls.
- IPEI–IPEI number of handset
- Handset–Handset model
- Firmware–firmware version in handset
- Subscription–indicates if handset is subscribed to a Spectralink IP-DECT/Virtual IP-DECT Server One.
- Registration–indicates if handset is registered to a SIP server.
- Latest activity–last time the server has been in contact with the handset.
  - Location Registration
  - Out of Range
  - Unknown
  - Handset turned off
- Site (only relevant–and visible–if using site-based paging or zone-based paging)–indicates the site where the handset is located.
- Zone (only relevant–and visible–if using zone-based paging)–indicates the zone where the handset is located.
- Nodes (only relevant–and visible–if using redundancy server)–indicates if handset is subscribed on the master server or backup server. For more information, see Design of Redundant Server Solution.



Note:

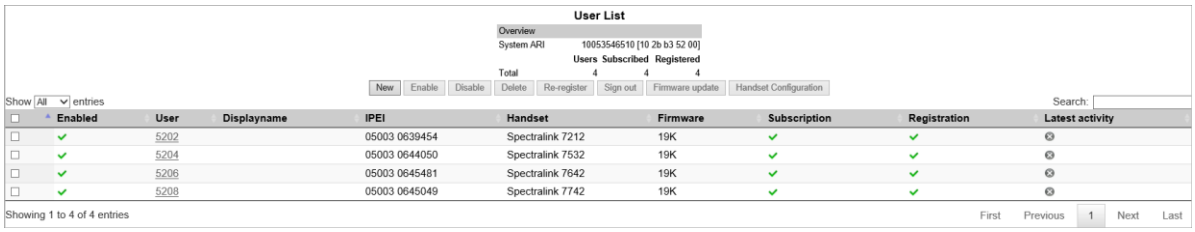
You can sort the information by clicking each header.

You can search for e.g. phone numbers, users, software etc. using the Search field (upper right side).

Tasks to Perform from User List

Selecting one or more users from the list you can do the following:

- view or change handset/user configurations
- get information about which site/zone the handset is in (only visible if using site-based paging or zone-based paging)
- search handset/user information
- enable/disable users
- delete users
- re-register users
- unsubscribe users
- update firmware in the handsets
- deregister a handset
- create handset configuration template (for more information, see Managing Handset Configuration and Configuration Groups)



Note:

You can also create users from the User List. For more information, see Registering a User.

To View or Change Handset/User Configuration

You can view or change all the user configurations of the wireless system through the web-based Administration Page.

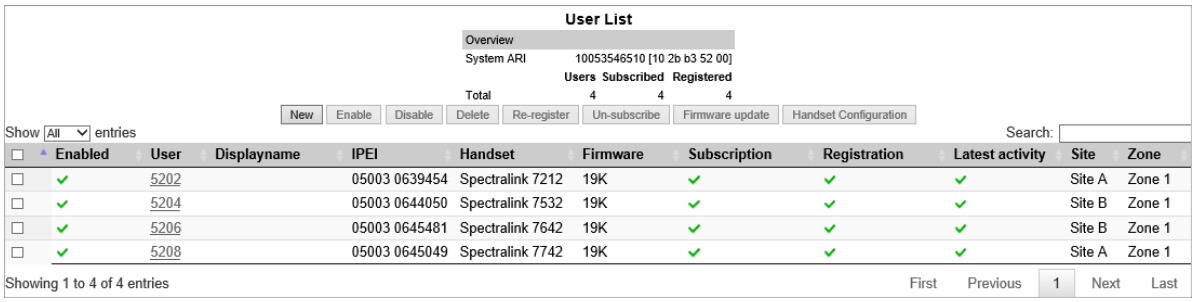
1. Click **Users**, and then click **List Users**.
2. The list will show all entries as default. You can search for information.

3 Click on the relevant user to change user configurations, such as the AC (authentication code). For more information, see Registering Users and Subscribing Handsets.

4 If changing user configuration settings, click **Save**.

To Get Information about Site and Zone

If using site-based paging or zone-based paging you can get information about which site and zone the handset is in.



User List

Overview

System ARI 10053546510 [10 2b b3 52 00]

	Users	Subscribed	Registered
Total	4	4	4

New | Enable | Disable | Delete | Re-register | Un-subscribe | Firmware update | Handset Configuration

Show All entries Search:

	Enabled	User	Displayname	IPEI	Handset	Firmware	Subscription	Registration	Latest activity	Site	Zone
☐	✔	5202		05003 0639454	Spectralink 7212	19K	✔	✔	✔	Site A	Zone 1
☐	✔	5204		05003 0644050	Spectralink 7532	19K	✔	✔	✔	Site B	Zone 1
☐	✔	5206		05003 0645481	Spectralink 7642	19K	✔	✔	✔	Site B	Zone 1
☐	✔	5208		05003 0645049	Spectralink 7742	19K	✔	✔	✔	Site A	Zone 1

Showing 1 to 4 of 4 entries First Previous 1 Next Last

The information is updated in the following situations:

- If the handset has performed a voice or messaging related activity.
- If using zone-based paging–and the handset in idle mode is moving between zone.

If no activity has been performed, the columns **Site** and **Zone** will show the value **Unknown**.

Note:

The information about site/zone can be useful in case of troubleshooting. E.g. if a handset does not receive an incoming call, you can check that site and zone shown, is the same as the physical location of the handset. A voice or messaging activity will update the site/zone registration. Remember to reload the web-based Administration Page.

To Search Handset/User Information

You can search for a registered handset/user in the system through the web-based Administration Page.

- Click **Users**, and then click **List Users**.
- In the **Search** field, enter relevant search string.

The search results are shown in the list.

To Disable/Enable User

As default a user is enabled. You can disable a user on the server and prevent this user from making calls from the handset.

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

2 On the **User List** page, select the relevant user(s) from the list.

3 Click either **Enable** or **Disable**.

To Delete User

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

2 On the **User List** page, select the relevant user(s) from the list.

3 Click **Delete**.

4 Click **OK** to confirm.

To Re-register User

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

2 On the **User List** page, select the relevant user(s) from the list.

3 Click **Re-register**.

To Unsubscribe User

You can unsubscribe a handset from the system.

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

2 On the **User List** page, select the relevant user(s) from the list.

3 Click **Unsubscribe**.

4 Click **OK** to confirm.

To Unsubscribe User

You can unsubscribe a handset from the system.

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

2 On the **User List** page, select the relevant user(s) from the list.

3 Click **Unsubscribe**.

4 Click **OK** to confirm.

To Update Handset Firmware

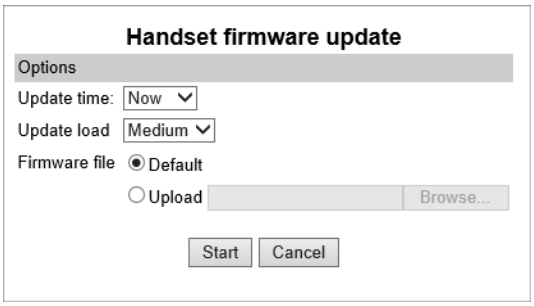
1 Click **Users**, and then click **List Users**.

2 On the **User List** page, select the relevant user(s) from the list.

3 Click **Firmware update**.

4 On the **Handset firmware update** page, enter the following data:

Field	*Setting*
Handset firmware update–Options	
Update time	Default value: **Now**. If you want to upload later, select an appropriate time within the next 24 hours.
Update load	Default value: **Medium** Select relevant upload capacity. The load corresponds to the number of maximum simultaneous updates. You can select between **Low**, **Medium** or **High**. **Low**: 1 handset at a time. **Medium**: 4 handsets per media resource. **High**: 16 handsets per media resource. Example: 2 media resources and High load = 2*16 = 32 simultaneous updates.
Firmware file	The firmware file can be either a previously uploaded default firmware file or a new firmware file chosen. A new firmware file must be a valid firmware file with the extension .bin. Select either **Default** or **Upload**.



5 Click Start.

Import/Export of Users or Delete Users

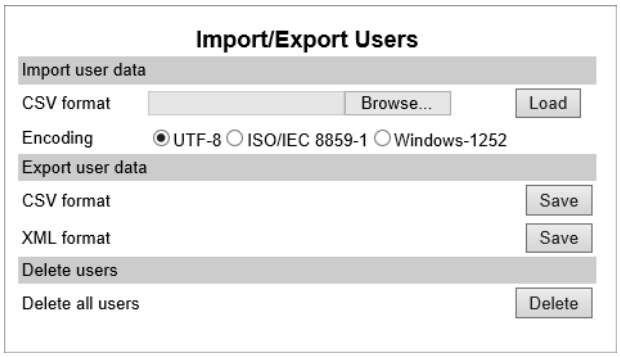
From the **Import/Export** page, you can import/export user data or delete all users.

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

2 On the **Import/Export Users** page, enter the following data:

Field	*Setting*
Import/Export Users–Import user data	
CSV format	If you want to import user data, browse for the CSV file to import, and click **Load**. To be able to import the data correctly, the CSV file must contain certain information and punctuation. For more information, see Appendix B: Example of Handset Registration Data–CSV Format.
Encoding	Select the correct encoding for the CSV file. You can choose between **UTF-8**, **ISO/IEC 8859-1** or **Windows-1252**. **Note**: The encoding depends on the software that was used to generate the CSV file. If you use Microsoft Windows, you will probably select Windows-1252.
Import/Export Users–Export user data	
CSV format	If you want to save the user data file in CSV format, click **Save**. The CSV format can be imported back into the server.
XML format	If you want to save the user data file in XML format, click **Save**. The XML format is used for provisioning. For more information, see *Provisioning Guide*.

Field	*Setting*
Import/Export Users–Delete users	
Delete all users	If you want to delete all users, click **Delete**.



Managing Handset Configuration and Configuration Groups

You can define different configuration groups with different handset configuration and assign users to a specific configuration group containing specific handset configurations. Besides a configuration group ID, the configuration groups must also have a version number. Handset configuration not only allows for groups of users to have different configuration, it also makes it possible to control what is displayed in the handset, as you can hide menus for the user. Situations where hiding menus are relevant can be if the functionality is not supported or not to be used by the group of users, or settings not to be controlled or changed by the user.

Note:

When uploading a handset configuration file into the Spectralink IP-DECT/Virtual IP-DECT Server One, the configuration group (Group ID) is the unique identifier.

The version number determines whether the configuration XML file is different from the existing file. If version number is different, the new handset configuration file is automatically uploaded to the handsets with matching group IDs.

Handset configuration not mentioned in the configuration XML file will remain unchanged. Therefore, be aware that when changing configuration groups–then if settings are set by the previous configuration group and not set for the new configuration group, the old setting will remain in the handset for that individual user. If some features mentioned in the configuration XML file are not supported in the handset, these features will be ignored.

For a complete description of all handset configuration, see Appendix D.

Examples of configuration groups in a company needing different handset configuration for the handsets could be e.g:

*Department examples **	*Configuration Group ID*	*Version number*	*Handset Configuration XML example*
Office	100	1	<?xml version="1.0"?> -<cota> -<info> <group>100</group> <version>1</version> </info> <data>Relevant Handset Configuration </data> </cota>
IT-department	101	1	<?xml version="1.0"?> -<cota> -<info> <group>101</group> <version>1</version> </info> <data>Relevant Handset Configuration </data> </cota>
Production	102	1	<?xml version="1.0"?> -<cota> -<info> <group>102</group> <version>1</version> </info> <data>Relevant Handset Configuration </data> </cota>

*) Only Configuration Group IDs are shown in the system. Therefore, Spectralink recommends keeping a list of the departments (and users) and their assigned handset configuration group.

Handset Configuration Steps Overview

To use Handset Configuration Over The Air, the following steps are necessary:

1 Make a plan defining:

- Needed Configuration Groups (Group ID must be unique) and Version number: Max number of configuration groups allowed: 99

  Accepted values for Group ID: 1–9999 Accepted values for Version number: 1–9999

- Which Handset Configuration settings each configuration group must contain.

  Different settings can be e.g. noisy environment for one group, HAC for another group or access to External Services for a third group etc.

- If settings are to be hidden to the user in the handset menu. A setting can be defined with a certain value in the Handset Configuration XML file, and then defined as hidden in the handset menu.

2 Create a Handset Configuration XML file by exporting existing handset configuration from a handset, make the relevant changes, and then save it.

Tip:

It is advisable to start with one handset and configure it as desired–this can then serve as a template for the rest of the users in the configuration group.

3 Assign relevant Configuration Group (Group ID) to each user.

For more information, see Assigning Configuration Groups (Group IDs) to Users.

4 Upload the Handset Configuration XML file.

For more information, see Uploading or Updating the Handset Configuration XML File.

5 Handset Configuration XML files can also be uploaded through provisioning. If so, create a .ver file to upload/update handset configuration.

The .ver file contains information about available Handset Configuration XML files to be provisioned into the Spectralink IP-DECT/Virtual IP-DECT Server One, including information about the version number.

For more information, see below.

Creating a Handset Configuration XML File

Spectralink

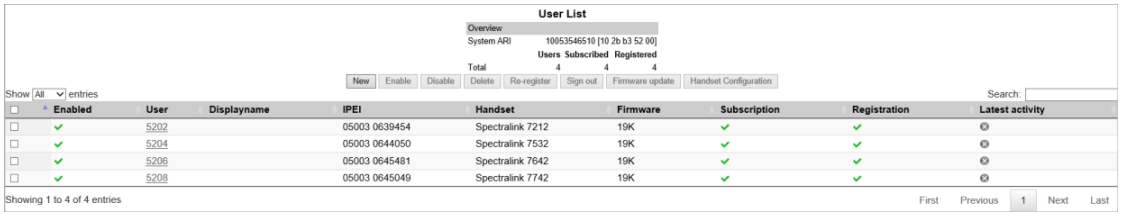
Ensure that you have made a plan for the different configuration groups.

Spectralink recommends keeping a list of the departments (and users) and their assigned handset configuration group.

To create a Handset Configuration XML file containing Group ID, Version number and handset configuration settings from the web-based Administration Page, do the following:

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

The list will show all users.



2 On the **User List** page, select the relevant user (the handset must be subscribed to the system), and then click **Handset Configuration** to export an existing Handset Configuration XML file.

3 On the **Handset Configuration Template** page, click **Export**.

The Handset Configuration XML file is downloaded and can now be used as a template.

For an example of an exported Handset Configuration XML file, see Appendix C: Handset Configuration XML File Example.

4 Open the exported Handset Configuration XML file in a text editor and:

- Assign the relevant Group ID and Version number.
- Edit/add/hide the desired functionality.

Note:

For a complete description of all handset configuration and possible values, see Appendix D.

Functionality in the menu_ elements can be hidden, e.g. menu_main, menu_advanced, menu_settings etc. When hiding a setting, the setting is locked at the same time. If not hiding a setting, the setting can be edited by the user.

To hide functionality in the handset menu, the relevant data string must contain the following attribute: **"false"**.

In the example below (GROUP101 VERSION1), the menu setting **ringing volume** is set to **false** and will not be visible in the handset menu. The ringing volume will have the locked value: **3**

```
<cota>
<info>
    <group>101</group>
    <version>1</version>
</info>
<data>
    <ringing_volume>
        <volume>3</volume>
    </ringing_volume>
    <menu_settings>
        <ringing_volume>false</ringing_volume>
        <ringing_tone>true</ringing_tone>
        <alert_volume>true</alert_volume>
        <vibrate>true</vibrate>
        <silent_mode>true</silent_mode>
        <auto_key_lock>true</auto_key_lock>
        <backlight>true</backlight>
        <auto_answer>true</auto_answer>
        <out_of_range>true</out_of_range>
        <missed_calls>true</missed_calls>
        <absent_in_charger>true</absent_in_charger>
        <bluetooth>true</bluetooth>
        <advanced>true</advanced>
    </menu_settings>
</data>
</cota>
```

In the example below (GROUP101 VERSION2), the menu setting **ringing volume** is set to **true** and will be visible in the handset menu. The ringing volume will have the editable value: **9**

```
<cota>
<info>
    <group>101</group>
    <version>2</version>
```

```
</info>
<data>
    <ringing_volume>
        <volume>9</volume>
    </ringing_volume>
    <menu_settings>
        <ringing_volume>true</ringing_volume>
        <ringing_tone>true</ringing_tone>
        <alert_volume>true</alert_volume>
        <vibrate>true</vibrate>
        <silent_mode>true</silent_mode>
        <auto_key_lock>true</auto_key_lock>
        <backlight>true</backlight>
        <auto_answer>true</auto_answer>
        <out_of_range>true</out_of_range>
        <missed_calls>true</missed_calls>
        <absent_in_charger>true</absent_in_charger>
        <bluetooth>true</bluetooth>
        <advanced>true</advanced>
    </menu_settings>
</data>
</cota>
```

Note:

Handset configuration not mentioned in the configuration XML file will remain unchanged. Therefore, be aware that when changing configuration groups -- then if settings are set by the previous configuration group and not set for the new configuration group, the old setting will remain in the handset for that individual user. If some features mentioned in the configuration XML file are not supported in the handset, these features will be ignored.

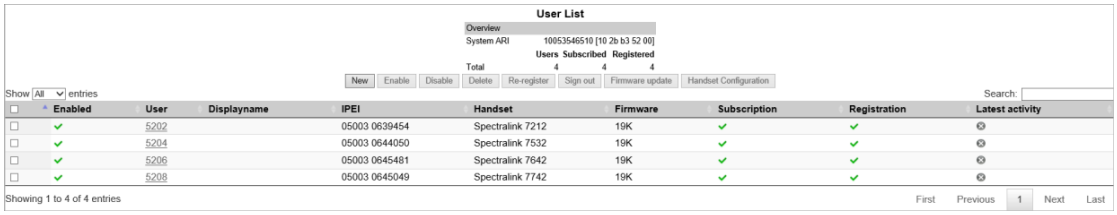
5 Save the Handset Configuration XML file.

Assigning Configuration Groups (Group IDs) to Users

To make use of Handset Configuration Over The Air it is necessary to assign a relevant configuration group to each user.

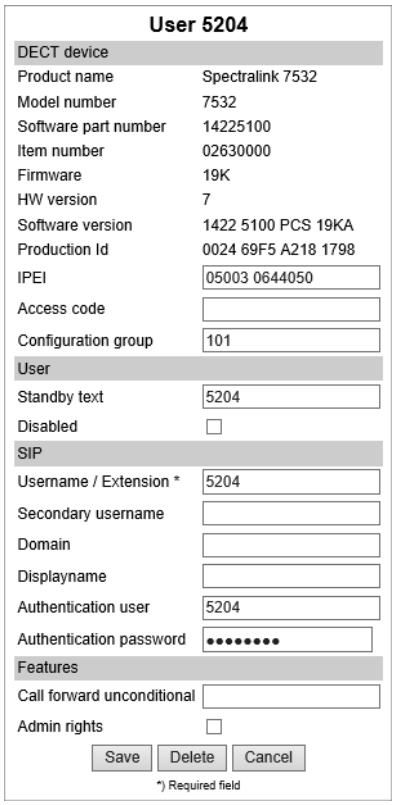
1 Click Users, and then click **List Users**.

The list will show all entries as default. You can search for information.



2 Click on the relevant user, and then enter the Group ID in the **Configuration Group** field.

In case you are changing a configuration group be aware, that when changing configuration groups -- then if settings are set by the previous configuration group and not set for the new configuration group, the old setting will remain in the handset for that individual user.



3 Click **Save**.

Ensure that automatic update (under **Users**> **Handset Configuration**> **Handset Configuration Update**) is enabled, when using handset configuration.

Note:

Assigning the Group ID to user(s) can also be done through:

- Provisioning. For more information, see *Provisioning Guide*. Enhanced Provisioning License required for the Spectralink IP-DECT Server 400/6500 and Spectralink Virtual IP-DECT Server One.
- Using OAM REST API.

An OAM-REST-API License for the relevant Spectralink IP-DECT/Virtual IP-DECT Server One is required to use the OAM REST API. You can find the OAM REST API document at http://support.spectralink.com/products.

Uploading or Updating the Handset Configuration XML File

Note:

Only Spectralink DECT Handset 7202/7212, 7502, 7522/7532, 7622/7642 and 7722/7742 with firmware PCS 19K_ or newer can be updated using Handset Configuration Over The Air.

Only Spectralink IP-DECT/Virtual IP-DECT Server One with firmware PCS 19C_ or newer support Handset Configuration Over The Air.

Handset Configuration Over The Air is not supported on redundant systems.

When having defined a Handset Configuration XML file and assigned the relevant Group IDs to each user, the file can be uploaded to the system. Up to 99 Handset Configuration XML files can be uploaded. You can define an automatic update.

Existing Handset Configuration XML files can also be updated by uploading an existing configuration group with different version number.

Tip:

To view an existing Handset Configuration XML file on the server, select the configuration group, click Export (under **Users**> **Handset Configuration**> **Handset Configuration Files**), and then open it in a text editor.

You can cancel a Handset Configuration XML file upload/update (under **Users**> **Handset Configuration>** Handset Update Status).

Note:

When uploading a handset configuration file into the Spectralink IP-DECT/Virtual IP-DECT Server One, the configuration group (Group ID) is the unique identifier.

The version number determines whether the configuration XML file is different from the existing file. If version number is different, the new handset configuration file is automatically uploaded to the handsets with matching group IDs.

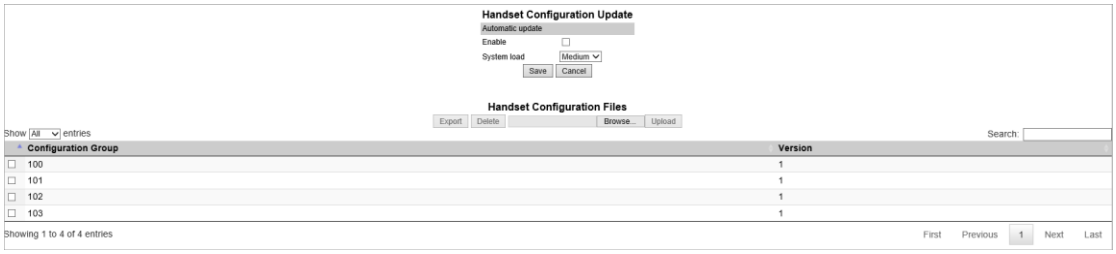
Handset configuration not mentioned in the configuration XML file will remain unchanged. Therefore, be aware that when changing configuration groups–then if settings are set by the previous configuration group and not set for the new configuration group, the old setting will remain in the handset for that individual user. If some features mentioned in the configuration XML file are not supported in the handset, these features will be ignored.

To Upload/Update the Handset Configuration XML File

1. Click **Users**, and then click **Handset Configuration**.
2. Under **Handset Configuration Files**, do the following:

Field	*Setting*
Handset Configuration Update–Automatic update	
Enable (Optional)	Default value: Disabled

Field	*Setting*
	Enable this, if you want to make automatic update possible. If enabled and new handsets are added to an existing uploaded configuration group, these are automatically updated after subscription has finished. Existing handsets that are added to a configuration group are also automatically updated. If a handset configuration update takes place while being in the menu on the handset, the user must exit menu and then re-enter before changes are visible. **Note**: If using provisioning for uploading the Handset Configuration XML file to the handsets, enabling automatic update is required. This can be done either through the XML configuration file or the web-based Administration Page. For more information, see *Provisioning Guide*.
System load (Optional)	Select relevant upload capacity. The load corresponds to the number of maximum simultaneous updates. Possible values: **Low**, **Medium** or **High**. Default value: Medium **Note**: If you schedule an upgrade during day hours, you would typically choose **Low** to **Medium** load to avoid any impact on users. Upgrade after hours typically means no user load, therefore, you can choose **High** priority.
	Click **Save**.
Handset Configuration Files	
Configuration Group	Information about the Group ID assigned to the user. E.g.: 100
Version	Information about the version of the Handset Configuration XML file.
Export	You can view an existing configuration file located on the server. Select the relevant configuration group from the list, and then click **Export**, if you want to export the Handset Configuration XML file and view it in a text editor.
Upload	Click **Browse** to find the relevant Handset Configuration XML file, and then click **Upload**, if you want to upload a Handset Configuration XML file. Click **OK** to return to **Handset Configuration Files** page. If the configuration group did not exist, it is added to the list. If the configuration group existed, but the version number differed, the existing configuration file is overwritten.
Handset Configuration Files	
Group	Information about the Group ID assigned to the user. E.g.: 100
IPEI	Information about IPEI of the handset.
User	Information about username in the configuration group.
Status	Information about upload status. E.g.: Pending, Progress or Postpone.
Progress	Information about the progress of the update.
	Click Cancel update if you want to stop an active update.



The Handset Configuration XML file is now uploaded to the relevant Configuration Group. No reboot of server is needed.

Note:

Handset Configuration XML files can also be uploaded through:

- Provisioning. For more information, see *Provisioning Guide*. Enhanced Provisioning License required for the Spectralink IP-DECT Server 400/6500 and Spectralink Virtual IP-DECT Server One.

To use provisioning, also a .ver file must be created listing the handset configuration files.

For more information about creating a .ver file for provisioning of the handset configuration files, see below.

- Using OAM REST API.

An OAM-REST-API License for the relevant Spectralink IP-DECT/Virtual IP-DECT Server One is required to use the OAM REST API. You can find the OAM REST API document at http://support.spectralink.com/products.

Creating a .Ver File if Using Provisioning

A Handset Configuration XML file must be created for each configuration group. To use provisioning, also a .ver file must be created listing the handset configuration files.

The .ver file contains information about available Handset Configuration XML files to be provisioned into the Spectralink IP-DECT/Virtual IP-DECT Server One, including information about the version number. E.g. GROUP100 VERSION1.

When provisioning the handset configuration file, the Spectralink IP-DECT/Virtual IP-DECT Server One reads the .ver file, and then starts downloading the handset configuration files.

The listed Handset Configuration XML files will only be provisioned, if the version numbers differ from existing handset configuration files.

To Create a xxxx-handset_config_list.ver File (in text editor)

Examples of .ver file:

0013d1800032-handset_config_list.ver

(0013d1800032 is the MAC adress of the Spectralink IP-DECT Server)

89fed27f-7c47-43f5-8347-cb854cedc538-handset_config_list.ver

(89fed27f-7c47-43f5-8347-cb854cedc538 is the UUID of the Spectralink Virtual IP-DECT Server One)

The .ver file can look like this: GROUP100 VERSION1 GROUP101 VERSION1 GROUP102 VERSION1 GROUP103 VERSION1

Note:

There must only be white space between GROUP and VERSION. The naming is case sensitive.

The .ver file describes that we in the example above have 4 Handset Configuration XML files:

“0013d1800032-handset_config_group_100.xml” / "89fed27f-7c47-43f5-8347-cb854cedc538-handset_config_group_100.xml"

“0013d1800032-handset_config_group_101.xml” / "89fed27f-7c47-43f5-8347-cb854cedc538-handset_config_group_101.xml”

“0013d1800032-handset_config_group_102.xml” / "89fed27f-7c47-43f5-8347-cb854cedc538-handset_config_group_102.xml”

“0013d1800032-handset_config_group_103.xml” / "89fed27f-7c47-43f5-8347-cb854cedc538-handset_config_group_103.xml”

When created, all handset configuration files and .ver file must be uploaded to the provisioning server with other provisioning files.

For more information about provisioning, see *Provisioning Guide*.

Chapter 21: System Management

Through the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One you can perform the following system management:

- make a backup of configuration file
- update system firmware (server, base stations, media resources and handsets)
- restart the system
- read system information and statistics
- change administration password
- reset the system
- block new calls during firmware update
- export/Import configuration file
- disable web-based Administration Page
- delete license
- configure different system settings–for more information, see Configuration Steps Overview.

Note:

System software can also be updated through provisioning. Besides provisioning of the server configuration file, you can also provision the handset configuration file and firmware files for base stations, media resources and handsets. For more information, see *Provisioning Guide*.

System software can also be updated using OAM REST API. An OAM-REST-API License for the relevant Spectralink IP-DECT/Virtual IP-DECT Server One is required to use the OAM REST API. You can find the OAM REST API document at http://support.spectralink.com/products.

Making a Back-Up and Restore of System

Through the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One you can save the following data:

- configuration data of the Spectralink IP-DECT/Virtual IP-DECT Server One
- registration and subscription data of the users and handsets
- system information

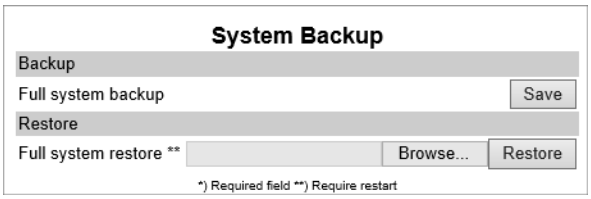
When saving the configuration data, you have an overall overview of the Spectralink IP-DECT/Virtual IP-DECT Server One which is useful in case of problem solving or if you want to do a system restore.

To Make a Back-Up or Restore of Configuration File

1 Click **Administration**, and then click **Backup**.

2 On the **System Backup** page, enter the following data:

Field	*Setting*
System Backup–Backup	
Full system backup	Click **Save**. A full system backup is performed and saved.
System Backup–Restore	
Full system restore	Click **Browse** to browse for the relevant backup file, and then click **Restore**.



3 If you have made a full system restore, reboot the system.

Updating Firmware

Note:

Contact your distributor for newest firmware.

Spectralink IP-DECT/Virtual IP-DECT Server One, Spectralink IP-DECT Base Station and Spectralink DECT Media Resource/Spectralink Virtual IP-DECT Media Resource firmware can be updated the following ways:

- Using the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One.
- Provisioning. For more information, see *Provisioning Guide*.
- Using OAM REST API.

  An OAM-REST-API License for the relevant Spectralink IP-DECT/Virtual IP-DECT Server One is required to use the OAM REST API. You can find the OAM REST API document at http://support.spectralink.com/products.

The Spectralink DECT Handset firmware can be updated the following ways:

- Over the Air (SUOTA–Software Update Over The Air) through the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One.
- Using the Handset Management Cradle and Handset and Repeater Management Tool. To update the Spectralink DECT Handset using the Handset and Repeater Management

Tool, acquisition of a Handset Management Cradle and download of Handset and Repeater Management Tool is required. Physical access to each Spectralink DECT Handset to be updated is also required.

For more information about the Handset Management Cradle and Handset and Repeater Management Tool, see *Handset User Guides* and *Handset and Repeater Management Tool User Guide*.

- Provisioning. For more information, see *Provisioning Guide*.
- Using OAM REST API.

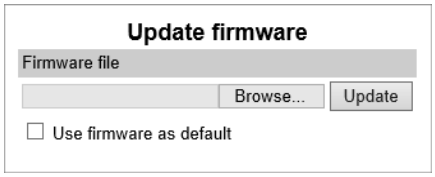
An OAM-REST-API License for the relevant Spectralink IP-DECT/Virtual IP-DECT Server One is required to use the OAM REST API. You can find the OAM REST API document at http://support.spectralink.com/products.

Note:

Before updating system software, always make a backup of the configuration. For more information, see Making a Back-Up and Restore of System.

To Update Spectralink IP-DECT/Virtual IP-DECT Server One Firmware

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



2 On the **Update firmware** page, click Browse to find the relevant firmware file.

Note:

The Spectralink IP-DECT Servers support doing firmware updates directly from a firmware file and also from firmware files contained in a ZIP file. Zip file firmware update is only supported on systems running firmware PCS 20B_ or newer. On the Spectralink Virtual IP-DECT Server One, it is required to use a ZIP file containing both the Spectralink Virtual IP-DECT Server One firmware (.ova file) and the Spectralink IP-DECT Server firmware (.bin file) in order to use the firmware as default for base stations and media resources.

Enable the **Use firmware as default** check box if you want the server firmware as default for all base stations and media resources (recommended).

Click **Update**.

Wait until the system has finished updating.

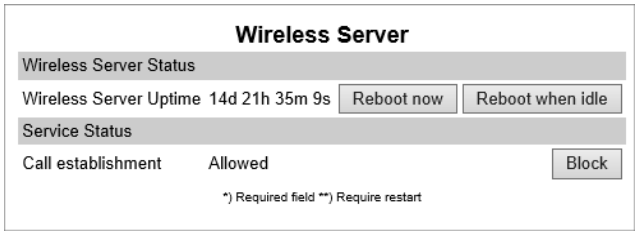
Caution:

Do not cut power.

3 Click **Reboot now** or **Back**. Clicking **Back**, you have the option to make further changes before the update is started.

4 Optionally, you can block new calls during a firmware update by clicking **Administration**, and then clicking **Wireless Server**.

On the **Wireless Server** page, under **Service Status**, click **Block**.



5 Click **Reboot now** or **Reboot when idle**.

To Update Spectralink IP-DECT Base Station Firmware

Note:

Not relevant to the Spectralink IP-DECT Server 200.

New firmware can be uploaded either through provisioning (license required) or manually.

Note:

Base stations can use default firmware, if selected when server firmware is uploaded. For more information, see To Update Spectralink IP-DECT/Virtual IP-DECT Server One Firmware.

Note:

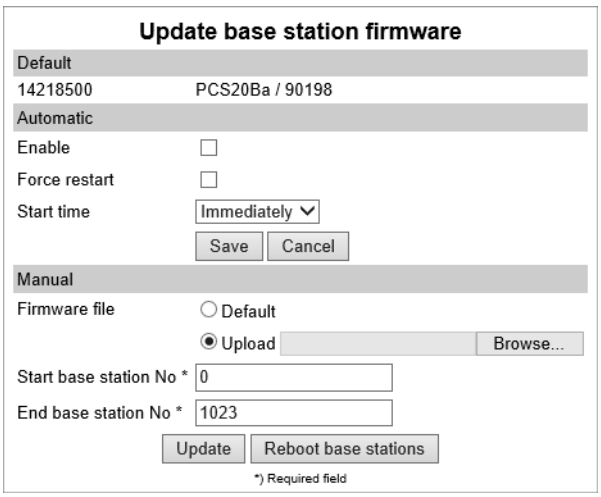
Automatic update of Spectralink IP-DECT Base Stations requires base stations with firmware version PCS 15 or newer.

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

2 On the **Update base station firmware** page, enter the following data:

Field	*Setting*
Update base station firmware–Default	
	Information about default firmware files type, version (PCS) and build number–if firmware files have been uploaded. **Note**: Once uploaded, default firmware will remain on the server until overwritten. **Note**: If the **Use firmware** as default check box on the **Update firmware** page is enabled (**Firmware**> **Wireless Server** or **Configuration**> **Provisioning**> **Firmware**), then the server firmware is uploaded as default for all base stations and

Field	*Setting*
	media resources (recommended). For the files to be updated in the **base station**, this must be executed either through manual update or automatic update.
Update base station firmware–Automatic	
Enable (Optional)	Default value: Disabled Enable this, if you want to make automatic update possible. The base stations will be automatically updated using the default firmware. Also new base stations automatically update to new default firmware when connected. **Note**: If the default firmware version changes, the update process will start automatically according to the chosen values in the **Force** and **Start time** fields. **Note**: Automatic update of Spectralink IP-DECT Base Stations requires base stations with firmware version PCS 15__ or newer. **Note**: Using provisioning for base stations, media resources and handsets, enabling automatic update is required. This can be done either through the XML configuration file or the web-based Administration Page. For more information, see Provisioning Guide.
Force (Optional)	When **Force** is enabled, the base stations will be updated at the selected Start time. If **Force** is disabled, the base stations will be updated when they become idle after the selected Start time.
Start time (Optional)	Default value: Immediately If you want to upload later, select an appropriate time within the next 24 hours.
	Click **Save**.
Update base station firmware–Manual	
Firmware file (Optional)	The firmware file can be either a previously uploaded default firmware file, or a new firmware file chosen. A new firmware file has to be a valid firmware file with the extension .bin or a zip file containing a valid firmware file. Select either **Default** or **Upload**. **Note**: Zip file firmware update is only supported on systems running firmware PCS 20B_ or newer.
Start base station No	The index number of the first base station to be updated. You can check base station numbers under **Administration**> **base stations**> **IP Base Stations**.
End base station No	The index number of the last base station to be updated.



3 Click **Update**. Selected base stations will be updated.

4 Click **Reboot base stations** if you want to reboot selected base stations.

Note:

If **Automatic update** is not enabled, Spectralink IP-DECT Base Stations can be rebooted manually after they have been updated.

To Update Spectralink DECT Media Resource/Spectralink Virtual IP-DECT Media Resource Firmware

Note:

Not relevant to the Spectralink IP-DECT Server 200/400.

Once uploaded, default firmware will remain on the server until overwritten or deleted. New firmware can be uploaded either through provisioning (license required) or manually.

Note:

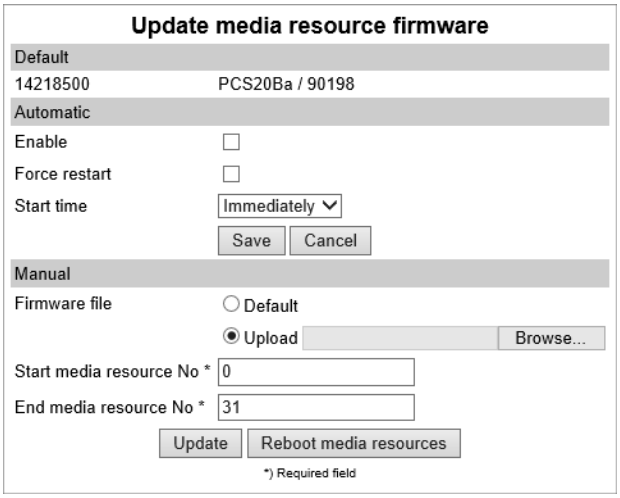
Media resources can use default firmware, if selected when server firmware is uploaded. For more information, see To Update Spectralink IP-DECT/Virtual IP-DECT Server One Firmware.

1 Click **Firmware**, and then click **Media Resource**.

2 On the **Update media resource firmware** page, enter the following data:

Field	*Setting*
Update media resource firmware–Default	
	Information about default firmware files type, version (PCS) and build number–if firmware files have been uploaded. **Note**: Once uploaded, default firmware will remain on the server until overwritten. **Note**: If the **Use firmware as default** check box on the **Update firmware** page is enabled (**Firmware**> **Wireless Server** or **Configuration**> **Provisioning**> **Firmware**), then the server firmware is uploaded as default for all base stations and media resources (recommended). For the files to be updated in the **media resource**, this must be executed either through manual update or automatic update.
Update media resource firmware–Automatic	
Enable (Optional)	Default value: Disabled Enable this, if you want to make automatic update possible. The media resources will be automatically updated using the default firmware. Also new media resources automatically update to new default firmware when connected. **Note**: If the default firmware version changes, the update process will start automatically according to the chosen values in the **Force** and **Start time** fields. **Note**: Using provisioning for base stations, media resources and handsets, enabling automatic update is required. This can be done either through the XML configuration file or the web-based Administration Page. For more information, see Provisioning Guide.
Force (Optional)	When **Force** is enabled, the media resources will be updated at the selected Start time. If **Force** is disabled, the media resources will be updated when they become idle after the selected Start time.
Start time (Optional)	Default value: Immediately If you want to upload later, select an appropriate time within the next 24 hours.
	Click **Save**.

Field	*Setting*
Update media resource firmware–Manual	
Firmware file (Optional)	The firmware file can be either a previously uploaded default firmware file, or a new firmware file chosen. A new firmware file has to be a valid firmware file with the extension .bin or a zip file containing a valid firmware file. Select either **Default** or **Upload**. **Note**: Zip file firmware update is only supported on systems running firmware PCS 20B_ or newer.
Start media resource No	The index number of the first media resource to be updated. You can check media resource numbers under **Administration**> **Media resource**.
End media resource No	The index number of the last media resource to be updated.



3 Click **Update**. Selected media resources will be updated.

4 Click **Reboot media resources** if you want to reboot selected media resources.

Note:

If **Automatic update** is not enabled, Spectralink DECT Media Resources/Spectralink Virtual IP-DECT Media Resources can be rebooted manually after they have been updated.

To Update Spectralink DECT Handset Firmware Over The Air (SUOTA)

Note:

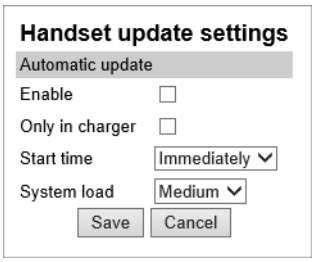
Only Spectralink DECT Handset 7202/7212, 7502, 7522/7532, 7622/7642, 7722/7742 and Spectralink DECT Handset Butterfly can be updated over the air (SUOTA).

The Spectralink DECT Handsets has a hardware platform that supports dual flash partition to ensure that the new firmware can be verified before it takes over from current running firmware.

1 Click **Firmware**, and then click **Handset**.

2 On the **Handset update settings** page, enter the following data:

Field	*Setting*
Handset update settings–Automatic update	
Enable (Optional)	Enable. This will make automatic update possible.
Only in charger (Optional)	If enabled, only handsets in charger will be updated.
Start time (Optional)	Default value: Immediately If you want to upload later, select an appropriate time within the next 24 hours.
System load (Optional)	Select relevant upload capacity. The load corresponds to the number of maximum simultaneous updates. Possible values: **Low**, **Medium** or **High**. Default value: Medium **Low**: 1 handset at a time. **Medium**: 4 handsets per media resource. **High**: 16 handsets per media resource. Example: 2 media resources and High load = 2*16 = 32 simultaneous updates. **Note**: If you schedule an upgrade during day hours, you would typically choose **Low** to **Medium** load to avoid any impact on Users. Upgrade after hours typically means no User load, therefore, you can choose **High** priority. **Warning**: If you set system load to **High**, then you risk that the process allocates all MR channels, which will block for new incoming and outgoing voice calls.



3 Click **Save**.

Note:

If you have already loaded handset firmware to the server, enabled the **Enable** check box and set Start time to **Immediately**, this will trigger firmware upload for the appropriate handsets as soon as you click **Save**.

Only handsets needing update will be updated. The update progress is shown in the handset display and on screen. If some of the handsets have already been updated, it will appear on the screen.

If the handset is disconnected during the update, "Abnormal release" appears in the update progress box. If the handset is not SUOTA capable, a message appears on the screen.

Note:

If update of a handset fails, the handset will be put back in the queue. A handset can fail up to 15 times before updating for that specific handset is given up. If a handset is located on the edge of the DECT coverage area it could fail-retry more often.

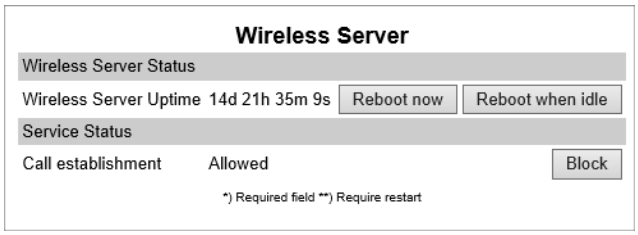
If battery level in handset is low, then the handset will refuse the update request.

Restarting System or Block Calls during Firmware Update

Through the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One you can restart he Spectralink IP-DECT/Virtual IP-DECT Server One or block new calls during firmware update.

To Restart System or Block New Calls

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



2. On the **Wireless Server** page, under **Wireless Server Status**, click **Reboot now** or **Reboot when idle** (when active calls have ended) if you want to restart the system.
3. On the **Wireless Server** page, under **Service Status**, click **Block** if you want to block for new calls during firmware update.
4. Click **OK** again.

Reading System Information

Through the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One you can read the following system information:

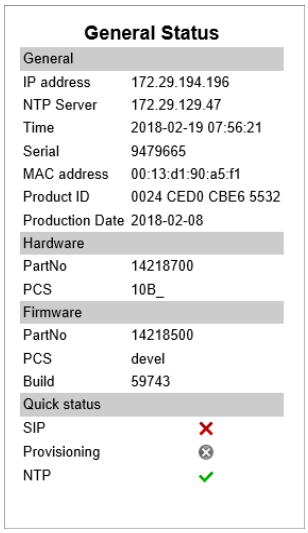
- General status
- Logs Information
- Wireless Server Information
- Statistics and Service Report–for more information, see Statistics and Service Report

General Status Information

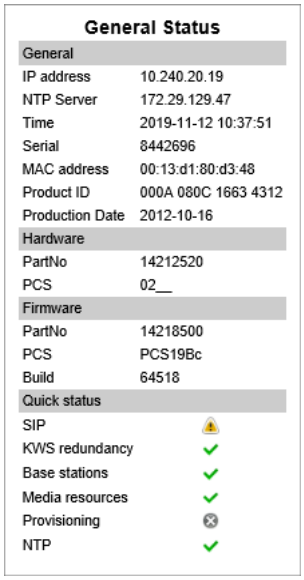
This page provides general system information such as hardware and firmware information.

- Click **Status**, and then click **General**. The **General Status** page appears.

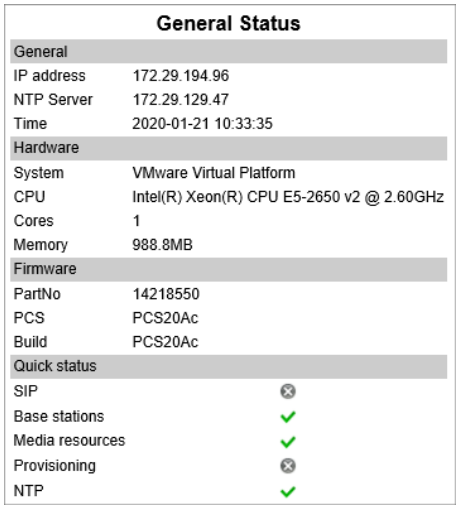
Example from Spectralink IP-DECT Server 200:



Example from Spectralink IP-DECT Server 6500:



Example from Spectralink Virtual IP-DECT Server One:



General Status	
General	
IP address	172.29.194.96
NTP Server	172.29.129.47
Time	2020-01-21 10:33:35
Hardware	
System	VMware Virtual Platform
CPU	Intel(R) Xeon(R) CPU E5-2650 v2 @ 2.60GHz
Cores	1
Memory	988.8MB
Firmware	
PartNo	14218550
PCS	PCS20Ac
Build	PCS20Ac
Quick status	
SIP	⊗
Base stations	✓
Media resources	✓
Provisioning	⊗
NTP	✓

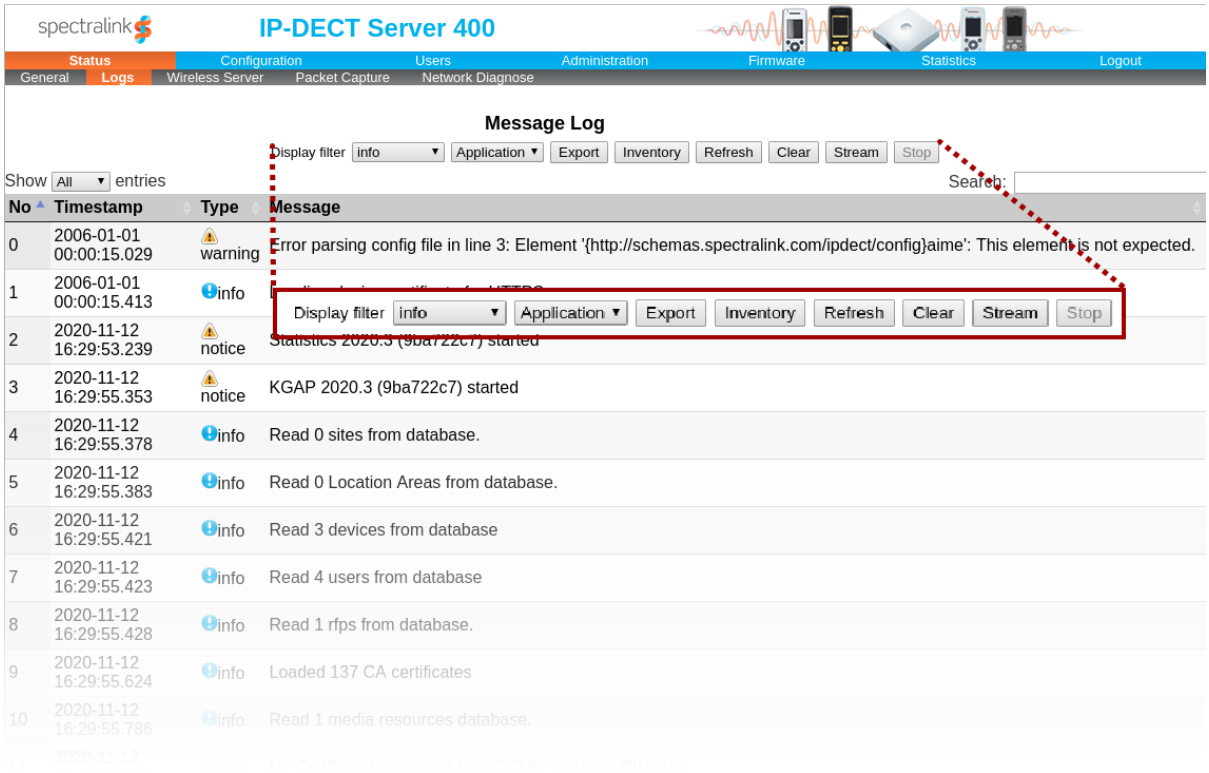
Description of quick statuses

				
SIP	All enabled SIP users are registered to the SIP server.	Problems for some users.	No users.	Problems for all users.
KWS redundancy	Connection to the redundancy peer is OK.	N/A	Not configured.	Not working.
Base stations	No synchronization loops, no auto synchronization and all enabled base stations are connected and synchronized.	Problems for some base stations.	Empty base stations.	Not connected and in sync.
Media resources	All enabled media resources are connected and at least one channel is available.	Problems for some media resources.	Empty media resources.	Not connected.
Provisioning	The latest communication with the provisioning server was successful.	N/A	Not configured.	Not working.
NTP	The latest communication with the NTP server was successful.	N/A	Not configured	Not working.
AMiE	Connected to AMiE.	N/A	N/A	Not connected.

Logs Information

This page provides log information such as media resource connection, base station connection and different types of statuses.

1 Click **Status**, and then click **Logs**. The **Message Log** page appears.



2 The **Display filter** dropdown list provides logging filter status options: Selecting notice info will show all types of statuses, selecting e.g. error will show errors and above (critical and emergency). Selecting emergency will show only emergencies.

- emergency (errors causing the system to malfunction for all calls)
- critical (events that do not occur under normal operation, cause major malfunction)
- error (events that do not occur under normal operation, cause minor malfunction)
- warning (events that do not occur under normal operation, may cause malfunction)
- notice info (events that occur under normal operation)

Note:

It is not necessary to export logs for each different status. All types will be part of the log file.

3 Other filters provide specific information:

- An **Application** log is a file of events, logged by the system. An **Audit** log is a chronological set of records documenting the sequence of activities.

  You can clear the message log buffer for **Application** logs. The **Audit** log cannot be deleted -- except when performing a factory reset.

  You can stream an **Application** log, whereas an **Audit** log cannot be streamed.

- The **Inventory** filter generates an inventory list. During (or after) installation/setup of the entire DECT system an inventory list can sometimes be requested from Spectralink sales/order management when creating SpectraCare or Software insurance.

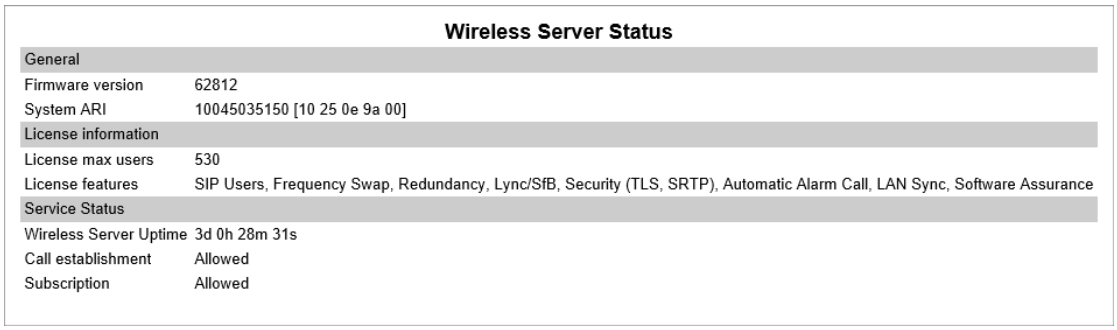
  The inventory lists all connected entities (servers, base stations, media resources and handsets).
- Click **Export** if you want to save the logs in a file.

Wireless Server Information

This page provides information about the firmware version and ARI code of the Spectralink IP-DECT/Virtual IP-DECT Server One.

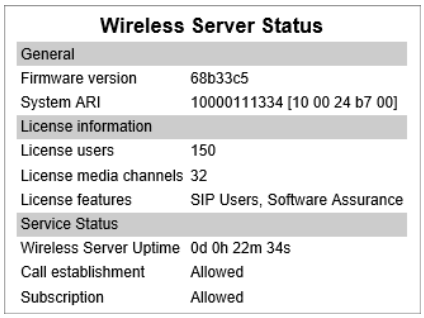
Click Status, and then click **Wireless Server**. The **Wireless Server Status** page appears.

Example from Spectralink IP-DECT Server 6500:



Wireless Server Status	
General	
Firmware version	62812
System ARI	10045035150 [10 25 0e 9a 00]
License information	
License max users	530
License features	SIP Users, Frequency Swap, Redundancy, Lync/SfB, Security (TLS, SRTP), Automatic Alarm Call, LAN Sync, Software Assurance
Service Status	
Wireless Server Uptime	3d 0h 28m 31s
Call establishment	Allowed
Subscription	Allowed

Example from Spectralink Virtual IP-DECT Server One:



Wireless Server Status	
General	
Firmware version	68b33c5
System ARI	10000111334 [10 00 24 b7 00]
License information	
License users	150
License media channels	32
License features	SIP Users, Software Assurance
Service Status	
Wireless Server Uptime	0d 0h 22m 34s
Call establishment	Allowed
Subscription	Allowed

Changing Administration Password

From the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One you can change the administration password. For more information, see Configuring Security Settings and Changing System Password.

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

2 On the **Security Configuration** page, enter the following data:

Field	*Setting*
Security Configuration–Administrator Authentication	
Current password	Enter the current password.
New username	Enter a new username. Note: Requires a reboot of the server.
New password (Optional)	Enter a new password.
New password again (Optional)	Enter the new password again to confirm.
Strict password requirements (Optional)	If enabling strict password requirements, the device can be configured to enforce certain security rules and naming conventions. **Note**: Once enabled, this setting can only be disabled by a factory reset (**Configuration**> **Factory Reset**) that will remove all configuration and user data.
Password expiration (Optional)	Select when you want the password to expire. Possible values: **Never**, **30 days** or **90 days**. Default value: **Never** **Note**: Once enabled, this setting can only be disabled by a factory reset (**Configuration**> **Factory Reset**) that will remove all configuration and user data.
Security Configuration–Data protection	
Allow unencrypted HTTP (Optional)	HTTPS is forced by default. If enabled, HTTP support is supported instead of HTTPS. **Note**: Enabling unencrypted HTTP can cause passwords and other sensitive data to be transmitted in clear text on the network.
Enable legacy TLS (Optional)	If enabled, TLS versions 1.0 and 1.1, certificates signed with the SHA-1 algorithm and CBC based ciphers are supported. **Note**: Enabling legacy TLS is required for security and interoperability with some older browsers and call handing platforms.
Allow remote logging (Optional)	If enabled, remote logging is allowed. Remote logging allows for Spectralink debug tools to extract debug information from the unit.
Remove user passwords from exported data (Optional)	If enabled, users passwords are prevented from being included when data are exported from the Spectralink IPDECT/Virtual IP-DECT Server One, e.g. when exporting the user list to XML files or CSV files. **Note**: Enabling this will exclude the user database from full system backups. **Note**: Once enabled, this setting can only be disabled by a factory reset (**Configuration**> **Factory Reset**) that will remove all configuration and user data.

3 Click **Save**.

Resetting System to Factory Settings

Through the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One you can reset the Spectralink IP-DECT/Virtual IP-DECT Server One to factory default settings (original configurations and empty user data base). Firmware version is not affected.

Note:

You can also reset the Spectralink IP-DECT Server and Spectralink DECT Media Resource to factory settings by pressing the Reset button.

To Reset System

1 Click **Configuration**, and then click **Factory Reset**.

2 Click **Reset**, and then click **OK**.

All configuration and user data are being erased and the system will reboot.

Note:

Information regarding Spectralink IP-DECT Server:

If you by mistake delete a license or perform a factory reset of the system (which will delete all loaded licenses), you can retrieve the license(s) again by entering the ARI code of the server in the Spectralink License Key Generator on Spectralink Corporation's support portal: http://support.spectralink.com/keycode.

- In the ARI (DECT) / **Serial number (Wi-Fi)** field, enter the ARI, and click **Submit**.
- Copy the license(s) into the web-based Administration Page (**Administration**> **License**> **Licenses**> **Load license**) and click **Load**.

If the license does not appear when entering the ARI of the system, contact Technicalsupport@spectralink.com.

Information regarding Spectralink Virtual IP-DECT Server One:

If you by mistake delete a license or perform a factory reset of the system (which will delete all loaded licenses), you must contact Spectralink Order Management via (EMEA and APAC) emeaom@spectralink.com or (NALA) nalaom@spectralink.com and provide Server ID (UUID) information of the server.

When receiving the license from Spectralink Order Management:

- Copy the license(s) into the web-based Administration Page (**Administration**> **License**> **Licenses**> **Load license**) and click **Load**.

Exporting/Importing Server Configuration File

Through the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One you can export and import the server configuration file.

When provisioning/importing a server configuration file into the Spectralink IP-DECT Server 200/400/6500 and Spectralink Virtual IP-DECT Server One, you can merge the

configurations in the provisioned/imported server configuration file. By merging the server configuration file, all other configurations in the server are preserved. If not using merge, all configurations not defined in the server configuration file are overwritten with default values. For more information about creating a configuration file to be merged, see To Create a Configuration File for Merging. More detailed merge examples are to be found in the Provisioning Guide.

Caution:

Before importing a configuration file, it is strongly recommended to check if it contains the parameter to disable the web-based Administration Page of the server. If provisioning is disabled, and a configuration file with the parameter…

```
<security>
   <allow_gui>false</allow_gui>
</security>
```

…is imported into the server, then the server cannot be accessed.

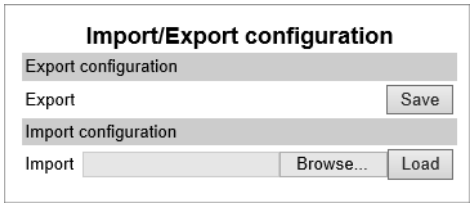
The only option to access the server again is by performing a factory reset!

For more information, see To Disable Web-Based Administration Page of Server.

To Import/Export Configuration File

1. Click **Configuration**, and then click **Import/Export**.
2. On the **Import/Export configuration** page, do the following:

Field	*Setting*
Import/Export–Export configuration	
Export	Click **Save**, if you want to export the configuration file. Save the configuration file.
Import/Export–Import configuration	
Import	Click **Browse**, if you want to search for a configuration file to be imported, select the relevant file, and then click **Load**.



3. Click **Reboot**.

To Create a Configuration File for Merging

To merge server configurations, you must manually append the root element (<config>) in the server configuration file with the following attribute:

```
<config merge_type="merge">
```

If there is no merge attribute or wrong/miss-spelled attribute value, all other configurations will be overwritten with default values as is the case without the attribute (the root element <config> alone).

Example 1 of Configuration File to be Merged

Below is an example of merging a license into a Spectralink IP-DECT/Virtual IP-DECT Server One. Existing configurations are preserved.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<config merge_type="merge">
    <license><NewLicenseString></license>
</config>
```

Example 2 of Configuration File to be Merged

Below is an example of disabling the web-based Administration Page of the Base Stations by mer- ging the configuration file into a Spectralink IP-DECT/Virtual IP-DECT Server One. Existing con- figurations are preserved.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<config merge_type="merge">
<rfp>
    <allow_gui>false</allow_gui>
</rfp>
</config>
```

Note:

For more detailed merging examples, see the *Provisioning Guide*.

Disabling Web-Based Administration Page

For security reasons, you can disable the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One/Spectralink IP-DECT Base Station, so that it cannot be accessed from a browser.

To Disable Web-Based Administration Page of Base Station

The web-based Administration Page of the Spectralink IP-DECT Base Station(s) can be disabled in the following ways:

- From the web-based Administration Page of the server (**Configuration**> **Wireless Server**> **Base Stations** page by disabling Allow web-based Administration Page). For more information, see Configuring Wireless Server Settings.
- Directly in the configuration file by entering the following:

  ```
  <rfp>
      <allow_gui>false</allow_gui>
  </rfp>
  ```

  Change "false" to "true" to enable it.

For more information about exporting/importing the configuration file, see Exporting/Importing Server Configuration File. The configuration file can also be provisioned into the server. For more information, see Provisioning Guide.

To Disable Web-Based Administration Page of Server

The web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One can only be disabled by entering the following directly in the configuration file:

```
<security>
   <allow_gui>false</allow_gui>
</security>
```

Change "false" to "true" to enable it.

Caution:

If the web-based Administration Page of the server is disabled, then the configuration file must be provisioned into the server.

Therefore, it is of high importance to ensure, that provisioning is NOT disabled (Method field) on the server (**Configuration**> **Provisioning**> **Provisioning Configuration** page) before disabling the web-based Administration Page of the server.

If provisioning is disabled, and a configuration file with the parameter

```
<security>
   <allow_gui>false</allow_gui>
</security>
```

is imported into the server, then the server cannot be accessed.

The only option to access the server again is by performing a factory reset!

For more information about provisioning, see *Provisioning Guide*.

For more information about exporting the configuration file, see Exporting/Importing Server Configuration File.

Deleting Licenses

1. Click **Administration**, and then click **License**.
2. On the **Licenses** page, under **Loaded licenses**, click **Delete**, to delete the relevant license.

Example from Spectralink IP-DECT Server 6500:

Example from Spectralink Virtual IP-DECT Server One:

Note:

Information regarding Spectralink IP-DECT Server:

If you by mistake delete a license or perform a factory reset of the system (which will delete all loaded licenses), you can retrieve the license(s) again by entering the ARI code of the server in the Spectralink License Key Generator on Spectralink Corporation's support portal: http://support.spectralink.com/keycode.

- In the ARI (DECT) / Serial number (Wi-Fi) field, enter the ARI, and click Submit.
- Copy the license(s) into the web-based Administration Page (Administration> License> Licenses> Load license) and click Load.

If the license does not appear when entering the ARI of the system, contact Technicalsupport@spectralink.com.

Information regarding Spectralink Virtual IP-DECT Server One:

If you by mistake delete a license or perform a factory reset of the system (which will delete all loaded licenses), you must contact Spectralink Order Management via (EMEA and APAC) emeaom@spectralink.com or (NALA) nalaom@spectralink.com and provide Server ID (UUID) information of the server.

When receiving the license from Spectralink Order Management:

- Copy the license(s) into the web-based Administration Page (**Administration**> **License**> **Licenses**> **Load license**) and click **Load**.

For information about loading a license, see Loading Licenses.

Chapter 22: Statistics and Service Report

On this page you can get an overall overview of how the system is running through different statistics and a service report. Statistics require a significant number of episodes (calls, handover, dropped calls etc.) to give valid ratios. The performance of the installation depends on both deployment (how well it is deployed) and building (construction, materials etc.). The service report contains several files with data used for troubleshooting and statistic information in general.

You can get statistics of the following:

- System
- Sites
- Media Resources
- Base Stations
- Devices
- Users
- Active Calls
- Dropped Calls
- Traffic Distribution

Note

Looking at all the different statistics and correlating information from the various statistic menus, you will begin to find patterns that could point in the direction of a given problem, e.g.:

If a user reports problems in a meeting room, start by looking under Dropped Calls. You will most likely find the user in question listed multiple times or a specific RFP number listed multiple times. Now take a look under Base Station. If the problem happens to occur during peak hours and you also have lots of Times busy incidents, this means that there is lack of speech capacity in the area where the base station is located.

Note

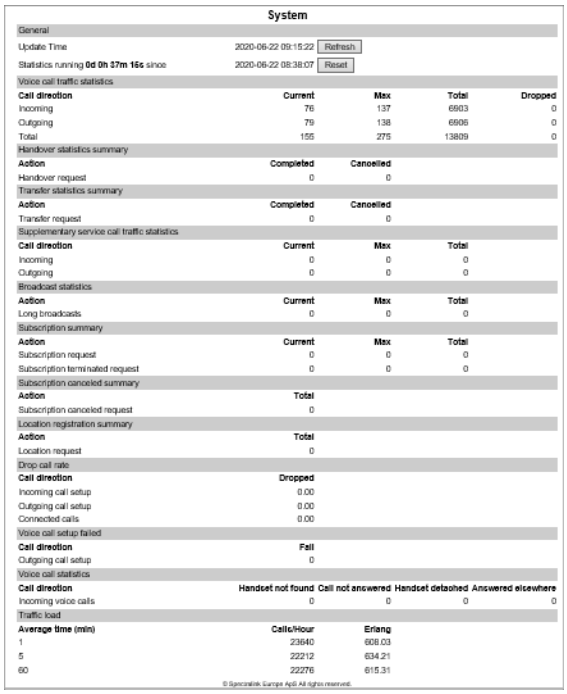
For more indepth information and to gain access to the Spectralink training material, you must attend training and become Spectralink Certified Specialist.

Please visit http://partneraccess.spectralink.com/training/classroom-training for more information and registration.

Statistics of System

This page is useful to get information about traffic on the Spectralink IP-DECT/Virtual IP-DECT Server One such as voice call traffic and message call traffic and it provides a summary of subscription and handover statistics. It also provides information about the traffic load (Erlang) of the installation which is useful when determining the number of media resources needed.

Click **Statistics**, and then click **System**. The **System** page appears.



System

General

Update Time	2020-06-22 09:15:22	Refresh
Statistics running **0d 0h 37m 16s** since	2020-06-22 08:38:07	Reset

Voice call traffic statistics

Call direction	Current	Max	Total	Dropped
Incoming	76	137	6903	0
Outgoing	79	138	6906	0
Total	155	275	13809	0

Handover statistics summary

Action	Completed	Cancelled
Handover request	0	0

Transfer statistics summary

Action	Completed	Cancelled
Transfer request	0	0

Supplementary service call traffic statistics

Call direction	Current	Max	Total
Incoming	0	0	0
Outgoing	0	0	0

Broadcast statistics

Action	Current	Max	Total
Long broadcasts	0	0	0

Subscription summary

Action	Current	Max	Total
Subscription request	0	0	0
Subscription terminated request	0	0	0

Subscription canceled summary

Action	Total
Subscription canceled request	0

Location registration summary

Action	Total
Location request	0

Drop call rate

Call direction	Dropped
Incoming call setup	0.00
Outgoing call setup	0.00
Connected calls	0.00

Voice call setup failed

Call direction	Fail
Outgoing call setup	0

Voice call statistics

Call direction	Handset not found	Call not answered	Handset detached	Answered elsewhere
Incoming voice calls	0	0	0	0

Traffic load

Average time (min)	Calls/Hour	Erlang
1	23640	606.03
5	22212	634.21
60	22276	615.31

- **General**: Elapsed time since last reboot and reset of statistics.
- **Voice call traffic statistics**: Current number of incoming calls, outgoing calls and the total of these since last reset. The different types of calls are divided into active calls, maximum number of simultaneous calls, overall number of calls since last reset. The total number shows incoming and outgoing calls for the entire period of time since last reset of statistics.
- **Handover statistics summary**: Number of completed and cancelled handovers. Cancelled handovers are not necessarily a problem -- you can have up to 30 % of cancelled handover on system level without experiencing any performance issues.
- **Transfer statistics summary**: Number of call transfers (both blind and attended call transfers).
- **Supplementary service call traffic statistics**: Number of calls using Spectralink proprietary messaging service (MSF, lone-worker, alarm button etc.)
- **Subscription summary**: Total of successful subscriptions and subscription terminations.
- **Subscription cancelled summary**: Total of failed handset subscriptions.

- **Location registration summary**: Total of location registrations. Location request counts every time a handset is turned on and registered with an IP-DECT/Virtual IP-DECT Server One.
- **Drop call rate**: Rate of dropped calls (abnormal releases).
- **Voice call setup failed**: Number of failed outgoing call setup from handsets.
- **Voice call statistics**: Number of voice calls not answered by the handset (specified by reason).
- **Traffic load**: Shows how much load has been on the system divided into intervals of 1, 5 and 60 minutes. Traffic load does not reflect a true image of the system load over a longer period of time -- therefore, the information is primary meant for load test purposes.

Note

You can delete all statistic traffic information by clicking **Reset Statistics** (without rebooting the Spectralink IP-DECT/Virtual IP-DECT Server One).

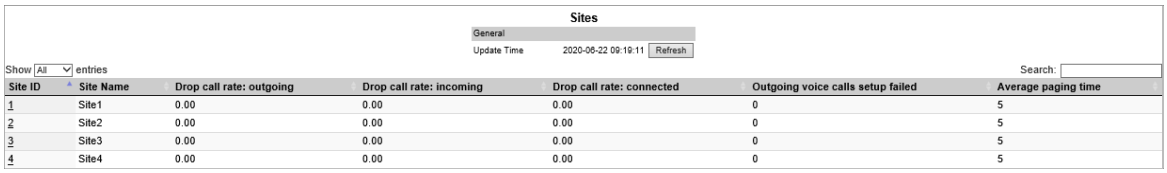
Statistics of Sites

Note

Only relevant if using sites or zone-based paging.

This page is useful to get statistic information on specific sites or zone.

Click **Statistics**, and then click **Sites**. The **Sites** page appears.



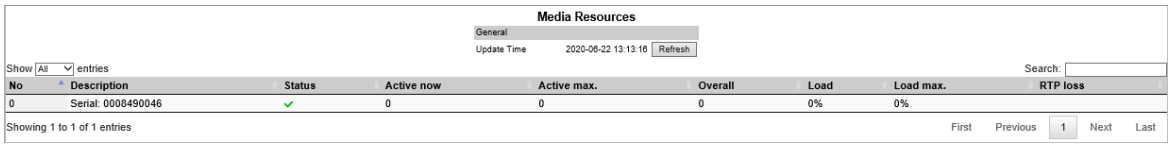
- **Site ID**: Site number (assigned automatically).
- **Site Name**: Name given to site.
- **Drop call rate: outgoing**: Number of dropped outgoing voice calls (all call states).
- **Drop call rate: incoming**: Number of dropped incoming voice calls (all call states).
- **Drop call rate: connected**: Number of dropped connected calls.
- **Outgoing voice calls setup failed**: Number of failed outgoing voice call setup from handset (counted in handset).
- **Average paging time**: Average paging time in seconds (time from server starts looking for handset until handset responds).

Statistics of Media Resources

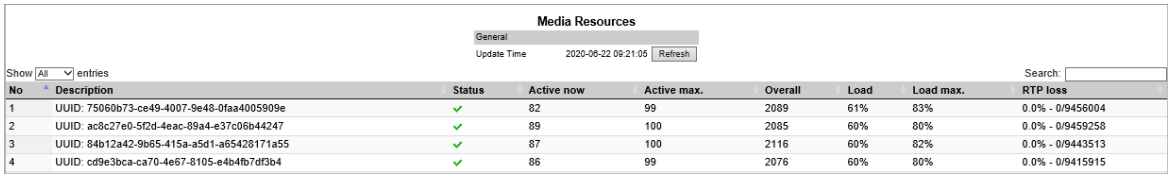
This page is useful to get statistical information about the media resource. It shows an overview of the media resources on the IP-DECT/Virtual IP-DECT system.

Click **Statistics**, and then click **Media Resources**. The **Media Resources** page appears.

Example from Spectralink IP-DECT Server 6500:



Example from Spectralink Virtual IP-DECT Server One:



- **No**: Consecutive index number (not changeable).
- **Description**: Can be changed to custom text (under **Administration>Media Resources**). If not changed, it displays the serial number/UUID.
- **Status**: Shows if the media resource is connected to the server. A disconnected media resource means, that it is disconnected in the configuration or does not have network connection to the server.
- **Active now**: Number of channels that are currently active.
- **Active max**: Maximum number of active channels used at the same time in a media resource.
- **Overall**: Number of calls that have been on the media resource in total since last reset.
- **Load**: Current load on the actual media resource. Normally, media resource load spreads evenly, but if you are using sites and have assigned specific base stations to be used with a specific media resource, then you may see an uneven load distribution.
- **Load max.**: If system load is approaching 90 % (**Load max.**) consider adding another media resource if system load will increase in the future.
- **RTP loss**: Detected RTP packet loss between the media resource and base station as well as between media resource and PBX/call manager. A notice message will be logged if the number of lost RTP packets is greater that 2 %.

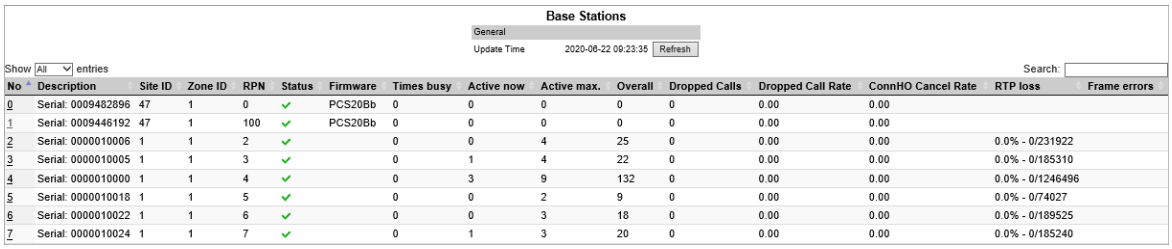
Note

You can search for a specific media resource in the **Search** field.

Statistics of Base Stations

This page is useful to get statistical information about the base station.

Click **Statistics**, and then click **Base Stations**. The **Base Stations** page appears.



Base Stations

General

Update Time 2020-06-22 09:23:35 Refresh

Show All entries Search:

No	Description	Site ID	Zone ID	RPN	Status	Firmware	Times busy	Active now	Active max.	Overall	Dropped Calls	Dropped Call Rate	ConnHO Cancel Rate	RTP loss	Frame errors
0	Serial: 0009482896	47	1	0	✔	PCS20Bb	0	0	0	0	0	0.00	0.00		
1	Serial: 0009446192	47	1	100	✔	PCS20Bb	0	0	0	0	0	0.00	0.00		
2	Serial: 0000010006	1	1	2	✔		0	0	4	25	0	0.00	0.00	0.0% - 0/231922	
3	Serial: 0000010005	1	1	3	✔		0	1	4	22	0	0.00	0.00	0.0% - 0/185310	
4	Serial: 0000010000	1	1	4	✔		0	3	9	132	0	0.00	0.00	0.0% - 0/1246496	
5	Serial: 0000010018	1	1	5	✔		0	0	2	9	0	0.00	0.00	0.0% - 0/74027	
6	Serial: 0000010022	1	1	6	✔		0	0	3	18	0	0.00	0.00	0.0% - 0/189525	
7	Serial: 0000010024	1	1	7	✔		0	1	3	20	0	0.00	0.00	0.0% - 0/185240	

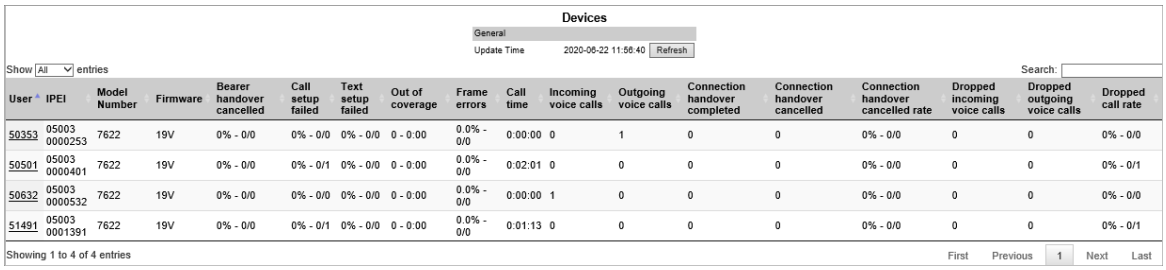
Column titles and what they mean:

- **No**: Consecutive index number (not changeable).
- **Description**: Can be changed to custom text (under **Administration> Base Station**). E.g. a descriptive text about placement (kitchen, basement, meeting room, department etc.). If not changed, it displays the serial number/UUID. For more information, see Administration of Spectralink IP-DECT Base Stations.
- **Site ID**: Site number (assigned automatically).
- **Zone ID**: Zone number (assigned automatically).
- **RPN**: The RPN is the Radio Part Number of the device and can be changed (under **Administration>Base Station**). Be careful not to re-use a RPN from a nearby base station. For more information, see Administration of Spectralink IP-DECT Base Stations.
- **Status**: Shows if the base station is connected to the server. A disconnected base station means lack of coverage.
- **Firmware**: Firmware version of base station.
- **Times busy**: This value should be close to 0, or the location may suffer from inadequate speech capacity. The information is interesting in case you are suffering from dropped calls or lack of speech capacity in a certain area. If the base station is busy multiple times, it indicates lack of speech capacity. Such a problem is easily solved by adding an extra base station.
- **Active now**: Number of traffic channels that are currently active.
- **Active max**: Maximum number of active traffic channels. If there have been times when the base station has been busy, **Active max** can show from 1 to 11, which is the maximum number of active traffic channels available in a Spectralink IP-DECT Base Station.
- **Overall**: Number of times the base stations have served an active channel.
- **Dropped Calls**: Number of dropped calls.
- **Dropped Call Rate**: Number of all dropped calls in percentage.
- **ConnHO Cancel Rate**: Number of cancelled connection handovers in percentage.

- **RTP loss**: Detected RTP packet loss between the media resource and base station as well as between media resource and PBX/call manager.
- **Frame errors**: An information message will be logged if the number of DECT frame errors detected by the base station is greater than 2 % and the duration of the connection is more than 5 seconds.

Statistics of Devices

Click **Statistics**, and then click **Device**. The **Devices** page appears.



Devices

General

Update Time 2020-06-22 11:56:40 Refresh

Show All entries Search:

User	IPEI	Model Number	Firmware	Bearer handover cancelled	Call setup failed	Text setup failed	Out of coverage	Frame errors	Call time	Incoming voice calls	Outgoing voice calls	Connection handover completed	Connection handover cancelled	Connection handover cancelled rate	Dropped incoming voice calls	Dropped outgoing voice calls	Dropped call rate
50353	05003 0000253	7622	19V	0% - 0/0	0% - 0/0	0% - 0/0	0 - 0:00	0.0% - 0/0	0:00:00	0	1	0	0	0% - 0/0	0	0	0% - 0/0
50501	05003 0000401	7622	19V	0% - 0/0	0% - 0/1	0% - 0/0	0 - 0:00	0.0% - 0/0	0:02:01	0	0	0	0	0% - 0/0	0	0	0% - 0/1
50632	05003 0000532	7622	19V	0% - 0/0	0% - 0/0	0% - 0/0	0 - 0:00	0.0% - 0/0	0:00:00	1	0	0	0	0% - 0/0	0	0	0% - 0/0
51491	05003 0001391	7622	19V	0% - 0/0	0% - 0/1	0% - 0/0	0 - 0:00	0.0% - 0/0	0:01:13	0	0	0	0	0% - 0/0	0	0	0% - 0/1

Showing 1 to 4 of 4 entries First Previous 1 Next Last

Column titles and what they mean:

- **User**: Username/extentions/SIPURI.
- **IPEI**: Unique serial number of the handset.
- **Model number**: The handset's technical model number.
- **Firmware**: Firmware version of handset.
- **Bearer handover cancelled**: Number of times a handset has attempted handover and cancelled. Bearer handover cancelled can be as high as 30 %. If higher, it usually indicates high traffic and few vacant channels or interference from a foreign radio source. (Counted in handset).
- **Call setup failed**: Call setup failed is an unintentional terminated call. This usually happens because the handset is not granted a vacant channel from any of the surrounding base stations. (Counted in handset).
- **Text setup failed**: Refers to failed message, e.g. call waiting, message waiting, text message, handset out of charger and similar. (Counted in handset).
- **Out of coverage**: The handset has not been able to maintain connectivity with the IP-DECT system for a given period of time. This is typically caused by the user when walking to e.g. the parking lot or a remote area with no coverage. (Counted in handset).
- **Frame errors**: Frame errors are typically caused by interference and in high traffic areas. Occurrence should be below 2 %.
- **Call time**: Accumulated call time per handset.
- **Incoming voice calls**: Number of incoming voice calls to handset.
- **Outgoing voice calls**: Number of outgoing voice call from handset.
- **Connection handover completed**: Number of successful handovers between base stations.

- **Connection handover cancelled**: Number of times a handset has attempted handover and cancelled. Connection handover cancelled can be as high as 30 %. If higher, it usually indicates high traffic and few vacant channels or interference from a foreign radio source.
- **Connection handover cancelled rate**: Number of cancelled connection handovers in percentage.
- **Dropped incoming voice calls**: Number of incoming voice calls that were abnormally terminated.
- **Dropped outgoing voice calls**: Number of outgoing voice calls that were abnormally terminated.
- **Dropped call rate**: Number of all dropped calls in percentage (both incoming and outgoing voice calls). This number should not be more than 1 %.

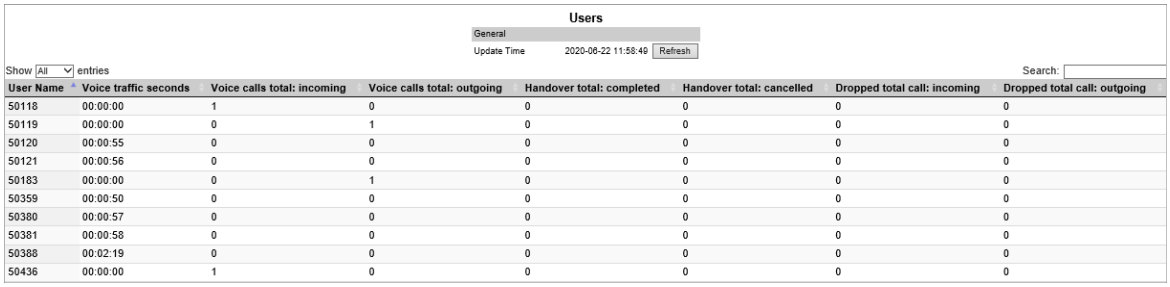
Statistics of Users

This page is useful to get statistic information about each individual user.

Note

User level statistics is different from device level statistics if using handset sharing.

Click **Statistics**, and then click **Users**. The **Users** page appears.



Column titles and what they mean:

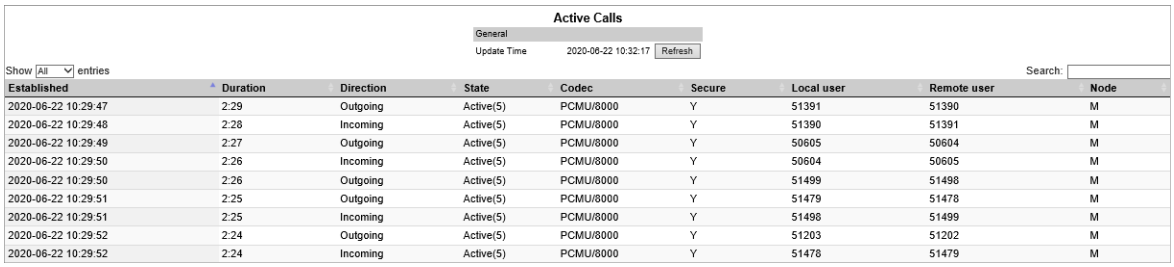
- **Username**: Username/extentions/SIP URI.
- **Voice traffic seconds**: Talktime.
- **Voice calls total: incoming**: Number of incoming voice calls to handset.
- **Voice calls total: outgoing**: Number of outgoing voice calls from handset.
- **Handover total: completed**: Number of successful handovers between base stations.
- **Handover total: cancelled**: Number of cancelled handover attempts between base stations (you can have several cancelled attempts and then a completed attempt without losing the call. According to DECT standard a handset is allowed to make 11 attempts within 3 seconds).
- **Dropped total call: incoming**: Number of incoming voice calls terminated due to involuntary lost radio connection (abnormal releases).

- **Dropped total call: outgoing**: Number of outgoing voice calls terminated due to involuntary lost radio connection (abnormal releases).

Statistics of Active Calls

Provides an overview of current calls in the system.

Click **Statistics**, and then click **Active Calls**. The **Active Calls** page appears.



Active Calls

General

Update Time 2020-06-22 10:32:17 Refresh

Show All entries Search:

Established	Duration	Direction	State	Codec	Secure	Local user	Remote user	Node
2020-06-22 10:29:47	2:29	Outgoing	Active(5)	PCMU/8000	Y	51391	51390	M
2020-06-22 10:29:48	2:28	Incoming	Active(5)	PCMU/8000	Y	51390	51391	M
2020-06-22 10:29:49	2:27	Outgoing	Active(5)	PCMU/8000	Y	50605	50604	M
2020-06-22 10:29:50	2:26	Incoming	Active(5)	PCMU/8000	Y	50604	50605	M
2020-06-22 10:29:50	2:26	Outgoing	Active(5)	PCMU/8000	Y	51499	51498	M
2020-06-22 10:29:51	2:25	Outgoing	Active(5)	PCMU/8000	Y	51479	51478	M
2020-06-22 10:29:51	2:25	Incoming	Active(5)	PCMU/8000	Y	51498	51499	M
2020-06-22 10:29:52	2:24	Outgoing	Active(5)	PCMU/8000	Y	51203	51202	M
2020-06-22 10:29:52	2:24	Incoming	Active(5)	PCMU/8000	Y	51478	51479	M

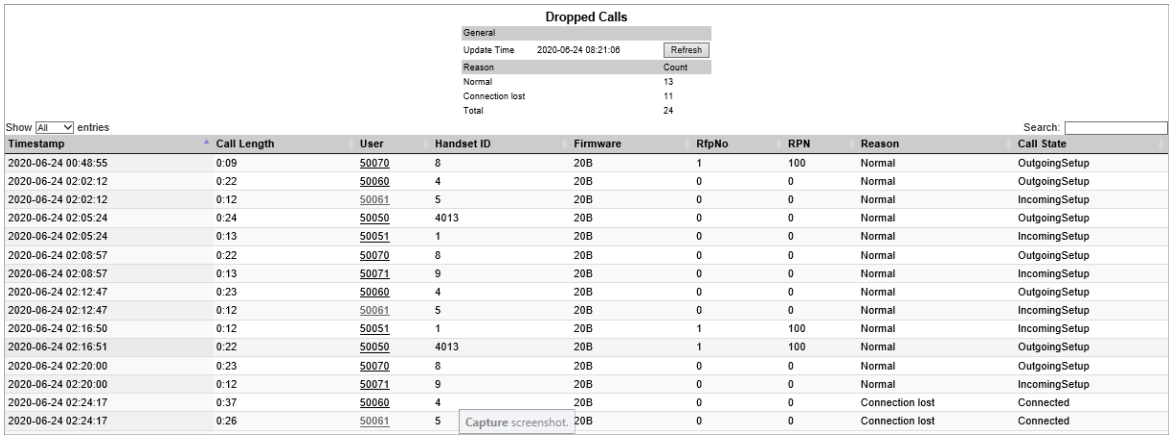
Column titles and what they mean:

- **Established**:Time stamp of beginning of call.
- **Duration**: Current length of the call.
- **Direction**: Indicates whether the call was made from outside (incoming call), or if the call was made from the DECT system (outgoing call).
- **State**: Refers to a specific point in a call session, e.g. call setup state, ringing state, etc. The information is saved in the log files and usually used for debugging.
- **Codec**: Codec being used.
- **Secure**: Shows if call is encrypted with SRTP. Y = encrypted, N = non-encrypted.
- **Local user** and **Remote user**: Local user identifies the local endpoint. If the call is local, you can also identify the remote endpoint.
- **Node**:(Only visible if running a redundant system on a Spectralink IP-DECT Server 6500 or Spectralink Virtual IP-DECT Server One). Shows which server the handsets are subscribed to -- master server (M) or backup (slave) server (S).

Statistics of Dropped Calls

This page is useful to get statistical information about dropped calls (abnormal releases).

Click **Statistics**, and then click **Dropped Calls**. The **Dropped Calls** page appears.



Dropped Calls

General		
Update Time	2020-06-24 08:21:06	Refresh

Reason	Count
Normal	13
Connection lost	11
Total	24

Show All entries Search:

Timestamp	Call Length	User	Handset ID	Firmware	RfpNo	RPN	Reason	Call State
2020-06-24 00:48:55	0:09	50070	8	20B	1	100	Normal	OutgoingSetup
2020-06-24 02:02:12	0:22	50060	4	20B	0	0	Normal	OutgoingSetup
2020-06-24 02:02:12	0:12	50061	5	20B	0	0	Normal	IncomingSetup
2020-06-24 02:05:24	0:24	50050	4013	20B	0	0	Normal	OutgoingSetup
2020-06-24 02:05:24	0:13	50051	1	20B	0	0	Normal	IncomingSetup
2020-06-24 02:08:57	0:22	50070	8	20B	0	0	Normal	OutgoingSetup
2020-06-24 02:08:57	0:13	50071	9	20B	0	0	Normal	IncomingSetup
2020-06-24 02:12:47	0:23	50060	4	20B	0	0	Normal	OutgoingSetup
2020-06-24 02:12:47	0:12	50061	5	20B	0	0	Normal	IncomingSetup
2020-06-24 02:16:50	0:12	50051	1	20B	1	100	Normal	IncomingSetup
2020-06-24 02:16:51	0:22	50050	4013	20B	1	100	Normal	OutgoingSetup
2020-06-24 02:20:00	0:23	50070	8	20B	0	0	Normal	OutgoingSetup
2020-06-24 02:20:00	0:12	50071	9	20B	0	0	Normal	IncomingSetup
2020-06-24 02:24:17	0:37	50060	4	20B	0	0	Connection lost	Connected
2020-06-24 02:24:17	0:26	50061	5	20B	0	0	Connection lost	Connected

Capture screenshot.

Column titles and what they mean:

- **Timestamp**: Time stamp of the dropped call.
- **Call Length**: Call length of the dropped call.
- **User**: Username/extentions/SIP URI.
- **Handset ID**: Internal ID (not relevant).
- **Firmware**: Firmware version of handset.
- **RfpNo**: Identifies which base station the user was connected to, when the call was terminated.
- **RPN**: Identifies Radio Part Number of the base station.
- **Reason**: Short message.
- **Call State**: State of the call.

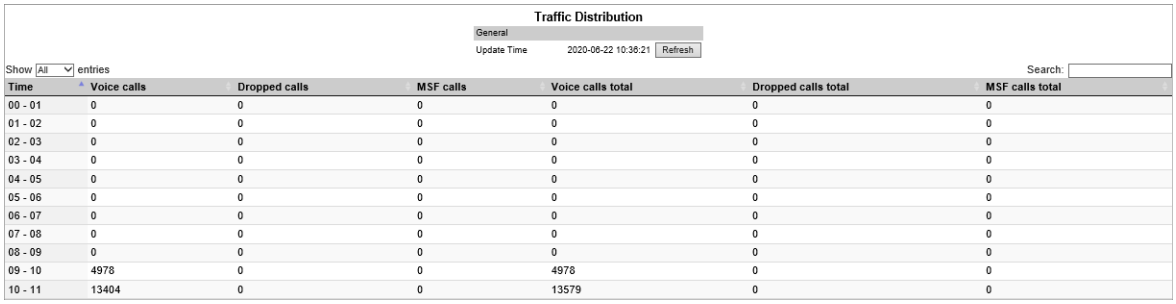
Note

Using the time stamp and RFP number information, you can often put together enough information from the other statistical information to point out a plausible reason for abnormal call releases.

Statistics of Traffic Distribution

This page is useful to get statistic information about traffic distribution during the last 24 hours.

Click **Statistics**, and then click **Traffic Distribution**. The **Traffic Distribution** page appears.



Traffic Distribution

General

Update Time 2020-06-22 10:36:21 Refresh

Show All entries Search:

Time	Voice calls	Dropped calls	MSF calls	Voice calls total	Dropped calls total	MSF calls total
00 - 01	0	0	0	0	0	0
01 - 02	0	0	0	0	0	0
02 - 03	0	0	0	0	0	0
03 - 04	0	0	0	0	0	0
04 - 05	0	0	0	0	0	0
05 - 06	0	0	0	0	0	0
06 - 07	0	0	0	0	0	0
07 - 08	0	0	0	0	0	0
08 - 09	0	0	0	0	0	0
09 - 10	4978	0	0	4978	0	0
10 - 11	13404	0	0	13579	0	0

Column titles and what they mean:

- **Time**: Hour of day.
- **Voice calls**: Number of successful voice calls.
- **Dropped calls**: Number of dropped calls (abnormal releases).
- **MSF calls**: Number of MSF calls (messages and alarms).
- **Voice calls total**: Total number of voice calls.
- **Dropped calls total**: Total number of dropped calls.
- **MSF calls total**: Total number of MSF calls (messages and alarms).

Service Report

The service report includes text files with an overview of server configuration, statistics, detected errors and problems.

1 Click **Statistics**, and then click **Service Report**. The **Service Report** page appears.

2 Click **Generate**.

This will generate a .tar file (e.g. ipdect-servicereport-bad9dce3-0e0d-466e-83de-01d713574cf4-20200) for download. Save and extract the file locally.

Statistic information used for debugging and statistics is contained in the tmp folder as .csv files (to be opened in an editor). If system is restarted all statistics is also reset!

Note

The server must run for about 10 minutes, before it can generate a service report. A service report is always required, if you need any support from Spectralink.

Please include description of observed [what & when] and expected behaviour. Additional logs and/or traces may be necessary on request from Spectralink support.

Chapter 23: OAM REST API

Third-party applications/services can use Spectralink's OAM REST API to operate, administrate and maintain the Spectralink IP-DECT Server200/400/6500 and Spectralink Virtual IP-DECT Server One- One. The OAM REST API provides the same configuration/settings/firmware update options etc. as the web-based Administration Page.

An OAM-REST-API License for the relevant Spectralink IP-DECT/Virtual IP-DECT Server One is required to use the OAM REST API. You can find the OAM REST API document at http://support.spectralink.com/products.

Chapter 24: Messaging Over MSF

With the MSF messages function you can send text messages to any MSF compatible handset connected to the Spectralink IP-DECT/Virtual IP-DECT Server One.

XML-RPC SDK Documentation

To setup the system to use MSF you must obtain the document “XML-RPC SDK” from the following e-mail address: aims@spectralink.com or go to this site: http://www.spectralink.com/partners/app-developers/aims-application-form and fill out an application form.

Chapter 25: Broadcast Messaging

Broadcast messaging is communication between one sender and a number of recipients. Broadcast messaging enables you to deliver information to a large number of recipients at the same time — i.e. all employees can instantly be notified of a fire alarm or be summoned for a company meeting.

Spectralink broadcast messaging is a one-way message that can be sent to a specified group of handsets, or to all handsets in your system simultaneously.

When using Spectralink broadcast messaging, your message can be transmitted as either a text message of maximum 19 or 55 characters or as a color icon including a short explanatory text depending on the application.

Note:

Only Spectralink Handsets 7622/7642/7722/7742 support broadcast messaging with icons.

Depending on the application, the broadcast message can also be an alarm call, an emergency call, or a fire alarm.

Broadcast Messaging Support Matrix

MSF Format	*Functions*	*DECT Servers*	*Base Stations*	*Handset Models*
MSF II	Broadcast Messages (19 Characters)	DECT Server 2500/8000 IP-DECT Server 200/400/6500 Virtual IP-DECT Server One	IP-RFP/RFP5/RFP6 Broadcast on RFP 4 requires firmware PCS 11	7202/7212 7522/7532 7502 7622/7642 7722/7742 Butterfly
MSF III	Broadcast Messages (55 Characters) Advanced color icon Support	DECT Server 2500/8000 IP-DECT Server 200/400/6500 Virtual IP-DECT Server One	IP-RFP/RFP5/RFP6 Broadcast on RFP 4 requires firmware PCS 11.	7622/7642 7722/7742

Components Supporting Broadcast Messaging

Following Spectralink solution components support broadcast messaging:

Broadcast Messaging Supported on Spectralink Handset	
Handset	**Software Version**
Spectralink Handset 7202/7212	Text (MSF II): All versions Icons: Not supported
Spectralink Handset 7502	Only very basic messaging.

Broadcast Messaging Supported on Spectralink Handset	
	Icons: Not supported
Spectralink Handset 7522/7532	Text (MSF II): All versions Icons: Not supported
Spectralink Handset 7622/7642	Text (MSF II/MSF III): All versions Icons: Supported
Spectralink Handset 7722/7742	Text (MSF II/MSF III): All versions Icons: Supported
Spectralink Handset Butterfly	Text: 12Ta or newer Icons: Not supported

Broadcast Messaging Supported on Spectralink IP-DECT Base Stations	
Base Station	**Software Version**
Spectralink IP-DECT Base Station	All versions

Broadcast Messaging Supported on Spectralink DECT Repeater	
Repeater	**Software Version**
Spectralink DECT Repeater	27A or newer

Broadcast Messaging Supported on Spectralink IP-DECT/Virtual IP-DECT Server One	
Server	**Software Version**
Spectralink IP-DECT Server 200	Text (MSF II): All versions Icons: All versions
Spectralink IP-DECT Server 400	Text (MSF II): All versions Icons: All versions
Spectralink IP-DECT Server 6500	Text (MSF II): All versions Icons: All versions
Spectralink Virtual IP-DECT Server One	Text (MSF II): All versions Icons: All versions

System Broadcast Messaging Capacity

In order not to overload your system, Spectralink recommends setting a maximum number of broadcast messages to be sent per minute. Spectralink recommends the following settings the for Spectralink IP-DECT/Virtual IP-DECT Server One.

Broadcast Messaging Capacity	
Server	**Max. no. of broadcast messages per minute**
Spectralink IP-DECT Server 200	20 broadcast messages
Spectralink IP-DECT Server 400	20 broadcast messages
Spectralink IP-DECT Server 6500	20 broadcast messages
Spectralink Virtual IP-DECT Server One	20 broadcast messages

There is no limit to the number of handsets that can receive broadcast messages simultaneously. However, it is only recommended to use broadcast messaging to a larger group of recipients.

Sending a broadcast message initiates the search function on all Spectralink IP-DECT Base Stations/Spectralink IP-DECT Server 200/400, which uses much more system capacity than a direct message. Thus, Spectralink recommends using direct messaging, rather than broadcast messaging, when sending a message to a few handsets.

Broadcast Messaging Handset Management

Configuring Broadcast Messaging

In order to receive broadcast messages, it is necessary to define and configure the different broadcast group numbers in the handsets.

With the Handset and Repeater Management Tool, you can create, update, and delete broadcast groups in each handset. You can define up to 16 groups per Spectralink DECT Handset.

For more information, see Handset and Repeater Management Tool User Guide.

Third-Party Application

In order to use broadcast messaging on the Spectralink DECT Handsets, a third-party application is needed. For more information contact one of Spectralink´s AIMS partners.

Chapter 26: Frequency Swap Support

Note:

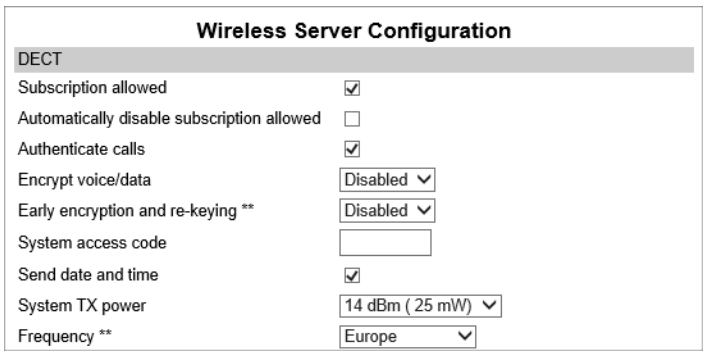
Not relevant to the Spectralink IP-DECT Server 200.

Frequency swap support allows the active radio frequency to be changed in accordance to geographical locations (example: changing from 1.8 GHz to 1.9 GHz, or visa versa).

A Frequency Swap License is required per Spectralink IP-DECT/Virtual IP-DECT Server One to be able to perform the frequency swap. Besides the Frequency Swap License, a special Spectralink DECT Handset 7212 (part no. 02610004) with a special configuration (and compliance to be compatible with frequency swap) is also required. For more information about the special handset, see Handset 7212 Supporting Frequency Swap (Part no. 02610004).

Frequency swap must be configured on the Spectralink IP-DECT/Virtual IP-DECT Server One when configuring Wireless Server settings.

On the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One under **Configuration**> **Wireless Server**> **Wireless Server Configuration–DECT**, a Frequency field is visible, when the Frequency Swap License is installed.



The Frequency field contains the following values:

- **Europe** (EMEA, Australia & New Zealand)
- **South America**
- **USA** (USA & Canada)

For more information about configuration of frequency swap, see Frequency Swap Support.

Note:

Configuration of frequency swap can also be done through Provisioning. For more information, see *Provisioning Guide*. The provisioning server must be set to perform a server restart after a frequency swap.

Using OAM REST API.

An OAM-REST-API License for the relevant Spectralink IP-DECT/Virtual IP-DECT Server One is required to use the OAM REST API. You can find the OAM REST API document at http://support.spectralink.com/products.

Handset 7212 Supporting Frequency Swap (Part no. 02610004)

The special Spectralink DECT Handset 7212 is a dual frequency handset, meaning that it listens to and can automatically swap between 1.8 GHz and 1.9 GHz. When connecting to the system, the handset automatically scans the different frequency bands, selecting the appropriate frequency band to use when required.

Note:

The Spectralink DECT Handset 7212 supporting Frequency Swap will always use DECT 6.0 output power = 100 mW.

Therefore, it is very important that the site is deployed assuming requirements for 1.9 GHz (1920–1930 MHz) and not 1.8 GHz as the 1.8 GHz deployment uses output power = 250 mW.

For more information about deployment, see *Synchronization and Deployment Guide*.

Chapter 27: Redundant System Configuration

Note: Redundancy licenses for Spectralink IP-DECT Server 6500 and Virtual IP-DECT Server One

Redundancy licenses are available for Spectralink IP-DECT Server 6500 and Virtual IP-DECT Server One only.

Redundancy licenses are not available for the Spectralink IP-DECT Server 200/400.

This section describes the redundancy feature in the Spectralink IP-DECT Server 6500 and Spectralink Virtual IP-DECT Server One.

Admin Tip: Introducing Redundancy Version 2.0 license

The 2020R3 release introduces Redundancy version 2.0. In Redundancy version 2.0, it is not necessary to know the ARI of the primary server when creating license to the secondary server. If two servers have the Redundancy version 2.0 license, they will internally transfer the primary server ARI to the secondary server. Additional configuration steps specific to redundancy are not required.

The redundancy feature of the Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One solution adds a backup server to the system, offering both better availability and better performance due to load balancing. By adding a backup server, the most critical failure point of the system is eliminated, allowing the system to continue running and provide service to the users, even when a server fails. Any active calls or sessions handled by the failed component will however be lost.

The redundancy feature is designed to be as non-intrusive as possible. Other than setting up two servers, configuration and administration of a redundant solution is not different from a single server solution. All configurations are executed on the master server, and everything is presented in the same familiar menus. Configuration data and statistics are automatically propagated between all the Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One entities, e.g. base stations, media resources and server. See Configuration of the Redundant Servers.

Note:

If a third-party application is connected to the Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One, e.g. a messaging application or a nurse call application, this application must connect to the master Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One.

In case of a failure in the master server, the application will not be able to communicate with the handsets unless the application is designed for redundancy.

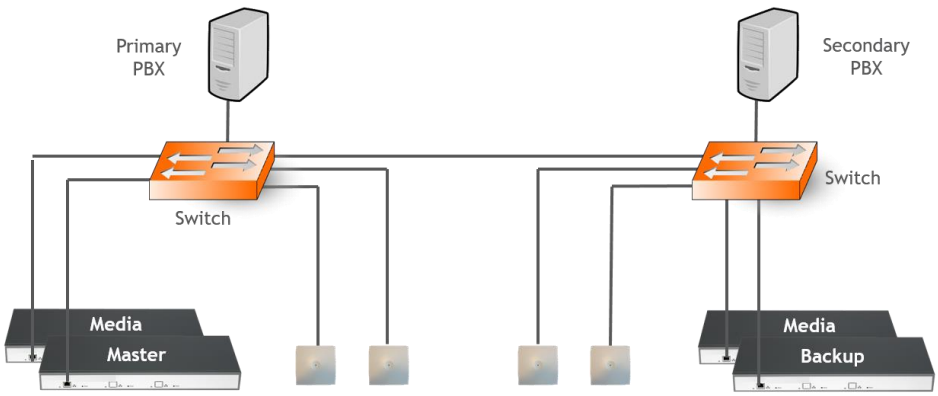
This is further described in the XML-RPC SDK document. To obtain this document go to this site: http://www.spectralink.com/partners/app-developers/aims-application-form and fill out an application form.

Design of Redundant Server Solution

This section describes how to design a redundant Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One solution.

Designing a redundant Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One solution is very similar to designing any other redundant network service. In a redundant Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One solution, the servers should be connected to separate switches, power groups etc.

Below is an example design of a redundant Spectralink IP-DECT Server 6500 solution including a master Spectralink IP-DECT Server 6500 and a redundant backup Spectralink IP-DECT Server.



Note:

- Use separate switches, power groups and servers in a redundant setup.
- Master server and backup server must have same firmware version.
- When upgrading firmware on base stations, servers and media resources, only reboot when all devices have been upgraded.
- Keep-alive packets using TCP on port 56017 are sent between the master server and backup server. Network administrators should make sure that this port is open.

How This Works

The redundancy feature works as a two-step function, adding the redundancy feature and the load balancing feature to the system. All users will be split up in two sections: a 50% of the users will be registered on the master Spectralink IP-DECT 6500 Server/Virtual IP-DECT Server One and 50% of the users on the backup server. This is indicated on **Users**> **List Users**> **User List** under **Node** (right side) by an M for master server and an S for backup server (see image below):

	Enabled	User	Displayname	IPEI	Handset	Firmware	Subscription	Registration	Latest activity	Node
☐	✓	9120	9120	05003 0503001	Spectralink 7622	18C	✓	⊗	✗	M
☐	✓	9121	9121	05003 0588063	Spectralink 75x2,76x2,77x2	18C	✓	✓	⚠	M
☐	✓	9122	9122	05003 0539899	Spectralink 7722	18C	✓	✓	✓	S

The users will not always be on the same system. After a reboot of the Spectralink IP-DECT 6500 Server/Virtual IP-DECT Server One some of the users may have changed servers, there is no option to connect a specific user to a specific server, this is done randomly by the system.

Both servers need to have the same licenses installed because both servers are acting as the same server with one configuration and the backup server is a load balancing server combined with the redundancy feature.

When a failure is discovered by the system, users, base stations and media resources are switched automatically to the “remaining” server. This means that servers, media resources and IP-DECT base stations MUST run the same firmware version.

Note: Upgrade software first

In case you need to firmware upgrade to minimize downtime, update Spectralink IP-DECT Base Stations, Spectralink DECT Media Resources, Spectralink Virtual IP-DECT Media Resources and Spectralink IP-DECT 6500 Server/Virtual IP-DECT Server One BEFORE rebooting any of them. This will ensure that no older firmware will try to connect to newer firmware. Also make sure that licenses loaded on to the master server are also loaded on to the backup server, or the system will not work.

Redundancy Licenses Generation

Admin Tip: Introducing Redundancy Version 2.0 license for Spectralink Virtual IP-DECT Server One

In Redundancy version 2.0, it is not necessary to know the ARI of the primary server when adding a redundancy license to the secondary server. When two servers have the same Redundancy version 2.0 license, they will internally transfer the primary server ARI to the secondary server.

Note:

If a license is installed on the master server, a corresponding license with proper permissions must be installed on the backup server to enable the redundancy features.

For example, if a 500-user license is installed on the master, a 500-user license must be installed on the backup as well.

How to Get Licenses for the Master/Backup Spectralink Virtual IP-DECT Server One

1. Send your Purchase Order (PO) including the Server ID (UUID) and the number of licenses needed to Spectralink Order Management via (EMEA and APAC) emeaom@spectralink.com or (NALA) nalaom@spectralink.com .

Note: Redundancy License part numbers

License required for Virtual IP-DECT Server One (part no. 1423 3241)

License required for IP-DECT Server 6500 (part no. 1423 2857)

2. When your order is processed, Order Management will send you an email including a license key for the relevant software license.
3. Load the new license code on both servers using the web-based Administration Page.
   - Click **Administration**, and then click **License**.
   - Copy the provided license key from your email, paste it in the **License** field, and then click **Load**.
   - Reboot the server to activate the license.
4. Loaded licenses can be seen on the web-based **Administration Page**> **Administration**> **Licenses**> **Loaded licenses**.

Note:

The Redundancy License adopts the ARI code of the master server. This is done in the case of a failure of the master server, the backup server will have the same ARI code, and therefore the handsets will still be subscribed to the ARI, as this does not change.

Note:

A backup server will look different after a Redundancy License has been installed, as the backup server adopts the ARI of the master server. The backup server will now have both a System ARI and a Device ARI (see **Status**> **Wireless Server**> **General**).

Configuration of the Redundant Servers

Set up the redundant servers with the idea that one will be the “master” and the other will be the “backup” (or “slave). Once redundancy is configured, the configuration of the master will be duplicated in the backup. This section explains how to create duplicate servers.

Configuring a Master Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One

The master Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One must be configured as a normal single server solution with base stations, media resources and users as “normal” and it must be verified that the desired functionality is working before enabling the redundancy feature, and the backup Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One is added.

1 Ensure that the Redundancy License is installed, and that the master server is configured correctly.

Admin Tip

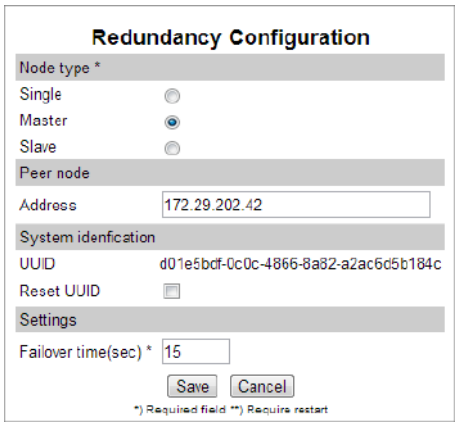
License installation requires reboot of system.

2 Click **Configuration**, and then click **Redundancy**.

3 On the **Redundancy Configuration** page, enter the following data:

Field	*Setting*
Redundancy Configuration–Node type	
Single	If selected, this will disable redundancy and configure for stand alone (normal single server solution). Select **Single**, if this device is to be a normal single server solution.
Master	If enabled, this will enable redundancy and configure the device as master server. The system will be controlled by this device. Select **Master**, if this device is to be the master server.
Slave	If enabled, this will enable redundancy and configure the device as backup (slave) server. The device will be controlled by a master server. Select **Slave**, if this device is to be the backup server.
Redundancy Configuration–Peer node	
Address	If master server, enter the fixed IP address or hostname for the backup Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One. If backup server, enter the fixed IP address or hostname for the master Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One.

Field	*Setting*
Redundancy Configuration–System identification	
UUID (Optional)	The UUID (unique ID) of the redundant system. This must be the same for master server and backup server for replication to be performed. The master server automatically generates the UUID. **Note**: When reset on the master server, the UUID is automatically generated, and when reset on the backup server, it is retrieved from the master server. The UUID must be reset when a master Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One is changed to a backup Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One, or when a backup Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One is moved to another solution.
Reset UUID (Optional)	If enabled, the UUID is reset if the UUID of the master server and backup server is not matching.
Redundancy Configuration–Settings	
Failover time(sec)	Enter value for failover time. Failure time is the time in seconds from the Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One detects a failure, until it initiates a failover operation and cause the other peer to take over. Default value: 15 sec For more information about failure time, see Failover time conditions.



4 Click **Save**.

Note:

Enabling or disabling the redundancy function on a given server, will not require a reboot of the Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One(s).

But, after clicking **Save**, all active calls can be dropped on base stations and media resources when the function is enabled/disabled as all media resources and base stations reconnect to the new setup.

Configuring a Backup Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One

On the backup Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One only basic network settings and redundancy settings need to be configured. All other settings are retrieved from the master Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One.

Note:

When setting up the backup server, the internal media resource is disabled as default. In case the redundant system must use the internal media resource, this must be configured under **Configuration**> **Wireless Server**> **Wireless Server Configuration**> **Media resources**> Add new as active before configuring the backup server.

1 Ensure that the Redundancy License is installed and configured with basic network settings.

Admin Tip

License installation requires reboot of system.

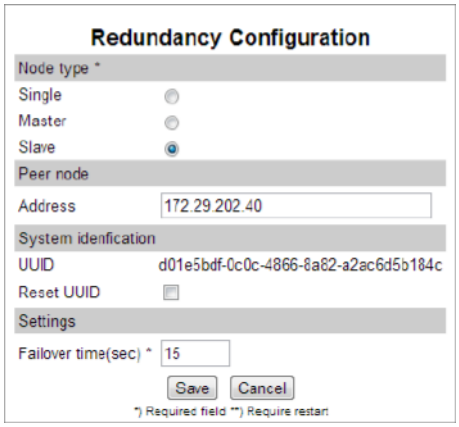
License installation requires reboot of system.

2 Click **Configuration**, and then click **Redundancy**.

3 On the **Redundancy Configuration** page, enter the following data:

Field	*Setting*
Redundancy Configuration–Node type	
Single	If selected, this will disable redundancy and configure for stand alone (normal single server solution). Select **Single**, if this device is to be a normal single server solution.
Master	If enabled, this will enable redundancy and configure the device as master server. The system will be controlled by this device. Select **Master**, if this device is to be the master server.
Slave	If enabled, this will enable redundancy and configure the device as backup (slave) server. The device will be controlled by a master server. Select **Slave**, if this device is to be the backup server.
Redundancy Configuration–Peer node	
Address	If master server, enter the fixed IP address or hostname for the backup Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One. If backup server, enter the fixed IP address or hostname for the master Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One.
Redundancy Configuration–System identification	
UUID (Optional)	The UUID (unique ID) of the redundant system. This must be the same for master server and backup server for replication to be performed. The master server automatically generates the UUID. **Note**: When reset on the master server, the UUID is automatically generated, and when reset on the backup server, it is retrieved from the master server. The UUID must be reset when a master Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One is changed to a backup Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One, or when a backup Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One is moved to another solution.
Reset UUID (Optional)	If enabled, the UUID is reset if the UUID of the master server and backup server is not matching.
Redundancy Configuration–Settings	
Failover time(sec)	Enter value for failover time.

Field	*Setting*
	Failure time is the time in seconds from the Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One detects a failure, until it initiates a failover operation and cause the other peer to take over. Default value: 15 sec For more information about failure time, see Failover time conditions.



4 Click **Save**.

All other configuration settings on the backup server will become unavailable on the web-based Administration Page (and only available on the master server).

5 Reboot the system.

Note:

If the company phone book feature on the Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One is to be used together with the redundancy feature, the company phone book needs to be configured for LDAP or BroadWorks. For more information, see To Get Phone Book Data through LDAP Server, CSV File or BroadWorks.

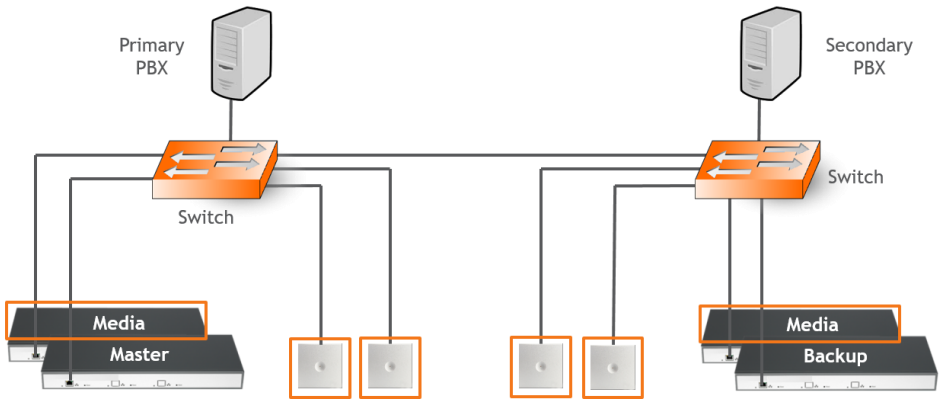
If the company phone book is configured to use a CSV file, it will not be compatible with the Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One when running in failover mode.

Configuring Base Station and Media Resource in a Redundant Solution

The base stations and media resources should be configured just as in a single Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One solution, and the server address should be set to the address of the master server. For more information, see Assigning the Server Address.

After connecting to the master server, the base stations and media resources will automatically be configured to connect to the backup server.

In the event that the master server fails, they will continue to provide service to the backup server. Below is an example of a Spectralink IP-DECT Server 6500 with media resource configured:



Note:

The license for the backup server contains an ARI change license (also known as ARI swap license), which means that the Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One redundant solution only refers to the ARI code of the master server, and not the ARI code of the backup server.

Administration Scenarios

This section describes a common configuration scenario as well as some common administration scenarios where either the master or the backup Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One fails.

Upgrading an Existing Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One Solution into a Redundant Solution

When ordering a Redundancy License to an existing running Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One solution, please remember to inform about the existing Spectralink IP-DECT/Virtual IP- DECT Server ARI code and the NEW backup servers ARI code, to make sure that the master redundancy license code is not generated to the wrong server. All handsets need to be re-subscribed if this happens because the backup servers ARI code will be changed to match the master server, and the whole redundant system refers to the ARI code of the master after the licenses have activated. And if the two servers license codes have been generated incorrectly, the re-register of all handsets has to be performed, and also a complete reconfiguration of the master server.

Temporary Failure on the Master Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One

In the case where the master server fails due to loss of power, network connection etc., the backup server will continue to provide service after a short failover time.

When the master server returns to operation, it will resume its normal operation in cooperation with the backup server.

However, during the failover situation, it will not be possible to change any configuration settings, add or remove users or change the subscription state of any handset.

Permanent Failure on the Master Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One

If the master server has been damaged, lost or had its data erased, it will have to be replaced by the backup server in order to return the system to normal operation mode. This is done by promoting the backup server to 'Master' and the backup server will then assume the responsibilities of a master server. The repaired or replaced master server can then be added as a new backup server, following the above procedure of setting up a backup server.

Note:

Please be aware that if for some reason a repaired or replaced former master server is reinstated as master, it should be done very carefully.

First, it must be configured as a backup server in order to get the current user data and configuration from the acting master server (e.g. the original backup server).

Subsequently, when all data are replicated from the acting master to the original master, the acting master can be demoted to backup server, and the acting backup server (e.g. the original master) can be re-instated as master server.

Failover time conditions

The default failover time is 15 seconds; however this may be adjusted in the Failover time setting (for more information, see Configuration of the Redundant Servers).

A failure is detected within 15 seconds, and the server will wait the specified failover time before initiating the failover operation.

The failover operation moves the users handled by the failing peer to the working peer by re-registering them to the PBX.

When re-registration is completed, the users are able to receive calls again. Outgoing calls can be performed shortly after the failover.

The speed of re-registration depends on the PBX, and the load on the system.

Failure on the Backup Spectralink IP-DECT Server 6500/Virtual IP-DECT Server One

A failure of the backup server will induce a short service outage, and the master server will reestablish full operation as a single server solution.

If the backup server resumes its operation, it will automatically return to be part of the redundant system. In case the backup server must be replaced, the new backup server must be added to the solution.

Chapter 28: Configuring Company Phone Book/Directory

You can set up the company phone book/directory in the server. As default, the company phone book is disabled.

The server can be configured in the following ways:

- Retrieving phone book data using LDAP/LDAPS server.

  Configuration of the LDAP based phone book in the Spectralink IP-DECT/Virtual IP-DECT Server One is carried out through the web-based Administration Page of the server.

- Importing phone book data from a CSV file.
- Retrieving phone book data from BroadWorks.

  You can select a combination of five BroadWorks phone books/directories on the Spectralink IP-DECT/Virtual IP-DECT Server One:

  - Enterprise Directory
  - Enterprise Common
  - Group Directory
  - Group Common
  - Personal Directory

  The BroadWorks phone books/directories are retrieved each time the user enters the phone book from the handset.

  The difference between Enterprise Directory/Group Directory and the Enterprise Common/Group Common is, that the Directory contains a list of contacts in the enterprise/group, whereas the Common is a list of commonly used contacts that are not in the enterprise/group.

Note:

When a company phone book has been enabled, the user can begin searching by pressing the top of navigation key on the handset (requires Spectralink DECT Handset with firmware PCS 17J or newer), or, if long key MSF Function is enabled, by pressing the keys 0 to 5.

For information about using the company phone book in the handset, see the relevant Handset User Guide.

To Get Phone Book Data through LDAP Server, CSV File or BroadWorks

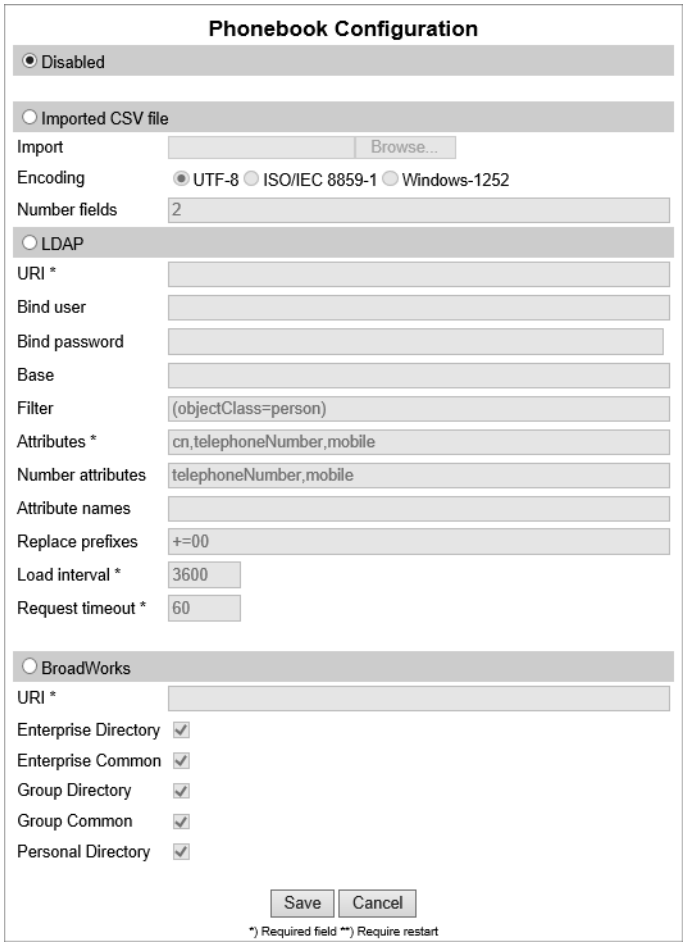
Configure the server to retrieve phone book data using LDAP server (or secure LDAP server), by importing phone book data from a CSV file or retrieve phone book data from BroadWorks.

1 Click **Administration**, and then click **Phonebook**.

2 On the **Phonebook Configuration** page, enter the following data:

Field	*Setting*
Phonebook Configuration–Disabled	
Disabled	As default, phone book configuration is disabled. You can configure the server to retrieve phone book data using LDAP server or by import of phone book data from a CSV file.
Phonebook Configuration–Imported CSV file	
Imported CSV file	Enable this if you want to import phone book data from CSV file.
Import	Browse for the CSV file to import. **Note**: The CSV file must contain correct format. For more information, see Example of CSV File Format.
Encoding	Select the correct encoding for the CSV file. You can choose between **UTF-8**, **ISO/IEC 8859-1** or **Windows-1252**. **Note**: The encoding depends on the software that was used to generate the CSV file. If you use Microsoft Windows, you will probably select Windows-1252.
Number fields	Enter the indexes of the columns containing dialable numbers.
Phonebook Configuration–LDAP	
LDAP	Enable this if you want to configure the server to retrieve phone book data using LDAP server. **Note**: Secure LDAP (LDAPS) communication occurs over port TCP 636. LDAPS communication to a global catalog server occurs over TCP 3269. When connecting to ports 636 or 3269, SSL/TLS is negotiated before any LDAP traffic is exchanged. If using secure LDAP (LDAPS), the necessary certificates must be installed. For more information about CA certificates, see Configuring Certificates. For an example of LDAP configuration, see Example of LDAP Configuration.
URI	Enter the URI of the LDAP server. E.g. ldap://example.org (or ldaps://example.org if using secure LDAP)
Bind user (Optional)	Enter the username used for authentication against LDAP. **Note**: It might be necessary to specify the path for username (DOMAIN\username). E.g. CN=Manager, DC=example, DC=com.
Bind password (Optional)	Enter the Bind user's password.
Base (Optional)	Enter the base path where the users are located in the LDAP structure. E.g. DC=example, DC=com.
Filter (Optional)	Enter the filter used for the LDAP query. The (objectClass=person) filter can be used successfully in most cases.
Attributes	Enter the LDAP attributes you want to query the LDAP for, separated by a comma. E.g. displayName,telephoneNumber, mobile.

Field	*Setting*
Number attributes (Optional)	Enter LDAP attributes that will be used to dial. E.g. telephoneNumber,mobile.
Attributes names (Optional)	Enter the attribute names you want to assign to the attributes specified above, separated by a comma. E.g. Name,Phone,Mobile.
Replace prefixes (Optional)	Enter the phone number prefixes to replace or strip, separated by a comma. E.g.: if the phone number is +45678912345, and that user has the extension 12345, then you specify “+456789” in the **Replace prefixes** field. Or if the phone number is “+456789123456” and “06789123456” must be dialed, then specify “+45=0”.
Load interval	Enter the interval in seconds for querying the LDAP server for updates. Default value: 3600 sec Possible values: 60–999999 sec
Request timeout	Enter the interval in seconds for timeout for LDAP requests. Default value: 60 sec Possible values: 5–3600 sec
Phonebook Configuration–LDAP	
BroadWorks	Enable this if you want to configure the server to retrieve phone book data using BroadWorks. You can select a combination of five BroadWorks phone books/directories on the Spectralink IP-DECT/Virtual IP-DECT Server One: • Enterprise Directory • Enterprise Common • Group Directory • Group Common • Personal Directory The BroadWorks phone books/directories are retrieved each time the user enters the phone book from the handset. The difference between Enterprise Directory/Group Directory and the Enterprise Common/Group Common is, that the Directory contains a list of contacts in the enterprise/group, whereas the Common is a list of commonly used contacts that are not in the enterprise/group. Each retrieved phonebook/directory entry consists of the following data: • **Name**–corresponding to the BroadWorks' "name" element or a concatenation of "firstname" and "lastname". • **Department**–corresponding to the BroadWorks' "department" element. • **Number**–corresponding to the BroadWorks' element with the following priority: 1: "number", 2: "phone", 3: "extension". • **Mobile**–corresponding to the BroadWorks' "mobile" element.
URI *	Enter the relevant URI of the BroadWorks server. E.g.: https://example.org
Enterprise Directory	Default value: Enabled
Enterprise Common	Default value: Enabled
Group Directory	Default value: Enabled
Group Common	Default value: Enabled
Personal Directory	Default value: Enabled



3 Click **Save**.

No restart is needed and the changes are accepted immediately.

Example of CSV File Format

An example of a CSV file format for phone book data could be:
"Label1","Label2","Label3","Label4","Label5"

"Field1",”Field2”,"Field3","Field4","Field5"

"Field1",”Field2”,"Field3","Field4","Field5"

The labels are column names displayed in the handset. The fields are the actual data for the records.

See the example below: "Name","Phone","Mobile","Department","Title"

"Peter Petersen",1000,20123456,"Sales","Manager"

"Niels Nielsen",1001,20123457,"R&D","Developer"

Example of LDAP Configuration

Chapter 29: Handset Sharing

Note:

Not relevant to the Spectralink IP-DECT Server 200.

The traditional concept of a communication device is to have a device (phone) assigned to a number (SIP user).

The basic concept of handset sharing is to break the link between the device and the user, and make it possible for any user to sign-in to any device.

This is typically done for one of two reasons.

The scenario requires more handsets than users.

One such scenario could be a certain user, which is required to have 24/7 operation, and where there is no or very little possibility for charging the handset while in use. Imagine a hospital with a nurse on duty. When the shift of the nurse on duty ends You can let the next nurse use a different handset (fully charged because it was not used by the previous nurse). This way several nurses can share a line/number without sharing a device. Normally 30 minutes of charging of the handset will be sufficient every 24 hours, thus under normal conditions it is not necessary to have extra devices only for the purpose of charging while not in use.

The scenario requires more users than handsets.

An example of this scenario can be that several users, each with their own number, need to use a phone on a site but not at the same time. E.g. a site with 10 different users working at the same site but only 4 users at any given time. The traditional approach

would require 10 devices. With handset sharing You can let the 10 users share 4 devices for cost-saving reasons.

To use the handset sharing feature, the acquisition of the Handset Sharing | IP-DECT/DECT Servers 400/6500/2500/8000 License or Handset Sharing 1 Year | Virtual IP-DECT Server One License.

This chapter covers these requirements.

- Firmware compatibility
- Configuration of handset sharing, including:
  - Configuration of user sign-in/sign-out
  - Adding Devices to Server
  - Adding Users to Servers
  - Handset Sharing and Provisioning

Handset Sharing-Firmware Compatibility

Note:

- The handset sharing feature is available on all Spectralink Handsets. Not all features are supported in all models.
- Non-Spectralink Handsets do not support handset sharing.
- Handsets must run firmware PCS 14_ or newer.
- The server must run firmware PCS 12M_ or newer.

Handset model	*Handset sharing support*	*Clear Call/Message list*
Non-Spectralink handsets	Not supported	Not supported
Spectralink 7202/7212	Supported	Not supported
Spectralink 7502	Supported	Not supported
Spectralink 7522/7532	Supported	Not supported
Spectralink 7622/7642	Supported	Supported
Spectralink 7722/7742	Supported	Supported
Spectralink Butterfly	Supported	Not supported

Adding Handset Sharing License

To enable handset sharing it is necessary to add a Handset Sharing License to the Spectralink IP- DECT/Virtual IP-DECT Server One.

For more information about ordering and loading license into the server, see Ordering Licenses and Loading Licenses.

Note:

When a Handset Sharing License is loaded and the Spectralink IP-DECT/Virtual IP-

DECT Server is rebooted, the web-based Administration Page will display users differently than without a Handset Sharing License.

The Users menu will have a **List Users** submenu and a **List Devices** submenu. The **List users**' submenu is for SIP user data and the **List devices** submenu is for device data.

Furthermore, the DECT access code which is used for securing DECT subscriptions is handled differently depending on whether a Handset Sharing License is present or not.

- Without handset sharing the DECT access code is part of the data for a specific user.
- With handset sharing the DECT access code is not a part of the data for a specific device.

If a user specific DECT access code is configured before installing the Handset Sharing License, the DECT access code will be used as device DECT access code and as (initial) user pin code.

Both can, however, be changed independently of each other, if a license is present.

Configuration of Handset Sharing

Configuration of handset sharing consists of the following tasks to be completed:

- Configuration of user sign-in/sign-out

  For more information, see User Sign-in/Sign-out.
- Adding Devices to Server

  For more information, see Adding Devices to Server.
- Adding Users to Servers

  For more information, see Adding Users to Server.
- Handset Sharing and Provisioning

  For more information, see Handset Sharing and Provisioning.

User Sign-in/Sign-out

Using a sign-in procedure, You can sign-in to the device and sign-out from the device from the handset instead of performing user administration from the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One. The advantage is, that no trusted server is required and no need for server user database synchronization to the Active Directory.

To utilize this feature, both handset sharing and handset login must be enabled.

Note:

This feature requires handset firmware PCS 17H or newer.

Note:

When a sign-in/sign-out is in progress, the handset will wait 120 seconds for user input. If no user input is received, the process will be aborted, and the handset will return to the state it was in before the sign-in/sign-out was initiated.

If a sign-in/sign-out is initiated while the user is busy, the sign-in will not be allowed.

Configuring Handset Login

Enable/Disable Handset Login on Spectralink IP-DECT/Virtual IP-DECT Server One

1. Ensure that support of the relevant call handler is enabled (**Configuration**> relevant Call handler (e.g. Skype for Business)).
2. Click **Configuration**, and then click **Wireless Server**.
3. On the **Wireless Server Configuration** page, under Handsets, enable the handset sharing features Handset sharing and Handset login:

Field	*Setting*
Wireless Server Configuration–DECT	
Subscription allowed (Optional)	If enabled, You can subscribe new handsets to the system. **Note**: Subscription will be disallowed after 120 seconds or when a subscription succeeds. If more time is needed or more handsets must be subscribed, it is necessary to disable the parameter **Automatically disable subscription allowed** below.
Automatically disable subscription allowed (Optional)	If enabled, subscriptions will automatically be disallowed after 120 seconds or when a subscription succeeds. If disabled, subscriptions will be allowed until explicitly disabled. Default value: Enabled **Note**: This feature is part of DECT Security Step A.
Authenticate calls (Optional)	If enabled, each individual DECT call will be authenticated.
Encrypt voice/data (Optional)	Encryption of voice/data packets transmitted via DECT. Possible values: **Disabled**, **Enabled** or **Required**. Default value: Required **Note**: Repeaters do not support encryption. If set to **Required**, the call is ended when handover is established on the repeater.

Field	*Setting*
Early encryption and re-keying (Optional)	If enabled, this enables encryption immediately after connection establishment and regular re-keying until connection termination. Possible values: **Disabled**, **Enabled** or **Required**. Default value: Disabled **Note**: Enabling early encryption may increase connectivity problems in areas with poor coverage. **Note**: Only Spectralink Handsets with firmware PCS 18Da or newer support **Required**. **Note**: This feature is part of DECT Security Step A.
System access code (Optional)	System wide DECT access code. The access code is from 0–8 decimal digits. **Note**: Individual user access code (AC) has precedence over system access code.
Send date and time (Optional)	If enabled, date and time will be sent to the handsets when a call is terminated. Default value: Enabled
System TX power (Optional)	Used for controlling (reducing) the output power of all connected base stations supporting power control. Unless set to default, this will override any base station specific power setting. Default value: Default (250 mW) **Note**: You can define a TX power value for a specific base station (**Administration**> **Base Station**).
Frequency (Optional) (Only visible if Frequency Swap License is loaded)	Radio Region used for DECT communication with handsets. With the Frequency Swap License installed, You can perform frequency swap between handsets. Besides the Frequency Swap License, a special Spectralink DECT Handset 7212 (part no. 02610004) with a special configuration (and compliance to be compatible with frequency swap) is also required. Possible values: • **Europe** (EMEA, Australia & New Zealand) • **South America** • **USA** (USA & Canada) When the frequency of the base stations is changed, handsets lose the signal from the base stations. Then, after a while, the handsets will try to find base stations (with same ARI–System ID) on the other frequency band. The server must be restarted after changing frequency. **Note**: You can change the frequency setting in the server using OAM-REST API. For more information, see OAM REST API. For more information about frequency swap and the special Spectralink DECT Handset, see Frequency Swap Support.
Allow bearer handovers to repeaters (Optional) (Not relevant to the Spectralink IP-DECT Server 200/400)	If enabled, bearer handover to repeaters is allowed. If disabled, handovers between a repeater and base station must take place as connection handovers. Default value: Enabled **Note**: If Zone-based paging is used, then bearer handover is not allowed, and this setting is overruled.
Wireless Server Configuration–Media resources (Not relevant to the Spectralink IP-DECT Server 200/400)	
Allow new (Optional)	If enabled, new media resources are allowed to connect to the server. Default value: Enabled

Field	*Setting*
Add new as active (Optional)	If enabled, new media resources will become active when added. Otherwise they must be activated manually under **Administration**> **Media Resource**> **Media Resource** page. Default value: Disabled **Note**: This must be enabled if setting up a redundant system using internal media resource.
Require encryption (Optional)	If enabled, the connection between the media resource and the Spectralink IP-DECT/Virtual IP-DECT Server One is required to be encrypted. **Note**: Enabling this, will only allow media resources with firmware PCS 17Fa or newer to connect. Default value: Disabled If not enabled, the connection will be encrypted if the media resource supports encryption.
Wireless Server Configuration–Base stations (Not relevant to the Spectralink IP-DECT Server 200)	
Allow new (Optional)	If enabled, new base stations are allowed to connect to the server. Default value: Enabled
Add new as active (Optional)	If enabled, new base stations will become active when added. Otherwise, they must be activated manually under **Administration**> **Base Station**> **Base Station** page. Default value: Disabled.
Require encryption (Optional)	If enabled, the connection between the base station and the Spectralink IP-DECT/Virtual IP-DECT Server One is required to be encrypted. **Note**: Enabling this, will only allow base stations with firmware PCS 17Fa or newer to connect. Default value: Disabled If not enabled, the connection will be encrypted if the base station supports encryption.
Media encryption (SRTP) (Optional)	If enabled, secure RTP for base station audio connections is used. Default value: Disabled **Note**: If not running PCS 20A_ or newer, this field is only visible if a Security (TLS, SRTP) License is loaded.
RFP port range start	Port range start for RFP local RTP ports. Default value: 57000 **Note**: You can change the value in case of conflicting ports.
Paging method (not relevant to Spectralink IP-DECT Server 200/400)	“Paging” is about incoming voice and messaging calls, where the Spectralink IP-DECT/Virtual IP-DECT Server One has to send out an announcement (through the relevant Spectralink IP-DECT Base Stations) asking the handset to choose a base station and start establishing a connection. Possible values: **Default**, **Multicast**, **Site-based** paging, Zone-based paging. Default value: Default If having more than 256 base stations connected on a site, default paging is not enough due to the amount of base stations. In this situation, if multicast signaling is supported, multicast is the preferred paging method. Other paging methods are site-based paging and zone-based paging. On a site with heavy voice/messaging load, Spectralink recommends using Zone-based paging instead of using multicast signaling. If **Multicast** is enabled, this will impose multicast support for the network. For more information, see Using Multicast Signaling for Paging. **Note**: For more information about deciding which paging method to use, see Spectralink IP-DECT Base Station Configuration Methods–Considerations. Please read the information carefully before continuing and ensure correct deployment of the base stations.

Field	*Setting*
Zone-based paging (Optional)	Zone-based paging is used when grouping base stations into zone in site(s). Not using zone will be substantial in most average systems. **Note**: Zone-based paging is built on the DECT Standard for Location Area Level (LAL). **Note**: The field Paging method must be set to Zone-based paging to be able to use zone-based paging. Possible values: **8 Zone (32 base stations per zone)**, **16 Zone (16 base stations per zone)** or **32 Zone (8 base stations per zone)**. Default value: 8 Zone (32 base stations per zone). For more information about zone-based paging, see Spectralink IP-DECT Base Station Configuration Methods–Considerations. Please read the information carefully before continuing and ensure correct deployment of the base stations. **Caution**: Assigning RPN's are essential for using zone-based paging, as the RPN decides which zone the Spectralink IP-DECT Base Station will be part of. If changing zone size later on after having configured the base stations and assigned RPN's, then all configuration must be redone. Therefore, consider your system needs carefully before and when deploying. **Note**: Enabling **Zone-based paging** ensures automatic update of handset locations. For more information about configuration of sites and zone, see Configuring Sites (and Zone).
Multicast address (Optional)	Multicast address used for signaling. Default value: 239.255.1.11 Please refer to RFC 2365 and RFC 4291 for details. **Note**: Only used with multicast signaling as paging method.
Multicast TTL (Optional)	The TTL is used to limit the propagation of the multicast packets across routers. Default value: 1 **Note**: The TTL is configurable and you can change the value according to network topology. For more information, see vendor specific documentation. **Note**: Only used with multicast signaling as paging method.
Default sync type (Optional)	This setting controls the default sync type for new base stations connecting to the server. Possible values: **Free running**, **Radio** or **LAN**. **Note**: Selecting **Free running** will configure each base station as a sync master. For more information, see also Synchronization and Deployment Guide. Default value: Radio **Note**: Multicast address and Multicast TTL are hardcoded, when selecting **LAN**. For more information, see Using Multicast for LAN.
LAN sync transport protocol (Optional)	The protocol transport layer used by PTP for LAN sync. Possible values: **Ethernet**, **IPv4** or **IPv6**. For more information about using LAN synchronization, see LAN-Based Synchronization.
LAN sync type of service (TOS/Diffserv) (Optional)	TOS/DiffServ values can be configured for PTP packets used for LAN sync. The values are entered in decimal. Network priority: Packets with higher TOS/DiffServ have higher priority on the network. 184 = critical (highest priority) 96 = flash 64 = immediate 32 = priority

Field	*Setting*
	0 = routine (lowest priority) Default value: 184 (Expedited Forwarding)

Allow web-based Administration
Page (Optional)
	If disabled, the web-based Administration Page (GUI) of all connected base stations will be disabled.
	Default value: Enabled
	Note: You can disable the web-based Administration
	Page directly in the configuration file by inserting the following:
	`<rfp>`
	`<allow_gui>false</allow_gui>`
	`</rfp>`
	Change "false" to "true" to enable it.
	For more information, see Disabling Web-Based Administration Page.

Wireless Server Configuration–Handsets (Not relevant to the Spectralink IP-DECT Server 200)	
Handset sharing (Optional)	Enabled by default when Handset Sharing License is loaded. Disable this, if handset sharing is not to be allowed. For more information about using handset sharing and configuring handset login, see Handset Sharing.
Handset login (Only visible if Lync/SfB + Security (TLS, SRTP) License is loaded)	If enabled, user credentials can be entered on the handset and no user configuration is required on the server. Use long key press 9 to login. (System dependent). For more information, see Configuring Handset Login and Handset User Guides.
Wireless Server Configuration–Application interface	
Username	Enter username required to access the application interface. Max. length: 31 characters.
New password (Optional)	Enter password required to access the application interface. Max. length: 31 characters.
New password again (Optional)	Confirm password required to access the application interface.
Enable MSF (Optional)	If enabled, access to the MSF application interface is supported. Default value: Disabled
Enable XML-RPC (Optional)	If enabled, access to the XML-RPC application interface is supported. Default value: Disabled
Internal messaging (Optional)	If enabled, internal messaging to allow handset-to-handset messaging without an external application is supported.
Enable FAS connectivity (Optional) (System dependent and only relevant if using ATEX handset)	If enabled, connectivity to FAS is supported. Default value: Disabled
ATEX handset GAP enrollment type (Optional) (Only relevant if using ATEX handset)	If enabled, GAP as enrollment type is used instead of DOIP enrollment type. Default value: Disabled
Wireless Server Configuration–Feature codes	
Enable (Optional)	If enabled, feature codes for controlling features from the handsets can be used.

Field	*Setting*
Call forward unconditional–enable (Optional)	Enable call forward unconditional by dialing this code (***21***), followed by the desired extension ($ = extension) and **#.** E.g.: ***21*$#** **Note**: You can change the code *21* on the Spectralink IP-DECT/Virtual IP-DECT Server One to fit your standard. For more information, see the relevant documentation available at http://support.spectralink.com/.
Call forward unconditional–disable (Optional)	Disable call forward unconditional by dialing this code (**#21#**).
Wireless Server Configuration–Languages	
Phone Language (Optional)	Language of system messages displayed in handset. Select the desired language from the list.
Wireless Server Configuration–MSF	
Enable Long-Press Key0–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key1-Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key2–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key3–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key4–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key5–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key6–Undefined (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press.
Enable Long-Press Key7–Undefined (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for replacing handsets as an admin rights user. For more information about creating an admin rights user, see Registering Users and Subscribing Handsets. For more information about handset replacement, see Admin Rights User.
Enable Long-Press Key8–Undefined (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press.
Enable Long-Press Key9–Handset Sharing (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for handset sharing. For more information, see Handset Sharing and User Sign-in/Sign-out.

4 Click **Save**.

Enable Handset Login on Spectralink DECT Handset

The Handset Login feature can be invoked in two ways:

- By utilizing MSF function number 9, either from the handset main menu or by long-pressing the '9' key (not supported by Handset 7502). Long-press must be enabled in the handset in the **Settings**> **Advanced**> **Long Key** menu. For more information, see Handset User Guides.
- Through the shortcut menu using the Sign in/out shortcut. For more information, see Handset User Guides.

Note:

If you cannot access the feature on your handset, contact your system administrator.

When invoking the Handset Login feature, a menu is presented allowing the user to select signing in with either extension and PIN (if configured) or with username and password. Entering the required credentials will allow the Spectralink IP-DECT/Virtual IP-DECT Server One to connect the user to the Call handler and the handset will be ready for use.

Signing into a Device from the Handset

When accessing the Sign in menu, you can choose between PIN Sign in or Sign in (PIN Sign in is only visible if PIN authentication is available and configured on the server of the call handler, e.g. Skype for Business).

1. When in idle mode, access the Sign in menu by using either Sign in/out shortcut or long-press key 9.
2. If selecting **PIN Sign in**:
   - Enter number and click **OK**.
   - Enter PIN, and click **OK**.
3. If selecting **Sign in**:
   - Enter user and click **OK**.
   - Enter password, and click **OK**.
4. The handset is now ready for use.

Signing out from a Device from the Handset

1. When in idle mode, sign out by using either Sign in/out shortcut or long-press key 9.
2. Select **Sign out** and click **OK**.

Note:

If supported by the handset the following lists are cleared in the handset, after a successful sign-in/sign-out:

- Incoming/outgoing/missed calls list
- Incoming/outgoing message list
- Task list
- Message template list

Adding Devices to Server

Devices can be added and subscribed without any SIP users associated. Devices are identified by the IPEI, which is a globally unique number identifying the Spectralink Handset.

Handsets can be added manually to the Spectralink IP-DECT/Virtual IP-DECT Server One by specifying an IPEI or they can be automatically created, when subscribed to the Spectralink IP-DECT/Virtual IP-DECT Server One.

Data are split in two categories.

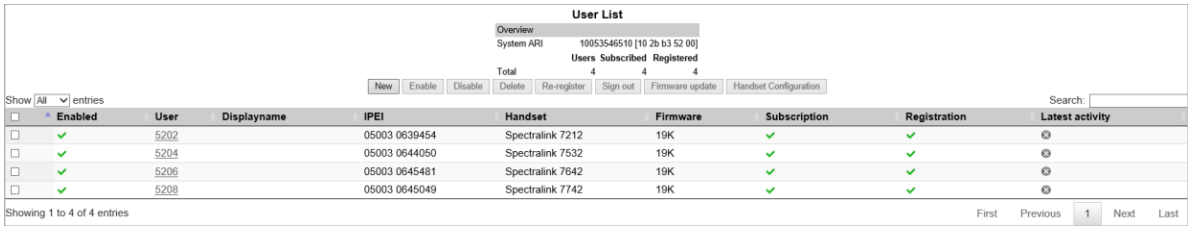
Device data (handset)

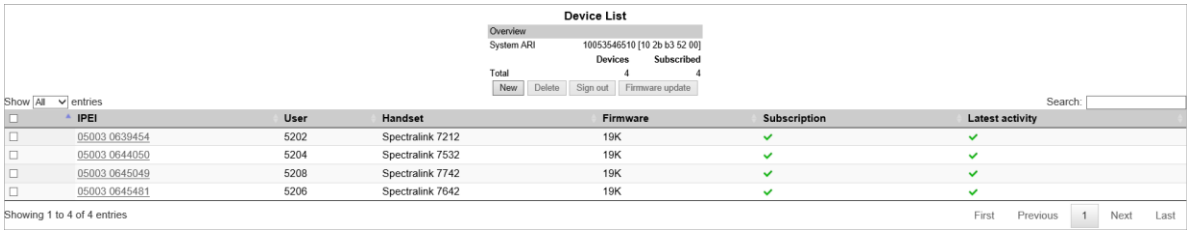
Device specific data includes an IPEI (mandatory) and an access code (optional). The access code is used for subscribing the device to the Spectralink IP-DECT/Virtual IP-DECT Server One.

User data (username, standby text, display name etc.)

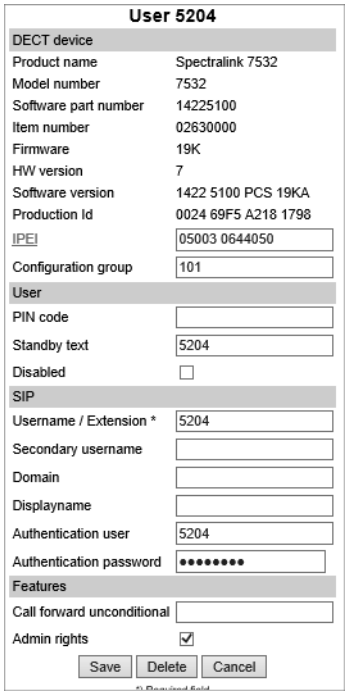
If a user is signed in, it will be visible in the **Users**> **List Users**> **User List**. Editing the username will allow the administrator to “sign-in” a user to the device or alternatively to sign-out” a user.

With handset sharing enabled, you now see not only the **List Users** menu item for the **Users**, but also a **List Devices** menu item for the handsets.





When clicking on a User under the **List Users** menu, you see that the **User** profile is very similar to the **User** profile without Handset Sharing License installed. See image below.



The IPEI field is still there, now with a new IPEI link and optional new PIN code field.

Note:

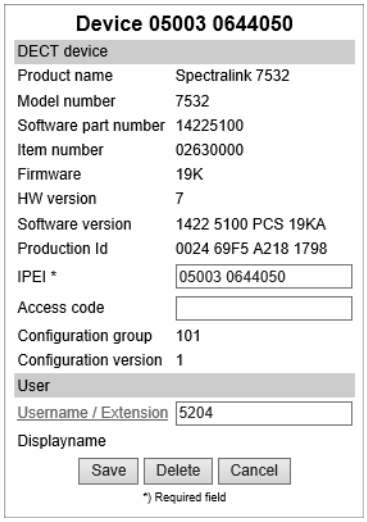
You may fill the new **PIN code** field for added security to prevent other users from linking a handset with your user profile.

When a user is linked to a handset, the IPEI link is active and can be clicked upon, and the IPEI text field holds the IPEI number of the linked handset.

Note:

A User with no linked handset will show an inactive IPEI link and no IPEI number in the IPEI text field.

On the **Device** profile, notice the **Username** / **Extension** link. If the handset is linked to a specific user, the text field will hold the extension number of that user and the **Username** / **Extension** link is active.



Clicking on **Username** / **Extension** the link will take you to the User profile of the linked handset. And when clicking on the **IPEI** link from the User profile, that will take you to the **Device** profile of the linked handset.

Note:

If the user is not linked to a handset, this **Username** / **Extension** link is inactive and there is no extension number in the associated text field.

For examples of handset sharing, see Handset Sharing Setup Examples.

Adding Users to Server

Users are identified by their SIP username. User data are split in four categories:

DECT device

Mainly used for information about associated device (if any). Furthermore, by editing the IPEI it is possible for the administrator to “sign-in” a user to the device or alternatively to “sign-out” a user.

User

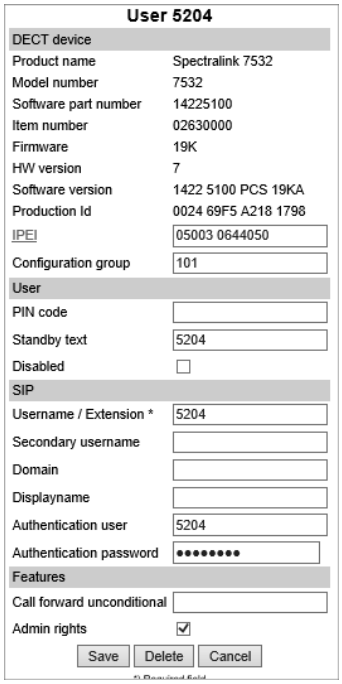
User data is data specific to a specific user. The Standby text is displayed in the handset when the user is signed-in. If no user is currently signed into a device the device will display “Signed out”. The user PIN code is used by the user to sign-in to a device.

SIP

The sip category consists of SIP data specific to the user.

Features

Features are user specific feature data.



Handset Sharing and Provisioning

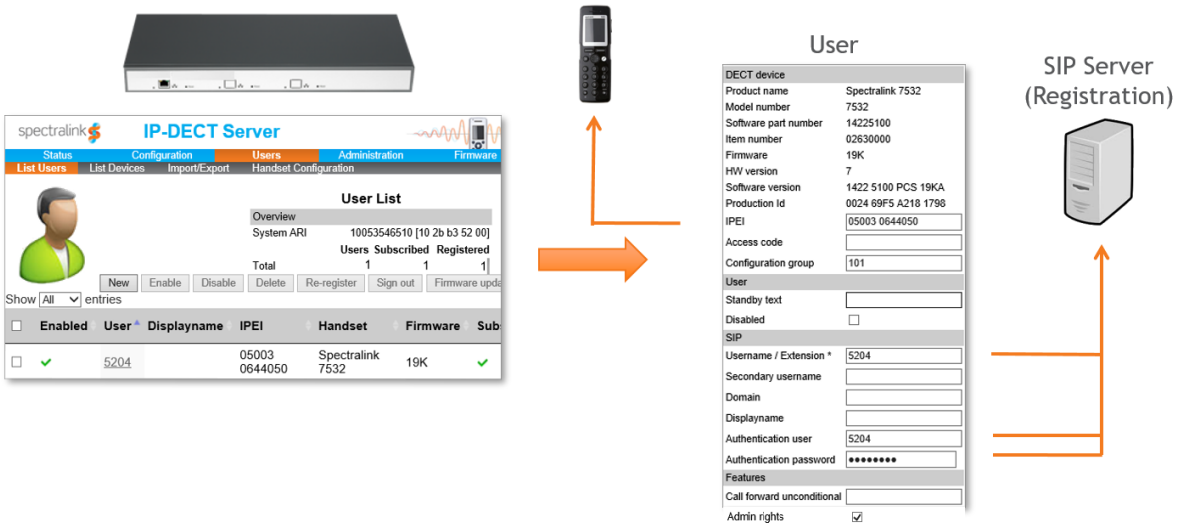
Handset sharing is used in combination with provisioning. Users can be provisioned via the <MAC/UUID>-users.xml file. Devices cannot be provisioned because the intention is that devices will be automatically created when they are subscribed.

Spectralink recommends provisioning users without an IPEI and let the user/device binding be handled by signing-in from the handsets.

Furthermore, Spectralink recommends not creating the devices manually via the web-based Administration Page, but let the system automatically create them when subscribed. For security reasons, Spectralink recommends restricting device subscription with a system access code.

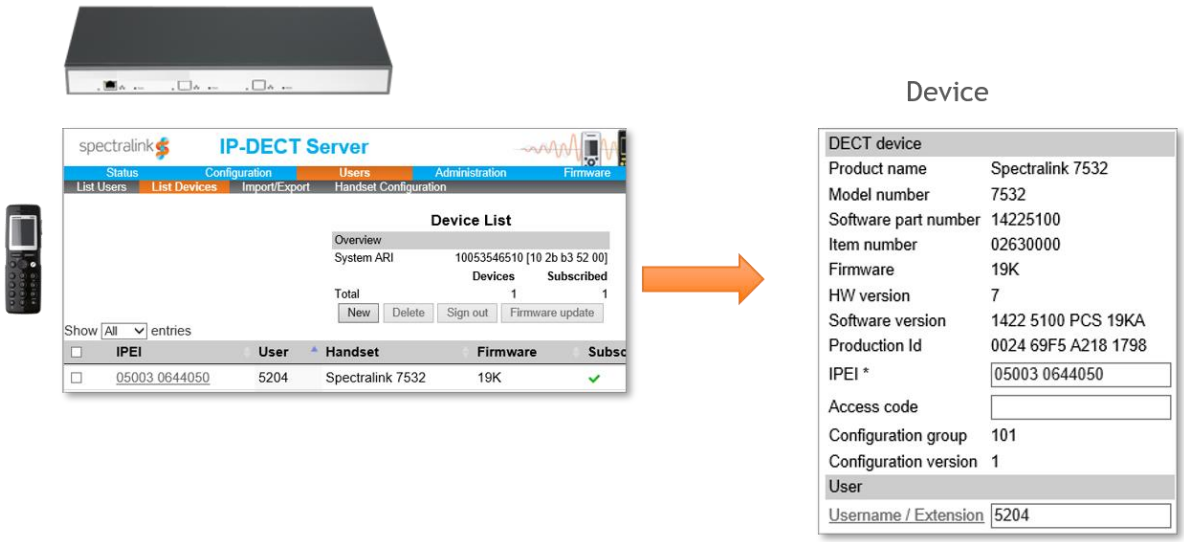
For more information about provisioning, see *Provisioning Guide*.

Handset Sharing Setup Examples



- Any handset can be linked with any User at any given time
- Handset sign-in and sign-out using PIN code
- IPEI link is active when User is linked to a handset
- PIN code field is used during handset sign-in

Once the Handset Sharing License is loaded onto the Spectralink IP-DECT/Virtual IP-DECT Server One, any handset can now be linked with any User at any given time, as long as that User is not linked with another handset. This happens during a process, where the User signs in with an arbitrary handset using the extension number of the User and an optional PIN code associated with the User.



- A Device is a subscribed handset
- A User (represented by Username / Extension link) is active when linked to a device

- Link handset to vacant User during subscription
- Link User to handset during User creation

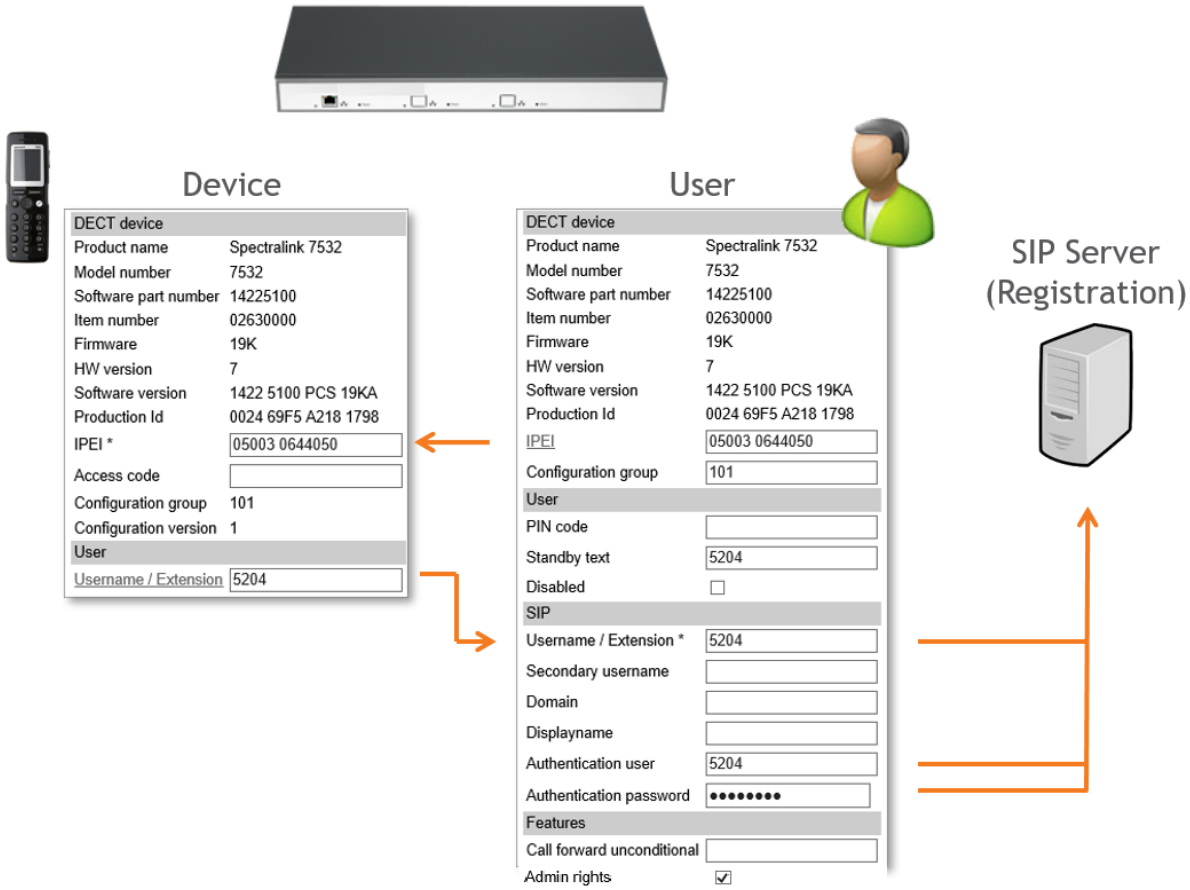
When clicking on an IPEI number under the **Device List** page, you see a **Device** profile which in essence is a unique handset, that has been subscribed to the Spectralink IP-DECT/Virtual IP-DECT Server One. The **Device** profile holds information about the handset's IPEI number and optional access code used, when the handset is subscribed to the Spectralink IP-DECT/Virtual IP-DECT Server One.

Note:

The access code should not be mistaken for the PIN code.

When subscribing a handset, you can choose to **link the handset to an existing vacant User** during the subscription process.

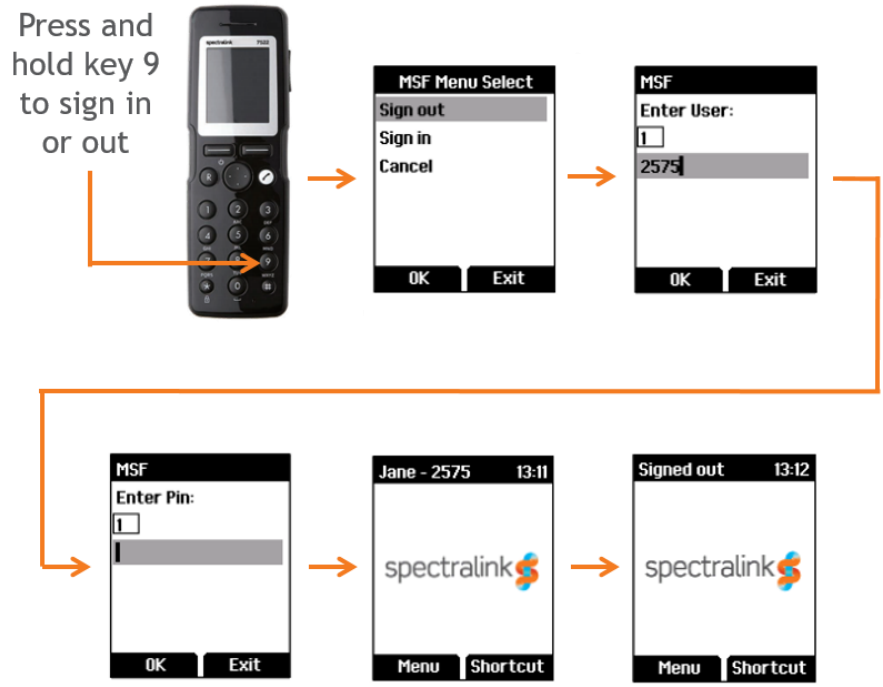
You can also work the other way around so that when creating a User you can choose to **link the user to an existing handset** by typing the IPEI. If the handset is already linked to another user, the handset will be released from that user and the handset will be linked with the user you are creating. For more information, see Registering a User.



- Device (handset) and User are linked
- User is registered with SIP Server

Above you see how a **Device** profile is linked to a **User** profile. Notice how the **IPEI** number and the **Username** / **Extension** number are associated, indicating a link between the Device and User. Also notice the User registration with the SIP Server.

Example of Setting Up Handsets for Handset Sharing



1. A Handset Sharing | IP-DECT/DECT Servers 400/6500/2500/8000 License or Handset Sharing 1 Year | Virtual IP-DECT Server One License must be loaded to the Spectralink IP-DECT/Virtual IP-DECT Server One.
2. Set up handset for Send MSF: **Menu**> **Settings**> **Advanced**> **Long key**> **Send MSF**.

Note:

Alternatively, if you need to do this for many handsets, use the Handset and Repeater Management Tool.

3. To sign in, press and hold key 9 until the sign in screen appears.
4. Select **Sign In**, and then enter the User number (typically your Extension number).
5. Enter the PIN code.
6. If sign-in is successful, the standby text will show in the display.
7. Long press key 9 to sign out. The standby text will show signed out upon successful sign out.

Chapter 30: Product Compatibility

If you have any questions about product compatibility, contact your system administrator.

You can use the Spectralink IP-DECT/Virtual IP-DECT Server One with other Spectralink products as identified by the type approval model ID and/or part number located on the label of the product.

Spectralink Products	
Spectralink Server	
Spectralink IP-DECT Server 200	K005 (72345600 / 72345601)
Spectralink IP-DECT Server 400	K005 (02344500 / 02344501)
Spectralink IP-DECT Server 6500	K006 (02350000)
Spectralink Virtual IP-DECT Server One	14233244
Power Supply, 8.0V DC (only IP-DECT Server 200/400)	84642600
External Antenna (with 1 m connection cable) (only IP-DECT Server 200/400)	02319507
Connection cable for External Antenna, 7.5 m (only IP-DECT Server 200/400)	14002706
Spectralink Base Station	
Spectralink IP-DECT Base Station 1G8	K005
Spectralink IP-DECT Base Station 1G9	K005
Power Supply, 8.0V DC	84642600
Spectralink DECT Repeater	
Spectralink DECT Repeater 1G8, 2 channels, with connector for external antenna	K018B (02440000)
Spectralink DECT Repeater 1G9, 2 channels, with connector for external antenna	K018B (02441000)
Spectralink DECT Repeater 1G8, 2 channels, without connector for external antenna	K018 (02441100)
Spectralink DECT Repeater 1G9, 2 channels, without connector for external antenna	K018 (02441200)
Spectralink DECT Repeater 1G8, 4 channels, with connector for external antenna	K018 (02441600)
Spectralink DECT Repeater 1G9, 4 channels, with connector for external antenna	K018 (02440200)
Spectralink DECT Repeater 1G8, 4 channels, without connector for external antenna	K018C (02334601)
External Antenna (with 1 m connection cable)	02319507
Connection cable for External Antenna, 7.5 m	14002706
Power Supply (9.0V DC, 350mA)	84642602
Repeater Programming Kit	02509210
Spectralink DECT Media Resource	
Spectralink DECT Media Resource (only IP-DECT Server 6500 and Virtual IP-DECT Server One)	K006

Spectralink Products	
Spectralink Virtual IP-DECT Media Resource	
Spectralink Virtual IP-DECT Media Resource (only Virtual IP-DECT Server One)	14233270
Spectralink Server Licenses for 200	
Lync/SfB + Security (TLS, SRTP) | IP-DECT Server 200 *	14075511
Lync/SfB + Security (TLS, SRTP) 3 Users | IP-DECTServer 200 *	14232830
OAM-REST-API | IP-DECT Server 200	14232835
Security (TLS, SRTP) | IP-DECT Server 200 *	14075281
Firmware Update License 12 Users. For server and handset firmware update. This license is built-in in the server firmware from R3-2020.	14232870
The following licenses are required from Q4-2018 and until R2-2020 (including R2-2020).	
Software Assurance 1 Year 12 Users | IP-DECT Server 200	14232800
Software Assurance 3 Years 12 Users | IP-DECT Server 200	14232801
Software Assurance 5 Years 12 Users | IP-DECT Server 200	14232842
* The Software Security Package is not needed on servers running PCS 20A_ or newer as security from R1-2020 is available without license.	
Spectralink Server Licenses for Server 400	
12 Channels + 24 Users | IP-DECT Server 400	14075500
Lync/SfB + Security (TLS, SRTP) | IP-DECT Server 400 *	14075510
Lync/SfB + Security (TLS, SRTP) 6 Users | IP-DECT Server 400 *	14232838
Multicell | IP-DECT Server 400	14075520
12 Channels + 24 Users + Multicell | IP-DECT Server 400	14075560
Multicell, Max voice channels, 48 Users | IP-DECT Server 400	14232839
Cisco Unified CM (Advanced Features) | IP-DECT Server 400	14075490
CTI | IP-DECT Server 400	14232868
LAN Sync | IP-DECT Server 400	14075600
Enhanced Provisioning | IP-DECT Server 400	14075701
OAM-REST-API | IP-DECT Server 400	14232836
Frequency Swap | IP-DECT/DECT Servers 400/6500/2500/8000	14075620
Handset Sharing | IP-DECT/DECT Servers 400/6500/2500/8000	14075460
Automatic Alarm Call | IP-DECT/DECT Servers 300/400/2500/6000/6500/8000	14075450
Security (TLS, SRTP) | IP-DECT/DECT Servers 400/6000/6500/2500/8000 *	14075280

Spectralink Products	
Additional repeaters (up to 6 repeaters) | IP-DECT Server 400	14075570
Software Assurance 1 Year 12 Users | IP-DECT Server 400	14232802
Software Assurance 3 Years 12 Users | IP-DECT Server 400	14232803
Software Assurance 5 Years 12 Users | IP-DECT Server 400	14232843
Software Assurance 1 Year 24 Users | IP-DECT Server 400	14232804
Software Assurance 3 Years 24 Users | IP-DECT Server 400	14232805
Software Assurance 5 Years 24 Users | IP-DECT Server 400	14232844
Software Assurance 1 Year 60 Users | IP-DECT Server 400	14232840
Software Assurance 3 Year 60 Users | IP-DECT Server 400	14232841
Software Assurance 5 Year 60 Users | IP-DECT Server 400	14232845

* The Software Security Package is not needed on servers running PCS 20A_ or newer as security from R1-2020 is available without license.

Spectralink Server Licenses for Server 6500	
150 Users | IP-DECT Server 6000/6500	14075210
500 Users | IP-DECT Server 6000/6500	14075220
1500 Users | IP-DECT Server 6000/6500	14075230
4096 Users | IP-DECT Server 6000/6500	14075240
Redundancy Master | IP-DECT Server 6000/6500	14075250
Redundancy Backup | IP-DECT Server 6000/6500	14075260
LAN Sync | IP-DECT Server 6500	14075610
Frequency Swap | IP-DECT/DECT Servers 400/6500/2500/8000	14075620
Cisco Unified CM (Advanced Features) | IP-DECT Server 6500	14075495
CTI | IP-DECT Server 6500	14232869
Lync/SfB + Security (TLS, SRTP) | IP-DECT Server 6000/6500 *	14075270
Enhanced Provisioning | IP-DECT Server 6500	14075700
OAM-REST-API | IP-DECT Server 6500	14232837
Handset Sharing | IP-DECT/DECT Servers 400/6500/2500/8000	14075460
Automatic Alarm Call | IP-DECT/DECT Servers 300/400/2500/6000/6500/8000	14075450
Security (TLS, SRTP) | IP-DECT/DECT Servers 400/6000/6500/2500/8000 *	14075280
Software Assurance 1 Year 30 Users | IP-DECT Server 6500	14232806

Spectralink Products	
Software Assurance 3 Years 30 Users | IP-DECT Server 6500	14232807
Software Assurance 5 Years 30 Users | IP-DECT Server 6500	14232846
Software Assurance 1 Year 150 Users | IP-DECT Server 6500	14232808
Software Assurance 3 Years 150 Users | IP-DECT Server 6500	14232809
Software Assurance 5 Years 150 Users | IP-DECT Server 6500	14232847
Software Assurance 1 Year 500 Users | IP-DECT Server 6500	14232810
Software Assurance 3 Years 500 Users | IP-DECT Server 6500	14232811
Software Assurance 5 Years 500 Users | IP-DECT Server 6500	14232848
Software Assurance 1 Year 1500 Users | IP-DECT Server 6500	14232812
Software Assurance 3 Years 1500 Users | IP-DECT Server 6500	14232813
Software Assurance 5 Years 1500 Users | IP-DECT Server 6500	14232849
Software Assurance 1 Year MAX Users | IP-DECT Server 6500	14232814
Software Assurance 3 Years MAX Users | IP-DECT Server 6500	14232815
Software Assurance 5 Years MAX Users | IP-DECT Server 6500	14232850

* The Software Security Package is not needed on servers running PCS 20A_ or newer as security from R1-2020 is available without license.

Spectralink Server Licenses for Virtual Server One	
Mandatory Base Licence ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One	14233244
30 Users | Virtual IP-DECT Server One	14233200
150 Users | Virtual IP-DECT Server One	14233201
500 Users | Virtual IP-DECT Server One	14233202
1500 Users | Virtual IP-DECT Server One	14233203
4096 Users | Virtual IP-DECT Server One	14233204
Lync/SfB 1 Year | Virtual IP-DECT Server One	14233252
Handset Sharing 1 Year | Virtual IP-DECT Server One	14233253
Enhanced Provisioning 1 Year | Virtual IP-DECT Server One	14233250
OAM-REST-API 1 Year | Virtual IP-DECT Server One	14233249
Frequency Swap | Virtual IP-DECT Server One	14233248
Redundancy Master | Virtual IP-DECT Server One	14233246
Redundancy Backup | Virtual IP-DECT Server One	14233247

Spectralink Products	
LAN Sync | Virtual IP-DECT Server One	14233245
32 Media Channels | Virtual IP-DECT Server One	14233270
16 Base Stations | Virtual IP-DECT Server One	14233233
64 Base Stations | Virtual IP-DECT Server One	14233234
256 Base Stations | Virtual IP-DECT Server One	14233235
1024 Base Stations | Virtual IP-DECT Server One	14233236
Software Assurance 1 Year 30 Users | Virtual IP-DECT Server One	14233211
Software Assurance 3 Years 30 Users | Virtual IP-DECT Server One	14233212
Software Assurance 1 Year 150 Users | Virtual IP-DECT Server One	14233213
Software Assurance 3 Years 150 Users | Virtual IP-DECT Server One	14233214
Software Assurance 1 Year 500 Users | Virtual IP-DECT Server One	14233215
Software Assurance 3 Years 500 Users | Virtual IP-DECT Server One	14233216
Software Assurance 1 Year 1500 Users | Virtual IP-DECT Server One	14233217
Software Assurance 3 Years 1500 Users | Virtual IP-DECT Server One	14233218
Software Assurance 1 Year 4096 Users | Virtual IP-DECT Server One	14233219
Software Assurance 3 Years 4096 Users | Virtual IP-DECT Server One	14233220

Chapter 31: Technical Specification

Below you will find technical specifications of the different Spectralink Server Solution components:

Spectralink IP-DECT Server 200

PROTOCOL SUPPORT

- Session Initiated Protocol (SIP)
- Broadcast Messaging
- Message Service Functions (MSF)
- XML-RPC
- OAM-REST-API

SIP VOIP SUPPORT

- Basic call
- CLIP
- Call Hold
- Call Transfer
- Call Waiting
- Music on Hold (MOH)

OPERATION AND MAINTENANCE

- Web GUI for administration and maintenance of the entire infrastructure
- HTTP with digest authentication
- HTTPS
- Syslog
- SNMP

SYSTEM ARCHITECTURE

- The Spectralink IP-DECT Server 200 is both a radio unit and a SIP integration unit to the host SIP Call Control / UC platform.
- 1 x Spectralink IP-DECT Server 200 and up to 3 x Spectralink DECT Repeaters (2 or 4 channel multi-cell)

12 wireless users/six simultaneous calls

SUPPORTED CODECS

- G.711 A-law and µ-law
- G.726 (32 kbps–4 bit ADPCM)
- G.729

NETWORK

- 10/100 Mbps Ethernet port
- Manual or dynamic host configuration protocol (DHCP)
- Time and date synchronization using Network Time Protocol (NTP)
- LED status indication

PROVISIONING

- Configuration
- User data
- Server firmware
- Handset firmware

RADIO INTERFACE

- RF output 20 to 24 dBm at antenna connection
- Sensitivity: typical -90 dBm measured at antenna connection at BER = 0.001
- Average transmit power: typical 5mW/ch (US) or 10mW/ch. (EU)
- Peak transmit power: typical 125mW (US) or 250mW (EU)
- Typical range:
  - Indoor: 20–50 m. (65–165 ft.)
  - Outdoor: 300 m. (1000 ft.)
- Full slot DECT radio (12 channels)
- Possible to connect external antenna (Only Spectralink External Antenna can be used)

ELECTRO MAGNETIC COMPATIBILITY (EMC) APPROVALS (REGULATORY STANDARDS)

- EMC: EN 301 489–1
- EMC: EN 301 489–6
- FCC RULES, FCC PART15
- ANSI C63.4

SAFETY (REGULATORY STANDARDS)

- UL60950-1
  - CAN/CSA-C22.2 No. 60950-1
  - AS/NZS 60950-1
- Safety: EN 60950–1

DECT RADIO APPROVAL

- EN 301 406

ENVIRONMENTAL CONDITIONS

- Operating temperature: 10–40º C (50–104º F)
- Storage temperature: -50–70º C (-58–158º F)
- Relative humidity: between 20% and 80% (non-condensing)
- Compliance with the requirements of EU directive 2015/863/EU (ROHS) and 2012/19/EU (WEEE)

ELECTRICAL REQUIREMENTS

- Power over Ethernet (IEEE 802.3af), mode A & B
- PoE Class 1 device
- Typical power consumption: 3 W per unit
- External power outlet (power supply must be ordered separately)
- External antenna connection (Only Spectralink External Antenna can be used)

PHYSICAL CHARACTERISTICS

- Size: 100 x 100 x 43 mm (3.94 x 3.94 x 1.69 in.)
- Weight: 120 gr. (4.2 oz)
- Black (Pantone Black)
- Wall-mountable, indoor
- Can be mounted upside down

INTEROPERABILITY

- For information about supported Call Control/Unified Communications (UC) (PBX and IP- PBX) platforms, visit http://support.spectralink.com/.

Spectralink IP-DECT Server 400

PROTOCOL SUPPORT

- Session Initiated Protocol (SIP)
- Broadcast Messaging
- Message Service Functions (MSF)
- XML-RPC
- OAM-REST-API

SIP VOIP SUPPORT

- Basic call
- CLIP
- Call Hold
- Call Transfer
- Call Waiting
- Music on Hold (MOH)

OPERATION AND MAINTENANCE

- Web GUI for administration and maintenance of the entire infrastructure
- HTTP with digest authentication
- HTTPS
- Syslog
- SNMP

SYSTEM ARCHITECTURE

- The Spectralink IP-DECT Server 400 is both a radio unit and a SIP integration unit to the host SIP Call Control / UC platform. Additionally, it controls and handles the Spectralink IP-DECT Base Stations.
- Single-cell configuration:
- 1 x Spectralink IP-DECT Server 400 and up to 3 x Spectralink DECT Repeaters (2 or 4 channel multi-cell)
- 12 wireless users/six simultaneous calls Optional 60 users *

Note:

* The Spectralink IP-DECT Server 400 does have 12 channels, but is limited to 6 channels in basic version.

- Multi-cell configuration:

1 x Spectralink IP-DECT Server 400, up to 9 x Spectralink IP-DECT Base Stations and up to 3 x Spectralink DECT Repeaters (2 or 4 channel multi-cell) connected on each Spectralink IP- DECT Server or Spectralink IP-DECT Base Station **.

12 wireless users/six simultaneous calls Optional 60 users/24 simultaneous calls

Note:

* * The Spectralink IP-DECT Base Station does have 12 channels, but only 11 can be used when synchronizing over the air.

SUPPORTED CODECS

- G.711 A-law and µ-law
- G.726 (32 kbps–4 bit ADPCM)
- G.729

NETWORK

- 10/100 Mbps Ethernet port
- Manual or dynamic host configuration protocol (DHCP)
- Time and date synchronization using Network Time Protocol (NTP)
- LED status indication

PROVISIONING

- Configuration
- User data
- Server firmware
- Base station firmware (License required)
- Handset firmware (License required)

RADIO INTERFACE

- RF output 20 to 24 dBm at antenna connection
- Sensitivity: typical -90 dBm measured at antenna connection at BER = 0.001
- Average transmit power: typical 5mW/ch (US) or 10mW/ch. (EU)
- Peak transmit power: typical 125mW (US) or 250mW (EU)

- Typical range:
  - Indoor: 20–50 m. (65–165 ft.)
  - Outdoor: 300 m. (1000 ft.)
- Full slot DECT radio (12 channels)
- Possible to connect external antenna (Only Spectralink External Antenna can be used)

ELECTRO MAGNETIC COMPATIBILITY (EMC) APPROVALS (REGULATORY STANDARDS)

- EMC: EN 301 489–1
- EMC: EN 301 489–6
- FCC RULES, FCC PART15
- ANSI C63.4

SAFETY (REGULATORY STANDARDS)

- UL60950-1
  - CAN/CSA-C22.2 No. 60950-1
  - AS/NZS 60950-1
- Safety: EN 60950–1

DECT RADIO APPROVAL

- EN 301 406

ENVIRONMENTAL CONDITIONS

- Operating temperature: 10–40º C (50–104º F)
- Storage temperature: -50–70º C (-58–158º F)
- Relative humidity: between 20% and 80% (non-condensing)
- Compliance with the requirements of EU directive 2015/863/EU (ROHS) and 2012/19/EU (WEEE)

ELECTRICAL REQUIREMENTS

- Power over Ethernet (IEEE 802.3af), mode A & B
- PoE Class 1 device
- Typical power consumption: 3 W per unit
- External power outlet (power supply must be ordered separately)
- External antenna connection (Only Spectralink External Antenna can be used)

PHYSICAL CHARACTERISTICS

- Size: 100 x 100 x 43 mm (3.94 x 3.94 x 1.69 in.)
- Weight: 120 gr. (4.2 oz)
- Grey-white (NCS 0502-Y)
- Wall-mountable, indoor
- Can be mounted upside down

INTEROPERABILITY

- For information about supported Call Control/Unified Communications (UC) (PBX and IP- PBX) platforms, visit http://support.spectralink.com/.

Spectralink IP-DECT Server 6500

PROTOCOL SUPPORT

- Session Initiated Protocol (SIP)
- Broadcast Messaging
- Message Service Functions (MSF)
- XML-RPC
- OAM-REST-API

SIP VOIP SUPPORT

- Basic call
- CLIP
- Call Hold
- Call Transfer
- Call Waiting
- Music on Hold (MOH)

OPERATION AND MAINTENANCE

- Web GUI for administration and maintenance of the entire infrastructure
- Provisioning, maintenance, and supervision of all infrastructure components and Spectralink 7000 handsets in the solution
- HTTP with digest authentication
- HTTPS
- Syslog
- SNMP

SYSTEM ARCHITECTURE

- The Spectralink IP-DECT Server 6500 is a control unit acting as a SIP integration unit to the host SIP Call Control / UC (IP-PBX) platform, which also controls and handles all other infra- structure elements
- Max. no. of:
  - Spectralink IP-DECT Base Stations: 1024
  - Simultaneous calls on each Spectralink IP-DECT Base Station: 12
  - Spectralink DECT Repeater on each Spectralink IP-DECT Base Station: 3
  - Spectralink DECT Media Resources: 32
  - Simultaneous calls with one Spectralink DECT Media Resource (G.711): 32
  - Simultaneous calls with 32 Spectralink DECT Media Resources: 1024
- Registered Spectralink 7000 handsets: scalable to 4096 stepwise: 30 users, 150 users, 500 users, 1500 users, 4096 users

SUPPORTED CODECS

- G.711 A-law and µ-law
- G.726 (32 kbps–4 bit ADPCM)
- G.729

NETWORK

- 10/100 Mbps Ethernet port
- Manual or dynamic host configuration protocol (DHCP)
- Time and date synchronization using Network Time Protocol (NTP)

PROVISIONING

- Configuration
- User data
- Server firmware
- Base station firmware (License required)
- Handset firmware (License required)

APPROVALS (REGULATORY STANDARDS)

- EN 55022
- EN 55024: A, A2
- FCC RULES, CRF47, PART15, class B digital device

SAFETY (REGULATORY STANDARDS)

- UL 60950-1 CAN/CSA-C22.2 No. 60950-1-03
- Safety: EN 60950–1

ENVIRONMENTAL CONDITIONS

- Operating temperature: 10–40º C (50–104º F)
- Storage temperature: -50–70º C (-58–158º F)
- Relative humidity: between 20% and 80% (non-condensing)
- Compliance with the requirements of EU directive 2015/863/EU (ROHS) and 2012/19/EU (WEEE)

ELECTRICAL REQUIREMENTS

- The supplied power for unit must be 110 to 240 AC nominal, 50/60 Hz

PHYSICAL CHARACTERISTICS

- Size: 440 x 199 x 44 mm (17.3 x 7.8 x 1.7 in.)
- Weight: 2,354 gr. (83.0 oz)
- Grey
- Rack and wall-mountable, indoor
- IP20

INTEROPERABILITY

- For information about supported Call Control/Unified Communications (UC) (PBX and IP- PBX) platforms, visit http://support.spectralink.com/.

Spectralink Virtual IP-DECT Server One

PROTOCOL SUPPORT

- Session Initiated Protocol (SIP)
- Broadcast Messaging
- Message Service Functions (MSF)
- XML-RPC
- OAM-REST-API

SIP VOIP SUPPORT

- Basic call

- CLIP
- Call Hold
- Call Transfer
- Call Waiting
- Music on Hold (MOH)

OPERATION AND MAINTENANCE

- Web GUI for administration and maintenance of the entire infrastructure
- Provisioning, maintenance, and supervision of all infrastructure components and Spectralink 7000 handsets in the solution
- HTTP with digest authentication
- HTTPS
- Syslog
- SNMP

SYSTEM ARCHITECTURE

- The Spectralink Virtual IP-DECT Server One is a control unit acting as a SIP integration unit to the host SIP Call Control / UC (IP-PBX) platform, which also controls and handles all other infrastructure elements
- Max. no. of:
  - Spectralink IP-DECT Base Stations: 2048
  - Simultaneous calls on each Spectralink IP-DECT Base Station: 12
  - Spectralink DECT Repeater on each Spectralink IP-DECT Base Station: 3
  - Spectralink DECT Media Resources: 32–each with 32 channels
  - Spectralink Virtual IP-DECT Media Resources: 16–each with up to 64 channels
  - Simultaneous calls with one Spectralink DECT Media Resource (G.711): 32
  - Simultaneous calls with 32 Spectralink DECT Media Resources: 1024
  - Simultaneous calls with one Spectralink Virtual IP-DECT Media Resource (G.711): 64
  - Simultaneous calls with 16 Spectralink Virtual IP-DECT Media Resource: 1024
- Registered Spectralink 7000 handsets: scalable to 4096 stepwise: 30 users, 150 users, 500 users, 1500 users, 4096 users

SUPPORTED CODECS

- G.711 A-law and µ-law
- G.726 (32 kbps–4 bit ADPCM)
- G.729

NETWORK

- 10/100 Mbps Ethernet port
- Manual or dynamic host configuration protocol (DHCP)
- Time and date synchronization

PROVISIONING

- Configuration
- User data
- Server firmware
- Base station firmware (License required)
- Handset firmware

INTEROPERABILITY

- For information about supported Call Control/Unified Communications (UC) (PBX and IP- PBX) platforms, visit http://support.spectralink.com/.

Spectralink IP-DECT Base Station

SYSTEM ARCHITECTURE

- The Spectralink IP-DECT Base Station does have 12 channels, but only 11 can be used when synchronizing over the air.

NETWORK

- 10/100 Mbps Ethernet port
- Manual or dynamic host configuration protocol (DHCP)
- Time and date synchronization from the Spectralink DECT Server
- Event logging
- LED status indication

PROVISIONING

- Base station firmware (License required on server)

RADIO INTERFACE

- RF output 20 to 24 dBm at antenna connection
- Sensitivity: typical -90 dBm measured at antenna connection at BER = 0.001
- Average transmit power: typical 5mW/ch (US) or 10mW/ch. (EU)

- Peak transmit power: typical 125mW (US) or 250mW (EU)
- Typical range:
  - Indoor: 20–50 m. (65–165 ft.)
  - Outdoor: 300 m. (1000 ft.)
- Full slot DECT radio (12 channels)
- Possible to connect external antenna (Only Spectralink External Antenna can be used)

ELECTRO MAGNETIC COMPATIBILITY (EMC) APPROVALS (REGULATORY STANDARDS)

- EMC: EN 301 489–1
- EMC: EN 301 489–6
- FCC RULES, FCC PART15, SubpartD; RSS-213
- IC Rules RSS213 Issue 2

SAFETY (REGULATORY STANDARDS)

- UL60950-1
  - CAN/CSA-C22.2 No. 60950-1
  - AS/NZS 60950-1
- Safety: EN 60950–1

DECT RADIO APPROVAL

- EN 301 406

ELECTRICAL REQUIREMENTS

- Power over Ethernet (IEEE 802.3af)
- PoE Class 1 device
- Typical power consumption: 2 W per unit
- External power supply option available
- External antenna connection (Only Spectralink External Antenna can be used)

ENVIRONMENTAL CONDITIONS

- Operating temperature: 10–40º C (50–104º F)
- Storage temperature: -50–70º C (-58–158º F)
- Relative humidity: between 20% and 80% (non-condensing)
- Compliance with the requirements of EU directive 2015/863/EU (ROHS) and 2012/19/EU (WEEE)

PHYSICAL CHARACTERISTICS

- Size: 100 x 100 x 43 mm (3.94 x 3.94 x 1.69 in.)
- Weight: 120 gr. (4.2 oz)
- Grey-white (NCS 0502-Y)
- Wall-mountable, indoor
- Can be mounted upside down

Note:

The Spectralink IP-DECT Base Station is regulatory-certified for frequency bands used in North America, Europe, Australia and New Zealand.

Spectralink DECT Repeater

SYSTEM CAPACITY WITHOUT EXTERNAL ANTENNA

- Max. number of traffic channels: two or four

SYSTEM CAPACITY WITH EXTERNAL ANTENNA

- Max. number of traffic channels: two or four
- Distance from base station to repeater with external antenna: up to 1,950 m. (6398 ft.)

RADIO INTERFACE

- RF output 20 to 24 dBm at antenna connection
- Sensitivity: typical -90 dBm measured at antenna connection at BER = 0.001
- Average transmit power: typical 5mW/ch (US) or 10mW/ch. (EU)
- Peak transmit power: typical 125mW (US) or 250mW (EU)
- Typical range:
  - Indoor: 20–50 m. (65–165 ft.)
  - Outdoor: 300 m. (1000 ft.)
- Full slot DECT radio (12 channels)
- Possible to connect external antenna (Only Spectralink External Antenna can be used)

DECT RADIO APPROVAL

- EN 301 406
- FCC RULES PART 15 / Subpart D, RSS-213

ELECTRO MAGNETIC COMPATIBILITY (EMC) APPROVALS (REGULATORY STANDARDS)

- EMC: EN 301 489–1
- EMC: EN 301 489–6

SAFETY (REGULATORY STANDARDS)

- UL 60950-1 CAN/CSA-C22.2 No. 60950-1-03
- Safety: EN 60950–1

ELECTRICAL REQUIREMENTS

- Maximum power consumption: 1.62W (Max. 2W)
- The power supply is 9VDC, 180mA.

ENVIRONMENTAL CONDITIONS

- Operating temperature: 0–55º C (32–131º F)
- Storage temperature: -50–70º C (-58–158º F)
- Relative humidity: between 20% and 80% (non-condensing)
- Compliance with the requirements of EU directive 2015/863/EU (ROHS) and 2012/19/EU (WEEE)

PHYSICAL CHARACTERISTICS

- Size: 100 x 100 x 43 mm (3.94 x 3.94 x 1.69 in.)
- Weight: 112.9 gr. (4 oz.)
- Grey-white (NCS 0502-Y)
- Wall-mountable, indoor

Spectralink External Antenna

ELECTRICAL PROPERTIES

- Frequency range: 1880-1930 MHz
- Impedance: 50 Ω (DC-path to ground)
- Polarization: RHCP
- Gain: 7.5–8.0 dB
- 3dB beamwidth horizontal: >62°
- 3dB beamwidth vertical: >62°
- Front to back ratio: >8 dB

- Return loss: < 15 dB
- Connector: SMB male
- One meter cable included

ENVIRONMENTAL CONDITIONS

- Operating temperature: -20º–55º C (-4º–131º F)
- Storage temperature: -40º–85º C (-40º–185º F)

PHYSICAL CHARACTERISTICS

- Size: 100 x 100 x 42 mm (4 x 4 x 1.7 in.)
- Weight: 120 gr. (4.2 oz.)
- Only for indoor usage

Chapter 32: Troubleshooting

In case of system errors, the following tasks can be part of the troubleshooting:

- Packet capture
- Network Diagnose
- Reading System Information, Logs, Statistics etc.
- Checking synchronization chain for loops
- Checking LAN Sync Performance
- Insufficient Software Assurance Licenses

Note:

For more in-depth information and to gain access to the Spectralink training material, you must attend training and become Spectralink Certified Specialist.

Please visit http://partneraccess.spectralink.com/training/classroom-training for more information and registration. You must log in to access this page.

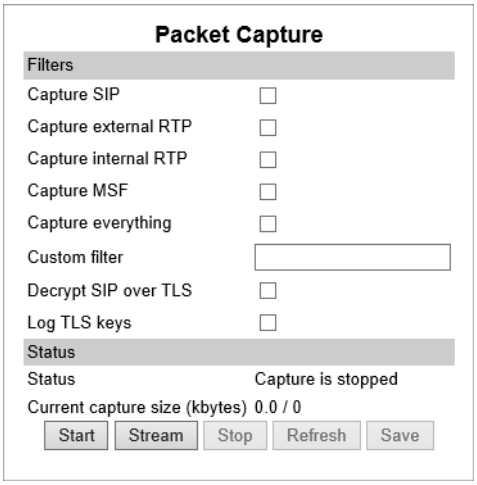
Packet Capture

Spectralink Support can request a packet capture of the overall system status.

To make a packet capture from the web-based Administration Page of the Spectralink IP-DECT/Virtual IP-DECT Server One:

1. Click **Status**, and then click **Packet Capture**.
2. On the **Packet Capture** page, enter the following data:

Field	*Setting*
Packet Capture–Filters	
Capture SIP (Optional)	If enabled, SIP signaling is captured.
Capture external RTP (Optional)	If enabled, all voice packages from other endpoints are captured.
Capture internal RTP (Optional)	If enabled, voice data between base stations is captured.
Capture MSF (Optional)	If enabled, MSF signaling is captured.
Capture everything (Optional)	If enabled, any kind of traffic is captured.
Custom filter (Optional)	Enter a custom filter in PCAP filter format to capture traffic.
Decrypt SIP over TLS (Optional)	If enabled, a decrypted version of SIP signaling sent over TLS is captured.
Log TLS keys (Optional)	If enabled, TLS master secrets are logged to a log file for later decryption of TLS in packet capture.
Packet Capture–Status	
Status	Shows the status of the capture progress.
Current capture size	Shows current capture size in kbytes.



3 If you want to start capturing the network packets,click **Start**, click **Stop** after trying to reproduce the expected failure/behaviour, and then click Save to download and save the packet capture file.

4 If you want to stream a packet capture, click **Stream**. A pcap file is downloaded automatically.

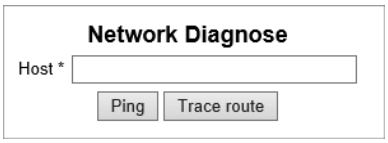
Note:

The Spectralink IP-DECT/Virtual IP-DECT Server One has a packet capture size limit of 10 megabytes. When this limit is reached, the packet capture will restart. When performing a streaming packet capture there is no size limit.

Network Diagnose

1 Click **Status**, and then click **Network Diagnose**.

2 On the **Network Diagnose** page, under **Host**, enter the relevant IP address or domain name:



3 Click **Ping** to send a ping request to the host to check if network is connected.

4 If you want to trace the route to the host, click **Trace route**.

Insufficient Software Assurance Licenses

If you see the following error message (and you cannot remove the progress bar): "Insufficient Software Assurance Licenses installed to upgrade"

This can mean one of two things:

- You do not have a software license associated with the server and will need to purchase Software Assurance to be able to download any software updates.
- Your Software Assurance License does not match the number of users (User license + default users).

For more information, see Ordering Licenses and Loading Licenses.

Chapter 33: Parameter Overview

Status

Status–General

Field	*Setting*
General Status–General	
IP address	IP address of the Spectralink IP-DECT/Virtual IP-DECT Server One.
NTP Server	IP address of the NTP Server.
Time	Time and date information.
Serial (Not relevant to Spectralink Virtual IP-DECT Server One)	Serial number of the Spectralink IP-DECT Server.
MAC address (Not relevant to Spectralink Virtual IP-DECT Server One)	MAC address of the Spectralink IP-DECT Server.
Product ID (Not relevant to Spectralink Virtual IP-DECT Server One)	Production ID of the Spectralink IP-DECT Server.
Production Date (Not relevant to Spectralink Virtual IP-DECT Server One)	Production Date of the Spectralink IP-DECT Server.
General Status–Hardware	
PartNo (Not relevant to Spectralink Virtual IP-DECT Server One)	Part number of the Spectralink IP-DECT Server hardware.
PCS (Not relevant to Spectralink Virtual IP-DECT Server One)	Hardware version
System (Only relevant to Spectralink Virtual IP-DECT Server One)	VMware Virtual Platform
CPU (Only relevant to Spectralink Virtual IP-DECT Server One)	E.g. Intel(R) Xeon(R) CPU E5-2650 v2 @ 2.60GHz
Cores (Only relevant to Spectralink Virtual IP-DECT Server One)	E.g. 1
Memory	E.g.1.0GB
General Status–Firmware	
PartNo	Part number of the Spectralink IP-DECT/Virtual IP-DECT Server One firmware
PCS	Firmware version
Build	Firmware build
General Status–Quick status	
SIP	OK if all enabled SIP users are registered to the SIP server.
KWS redundancy (Only visible if license loaded)	OK if the connection to redundancy peer is OK.
Base stations	OK if no synchronization loops, no auto synchronization and all enabled base stations are connected and synchronized.

Field	*Setting*
Media resources	OK if all enabled media resources are connected and at least one channel is available.
Provisioning	OK if the latest communication with the provisioning server was successful.
NTP (Network Time Protocol)	OK if the latest communication with the NTP server was successful.
AMiE (Only visible if configured to AMiE)	OK if connected to AMiE. For more information about configuring the server to use AMiE, see Advanced Mobile Intelligence for Enterprises (AMiE).

Status–Logs

Field	*Setting*
Message Log	
Display filter	From the **Display filter** list you can select between **emergency**, **critical**, **error**, **warning**, **notice** or **info** depending on the logs you want to see. Furthermore, select between **Application** or **Audit** to get the wanted log type. The different types of statuses are: • emergency (errors causing the system to malfunction for all calls) • critical (events that do not occur under normal operation, cause major malfunction) • error (events that do not occur under normal operation, cause minor malfunction) • warning (events that do not occur under normal operation, may cause malfunction) • notice info (events that occur under normal operation) An **Application** log is a file of events, logged by the system. An **Audit** log is a chronological set of records documenting the sequence of activities. You can clear the message log buffer for **Application** logs. The **Audit** log cannot be deleted -- except when performing a factory reset. You can stream an **Application** log, whereas an **Audit** log cannot be streamed.

Status–Wireless Server

Field	*Setting*
Wireless Server Status–General	
Firmware version	Wireless Server firmware version. E.g. 59015
System ARI	E.g. 1005354651
Wireless Server Status–License information	
License users	E.g. 30
License media channels (Only relevant to Spectralink Virtual IP-DECT Server One)	E.g. 32 32 internal media channels is default on Spectralink Virtual IP-DECT Server One, with the Mandatory Base Licence ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IPDECT Server License installed. You can load a 32 Media Channels | Virtual IP-DECT Server One License into the Spectralink Virtual IP-DECT Server One increasing the number of internal media channels to 64 media channels.
License features	E.g. Handset sharing, Enhanced Provisioning, Redundancy, Security, LAN Sync, depending on the solution.

Field	*Setting*
Wireless Server Status–Service Status	
Wireless Server Uptime	Wireless Server uptime since last restart.
Call establishment	Call establishment status. E.g. Allowed. Defined under **Administration**> **Wireless Server**.
Subscription	Subscription status. E.g. Allowed. Defined under **Configuration**> **Wireless Server**.

Status–Packet Capture

Field	*Setting*
Packet Capture–Filters	
Capture SIP (Optional)	If enabled, SIP signaling is captured.
Capture external RTP (Optional)	If enabled, all voice packages from other endpoints are captured.
Capture internal RTP (Optional)	If enabled, voice data between base stations is captured.
Capture MSF (Optional)	Capture MSF (Optional)
Capture everything (Optional)	If enabled, any kind of traffic is captured.
Custom filter (Optional)	Enter a custom filter in PCAP filter format to capture traffic.
Decrypt SIP over TLS (Optional)	If enabled, a decrypted version of SIP signaling sent over TLS is captured.
Log TLS keys (Optional)	If enabled, TLS master secrets are logged to a log file for later decryption of TLS in packet capture.
Packet Capture–Status	
Status	Shows the status of the capture progress.
Current capture size	Shows current capture size in kbytes.

Status–Network Diagnose

Field	*Setting*
Network Diagnose	
Host	Enter the relevant IP address or domain name.
	Click **Ping** to send a ping request to the host to check if network is connected. Click **Trace** route if you want to trace the route to the host.

Configuration

Configuration–General

Field	*Setting*
General Configuration–IPv4	
Method	Default value: DHCP assigned (dynamic IP address) Select Use Static **IP Address** to configure a static IP address. **Note**: When using a static IP address, it is also necessary to configure other network settings below such as DNS and NTP settings. For more information, see also Recommended Network Configuration.
IP addr	Enter the IP address of the Spectralink IP-DECT/Virtual IP-DECT Server One.

Field	*Setting*
Netmask	Enter a new network mask. Contact your system administrator for more information.
Gateway	Enter the IP address of the default gateway. The default gateway serves as an access point to another network. Contact your system administrator for more information.
MTU (Maximum Translation Unit) (Optional)	Enter the size of the largest packet, that your network protocol can transmit.
General Configuration–Ipv6	
Method (Optional)	Default value: Disabled If not using IPv4, select **Static** to set the following settings manually: IPv6 address, Subnet Prefix Length, Default Gateway, Primary DNS Server, and Secondary DNS Server. Other possible settings are: • **Stateless Address Autoconfiguration (SLAAC)**: An IPv6 address is automatically generated based on the prefix being advertised on the connected network. • **Statefull (DHCPv6)**: IPv6 address, DNS servers and DNS search list will be obtained from router.
Address/prefix (Optional)	You can enter a prefix (Static IPv6 address with an optional prefix length). Address and prefix length must be separated by: /
Default gateway (Optional)	Enter IP address of the default gateway. The default gate way serves as an access point to another network.
General Configuration–Ethernet	
VLAN (Optional)	You can enter the VLAN Identifier (VID) according to IEEE 802.1Q specifying the VLAN to which the device belongs. **Note**: If this setting is used, network access from outside the VLAN is no longer possible. The Spectralink IP-DECT/Virtual IP-DECT Server One supports 4094 different VLANs. Possible values: 1-4094
General Configuration–DNS (Domain Name System)	
Hostname (FQDN)(Optional)	The hostname (Fully Qualified Domain Name) will be inserted into the SIP Contact and via headers. The hostname will also be published via DHCP, and if the network infrastructure supports it, the device will be reachable via this hostname. E.g. Example.spectralink.com
Search Domain (Optional)	Domain name used for resolving host names without a domain.
Primary Server (Optional)	Enter the IP address of the Primary DNS server.
Secondary Server (Optional)	Enter the IP address of the Secondary DNS server.
General Configuration–NTP (Network Time Protocol)	
Server (Optional)	Enter the IP address of the NTP server from which the system will obtain the current time.
Time zone (Optional)	Select the wanted time zone. The time zone include daylight saving times.
Posix timezone string (Optional)	Customized time zone setting. The string must be in POSIX time zone format.
General Configuration–UPnP	
Enabled (Optional)	Enabled by default. If enabled, the device is UPnP discoverable.

Field	*Setting*
	UPnP is an acronym for Universal Plug and Play. If the IP address of the device is unknown (e.g. forgotten or DHCPassigned), UPnP can be used to easily identify the IP address of the device. **Note**: If **My Network Places** in Windows is setup to show icons for networked UPnP devices, every Spectralink IPDECT/Virtual IP-DECT Server One, Media resource and Base station will be present in **My Network Places**.
Broadcast announcements (Optional)	Specifies if UPnP announcements are broadcasted. If enabled, the device broadcasts announcements automatically.
General Configuration–Remote syslog	
Host (Optional)	Enter the host or IP address of the remote syslog server. If specified, messages will be sent to the server.
Port	Server port used for remote syslog. Default value: 514
Facility	Remote syslog facilities used for log messages. Default value: Local 0 Refer to RFC5424.
Level	Log level to send via syslog. Possible values: **emergency**, **critical**, **error**, **warning**, **notice**, **info** or **debug**. Default value: Info
Scope (Optional)	Scope of syslog settings. If set to **all**, the settings will override any local settings on e.g. connected base stations. If set to **server only**, these settings will only apply to the server. If set to **server and mr**, these settings will only apply to the server and media resource. Default value: all
General Configuration–SNMP	
Enabled (Optional)	If enabled, access to the SNMP is allowed, and the server will respond to SNMP requests.
Community (Optional)	SNMP Community name (public). The server will respond to requests from a manager in this community.
Trap host (Optional)	Address of SNMP trap host to which SNMP traps are sent.
Trap community (Optional)	SNMP trap Community name used for sending traps.
System location (Optional)	Information about the physical location of this host. E.g. telephone closet, 3rd floor
System contact (Optional)	The textual identification of the contact person for this host, together with information about how to contact them.

Configuration–Wireless Server

Field	*Setting*
Wireless Server Configuration–DECT	
Subscription allowed (Optional)	If enabled, you can subscribe new handsets to the system. **Note**: Subscription will be disallowed after 120 seconds or when a subscription succeeds. If more time is needed or more handsets must be subscribed, it is necessary to disable the parameter **Automatically disable subscription allowed** below.

Field	*Setting*
Automatically disable subscription allowed (Optional)	If enabled, subscriptions will automatically be disallowed after 120 seconds or when a subscription succeeds. If disabled, subscriptions will be allowed until explicitly disabled. Default value: Enabled **Note**: This feature is part of DECT Security Step A.
Authenticate calls (Optional)	If enabled, each individual DECT call will be authenticated.
Encrypt voice/data (Optional)	Encryption of voice/data packets transmitted via DECT. Possible values: Disabled, Enabled or Required. Default value: Required **Note**: Repeaters do not support encryption. If set to **Required**, the call is ended when handover is established on the repeater.
Early encryption and re-keying (Optional)	If enabled, this enables encryption immediately after connection establishment and regular re-keying until connection termination. Possible values: **Disabled**, **Enabled** or **Required**. Default value: Disabled **Note**: Enabling early encryption may increase connectivity problems in areas with poor coverage. **Note**: Only Spectralink Handsets with firmware PCS 18Da or newer support **Required**. **Note**: This feature is part of DECT Security Step A.
System access code (Optional)	System wide DECT access code. The access code is from 0–8 decimal digits. **Note**: Individual user access code (AC) has precedence over system access code.
Send date and time (Optional)	If enabled, date and time will be sent to the handsets when a call is terminated. Default value: Enabled
System TX power (Optional)	Used for controlling (reducing) the output power of all connected base stations supporting power control. Unless set to default, this will override any base station specific power setting. Default value: Default (250 mW) **Note**: You can define a TX power value for a specific base station (**Administration**> **Base Station**).
Frequency (Optional) (Only visible if Frequency Swap License is loaded)	Radio Region used for DECT communication with handsets. With the Frequency Swap License installed, you can perform frequency swap between handsets. Besides the Frequency Swap License, a special Spectralink DECT Handset 7212 (part no. 02610004) with a special configuration (and compliance to be compatible with frequency swap) is also required. Possible values: • **Europe** (EMEA, Australia & New Zealand) • **South America** • **USA** (USA & Canada) When the frequency of the base stations is changed, handsets lose the signal from the base stations. Then, after a while, the handsets will try to find base stations (with same ARI–System ID) on the other frequency band. The server must be restarted after changing frequency. **Note**: You can change the frequency setting in the server using OAM-REST API. For more information, see OAM REST API. For more information about frequency swap and the special Spectralink DECT Handset, see Frequency Swap Support.

Field	*Setting*
Allow bearer handovers to repeaters (Optional) (Not relevant to the Spectralink IP-DECT Server 200/400)	If enabled, bearer handover to repeaters is allowed. If disabled, handovers between a repeater and base station must take place as connection handovers. Default value: Enabled **Note**: If Zone-based paging is used, then bearer handover is not allowed, and this setting is overruled.
Wireless Server Configuration–Media resources (Not relevant to the Spectralink IP-DECT Server 200/400)	
Allow new (Optional)	If enabled, new media resources are allowed to connect to the server. Default value: Enabled
Add new as active (Optional)	If enabled, new media resources will become active when added. Otherwise they must be activated manually under **Administration**> **Media Resource**> **Media Resource** page. Default value: Disabled **Note**: This must be enabled if setting up a redundant system using internal media resource.
Require encryption (Optional)	If enabled, the connection between the media resource and the Spectralink IP-DECT/Virtual IP-DECT Server One is required to be encrypted. **Note**: Enabling this, will only allow media resources with firmware PCS 17Fa or newer to connect. Default value: Disabled If not enabled, the connection will be encrypted if the media resource supports encryption.
Wireless Server Configuration–Base stations (Not relevant to the Spectralink IP-DECT Server 200)	
Allow new (Optional)	If enabled, new base stations are allowed to connect to the server. Default value: Enabled
Add new as active (Optional)	If enabled, new base stations will become active when added. Otherwise, they must be activated manually under **Administration**> **Base Station**> **Base Station** page. Default value: Disabled
Require encryption (Optional)	If enabled, the connection between the base station and the Spectralink IP-DECT/Virtual IP-DECT Server One is required to be encrypted. **Note**: Enabling this, will only allow base stations with firmware PCS 17Fa or newer to connect. Default value: Disabled If not enabled, the connection will be encrypted if the base station supports encryption.
Media encryption (SRTP) (Optional)	If enabled, secure RTP for base station audio connections is used. Default value: Disabled **Note**: If not running PCS 20A_ or newer, this field is only visible if a Security (TLS, SRTP) License is loaded.
RFP port range start	Port range start for RFP local RTP ports. Default value: 57000 **Note**: You can change the value in case of conflicting ports.
Paging method (not relevant to Spectralink IP-DECT Server 200/400)	“Paging” is about incoming voice and messaging calls, where the Spectralink IP-DECT/Virtual IP-DECT Server One has to send out an announcement (through the relevant Spectralink IP-DECT Base Stations) asking the handset to choose a base station and start establishing a connection. Possible values: **Default**, **Multicast**, **Site-based paging**, **Zone-based paging**.

Field	*Setting*
	Default value: Default If having more than 256 base stations connected on a site, default paging is not enough due to the amount of base stations. In this situation, if multicast signaling is supported, multicast is the preferred paging method. Other paging methods are site-based paging and zone-based paging. On a site with heavy voice/messaging load, Spectralink recommends using Zone-based paging instead of using multicast signaling. If **Multicast** is enabled, this will impose multicast support for the network. For more information, see Using Multicast Signaling for Paging. **Note**: For more information about deciding which paging method to use, see Spectralink IP-DECT Base Station Configuration Methods–Considerations. Please read the information carefully before continuing and ensure correct deployment of the base stations.
Zone-based paging (Optional)	Zone-based paging is used when grouping base stations into zone in site(s). Not using zone will be substantial in most average systems. **Note**: Zone-based paging is built on the DECT Standard for Location Area Level (LAL). Note: The field Paging method must be set to **Zone-based paging** to be able to use zone-based paging. Possible values: **8 Zone (32 base stations per zone)**, **16 Zone (16 base stations per zone)** or **32 Zone (8 base stations per zone)**. Default value: 8 Zone (32 base stations per zone). For more information about zone-based paging, see Spectralink IP-DECT Base Station Configuration Methods–Considerations. Please read the information carefully before continuing and ensure correct deployment of the base stations. **Caution**: Assigning RPN's are essential for using zone-based paging, as the RPN decides which zone the Spectralink IP-DECT Base Station will be part of. If changing zone size later on after having configured the base stations and assigned RPN's, then all configuration must be redone. Therefore, consider your system needs carefully before and when deploying. **Note**: Enabling Zone-based paging ensures automatic update of handset locations. For more information about configuration of sites and zone, see Configuring Sites (and Zone).
Multicast address (Optional)	Multicast address used for signaling. Default value: 239.255.1.11 Please refer to RFC 2365 and RFC 4291 for details. **Note**: Only used with multicast signaling as paging method.
Multicast TTL (Optional)	The TTL is used to limit the propagation of the multicast packets across routers. Default value: 1 **Note**: The TTL is configurable and you can change the value according to network topology. For more information, see vendor specific documentation. **Note**: Only used with multicast signaling as paging method.
Default sync type (Optional)	This setting controls the default sync type for new base stations connecting to the server. Possible values: **Free running**, **Radio** or **LAN**. **Note**: Selecting **Free running** will configure each base station as a sync master. For more information, see also Synchronization and Deployment Guide. Default value: Radio **Note**: Multicast address and Multicast TTL are hardcoded, when selecting **LAN**. For more information, see Using Multicast for LAN.

Field	*Setting*
LAN sync transport protocol (Optional)	The protocol transport layer used by PTP for LAN sync. Possible values: **Ethernet**, **IPv4** or **IPv6**. For more information about using LAN synchronization, see LAN-Based Synchronization.
LAN sync type of service (TOS/Diffserv) (Optional)	TOS/DiffServ values can be configured for PTP packets used for LAN sync. The values are entered in decimal. Network priority: Packets with higher TOS/DiffServ have higher priority on the network. 184 = critical (highest priority) 96 = flash 64 = immediate 32 = priority 0 = routine (lowest priority) Default value: 184 (Expedited Forwarding)

Allow web-based Administration Page (Optional)	If disabled, the web-based Administration Page (GUI) of all connected base stations will be disabled.
	Default value: Enabled
	Note: You can disable the web-based Administration Page directly in the configuration file by inserting the following:
	`<rfp>`
	`<allow_gui>false</allow_gui>`
	`</rfp>`
	Change "false" to "true" to enable it.
	For more information, see Disabling Web-Based Administration Page.

Wireless Server Configuration–Handsets (Not relevant to the Spectralink IP-DECT Server 200)	
Handset sharing (Optional)	Enabled by default when Handset Sharing License is loaded. Disable this, if handset sharing is not to be allowed. For more information about using handset sharing and configuring handset login, see Handset Sharing.
Handset login (Only visible if Lync/SfB + Security (TLS, SRTP) License is loaded)	If enabled, user credentials can be entered on the handset and no user configuration is required on the server. Use long key press 9 to login. (System dependent). For more information, see Configuring Handset Login and Handset User Guides.
Wireless Server Configuration–Application interface	
Username	Enter username required to access the application interface. Max. length: 31 characters.
New password (Optional)	Enter password required to access the application interface. Max. length: 31 characters.
New password again (Optional)	Confirm password required to access the application interface.
Enable MSF (Optional)	If enabled, access to the MSF application interface is supported. Default value: Disabled
Enable XML-RPC (Optional)	If enabled, access to the XML-RPC application interface is supported. Default value: Disabled
Internal messaging (Optional)	If enabled, internal messaging to allow handset-to-handset messaging without an external application is supported.
Enable FAS connectivity (Optional) (System dependant and only relevant if using ATEX handset)	If enabled, connectivity to FAS is supported. Default value: Disabled

Field	*Setting*
ATEX handset GAP enrollment type (Optional) (Only relevant if using ATEX handset)	If enabled, GAP as enrollment type is used instead of DOIP enrollment type. Default value: Disabled
Wireless Server Configuration–Feature codes	
Enable (Optional)	If enabled, feature codes for controlling features from the handsets can be used.
Call forward unconditional–enable (Optional)	Enable call forward unconditional by dialing this code (***21***), followed by the desired extension ($ = extension) and #. E.g.: ***21*$#** **Note**: You can change the code *21* on the Spectralink IP-DECT/Virtual IP-DECT Server One to fit your standard. For more information, see the relevant documentation available at http://support.spectralink.com/.
Call forward unconditional–disable (Optional)	Disable call forward unconditional by dialing this code (**#21#**).
Wireless Server Configuration–Languages	
Phone Language (Optional)	Language of system messages displayed in handset. Select the desired language from the list.
Wireless Server Configuration–MSF	
Enable Long-Press Key0–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key1–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key2–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key3–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key4–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key5–Phonebook (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for company phone book.
Enable Long-Press Key6–Undefined (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press.
Enable Long-Press Key7–Undefined (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for replacing handsets as an admin rights user. For more information about creating an admin rights user, see Registering Users and Subscribing Handsets. For more information about handset replacement, see Admin Rights User.
Enable Long-Press Key8–Undefined (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press.
Enable Long-Press Key9–Handset Sharing (Optional)	If enabled, allow Spectralink IP-DECT/Virtual IP-DECT Server One to use this long key press for handset sharing. For more information, see Handset Sharing and User Sign-in/Sign-out.

Configuration–Media Resource

Field	*Setting*
Media Resource Configuration–Media resource	
Enable internal	If enabled, the internal media resource will start up and connect.

Field	*Setting*
	If disabled, CPU power is increased. Additional media resource will take over then, if installed. Default value: Enabled **Note**: If configuring a system with Spectralink DECT Media Resources or Spectralink Virtual IP-DECT Media Resources, Spectralink recommends disabling the internal media resource of the Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One when: • The system handles more than 20 simultaneous calls. • There are more than 500 users (200 users if using Lync/ Skype for Business).

Configuration–Security

Field	*Setting*
Security Configuration–Administrator Authentication	
Current password	Enter the current password.
New username	Enter a new username. **Note**: Requires a reboot of the server.
New password (Optional)	Enter a new password.
New password again (Optional)	Enter the new password again to confirm.
Strict password requirements (Optional)	If enabling strict password requirements, the device can be configured to enforce certain security rules and naming conventions. For more information, see Parameter Overview. **Note**: Once enabled, this setting can only be disabled by a factory reset (**Configuration**> **Factory Reset**) that will remove all configuration and user data.
Password expiration (Optional)	Select when you want the password to expire. Possible values: **Never**, **30 days** or **90 days**. Default value: **Never** **Note**: Once enabled, this setting can only be disabled by a factory reset (**Configuration**> **Factory Reset**) that will remove all configuration and user data.
Security Configuration–Data protection	
Allow unencrypted HTTP (Optional)	HTTPS is forced by default. If enabled, HTTP support is supported instead of HTTPS. **Note**: Enabling unencrypted HTTP can cause passwords and other sensitive data to be transmitted in clear text on the network.
Enable legacy TLS (Optional)	If enabled, TLS versions 1.0 and 1.1, certificates signed with the SHA-1 algorithm and CBC based ciphers are supported. **Note**: Enabling legacy TLS is required for security and interoperability with some older browsers and call handing platforms.
Allow remote logging (Optional)	If enabled, remote logging is allowed. Remote logging allows for Spectralink debug tools to extract debug information from the unit.
Remove user passwords from exported data (Optional)	If enabled, users passwords are prevented from being included when data are exported from the Spectralink IP-DECT/Virtual IP-DECT Server One, e.g. when exporting the user list to XML files or CSV files. **Note**: Enabling this will exclude the user database from full system backups. **Note**: Once enabled, this setting can only be disabled by a factory reset (**Configuration**> **Factory Reset**) that will remove all configuration and user data.

Configuration–Certificates

Field	*Setting*
Certificates–Device certificate chain (Not relevant to Spectralink Virtual IP-DECT	
	Overview of device certificates. These are non-changeable. Examples of device certificates are: Device certificate, SpectraLink Issuing CA / Spectralink Inc. and SpectraLink Root CA / Spectralink Inc.
Certificates–Host key	
Key file	Click either **Generate** or **Browse** to find the relevant host key file (*.pem file). **Note**: Creating a new host key is not necessary when renewing a certificate. Click **Remove**, if you want to remove a host key. You must have removed the host certificate before removing the host key.
Password (Optional)	Enter a password.
	Click **Import Key**, if you want to import the host key.
Certificates–Host certificate chain	
Certificate file	Click **Generate Request** or **Browse** to find the relevant host certificate file (*.crt file). If generating a request, the host certificate signing request will be downloaded. **Note**: The generated certificate request will include Common Name and Subject Alternative Name fields containing the host name configured in **Configuration**> **General** page. If other fields a required, the host key and certificate must be generated using external tools. **Note**: • If no host certificate is installed on a Spectralink IPDECT Server 200/400/6500, it will fall back to using the built-in device certificate signed by Spectralink. • If no host certificate is installed on a Spectralink Virtual IP-DECT Server One, it will automatically generate a self-signed certificate.
Password (Optional)	Enter a password.
Type	Select between the following certificate types; **X.509** or **PKCS#12**.
	Click **Import Certificate**, if you want to import the certificate. Click **Remove**, if you want to remove a certificate. **Note**: If a certificate already exists, it must be removed before you can import a new one.

Configuration–SIP

Field	*Setting*
SIP Configuration–General	
Local port	Enter the local port number. The local port is the port on which the Spectralink IPDECT/Virtual IP-DECT Server One listens for incoming SIP-signaling. The default local port number is 5060.
Transport	Transport mechanism used for SIP messages. Possible values: **UDP**, **TCP** or **TLS**. **Note**: If TLS is used as SIP Transport Method, it is necessary to import host certificate and CA certificates into the server.

Field	*Setting*
	For more information, see Configuring Certificates.
DNS method	Used for looking up the destination of SIP messages. Possible values: **A records** or **DNS SRV**.
Default domain	Used for SIP registration. Enter the name of the domain. **Note**: If no user specific domain is configured under a specific user, the handsets registered on the Spectralink IP-DECT/Virtual IP-DECT Server One will use the default domain as the domain part of the SIP URI; e.g. John Doe <sip:1234@example.org> If only one SIP PBX is used and no domain is available, enter the IP address of PBX here.
Register each endpoint on separate port (Optional)	If enabled, separate local ports for each endpoint are used, instead of the global local port.
Send all messages to current registrar (Optional)	If enabled, all non-REGISTER requests to the current registrar will be sent, when more proxies are available.
Allow internal routing fallback	**Allow internal routing fallback** must be enabled if Secondary username is defined.
Registration expire(sec)	The maximum time between re-registrations. The registrar can signal a shorter time-out. Default value: 3600 sec
Max pending registrations	The maximum amount of pending SIP registrations allowed. The setting can range from 1 to 100 simultaneous SIP registrations. Default value: 1 To increase SIP registration speed, you can increase the value for faster registration handling (system dependant).
Handset power off action (Optional)	Action performed when a handset is turned off. Possible values: Ignore or **De-register**. If **De-register** is selected, the handset will de-register when turned off. Default value: Ignore
Max forwards	The maximum number of proxies outgoing messages are allowed to traverse. Default value: 70
Client transaction timeout (msec)	Controls timer B and F as specified in RFC 3261. Increase this to eliminate time out errors or decrease it to reduce fail over time. Default value: 16000 msec
Blacklist timeout(sec)	Controls the timeout duration for a SIP server to be blacklisted, after losing connection to the server. After leaving the blacklist, the server will reattempt to establish connection. The setting can be set in the range of 5 sec to 600 sec. Default value: 30 sec **Note**: Instead of being a strict timeout, the timeout is considered loose. This means that the setting guarantees that at least the specified time will elapse before trying to reconnect. Thus, more time may elapse, depending on the activeness of the server, as the timeout is checked at given server SIP activities.
SIP type of service (TOS/Diffserv)	TOS/Diffserv used for SIP signaling. Entered in decimal. Default value: 96 (AF–Assured Forwarding)
SIP 802.1p Class-of-Service	This is the 802.1p PCP and must be between 0 and 7. The setting requires VLAN tagging. Default value: 3
GRUU (Optional)	If enabled, Globally Routable User Agent URIs are supported.

Field	*Setting*
	Default value: Enabled
Use SIPS URI (Optional)	Normally, SIP communication on a TLS connection uses the SIPS: URI scheme. Disabling this option causes the Wireless Server to use the SIP: URI scheme with a transport=tls parameter for TLS connections. Default value: Disabled
TLS allow insecure (Optional)	By default, UDP and TCP transports are disabled when TLS transport is the default. If this setting is enabled, UDP and TCP are allowed as fallback if TLS fails. Default value: Disabled
TCP ephemeral port in contact address (Optional)	If enabled, the TCP ephemeral port (the local TCP port of the outgoing connection) to the contact header, used in outgoing SIP messages, is added.
NAT keepalive (Optional)	If enabled, the Spectralink IP-DECT/Virtual IP-DECT Server One sends UDP packets periodically to ensure that NAT translation continues. If not enabled, the port may be closed down for security reasons (as a consequence call will be dropped or disrupted). Possible values: **Disabled**, **CRLF (rfc5626)** or **SIP OPTIONS (rfc3261)**. Default value: CRLF (RFC 5626) **Note**: **CRLF** is only used for TCP transport. **SIP OPTIONS** is used for both UDP and TCP transports. If using UDP transport, then NAT keepalive is disabled unless you select **SIP OPTIONS**.
NAT keepalive interval (sec) (Optional)	If NAT keepalive is enabled, specify the interval at which NAT keepalive packets must be sent. Possible values: 10, 20 or 30 sec Default value: 30 sec
Send Hold before REFER (Optional)	If enabled, all calls are put on hold before initiating a call transfer using a REFER message. Some call control platforms require this to be disabled, otherwise the transfer target may stay on hold after a transfer has completed. Default value: Enabled
Convert SIP URI to phone number (Optional)	If enabled, the Spectralink IP-DECT/Virtual IP-DECT Server One converts the callers SIP URI received from the PBX to a phone number, e.g. “SIP:1234@example.com” to “1234”. The phone number is then displayed in a DECT handset as the caller ID instead of the SIP URI. **Note**: Conversion of SIP URIs makes the Call back feature unusable for users on a different domain. Default value: Enabled
SIP Configuration–Proxies	
Proxies (Optional)	**Priority**: The priority for using this proxy. Possible Value 1-4. **Weight**: The weight for using this proxy if more proxies have the same priority. Possible value 1–65.000 higher weight gives priority. Default value: 100 **URI**: The URI or IP address of the proxy
SIP Configuration–Authentication	
Default user (Optional)	Default username used for SIP authentication. **Note**: If no handset specific authentication username/-password is configured, handsets registered on the Spectralink IP-DECT/Virtual IP-DECT Server One will use the default username/password.

Field	*Setting*
Default password (Optional)	Enter password.
Realm (Optional)	The realm presented by the proxy when requesting authentication. If this field is non-empty, authentication passwords will be encrypted. **Note**: When the realm is changed, all stored SIP passwords will be invalid.
SIP Configuration–DTMF signaling	
Send as RTP (Optional)	If enabled, keypad signaling will be sent as RTP event codes.
Offered RFC2833 payload type (Optional)	Payload type for RFC2833 in SDP offers. Default value: 96
Send as SIP INFO (Optional)	If enabled, keypad signalling will be sent as SIP INFO messages.
Tone duration(msec)	Enter the time length of the tone in milliseconds. Default value: 270 msec
SIP Configuration–Message waiting indication	
Enable indication (Optional)	If enabled, MWI is displayed in the handset.
Enable subscription (Optional)	If enabled, you can subscribe to MWI indications from the SIP proxy.
Subscription expire (sec)	Enter the number of seconds before MWI subscription will be renewed. Default value: 3600 sec
SIP Configuration–Media	
Packet duration (msec)	Packet duration for transmitted RTP Packets. Possible values: 10, 20 or 40 msec
Media type of service (TOS/Diffserv)	TOS/Diffserv used for RTP (Media) signaling entered in decimal. Default value: 184 (EF–Expedited Forwarding)
Media 802.1p Class-of-Service	This is the 802.1p PCP and must be between 0 and 7. The setting requires VLAN tagging. Default value: 5
Port range start	Port range start for local RTP ports. Default value: 58000
Codec priority	Define the priorities of codecs. Possible values: **PCMU**, **PCMA**, **G.726** or **G.729**.
Add G729A media type for G.729 codec (Optional)	If enabled, the Spectralink IP-DECT/Virtual IP-DECT Server One will use G.729A/8000 as the media type for the G.729 codec in addition to the standard G.729/8000. This allows interoperability with endpoints that uses the incorrect G.729A/8000 value. Default value: Disabled
SDP answer with preferred codec (Optional)	Specifies if the media handling should ignore the remote SDP offer codec priorities.
SDP answer with a single codec (Optional)	Specifies if the media handling should provide only a single codec in SDP answers.
Ignore SDP version (Optional)	Ignore the version of the SDP received from remote endpoints.
Enable media encryption (SRTP) (Optional)	If enabled, external SRTP is supported and optional. It must be negotiated with the remote endpoint. Default value: Enabled **Note**: If not running PCS 20A_ or newer, this field is only visible if a Security (TLS, SRTP) License is loaded.
Require media encryption (SRTP) (Optional)	If enabled, the usage of SRTP is required and SRTP must be negotiated with the remote endpoint. If negotiation of SRTP with the remote endpoint is unsuccessful, call establishment is aborted. Default value: Disabled

Field	*Setting*
	Note: If not running PCS 20A_ or newer, this field is only visible if a Security (TLS, SRTP) License is loaded.
Include lifetime in SDES offers (Optional)	Handles the RFC 4568 SRTP lifetime key parameter in SDP offers. Default value: Disabled **Note**: If not running PCS 20A_ or newer, this field is only visible if a Security (TLS, SRTP) License is loaded.
Include MKI in SDES offers (Optional)	Handles the RFC 4568 SRTP Master Key Index Parameter in SDP offers. Default value: Disabled **Note**: If not running PCS 20A_ or newer, this field is only visible if a Security (TLS, SRTP) License is loaded.
Enable ICE (Optional)	If enabled, support for Interactive Connectivity Establishment (ICE) (RFC 5245) is allowed.
Enable TURN (Optional)	If enabled, support for Interactive Connectivity Establishment (ICE) (RFC 5245) is allowed.
TURN server (Optional)	Enter TURN server address.
TURN username (Optional)	Enter TURN server username. If left blank, the per-user authentication username will be used.
TURN password (Optional)	Enter TURN password. If left blank, the per-user authentication password will be used.
SIP Configuration–Call status	
Play on-hold tone (Optional)	If enabled, on-hold tone is received in remote end when placed on hold. **Note**: This might conflict with Music-on-Hold.
Provide Music-on-Hold (Optional)	If enabled, Music-on-Hold is played for the remote end.
Display status messages (Optional)	If enabled, call status messages are received in the handset.
'#' key ends overlap dialing (Optional)	If enabled, pressing the # key dials number in overlap dialing.
Call waiting (Optional)	If enabled, call waiting is supported.
Allow automatic offhook (Optional)	If enabled, automatic offhook is allowed for intercom features.

Configuration–Redundancy

Field	*Setting*
Redundancy Configuration–Node type	
Single	If selected, this will disable redundancy and configure for stand alone (normal single server solution). Select **Single**, if this device is to be a normal single server solution.
Master	If enabled, this will enable redundancy and configure the device as master server. The system will be controlled by this device. Select **Master**, if this device is to be the master server.
Slave	If enabled, this will enable redundancy and configure the device as backup (slave) server. The device will be controlled by a master server. Select **Slave**, if this device is to be the backup server.
Redundancy Configuration–Peer node	
Address	If master server, enter the fixed IP address or hostname for the backup Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One. If backup server, enter the fixed IP address or hostname for the master Spectralink IP-DECT Server 6500/Spectralink Virtual IP-DECT Server One.

Field	*Setting*
Redundancy Configuration–Peer node	
UUID (Optional)	The UUID (unique ID) of the redundant system. This must be the same for master server and backup server for replication to be performed. The master server automatically generates the UUID. **Note**: When reset on the master server, the UUID is automatically generated, and when reset on the backup server, it is retrieved from the master server. The UUID must be reset when a master Spectralink IP-DECT/Virtual IP-DECT Server One is changed to a backup Spectralink IP-DECT/Virtual IP-DECT Server One, or when a backup Spectralink IP-DECT/Virtual IPDECT Server is moved to another solution.
Reset UUID (Optional)	If enabled, the UUID is reset if the UUID of the master server and backup server is not matching.
Redundancy Configuration–Settings	
Failover time(sec)	Enter value for failover time. Failure time is the time in seconds from the Spectralink IPDECT/Virtual IP-DECT Server One detects a failure, until it initiates a failover operation and cause the other peer to take over. Default value: 15 sec For more information about failure time, see Failover time conditions.

Configuration–Provisioning

Field	*Setting*
Provisioning Configuration–Server	
Method	The Spectralink IP-DECT/Virtual IP-DECT Server One must know the protocol and address of server containing the firmware and configuration. The Spectralink IP-DECT/Virtual IP-DECT Server One can use the following methods to obtain the provisioning server URL: • **Disabled** (The Spectralink IP-DECT/Virtual IP-DECT Server One will not use provisioning) • **Static** (The administrator must manually specify the URL of the provisioning server) • **DHCP** (Option 66) Select the relevant method for obtaining the URL of the provisioning server. Default value: DHCP
URL	If using Static for obtaining the URL of the provisioning server, enter an URL. Accepted format of URL is: [<protocol>://[<username>:<password>@]]<host>[:<port>][/<path>] Examples: • 10.0.0.10 • tftp://provisioning.test.com • ftp://192.168.0.1 • ftp://user:password@provisioning.example.com • http://server.example.com/boot. • https://server.example.com:10443/boot
Provisioning Configuration–Checking	
Interval (minutes)	The interval between polling the provisioning server. If the value is set to 0, then periodic polling is disabled. Enter a value if you want to use polling for checking updates automatically.

Field	*Setting*
Time (hh:mm)	Enter a value to poll the provisioning server at a specific time each day. Leave it empty if not using polling.
NOTIFY check_sync	Possible values: **Disabled**, **Update** or **Reboot**. If **Disabled** is selected, polling (defining specific time/interval for automatic check for new updates) is used. If **Update** is selected, then SIP Notify Check-Sync is used for automatic notification of new updates. Using this method is the optimum way to handle updates. Default value: Disabled
Provisioning Configuration–Server configuration	
Import	Enable. If enabled, this will make automatic update possible if a default firmware file is available.
Provisioning Configuration–Users	
Import	Enable. If enabled, this will make automatic update possible.
Provisioning Configuration–Handset configuration (Only relevant to Spectralink IP-DECT Servers and Spectralink Virtual IP-DECT Server One)	
Import	Enable. If enabled, this will make automatic update possible if a .ver file and handset configuration files are available.
Provisioning Configuration–Firmware	
Wireless Server (Only relevant to Spectralink IP-DECT Server 200)	Enter name of firmware image file. Must match file name on provisioning server. Leave empty for no firmware download.
Wireless Server (Only relevant to Spectralink IP-DECT Server 400/6500 and Spectralink Virtual IP-DECT Server One)	Enter name of firmware image file. Must match file name on provisioning server. Leave empty for no firmware download. Enable the **Use firmware as default** check box if you want the server firmware as default for all base stations and media resources (recommended).
Handset–Butterfly	Enter name of firmware image file (-Over-the-Air.bin). Must match file name on provisioning server. Leave empty for no firmware download.
Handset–75x2, 76x2 and 77x2 series	Enter name of firmware image file (-Over-the-Air.bin). Must match file name on provisioning server. Leave empty for no firmware download.
Handset–72x2 series	Enter name of firmware image file (-Over-the-Air.bin). Must match file name on provisioning server. Leave empty for no firmware download.
Handset–OEM	Enter name of firmware image file. Must match file name on provisioning server. Leave empty for no firmware download.

Configuration–Import/Export

Field	*Setting*
Import/Export–Export configuration	
Export	Click **Save**, if you want to export the configuration file. Save the configuration file.
Import/Export–Import configuration	
Import	Click **Browse**, if you want to search for a configuration file to be imported, select the relevant file, and then click **Load**.

Users

Users–List Users–User

Field	*Setting*
User–DECT device	
Product name	After registration of user and subscription of handset, this field will contain information about the handset product name. E.g. Spectralink 7532
Model number	After registration of user and subscription of handset, this field will contain information about the handset's technical model number. E.g. 7532
Software part number	After registration of user and subscription of handset, this field will contain information about the software part number. E.g. 14225100
Firmware	After registration of user and subscription of handset, this field will contain information about the firmware version. E.g. PCS 19K
IPEI (Optional)	If a specific handset is being subscribed for this user, enter the IPEI number of the actual handset (the IPEI number is readable from the label on the product). If this is not the case, this field can be left empty and it will auto-fill when the handsets subscribe. **Note**: A SIP REGISTER will not be sent before there is an IPEI number present. **Note**: Programming of IPEI number into the system database is necessary to enable service to the handset. **Note**: If handset sharing is used, the IPEI label will be a link, that you can click on and link to a device. For more information, see Adding Devices to Server.
Access code (Optional)	Administrators can define a system wide or individual access code as extra wireless security during the subscription process. **Note**: Some 3rd party phOne may need an Access code to register to the Spectralink IP-DECT/Virtual IP-DECT Server One.
Configuration group (Optional)	If using handset configuration, enter the Group ID of the Configuration Group. For more information, see Managing Handset Configuration and Configuration Groups.
User–User	
PIN code (Optional) (Only visible if Handset Sharing License is loaded)	Enter a code in the PIN code field for added security to prevent other users from linking a handset with your user profile.

Field	*Setting*
	The PIN code associates the user with a handset. For more information, see User Sign-in/Sign-out. See also Lync/Skype for Business Interoperability Guide.
Standby text (Optional)	Enter a standby text. **Note**: Disallowed characters: <>\" A standby text is a fixed label shown in the top left part of the screen on the DECT handset when in idle state. **Note**: This feature is only available if Spectralink DECT handsets are being used. If third-party DECT handsets are being subscribed, this feature is not supported.
Disabled (Optional)	If enabled, the user is disabled. **Note**: A disabled user cannot make calls from the handset.
User–SIP	
Username/Extension	Must contain information used for SIP registration etc. E.g. the "user" in a SIP URI. **Note**: Allowed characters: a-z, A-Z, 0-9, -_.!~*'()&=+$,;?/
Secondary username (Optional)	Enter a Secondary username. **Note**: Allowed characters: a-z, A-Z, 0-9, -_.!~*'()&=+$,;?/ The Secondary username can be used to make voice calls, if the connection to the SIP PBX is lost. The Secondary username must be globally unique. In some PBXs there is a mapping between username and number (e.g. Username = hz2539jk, Number = 1234). If the connection to the SIP PBX is lost, then you can make the mapping internally by defining a Secondary username. **Note**: The feature MUST be used with SIP setting **Allow internal routing fallback** enabled. For more information, see Configuring SIP and IP-PBX Settings.
Domain (Optional)	Enter the domain part of a SIP URI. **Note**: Allowed characters: a-z, A-Z, 0-9, .- E.g. example.org in John Doe<sip:1234@example.org> **Note**: If not configured, the default domain entered under SIP configuration will be used.
Display name (Optional)	Enter the name of the user (e.g. caller ID). **Note**: Disallowed characters: <>\" E.g. John Doe in John Doe<sip:1234@example.org> **Note**: If Cisco Unified CM (Advanced Features) License is loaded, the Cisco Unified CM will not use this, but it may ease the administration of users within the Spectralink IP-DECT Server.
Authentication user (Optional)	Enter the user ID of the end user. E.g. **JohnDoe** or **5204**. **Note**: Disallowed characters: <>\" **Note**: The username will override the Default User field under SIP Configuration. Priority: 1. Authentication user set for individual users 2. Authentication user set in server SIP settings 3. Username set for individual users
Authentication password (Optional)	Enter the digest credential of the end user. **Note**: Disallowed characters: <>\"

Field	*Setting*
	Note: The password will override the Default Password field under SIP Configuration.
User–Features	
Call forward unconditional (Optional)	A Call Forward Unconditional (an extension to forward calls to) can be added/removed via the web-based Administration Page. **Note**: Allowed characters: a-z, A-Z, 0-9, -_.!~*'()&=+$,;?/
Admin rights (Optional)	If enabled, the user becomes an admin rights user with the ability to replace a broken handset. For more information about replacing a handset as an admin rights user, see Admin Rights User.

Users–List Devices–Device

Field	*Setting*
Device–DECT device	
Model	After registration of user and subscription of handset, this field will contain information about the handset model. E.g. Spectralink 7742
Software part number	After registration of user and subscription of handset, this field will contain information about the software part number. E.g. 14225100
Item number	E.g. 02630000
Firmware	After registration of user and subscription of handset, this field will contain information about the firmware version. E.g. PCSJA.
HW version	E.g. 6
Production Id	E.g. 0024 065F 3C25 714C
IPEI (Optional)	If a specific handset is being subscribed for this extension, enter the IPEI number of the actual handset. (The IPEI number is readable from the label on the product). If this is not the case this field can be left empty and it will auto-fill when the handsets subscribe. **Note**: A SIP REGISTER will not be sent before there is an IPEI number present. **Note**: Programming of IPEI number into the system database is necessary to enable service to the handset.
Access code (Optional)	Administrators can define a system wide or individual access code as extra wireless security during the subscription process. **Note**: Some 3rd party phOne may need an Access code to register to the Spectralink IP-DECT/Virtual IP-DECT Server One.
Configuration group	If using handset configuration, this field will contain information about which configuration group the handset is in. For more information, see Managing Handset Configuration and Configuration Groups.
Configuration version	If using handset configuration, this field will contain information about the version of the Handset Configuration XML file. For more information, see Managing Handset Configuration and Configuration Groups.
Device–User	
Username / Extension	If the handset is linked to a specific user, the text field will hold the extension number of that user and the **Username** / **Extension** link is active. **Note**: Clicking on the link will take you to the User profile of the linked handset.

Field	*Setting*
	If the user is not linked to a handset, the link is inactive and there is no extension number in the text field.
Display name (Optional)	After creation of user, this field will contain information about username (e.g. caller ID). E.g. John Doe in JohnDoe<sip:1234@example.org>

Users–List User–Handset firmware update

Field	*Setting*
Handset firmware update–Options	
Update load	Select relevant upload capacity. The load corresponds to the number of maximum simultaneous updates. Possible values: **Low**, **Medium** or **High**. Default value: Medium
Start time	Default value: **Now** If you want to upload later, select an appropriate time within the next 24 hours.
Firmware file	The firmware file can be either a previously uploaded default firmware file, or a new firmware file chosen. A new firmware file must be a valid firmware file with the extension .bin. Select either **Default** or **Upload**.

Users–Import/Export

Field	*Setting*
Import/Export Users–Import user data	
CSV format	If you want to import user data, browse for the CSV file to import, and click **Load**. To be able to import the data correctly, the CSV file must contain certain information and punctuation. For more information, see Appendix B: Example of Handset Registration Data–CSV Format.
Encoding	Select the correct encoding for the CSV file. You can choose between **UTF-8**, **ISO/IEC 8859-1** or **Windows-1252**. **Note**: The encoding depends on the software that was used to generate the CSV file. If you use Microsoft Windows, you will probably select Windows-1252.
Import/Export Users–Export user data	
CSV format	If you want to save the user data file in CSV format, click **Save**. The CSV format can be imported back into the server.
XML format	If you want to save the user data file in XML format, click **Save**. The XML format is used for provisioning. For more information, see *Provisioning Guide*.
Import/Export Users–Delete users	
Delete all users	If you want to delete all users, click **Delete**.

Users–Handset Configuration

Field	*Setting*
Handset Configuration Update–Automatic update	
Enable (Optional)	Default value: Disabled

Field	*Setting*
	Enable this, if you want to make automatic update possible. If enabled and new handsets are added to an existing uploaded configuration group, these are automatically updated after subscription has finished. Existing handsets that are added to a configuration group are also automatically updated. If a handset configuration update takes place while being in the menu on the handset, the user must exit menu and then re-enter before changes are visible. **Note**: If using provisioning for uploading the Handset Configuration XML file to the handsets, enabling automatic update is required. This can be done either through the XML configuration file or the web-based Administration Page. For more information, see *Provisioning Guide*.
System load (Optional)	Select relevant upload capacity. The load corresponds to the number of maximum simultaneous updates. Possible values: **Low**, **Medium** or **High**. Default value: Medium **Note**: If you schedule an upgrade during day hours, you would typically choose **Low** to **Medium** load to avoid any impact on users. Upgrade after hours typically means no user load, therefore, you can choose **High** priority.
	Click **Save**.
Handset Configuration Files	
Configuration Group	Information about the Group ID assigned to the user. E.g.: 100
Version	Information about the version of the Handset Configuration XML file.
Export	You can view an existing configuration file located on the server. Select the relevant configuration group from the list, and then click **Export**, if you want to export the Handset Configuration XML file and view it in a text editor.
Upload	Click **Browse** to find the relevant Handset Configuration XML file, and then click Upload, if you want to upload a Handset Configuration XML file. Click **OK** to return to **Handset Configuration Files** page. If the configuration group did not exist, it is added to the list. If the configuration group existed, but the version number differed, the existing configuration file is overwritten.
Handset Update Status	
Group	Information about the Group ID assigned to the user. E.g.: 100
IPEI	Information about IPEI of the handset.
User	Information about username in the configuration group.
Status	Information about upload status. E.g.: Pending, Progress or Postpone.
Progress	Information about the progress of the update.
	Click **Cancel update** if you want to stop an active update.

Administration

Administration–Wireless Server

Field	*Setting*
Wireless Server–Wireless Server Status	
Wireless Server Uptime	Click **Reboot now** or **Reboot when idle** (when active calls have ended), if you want to restart the system.
Wireless Server–Service Status	
Call establishment	Default set to allowed. Click **Block**, if you want to block for new calls during firmware update.

Administration–License

Field	*Setting*
Licenses–System info (Only relevant to Spectralink Virtual IP-DECT Server One)	
Server ID	Server ID (also called UUID) is the ID of the virtual machine. This Server ID is provided automatically when creating the virtual machine. E.g.: 89fed27f-7c47-43f5-8347-cb854cedc538 **Note**: Server ID (UUID) must be used to order further licenses. If the virtual machine is to run as a Spectralink Virtual IPDECT Server One, you must order the Mandatory Base License ARI 150 Users 64 Base Stations 32 Media Channels | Virtual IP-DECT Server One License, which also provides you with an ARI. If the virtual machine is to run as a Spectralink Virtual IPDECT Media Resource (no ARI needed), you must order a 32 Media Channels | Virtual IP-DECT Server One License.
Licenses–Load license	
License	Copy the provided license key from your email, paste it in the **License** field, and then click **Load** to load the license. For more information about ordering licenses, see Ordering Licenses and Loading Licenses.
Licenses–Loaded licenses	
Key	Overview of loaded licenses. Click **Delete**, if you want to delete a license.
Licenses–Active License Summary	
Users	Shows details about user license. E.g. 30
Features	Shows details about enabled license required features. E.g. Handset Sharing, Enhanced Provisioning Interface.

Administration–Media Resource–Media Resource

Field	*Setting*
Media Resource–General	
IP address (Read only)	Current IP address of the media resource. **Note**: If the field is empty, the media resource is an internal media resource.

Field	*Setting*
Serial/UUID	Serial number of the Spectralink IP-DECT Server 6500 or UUID of the Spectralink Virtual IP-DECT Server One.
TLS fingerprint	The TLS fingerprint identifies the key associated with the certificate installed in the media resource. This can be used to verify the connected media resource by comparing the TLS fingerprint with the **Key ID** field of the **Host Key** (web-based Administration Page of the media resource> **Configuration**> **Certificates**> **Host key** page> **Key ID** column). E.g.: 46 d5 f5 c0 8c 24 42 49 f1 bc ee 75 28 55 7f d3 b5 9a 11 b2
Description (Optional)	Enter a description. Spectralink recommends using a description of the physical location.
Site	Default value: None You can define sites for devices that are located at the same location. To assign a site to the media resource, select the relevant site from the list. For information about defining sites, see Defining a Site for the Media Resource and Base Stations.
Disabled (Optional)	If enabled, the media resource will be disabled. **Note**: If **Add new as active** is enabled (**Configuration**> **Wireless Server**> **Media resources**), then this will be unset by default when adding a new media resource.

Administration–Base Station–Base Station

Field	*Setting*
Base Station–General	
IP address (Read only)	Current IP address of the base station.
Description (Optional)	Enter a description. Spectralink recommends using a description of the physical location.
RPN	Radio Part Number of the base station. **Note**: If using zone-based paging, assigning base stations and RPN's are essential, as the RPN decides which zone the Spectralink IP-DECT Base Station will be part of. For more information, see Example of Defining Sites, Zone and Assigning Numbers to Base Stations. If using radio-based synchronization in connection with zone-based paging, RPN's must be assigned to the relevant zone before defining synchronization chain.
Site	Default value: None You can define sites for devices that are located at the same location. To assign a site to the base station, select the relevant site from the list. For information about defining sites, see Defining a Site for the Media Resource and Base Stations.
Disabled (Optional)	If enabled, the base station will be disabled. **Note**: If **Add new as active** is enabled (**Configuration**> **Wireless Server**> **Base stations**), then this will be unset by default when adding a new base station.
TX power (Optional)	Used for controlling the output power for this specific base station. Select another value from the list, if you need to change the output power. Default value: Default (250 mW). If Frequency is set to **USA**, the default value is 100 mW. **Note**: If a system TX power other than default is set for the whole system (**Configuration**> **Wireless Server**> **DECT**), that setting will override this setting.

Field	*Setting*
External antenna mode (Optional)	Determines which antenna(s) are used when an external antenna is connected. Possible values: **Use Internal & external antenna**, **Use internal antenna only** or **Use external antenna only**. Default value: Use Internal & external antenna **Note**: This setting is ignored when no external antenna is connected. **Note**: When using external antenna, the range is reduced by up to 50%.
Base Station–Synchronization	
Type	This setting controls the synchronization type used for the specific base station/DECT radio. Possible values: **Free running**, **Radio**, **LAN** or **Radio/LAN Gateway**. Select **Free running**, if you want to configure this base station as sync master. Otherwise select either **Radio**, **LAN** or **Radio/LAN Gateway**, depending on the synchronization method. Default value: Radio **Note**: Automatic configuration of radio synchronization is supported on systems running firmware PCS 20B_ or newer. For more information, see Automatic Configuration of Radio Synchronization. **Note**: To be able to select **LAN** or **Radio/LAN Gateway**, acquisition of a LAN Synchronization License is required. **Note**: System wide settings for synchronization are located under **Configuration**> **Wireless Server**> **Base stations**. For more information, see Synchronization and Deployment Guide.
Auto radio sync (deployment only) (Optional)	If enabled, the base station will be auto synchronized while deploying the system. **Note**: This must only be used while deploying the system.
Primary radio sync (RPN) (Optional)	RPN identifying the base station used for primary radio synchronization.
Secondary radio sync (RPN) (Optional)	RPN identifying the base station used for secondary radio synchronization.
Base Station–RSSI map (Only visible if more than one base station on the system)	
RPN/RSSI dB/Offset	Possible to see the RSSI values of the base stations the selected base station is synchronizing on (Primary sync/Secondary (Alternative) sync). For more information about RSSI values, see Synchronization and Deployment Guide.

Administration–Sites–New site

Field	*Setting*
New site–General	
Name	Enter a name for the site. E.g. Site A, Site B, Site C.

Administration–Phonebook

Field	*Setting*
Phonebook Configuration–Disabled	
Disabled	As default, phone book configuration is disabled.

Field	*Setting*
	You can configure the server to retrieve phone book data using LDAP server or by import of phone book data from a CSV file.
Phonebook Configuration–Imported CSV file	
Imported CSV file	Enable this if you want to import phone book data from CSV file.
Import	Browse for the CSV file to import. **Note**: The CSV file must contain correct format. For more information, see Parameter Overview.
Encoding	Select the correct encoding for the CSV file. You can choose between **UTF-8**, **ISO/IEC 8859-1** or **Windows-1252**. **Note**: The encoding depends on the software that was used to generate the CSV file. If you use Microsoft Windows, you will probably select Windows-1252.
Number fields	Enter the indexes of the columns containing dialable numbers.
Phonebook Configuration–LDAP	
LDAP	Enable this if you want to configure the server to retrieve phonebook data using LDAP server. **Note**: Secure LDAP (LDAPS) communication occurs over port TCP 636. LDAPS communication to a global catalog server occurs over TCP 3269. When connecting to ports 636 or 3269, SSL/TLS is negotiated before any LDAP traffic is exchanged. If using secure LDAP (LDAPS), the necessary certificates must be installed. For more information about CA certificates, see Configuring Certificates. For an example of LDAP configuration, see Parameter Overview.
URI	Enter the URI of the LDAP server. E.g. ldap://example.org (or ldaps://example.org if using secure LDAP)
Bind user (Optional)	Enter the username used for authentication against LDAP. Note: It might be necessary to specify the path for username (DOMAIN\username). E.g. CN=Manager, DC=example, DC=com.
Bind password (Optional)	Enter the Bind user's password.
Base (Optional)	Enter the base path where the users are located in the LDAP structure. E.g. DC=example, DC=com.
Filter (Optional)	Enter the filter used for the LDAP query. The (object Class s= person) filter can be used successfully in most cases.
Attributes	Enter the LDAP attributes you want to query the LDAP for, separated by a comma. E.g. displayName,telephoneNumber, mobile.
Number attributes (Optional)	Enter LDAP attributes that will be used to dial. E.g. telephoneNumber,mobile.
Attributes names (Optional)	Enter the attribute names you want to assign to the attributes specified above, separated by a comma. E.g. Name,Phone,Mobile.
Replace prefixes (Optional)	Enter the phone number prefixes to replace or strip, separated by a comma. E.g.: if the phone number is +45678912345, and that user has the extension 12345, then you specify "+456789" in the **Replace prefixes** field. Or if the phone number is "+456789123456" and "06789123456" must be dialed, then specify "+45=0".
Load interval	Enter the interval in seconds for querying the LDAP server for updates. Default value: 3600 sec Possible values: 60–999999 sec

Field	*Setting*
Request timeout	Enter the interval in seconds for timeout for LDAP requests. Default value: 60 sec Possible values: 5–3600 sec
Phonebook Configuration–BroadWorks	
BroadWorks	Enable this if you want to configure the server to retrieve phonebook data using BroadWorks. You can select a combination of five BroadWorks phonebooks/directories on the Spectralink IP-DECT/Virtual IP-DECT Server One: • Enterprise Directory • Enterprise Common • Group Directory • Group Common • Personal Directory The BroadWorks phone books/directories are retrieved each time the user enters the phone book from the handset. The difference between Enterprise Directory/Group Directory and the Enterprise Common/Group Common is, that the Directory contains a list of contacts in the enterprise/group, whereas the Common is a list of commonly used contacts that are not in the enterprise/group. Each retrieved phonebook/directory entry consists of the following data: • **Name**–corresponding to the BroadWorks' "name" element or a concatenation of "firstname" and "lastname". • **Department**–corresponding to the BroadWorks' "department" element. • **Number**–corresponding to the BroadWorks' element with the following priority: 1: "number", 2: "phone", 3: "extension". • **Mobile**–corresponding to the BroadWorks' "mobile" element.
URI *	Enter the relevant URI of the BroadWorks server. E.g.: https://example.org
Enterprise Directory	Default value: Enabled
Enterprise Common	Default value: Enabled
Group Directory	Default value: Enabled
Group Common	Default value: Enabled
Personal Directory	Default value: Enabled

Administration–Backup

Field	*Setting*
System Backup–Backup	
Full system backup	Click **Save**. A full system backup is performed and saved.
System Backup–Restore	
Full system restore	Click **Browse** to browse for the relevant backup file, and then click **Restore**.

Firmware

Firmware–Wireless Server

Field	*Setting*
Update firmware–Firmware file	
	Click Browse to browse for the relevant firmware file. **Note**: The Spectralink IP-DECT Servers support doing firmware updates directly from a firmware file and also from firmware files contained in a ZIP file. Zip file firmware update is only supported on systems running firmware PCS 20B_ or newer. On the Spectralink Virtual IP-DECT Server One, it is required to use a ZIP file containing both the Spectralink Virtual IP-DECT Server One firmware (.ova file) and the Spectralink IP-DECT Server firmware (.bin file) in order to use the firmware as default for base stations and media resources. Enable the **Use firmware as default** check box if you want the server firmware as default for all base stations and media resources (recommended). Click **Update** to update the firmware file.

Firmware–Media Resource

Field	*Setting*
Update media resource firmware–Default	
	Information about default firmware files type, version (PCS) and build number -- if firmware files have been uploaded. **Note**: Once uploaded, default firmware will remain on the server until overwritten. **Note**: If the **Use firmware as default** check box on the Update firmware page is enabled (**Firmware**> **Wireless Server** or **Configuration**> **Provisioning**> **Firmware**), then the server firmware is uploaded as default for all base stations and media resources (recommended). For the files to be updated in the **media resource**, this must be executed either through manual update or automatic update.
Update media resource firmware–Automatic	
Enable (Optional)	Default value: Disabled Enable this, if you want to make automatic update possible. The media resources will be automatically updated using the default firmware. Also new media resources automatically update to new default firmware when connected. **Note**: If the default firmware version changes, the update process will start automatically according to the chosen values in the **Force** and **Start** time fields. **Note**: Using provisioning for base stations, media resources and handsets, enabling automatic update is required. This can be done either through the XML configuration file or the web-based Administration Page. For more information, see *Provisioning Guide*.
Force (Optional)	When **Force** is enabled, the media resources will be updated at the selected Start time. If **Force** is disabled, the media resources will be updated when they become idle after the selected Start time.
Start time (Optional)	Default value: Immediately If you want to upload later, select an appropriate time within the next 24 hours.
	Click **Save**.

Field	*Setting*
Update media resource firmware–Manual	
Firmware file (Optional)	The firmware file can be either a previously uploaded default firmware file, or a new firmware file chosen. A new firmware file has to be a valid firmware file with the extension .bin or a zip file containing a valid firmware file. Select either **Default** or **Upload**. **Note**: Zip file firmware update is only supported on systems running firmware PCS 20B_ or newer.
Start media resource No	The index number of the first media resource to be updated. You can check media resource numbers under **Administration**> **Media resource**.
End media resource No	The index number of the last media resource to be updated.

Firmware–Base Station

Field	*Setting*
Update base station firmware–Default	
	Information about default firmware files type, version (PCS) and build number -- if firmware files have been uploaded. **Note**: Once uploaded, default firmware will remain on the server until overwritten. **Note**: If the Use firmware as default check box on the Update firmware page is enabled (**Firmware**> **Wireless Server** or **Configuration**> **Provisioning**> **Firmware**), then the server firmware is uploaded as default for all base stations and media resources (recommended). For the files to be updated in the **base station**, this must be executed either through manual update or automatic update.
Update base station firmware–Automatic	
Enable (Optional)	Default value: Disabled Enable this, if you want to make automatic update possible. The base stations will be automatically updated using the default firmware. Also new base stations automatically update to new default firmware when connected. **Note**: If the default firmware version changes, the update process will start automatically according to the chosen values in the **Force** and **Start** time fields. **Note**: Automatic update of Spectralink IP-DECT Base Stations requires base stations with firmware version PCS 15__ or newer. **Note**: Using provisioning for base stations, media resources and handsets, enabling automatic update is required. This can be done either through the XML configuration file or the web-based Administration Page. For more information, see *Provisioning Guide*.
Force (Optional)	When **Force** is enabled, the base stations will be updated at the selected Start time. If **Force** is disabled, the base stations will be updated when they become idle after the selected Start time.
Start time (Optional)	Default value: Immediately If you want to upload later, select an appropriate time within the next 24 hours.
	Click **Save**.
Update base station firmware–Manual	
Firmware file (Optional)	The firmware file can be either a previously uploaded default firmware file, or a new firmware file chosen. A new firmware file has to be a valid firmware file with the extension .bin or a zip file containing a valid firmware file.

Field	*Setting*
	Select either **Default** or **Upload**. **Note**: Zip file firmware update is only supported on systems running firmware PCS 20B_ or newer.
Start base station No	The index number of the first base station to be updated. You can check base station numbers under **Administration**> **Base Stations**> **IP Base Stations**.
End base station No	The index number of the last base station to be updated.

Firmware–Handset

Field	*Setting*
Handset update settings–Automatic update	
Enable (Optional)	Enable. This will make automatic update possible.
Only in charger (Optional)	If enabled, only handsets in charger will be updated.
Start time (Optional)	Default value: Immediately If you want to upload later, select an appropriate time within the next 24 hours.
System load (Optional)	Select relevant upload capacity. The load corresponds to the number of maximum simultaneous updates. Possible values: **Low**, **Medium** or **High**. Default value: Medium **Low**: 1 handset at a time. **Medium**: 4 handsets per media resource. **High**: 16 handsets per media resource. Example: 2 media resources and High load = 2*16 = 32 simultaneous updates. **Note**: If you schedule an upgrade during day hours, you would typically choose **Low** to **Medium** load to avoid any impact on Users. Upgrade after hours typically means no User load, therefore, you can choose **High** priority. **Warning**: If you set system load to **High**, then you risk that the process allocates all MR channels, which will block for new incoming and outgoing voice calls.

Appendix A: Intercom (Push-To-Talk)

Using a Spectralink IP-DECT/Virtual IP-DECT Server One, an auto-answer feature, intercom, is available, making it possible to use intercom and loudspeaker calls if numbers for intercom groups are defined on the SIP PBX.

Activation of Intercom using Headers

If an INVITE with an Alert-Info header, a Call-Info header or an Answer-Mode header is received, you can make a Spectralink DECT Handset automatically answer the call, mute the microphone and turn on speakerphone.

Note:

The reason for handling several headers for activating the Push-to-Talk feature is that different SIP PBXs have different default implementations.

The following list of headers will activate intercom (auto-answer) when sent from the SIP PBX to the Spectralink IP-DECT/Virtual IP-DECT Server One:

- Alert-Info: Auto Answer
- Alert-Info: info=alert-autoanswer
- Alert-Info: Ring Answer
- Alert-Info: info=RingAnswer
- Alert-Info: Intercom
- Alert-Info: info=intercom
- Call-Info: =\;answer-after=0
- Call-Info: ;answer-after=0
- Answer-Mode: Auto (This is according to RFC 5373)

Note:

The **Alert-Info** header can also be used to control external/internal ring pattern. This feature is not affected by the addition of the loudspeaker call feature.

The following **Alert-Info** headers can be used to enable internal ringing (external ringing is default).

- Alert-Info: <internal>
- Alert-Info: <alert-internal>
- Alert-Info: internal
- Alert-Info: alert-internal

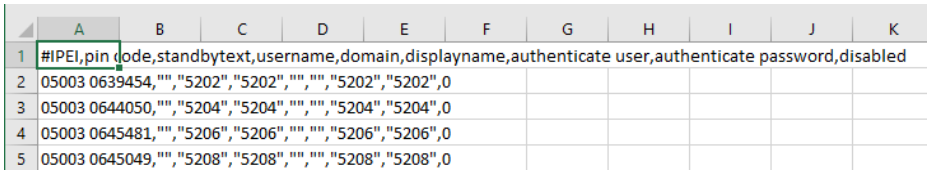
Appendix B: Example of Handset Registration Data-CSV Format

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

#IPEI,access code,standbytext,username,domain,displayname,authenticate user,authenticate password,disabled

Note:

If you want to leave out some of the information, e.g. standbytext, you must keep the commas, e.g.:
#IPEI,access code,,username,domain,displayname,authenticate user,authenticate password,disabled.



	A	B	C	D	E	F	G	H	I	J	K
1	#IPEI,pin code,standbytext,username,domain,displayname,authenticate user,authenticate password,disabled										
2	05003 0639454,"","5202","5202","","","5202","5202",0										
3	05003 0644050,"","5204","5204","","","5204","5204",0										
4	05003 0645481,"","5206","5206","","","5206","5206",0										
5	05003 0645049,"","5208","5208","","","5208","5208",0										

For more information about importing user data, see Import/Export of Users or Delete Users.

Note:

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

Appendix C: Handset Configuration XML File Example

```
<cota>
    <info>
        <group>100</group>
        <version>1</version>
    </info>
    <data>
        <ringing_volume>
            <volume>7</volume>
        </ringing_volume>
        <ringing_tone>
            <tone>6</tone>
        </ringing_tone>
        <alert_volume>
            <volume>2</volume>
        </alert_volume>
        <vibrate>
            <active>true</active>
        </vibrate>
        <silent_mode>
            <active>false</active>
            <settings>
                <display_flashing>true</display_flashing>
                <vibrate>true</vibrate>
                <short_ring>false</short_ring>
            </settings>
        </silent_mode>
        <auto_key_lock>
            <active>false</active>
        </auto_key_lock>
        <backlight>
            <timeout_state>off</timeout_state>
            <delay>5</delay>
        </backlight>
        <auto_answer>
            <active>false</active>
            <when_to_answer>
                <value>after_first_ring</value>
                <after_first_ring>
                    <audio_options>internal</audio_options>
                    <also_in_charger>false</also_in_charger>
                </after_first_ring>
            </when_to_answer>
        </auto_answer>
        <out_of_range>
            <active>false</active>
            <notifications>tone_and_icon</notifications>
        </out_of_range>
        <show_missed_calls>
            <active>true</active>
```

```
</show_missed_calls>
<absent_in_charger>
    <active>false</active>
</absent_in_charger>
<bluetooth>
    <active>false</active>
    <settings>
        <auto_connect>false</auto_connect>
        <headset_volume>4</headset_volume>
    </settings>
</bluetooth>
<language>
    <set>english</set>
</language>
<headset>
    <alerting>false</alerting>
    <volume>4</volume>
</headset>
<hearing_aid_compatibility>
    <active>false</active>
</hearing_aid_compatibility>
<microphone_gain>
    <value>0_dB</value>
</microphone_gain>
<ear_gain>
    <value>0_dB</value>
</ear_gain>
<longkey>
    <value>speed_dial</value>
    <individual_settings>
        <key_0>speed_dial</key_0>
        <key_1>speed_dial</key_1>
        <key_2>speed_dial</key_2>
        <key_3>speed_dial</key_3>
        <key_4>speed_dial</key_4>
        <key_5>speed_dial</key_5>
        <key_6>speed_dial</key_6>
        <key_7>speed_dial</key_7>
        <key_8>speed_dial</key_8>
        <key_9>speed_dial</key_9>
    </individual_settings>
</longkey>
<economy_mode>
    <active>true</active>
</economy_mode>
<alarm_key>
    <state>send_msf</state>
    <speed_dial>
        <loudspeaker>false</loudspeaker>
    </speed_dial>
</alarm_key>
<rolling_tasks>
    <time_in_sec>5</time_in_sec>
    <indication_interval>1</indication_interval>
</rolling_tasks>
<auto_login>
```

```
    <active>false</active>
</auto_login>
<time_and_date>
    <time_format>24_hour</time_format>
    <date_format>DD/MM/YYYY</date_format>
</time_and_date>
<minimum_ring_time>
    <period>off</period>
</minimum_ring_time>
<compatibility>
    <cs1k>false</cs1k>
    <extended_location_registration>true</extended_location_registration>
</compatibility>
<handover_profile>
    <profile>normal</profile>
</handover_profile>
<local_tOne>
    <country>germany</country>
</local_tOne>
<message_list_content>
    <show>text</show>
</message_list_content>
<noisy_environment>
    <active>false</active>
</noisy_environment>
<flash_led_on_call>
    <active>false</active>
</flash_led_on_call>
<msf_tOne_in_a_call>
    <sound>normal</sound>
    <vibrate>false</vibrate>
</msf_tOne_in_a_call>
<dect_security>
    <monitoring>
        <active>false</active>
    </monitoring>
</dect_security>
<standby_text>
    <value>Spectralink</value>
</standby_text>
<logo>
    <type>standard</type>
</logo>
<shortcut>
    <phonebook_add_name>false</phonebook_add_name>
    <auto_answer>false</auto_answer>
    <auto_key_lock>false</auto_key_lock>
    <backlight>false</backlight>
    <headset>false</headset>
    <message_inbox>false</message_inbox>
    <message_new>false</message_new>
    <message_templates>false</message_templates>
    <ringing_tone>false</ringing_tone>
    <silent_mode>false</silent_mode>
    <status>false</status>
```

```
    <vibrate>false</vibrate>
    <task_list>false</task_list>
    <noisy_environment>false</noisy_environment>
    <phonebook>false</phonebook>
    <external_services>false</external_services>
    <sign_in_out>true</sign_in_out>
    <screen_lock>false</screen_lock>
    <lone_worker_mode>true</lone_worker_mode>
</shortcut>
<power_off_password>
    <password></password>
</power_off_password>
<in_call_volume>
    <volume>3</volume>
</in_call_volume>
<tear_off_alarm>
    <state>off</state>
    <prealarm>false</prealarm>
    <speed_dial>
        <loudspeaker>false</loudspeaker>
    </speed_dial>
    <indication>false</indication>
    <prealarm_indication>false</prealarm_indication>
    <prealarm_4x>false</prealarm_4x>
    <trigger_time>0</trigger_time>
    <prealarm_trigger_time>0</prealarm_trigger_time>
</tear_off_alarm>
<running_detector_alarm>
    <state>off</state>
    <prealarm>false</prealarm>
    <speed_dial>
        <loudspeaker>false</loudspeaker>
    </speed_dial>
    <indication>false</indication>
    <prealarm_indication>false</prealarm_indication>
    <prealarm_4x>false</prealarm_4x>
    <trigger_time>0</trigger_time>
    <prealarm_trigger_time>0</prealarm_trigger_time>
</running_detector_alarm>
<man_down_alarm>
    <state>off</state>
    <prealarm>false</prealarm>
    <speed_dial>
        <loudspeaker>false</loudspeaker>
    </speed_dial>
    <indication>false</indication>
    <prealarm_indication>false</prealarm_indication>
    <prealarm_4x>false</prealarm_4x>
    <trigger_time>0</trigger_time>
    <prealarm_trigger_time>0</prealarm_trigger_time>
</man_down_alarm>
<screen_lock>
    <active>false</active>
    <auto_lock_time>18</auto_lock_time>
    <unlock_attempts>3</unlock_attempts>
    <minimum_pin_length>6</minimum_pin_length>
```

```
    <pin></pin>
</screen_lock>
<menu_main>
    <phonebook>true</phonebook>
    <call_register>true</call_register>
    <messages>true</messages>
    <msf_functions>true</msf_functions>
    <external_services>true</external_services>
    <presence>true</presence>
    <status>true</status>
    <settings>true</settings>
</menu_main>
<menu_phonebook>
    <find>true</find>
    <add>true</add>
    <speed_dial>true</speed_dial>
    <delete>true</delete>
</menu_phonebook>
<menu_call_register>
    <incoming>true</incoming>
    <outgoing>true</outgoing>
    <missed>true</missed>
    <delete>true</delete>
</menu_call_register>
<menu_messages>
    <new>true</new>
    <inbox>true</inbox>
    <outbox>true</outbox>
    <erase>true</erase>
    <templates>true</templates>
    <task>true</task>
</menu_messages>
<menu_status>
    <silent_mode>true</silent_mode>
    <headset>true</headset>
    <auto_answer>true</auto_answer>
    <economy_mode>true</economy_mode>
    <battery>true</battery>
    <ringing_tone>true</ringing_tone>
    <ringing_volume>true</ringing_volume>
    <rssi>true</rssi>
    <survey>true</survey>
    <general_information>true</general_information>
</menu_status>
<menu_settings>
    <ringing_volume>true</ringing_volume>
    <ringing_tone>true</ringing_tone>
    <alert_volume>true</alert_volume>
    <vibrate>true</vibrate>
    <silent_mode>true</silent_mode>
    <auto_key_lock>true</auto_key_lock>
    <backlight>true</backlight>
    <auto_answer>true</auto_answer>
    <out_of_range>true</out_of_range>
    <missed_calls>true</missed_calls>
```

```
    <absent_in_charger>true</absent_in_charger>
    <bluetooth>true</bluetooth>
    <advanced>true</advanced>
</menu_settings>
<menu_backlight>
    <on_off>true</on_off>
    <settings>true</settings>
</menu_backlight>
<menu_silent_mode>
    <on_off>false</on_off>
    <settings>true</settings>
</menu_silent_mode>
<menu_auto_answer>
    <on_off>true</on_off>
    <settings>true</settings>
</menu_auto_answer>
<menu_out_of_range>
    <on_off>true</on_off>
    <settings>true</settings>
</menu_out_of_range>
<menu_advanced>
    <language>true</language>
    <headset>true</headset>
    <hearing_aid_compatibility>true</hearing_aid_compatibility>
    <microphone_gain>true</microphone_gain>
    <long_key>true</long_key>
    <economy_mode>true</economy_mode>
    <alarms>true</alarms>
    <master_handset>true</master_handset>
    <rolling_tasks>true</rolling_tasks>
    <login>true</login>
    <time_and_date>true</time_and_date>
    <minimum_ring_time>true</minimum_ring_time>
    <compatibility>true</compatibility>
    <handover_profile>true</handover_profile>
    <local_tOne>true</local_tOne>
    <message_list_content>true</message_list_content>
    <noisy_environment>true</noisy_environment>
    <flash_led_on_call>true</flash_led_on_call>
    <msf_tOne_in_a_call>true</msf_tOne_in_a_call>
    <dect_security>true</dect_security>
    <screen_lock>true</screen_lock>
    <echo_canceller>true</echo_canceller>
</menu_advanced>
<menu_headset>
    <on_off>true</on_off>
    <settings>true</settings>
</menu_headset>
<menu_long_key>
    <all>true</all>
    <individual>true</individual>
</menu_long_key>
<menu_long_key_individual>
    <key_0>true</key_0>
    <key_1>true</key_1>
```

```
            <key_2>true</key_2>
            <key_3>true</key_3>
            <key_4>true</key_4>
            <key_5>true</key_5>
            <key_6>true</key_6>
            <key_7>true</key_7>
            <key_8>true</key_8>
            <key_9>true</key_9>
         </menu_long_key_individual>
         <menu_alarms>
            <alarm_key>true</alarm_key>
            <tear_off>true</tear_off>
            <running_detector>true</running_detector>
            <man_down>true</man_down>
         </menu_alarms>
         <menu_screen_lock>
            <on_off>true</on_off>
            <settings>true</settings>
         </menu_screen_lock>
         <echo_canceller>
            <active>false</active>
         </echo_canceller>
      </data>
   </cota>
```

Appendix D: Configuration Parameters

Please see the entire configuration document starting on the next page.

Configurations for Spectralink Servers
DECT 2500/8000,
IP-DECT 200/400/6500 and
Virtual IP-DECT Server One

ToC:

1. Introduction

This document lists configuration parameters for Spectralink DECT and IP-DECT servers.

The configuration parameters are stored in an XML file and have a hierarchical structure with the root element <config> and sub elements grouped together based on relations. This document presents the hierarchical structure with a →
For example, the configuration:

feature_codes → call_forward → unconditional → enable

represents the following XML structure where the characters #21# are the value of the parameter.

```
<feature_codes>
    <call_forward>
        <unconditional>
            <enable>#21#<enable>
        </unconditional>
    </call_forward>
</feature_codes>
```

Some configurations are represented as arrays. For example the following configuration has three arrays, shelf, card and port which can be of any number depending on installation:

bif08 → shelf[] → card[] → port[] → enable (ex. bif08 → shelf1 → card2 → port3 → enable)

1.1 Revision history

Date	Initials	Changes	Version
2017-03-06	KIE	Initial version	001
2017-06-07	KIE	External version	002
2017-06-26	KIE	Added descriptions	003
2017-08-23	KIE	Added configurations for provisioning and automatic update of handsets, base stations and media resources	004
2017-11-13	KIE	Changed provisioning configurations and added security configurations	005
2018-02-08	KIE	Changed Suota Load description	006
2018-02-20	KIE	Added IP-DECT 200	007
2018-05-02	KIE	Changed description for Phonebook source	008
2018-05-15	KIE	Corrections: ipv6.methods, global_tx_power and network.vlan	009
2018-05-18	SOS	Added nat_keepalive and nat_keepalive_interval	010
2018-05-23	KIE	Added dect.early_encryption_rekeying and dect.subscription_window. Changed options and default setting of encrypt_voice_data	011
2018-05-30	KIE	Removed media_resource.server and rfp.server as they are a MR and a RFP configurations respectively. Changes: ptp.transport, rfp.ptp.cos and rfp.ptp.tos	012
2018-06-15	SOS	Added redundancy.peer.factoryid	013
2018-08-29	KIE	Changed default value of dect.early_encryption_rekeying from enabled to disabled	014
2018-09-19	TQD	Added new setting rfp.auto.source_digital	015
2018-10-03	MMM	Added new setting sip.blacklist_timeout & sip.registration_max_pending	016
2018-10-08	SOS	Added new settings rfp.gui_allowed & server.gui_allowed	017
2018-10-17	SOS	Changed rfp.gui_allowed to rfp.allow_gui and server.gui_allowed to security.allow_gui	018
2018-11-02	KIE	Added options to sip.registration_max_pending	019

2019-04-05	MMM	Added option ”sip.allow_internal_routing”	020
2019-05-28	MTH	Added ”sip.application.enable_fas”	021
2019-09-02	SOS	Added “dect.global_lal	022
2019-10-03	MTH SSOE KIE	Added “application. enable_atex_gap” Added “provisioning.cota.check” Added “sip.hold_before_refer” Added “security.legacy_tls” Removed Taiwan and China from “dect.frequency” Added “rfp.paging_method”	023
2019-10-23	MTH	Changed description for global_lal and paging methode	024
2019-10-30	KIE	Added settings for “phonebook.broadworks” and added broadworks to phonebook.source	025
2019-12-02	TQD KIE	Added “sip.convert_sip_uri_to_phone” Added “dect.radio.HandoverInfo” Added licensee Added Virtual IP-DECT Server One to document title.	026
2020-04-23	MTH	Removed Licensee	027
2020-06-25	MMM	Added AMiE configurations: • “amie.enable” • “amie.region” • “amie.server” • “amie.auth_token” • “amie.proxy”	028
2020-06-26	IC	Added Statistics threshold configurations	029
2020-11-03	IC	Added COTA default configurations	030

2. Configurations

* = hidden or license required

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
amie	enable		x	true/false	false	If enabled, the IP-DECT Server will attempt to raise a connection to AMiE.
	region		x	IE, custom	IE	AMiE regions available. If "custom" is selected, the next field "server" defines where the IP-DECT Server connects to.
	server		x	-	-	AMiE custom server name.
	auth_token		x	-	-	Specifies the authentication token, used to authenticate the IP-DECT Server towards AMiE. The token is generated in AMiE and is unique to the registered IP-DECT Server.
	proxy		x	-	-	It is possible to use a HTTP proxy when connecting to AMiE.
app_db	ab_always_onhook_on_busytone	x		true/false	false	Specifies if the DECT server should always try to detect busy tone and release incoming call on analog lines as they were auto answered.
application	enable_rpc	x	x	true/false	false	Specifies if the XML-RPC application interface is enabled.
	enable_msf		x	true/false	false	Specifies if the MSF application interface is enabled.
	internal_messaging (same as: system_events → msf_between_pp on 2500/8000)		x	true/false	true	Controls if messaging between handsets is handled internally or by an external application. If enabled messages will be handled internally.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
	enable_fas		x	True/false	false	Specifies if the connectivity to FAS is enabled. FAS is a vendor specific messaging server.
	enable_atex_gap		x	True/false	false	Specifies if GAP as enrolment type for Atex handsets is enabled, if not enabled DoIP enrolment type will be used.
	password	x	x	-	Default: IP-DECT Server 400/6500 “f621c2268a8df249 55ef4052bfbb80cf” (password “ip6500” encrypted) Default: DECT Server 2500/8000 “8e49ea4c7249f802a983ad c7d50375f1”(password “kws8000” encrypted)	Specifies the password required for applications to log in.
	username	x	x	-	GW-DECT/admin	Specifies the user name required for applications to log in.
cota	reset → menus		x	true/false	true	Specifies if Handset Configuration reset to default command will reset device menus
	reset → settings		x	true/false	true	Specifies if Handset Configuration reset to default command will reset device settings
bif08	shelf[] → card[] → port[] → enable	x		true/false	true	Specifies if the base station at the given location is enabled or disabled.
dect	auth_call (same as: system_events → auth_call on 2500/8000)		x	true/false	true	Specifies if DECT authentication should be used when establishing calls.
	accesscode (same as: system_events → system_access_code on 2500/8000)		x	-	-	Specifies a system wide DECT access code required for subscribing handsets. The access code is from 0 to 8 decimal digits. Access codes assigned for specific users will override this setting.
	early_encryption_rekeying		x	disabled/enabled/required	disabled	If enabled, this enables encryption immediately after connection establishment and regular re-keying until connection termination

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
	encrypt_voice_data (same as: system_events → encrypt_voice_data on 2500/8000)		x	disabled/enabled/required	required	Specifies if DECT encryption should be used for voice calls.
	global_tx_power	x	x	0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	0	Specifies the output power (dBm) of all connected base stations supporting power control.
*	handset_login		x	true/false	false	Specifies if handset login is enabled or disabled.
	handset_sharing		x	true/false	false	Specifies if handset sharing is enabled or disabled.
	send_date_time (same as: system_events → send_date_time on 2500/8000)		x	true/false	true	Specifies if the date and time should be sent to the handsets.
	subscription_allowed (same as: system_events → subscription_allowed on 2500/8000)		x	true/false	true	Specifies if handset subscription is allowed.
	subscription_window		x	true/false	true	If set, subscriptions will automatically be disallowed after 120 seconds or when a subscription succeeds
*	frequency	x	x	Europe, South America, USA	-	Specifies the DECT frequency band to be used. Europe (EMEA, Australia and New Zealand). USA (USA & Canada).
	allow_long_messages		x	true/false	true	Specifies if long MSF messages and long call back numbers are allowed.
*	radio → ExternalAntenna	x		0 = both 1 = internal 2 = external	0	Specifies which antenna(s) are used when an external antenna is connected. This setting is ignored when no external antenna is connected.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
	global_lal		x	Location Area Level (LAL). Called zones in web GUI. Possible zones. 0 = No zones (is set to zero if paging method is different from "Zone based") 3 = 32 base stations per zone. 4 = 16 base stations per zone. 5 = 8 base stations per zone.	0	Sets the Location Area Level (LAL), also called zones in web GUI. dect_global_lal is used when paging method "rfp.paging_method" is set to "zone based". The global_lal value determine how many zones a site is divided into. Currently 3 zone sizes are available. 8, 16 or 32 base stations per zone
	radio→ HandoverInfo	x	x	1 = Disallow 3 = Allow		Allow/disallow bearer handover between repeater and base station.
license		x	x	A comma separated list of licenses	-	Stores the license, if installed.
feature_ codes	enable	x	x	true/false	false	Enables/disables local handling of feature codes.
	call_forward → unconditional →disable	x	x	-	*21*$#	Specifies the feature code used for disabling unconditional call forward (CFU). The feature code users must dial to disable unconditional call forward. D
	call_forward → unconditional →enable	x	x	-	#21#	Specifies the feature code used for enabling unconditional call forward (CFU).
*	call_forward → voicemail →enable	x	x	-	*21*	Specifies the feature code used for enabling voicemail call forwarding.
*	pickup →local	x	x	-	**3	Specifies the feature code used for picking up a local call.
*	pickup →group_other	x	x	-	**8	Specifies the feature code used for picking up a call in an associated group.
*	conference →meetme	x	x	-	**5$	Specifies the feature code used for starting a Meet-Me conference.
*Handset_ sharing	deAssign1	x		-	Logged out by another user	Specifies the text displayed in a handset if a user is logged out by another user.
*	deAssign2	x		-	Logged out by coexist timer	Specifies the text displayed in a handset if a user is logged out by the coexist timer.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
*	deAssign3	x		-	Logged out by charger	Specifies the text displayed in a handset if placed in a charger.
*	hs_react_multicharger	x		0x00, 0x01, 0x02, 0x04, 0x08 (All chargers, Multi charger only, No action, Power on/off, Long press 8)	0x01	Specifies when to start login/logout procedure. **All Chargers:** Shared handsets will login/logout in all chargers. **Multi charger only:** Shared handsets will login/logout in multi chargers only. **No action:** Shared handsets will NOT login/logout if placed in any charger type. **Power on/off:** is ticked, the shared handset will login/logout if the handset is respectively powered up or down. **Long press 8** is ticked, the shared handset will start the login/logout procedure when the "8" key on the shared handset is pressed for about 2 seconds.
*	linebusy	x		-	Extension busy	Specifies the text displayed in a handset if a user tries to login to a busy extension.
*	max_simul_users	x		1/2/3	1	Specifies the number of simultaneous users for a specific line. All assigned phone on a line will ring on incoming calls, all phones will receive incoming MSF; If one phone have an active call, then the other phone on that line can't make calls.
*	text1	x		-	Enter Extension	Specifies the text displayed in a handset when a login procedure begins. The text is displayed when user is prompted to enter an extension number.
*	text2	x		-	Failed: re-enter DN	Specifies the text displayed in a handset when a login procedure begins. The text is displayed when user is prompted to re-enter an extension number.
*	text3	x		-	Enter Password	Specifies the text displayed in a handset when a login procedure begins. The text is displayed when user is prompted to enter a password.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
*	text4	x		-	Failed: re-enter password	Specifies the text displayed in a handset when a login procedure begins. The text is displayed when user is prompted to re-enter a password.
*	timeout_assigned	x		0 – 240 hours	24	Specifies the time that a handset can be subscribed to a line.
*	timeout_simul_users	x		0 – 240 minutes	5	Specifies the time that users can coexist on the same line. The oldest line subscriptions will be removed on timeout.
installation	auto_restart	x		"enabled, Day, Hour, Minute, Weekday, DayWeekOrMonth"	0,20,2,15,2,1	Specifies if automatic restart of DECT server is enabled or disabled.
	company → Address	x		-	Address	Specifies the company's address
	company → city	x		-	City	Specifies the company's city
	company → contact_person	x		-	Contact person	Specifies the company's contact person
	company → country	x		-	Country	Specifies the company's country
	company → direct_email	x		-	Direct email address	Specifies the company's direct email address
	company → direct_phone	x		-	Direct phone number	Specifies the company's direct phone number
	company → fax	x		-	Fax number	Specifies the company's fax number
	company → name	x		-	Company name	Specifies the company name. The company name will be added to the start of all file names in system generated service reports.
	company → phone	x		-	Phone number	Specifies the company's phone number
	company → state	x		-	State	Specifies the company's state
	company → zip	x		-	Zip	Specifies the company's zip
	email → mail_timing	x		-	0	Specifies how often an email should be sent.
	email → reciepient_address	x		-	KWS8000Statistics@spectralink.com	Specifies who shall receive the email
	email → reply_address	x		-	kws8000@emea430.dk	Specifies an email address to reply to.
	email → smtp_address	x		-	-	Specifies the address of the mail server to use.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
	email → smtp_password	x		-	-	Specifies the password of the user on the mail server to use. Writing “none” will reset the password.
	email → smtp_port	x		-	25	Specifies the port on the mail server to use.
	email → smtp_user	x		-	-	Specifies the user name on the mail server to use.
language		x	x	da, de, cs, en, es, fi, fr, it, nl, nb, pl, pt, ru, sv, tr	en	Specifies the language of system messages displayed on phones.
log	syslog → facility		x	0 - 23	16 (local 0)	Specifies the remote syslog facility used for log messages. Refer to RFC5424 for details.
	syslog → host		x	-	-	Specifies the remote syslog server host address.
	syslog → level		x	emergency, critical, error, warning, notice, info, debug	info	Used to specify what log levels to send via syslog. All log messages that have a higher level than the one specified will be sent.
	syslog → port		x	-	514	Specifies the remote port of the syslog server.
	syslog → scope_of_settings		x	all, server only, server and mr	all	Specifies the scope of syslog. The setting all applies to server, media resource and base stations. The setting server and mr applies to Server and media resources. The setting server only applies to the server.
phonebook	source	x	x	disabled, ldap, csv, broadworks	disabled	Specifies the Phonebook source of data. Disabled, use an LDAP server, import a CSV file or retrieve phonebooks/directories from a BroadWorks server.
	csv_number_fields	x	x	-	2	Specifies the indexes of the columns that contain dialable numbers.
	encoding	x	x	utf-8, windows-1252, iso8859-1	utf-8	Specifies the character encoding of the imported CSV file.
	ldap_uri	x	x	-	-	The URI of the LDAP server.
	ldap_bind_user	x	x	-	-	user name used to login to the LDAP server.
	ldap_bind_password	x	x	-	-	Password used to login to the LDAP server.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
	ldap_base	x	x	-	-	The base path where the users are located in the LDAP structure.
	ldap_filter	x	x	refer to RFC4515	(objectClass=person)	The filter used for the LDAP query. The (objectClass=person) filter can be used successfully in most cases.
	ldap_attributes	x	x	-	cn,telephoneNumber,mobile	The LDAP attributes to retrieve and user.
	ldap_number_attributes	x	x	-	telephoneNumber,mobile	Specifies the name of the LDAP attributes that contain dialable numbers.
	ldap_names	x	x	-	-	The attribute names assigned to the Attributes specified, separated by a comma.
	ldap_prefixes	x	x	-	+=00	The phone number prefixes to replace or strip, separated by a comma. For example, if the phone number is +45678912345 and the user must dial the 12345 extension, then “+456789” is specified in the strip prefixes field. If a "=" is added, the prefix will be replaced instead of stripped. For example, if the phone number is +4576280001 and the user must dial the 004576280001 extension, then “+=00” is specified in the strip prefixes field.
	ldap_refresh_interval	x	x	sec	3600	The interval in seconds for querying the LDAP server for updates.
	broadworks → url		x	-	-	Specifies the URL of the BroadWorks server
	broadworks → enterprisedirectory		x	true/false	true	Specifies if Enterprise directory is enabled.
	broadworks → enterprisecommon		x	true/false	true	Specifies if Enterprise common is enabled.
	broadworks → groupdirectory		x	true/false	true	Specifies if Group directory is enabled.
	broadworks → groupcommon		x	true/false	true	Specifies if Group common is enabled.
	broadworks → personaldirectory		x	true/false	true	Specifies if Personal Directory is enabled.
media_ resource	enabled		x	true/false	true	Specifies if the internal media resource if enabled.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
mr	auto → enable		x	true/false	false	Specifies if automatic update is enabled or disabled.
	auto → start_time		x	immediately, hh:mm	immediately	Specifies when to perform the update, immediately or at a specific time within 24h.
	auto → force		x	true/false	false	Specifies if an automatic update should be executed immediately or wait until devices are idle.
msf	local_longpress_0	x		true = Phonebook false = Send key to interface	true	Specifies whether the DECT Server shall handle long key press (from handsets) locally (default) or the key strokes shall be send to messaging interface (XML-RPC or EMD).
	local_longpress_1	x		true = Phonebook false = Send key to interface	true	Same as local_longpress_0
	local_longpress_2	x		true = Phonebook false = Send key to interface	true	Same as local_longpress_0
	local_longpress_3	x		true = Phonebook false = Send key to interface	true	Same as local_longpress_0
	local_longpress_4	x		true = Phonebook false = Send key to interface	true	Same as local_longpress_0
	local_longpress_5	x		true = Phonebook false = Send key to interface	true	Same as local_longpress_0
	local_longpress_6	x		Not used false/true = Send key to interface	true	Same as local_longpress_0
	local_longpress_7	x		true = Master handset false = Send key to interface	true	Same as local_longpress_0
	local_longpress_8	x		true = Handset Sharing false = Send key to interface	true	Same as local_longpress_0
	local_longpress_9	x		true = SFB Sign In/out false = Send key to interface	true	Same as local_longpress_0
network	bootproto	x	x	dhcp/static	8000: static 6500: dhcp	Specifies if the IP configuration is provided by DHCP or static.
	dns1	x	x	-	-	Specifies the Primary DNS.

Configuration parameter	Dect	IP-Dect	Options	Default	Description
dns2	x	x	-	-	Specifies the secondary DNS.
domain	x	x	-	-	Specifies the name of the domain the system belongs to.
gateway	x	x	-	-	Specifies the IP address of the default gateway.
hostname	x	x	-	-	Specifies a hostname that will be inserted into headers in SIP and published via DHCP making the device appear in the DNS.
http-port	x		-	80	Specifies the HTTP port number of the server.
ipaddr	x	x	-	-	Specifies the IPv4 address of the server.
ipv4enable	x		true/false	true	Specifies if IPv4 is enabled or disabled.
ipv6addr	x		-	-	Specifies the static IPv6 address of the server.
ipv6 → ipaddr		x	-	-	Specifies the static IPv6 address of the server with an optional prefix length. Address and prefix length must be separated by a /
ipv6ctype	x		static, slaac, dhcp, llo	slaac	Specifies the IPv6 connection type. **Manual:** Manually setting the IPv6 address, Subnet Prefix Length, Default Gateway, Primary DNS Server, and Secondary DNS Server. **Stateless Address Autoconfiguration (SLAAC):** An IPv6 address is automatically generated based on the prefix being advertised on the connected network. **DHCPv6:** IPv6 address, DNS servers and DNS search list will be obtained from router. **Link-local-address:** A Link-local address is automatically generated using EUI-64. This address is only reachable with other IPv6-capable devices on the LAN side.

Configuration parameter	Dect	IP-Dect	Options	Default	Description
ipv6 → method		x	disabled/static/dhcp/slaac	disabled	Specifies the IPv6 connection method. **disable:** IPv6 is disabled. **static:** Manually setting the IPv6 address, Subnet Prefix Length, Default Gateway, Primary DNS Server, and Secondary DNS Server. **slaac:** An IPv6 address is automatically generated based on the prefix being advertised on the connected network. **dhcp:** IPv6 address, DNS servers and DNS search list will be obtained from router.
ipv6enable	x		true/false	false	Specifies if IPv6 is enabled or disabled.
ipv6gateway	x		-	-	Specifies the IPv6 address of the default gateway.
ipv6 → gateway		x	-	-	Specifies the IPv6 address of the default gateway.
ipv6mtu	x		1280 bytes - 64KB	0 (use default value)	Specifies the IPv6 Maximum Transmission Unit.
ipv6prefix	x		0 - 128	64	Specifies the subnet's prefix length.
mac	x		-	-	Specifies the system's mac address.
mtu	x	x	576 bytes - 1500 bytes	0 (use default value)	Specifies the Maximum Transmission Unit.
netmask	x	x	-	-	Specifies the network mask.
ntp	x	x	-	-	Specifies the address of the NTP server.
ntp → enable	x		true/false	false	Specifies if the should contact the given NTP server or not
telnet-port	x		-	10000	Specifies the port number for telnet connections.
timezone	x	x	Europe, USA & Canada, Non-geographic, other	CET	Specifies the time zone in Posix time zone string format.
vlan	x	x	1 - 4095	-1	Specifies the VLAN to which the device belongs.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
provisioning	check → check_sync	x	x	disabled/update/reboot	disabled	Specifies how the Spectralink IP-DECT Server or DECT Server will react to SIP NOTIFY check-sync events. disabled - do not react. reboot - reboot and check for updates update - check for updates and reboot if necessary.
	check → interval	x	x	minutes	0	Specifies a checking interval for updates.
	check → time	x	x	hh:mm	-	Specifies a certain checking time for each day. The format is HH:MM.
	config → check	x	x	true/false	true	Specifies if the Spectralink IP-DECT Server or DECT Server will try to download and import configurations from the provisioning server.
	cota → check		x	true/false	false	Specifies if the IP-DECT server will try to download the handset configuration files
	firmware → kws	x	x	file name	-	Specifies the name of the firmware image to use for a Spectralink IP-DECT Server or DECT Server. The Spectralink IP-DECT Server or DECT Server checks for a version file and a binary file. They must be located as /.bin.ver and /.bin
	firmware → default_kws		x	true/false	false	Specifies whether to use Wireless Server firmware as default for all Base Stations and Media Resources.
	firmware → rfp	x		file name	-	Specifies the name of the firmware image to use for Spectralink IP-Base stations. The Spectralink IP-DECT Server or DECT Server checks for a version file and a binary file. They must be located as /.bin.ver and /.bin
	firmware → rfp6	x		file name	-	Specifies the name of the firmware image to use for Spectralink RFP6 Digital-Base stations. The Spectralink IP-DECT Server or DECT Server checks for a version file and a binary file. They must be located as /.bin.ver and /.bin

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
	firmware → pp14208700	x	x	file name	-	Specifies the name of the firmware image to use for Spectralink Butterfly handsets. The Spectralink IP-DECT Server or DECT Server checks for a version file and a binary file. They must be located as /.bin.ver and /.bin
	firmware → pp14225100	x	x	file name	-	Specifies the name of the firmware image to use for Spectralink 75x2, 76x2 and 77x2 series handsets. The Spectralink IP-DECT Server or DECT Server checks for a version file and a binary file. They must be located as /.bin.ver and /.bin
	firmware → pp14225110	x	x	file name	-	Specifies the name of the firmware image to use for Spectralink 72x2 series handsets. The Spectralink IP-DECT Server or DECT Server checks for a version file and a binary file. They must be located as /.bin.ver and /.bin
	firmware → pp14225190	x	x	file name	-	Specifies the name of the firmware image to use for Spectralink OEM handsets. The Spectralink IP-DECT Server or DECT Server checks for a version file and a binary file. They must be located as /.bin.ver and /.bin
	server → method	x	x	dhcp/static/disabled	dhcp	Specifies how can the Spectralink IP-DECT Server or DECT Server obtain the provisioning server address.
	server → url	x	x	-	-	Specifies the static provisioning server URL.
	users → check	x	x	true/false	false	Specifies if the Spectralink IP-DECT Server or DECT Server will try to download and import users from the provisioning server.
RS232	shelf → card0 → port1 → conf	x		Baud rate: 100, 150, 200, 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400 Data bits: 7, 8 Stop bits: 1, 2 Parity: None, Odd, Even, Mark, Space	115200,8,1,N	Specifies the Baud rate, Data bits, Stop bits and parity of a serial connection.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
	shelf → card0 → port1 → flow	x		None CTS & RTS XON & XOFF	CTS/RTS	Specifies the Flow control of a serial connection.
	shelf → card0 → port1 → modeminit	x		ON/OFF	ON	Specifies if a connected modem should be initialized.
	shelf → card0 → port1 → msgprotocol	x		Standard EMD, Old KWS1500 MSF, TAP 1.8	Standard EMD	Specifies the messaging protocol to use.
	shelf1 → card0 → port1 → useoldmsfreleasecodes	x		false/true	true	If OldKWS1500 is set a msgprotocol then some newer release codes can be converted to codes used in KWS1500
rfp	default_sync_type	x	x	free running, radio, lan	radio	Specifies the synchronisation type used for the DECT radio.
	media → port		x	-	57000	Specifies the start port for media.
	multicast → address	x	x	-	-	Specifies the multicast address for RFP signalling.
	auto → enable	x	x	true/false	false	Specifies if automatic update is enabled or disabled. Only applies to IP base stations.
	auto → start_time	x	x	immediately, hh:mm	immediately	Specifies when to perform the update, immediately or at a specific time within 24h. Only applies to IP base stations.
	auto → force	x	x	true/false	false	Specifies if an automatic update should be executed immediately or wait until devices are idle. Only applies to RFP6 base stations.
	auto → enable_digital	x		true/false	false	Specifies if automatic update is enabled or disabled. Only applies to RFP6 base stations.
	auto → source_digital	x		builtin/loaded	builtin	Specifies the firmware source to be used in update. builtin: Built-in in server firmware. loaded: Upload by user or via provisioning server.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
	auto → start_time_digital	x		immediately, hh:mm	immediately	Specifies when to perform the update, immediately or at a specific time within 24h. Only applies to RFP6 base stations.
	auto → force_digital	x		true/false	false	Specifies if an automatic update should be executed immediately or wait until devices are idle. Only applies to IP base stations.
	paging_method		x	0-3 Paging method: 0: Default paging method. 1: Multicast paging method. 2: Site based paging method. 3: Zone based paging method.	0	Specifies the paging method to use to handle incoming calls. Basically, it's about how to page a handset. "Default" sends paging to all base stations individually. "Multicast" sends paging to all base stations at once. "Site based" Sends paging to all base stations on a specific site. "Zone based" Sends paging to all base stations in specific zone, within a specific site. Since changing this setting can affect all calls please read the installation and configuration guide carefully before changing this setting.
	multicast → ttl	x	x	1-255	1	Specifies the TTL for RFP multicast.
*	ptp → cos	x	x	0-7	-1	Specifies LAN sync class of service.
*	ptp → tos	x	x	0-255	184	Specifies LAN sync type of service.
*	ptp → transport	x	x	l2/ipv4/ipv6	ipv4	Specifies the procotol transport layer used by PTP for LAN sync.
	allow_gui		x	true/false	true	Controls if the web-GUI is accessible or not.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
security	allow_new_media_resource	x	x	true/false	true	Controls whether new media resources are allowed to connect to the Spectralink IP-DECT/DECT Server. Any media resource which is known by the Spectralink IP-DECT Server or DECT Server i.e. has been connected before, is allowed to connect regardless of this setting; however new (unknown) media resources will not be allowed if this setting is false.
	allow_gui		x	true/false	true	Controls if the web-GUI is accessible or not
	allow_new_rfp	x	x	true/false	true	Controls whether new base stations are allowed to connect to the Spectralink IP-DECT/DECT Server. Any base stations which is known by the Spectralink IP-DECT Server or DECT Server i.e. has been connected before, is allowed to connect regardless of this setting; however new (unknown) base stations will not be allowed if this setting is false.
	allow_new_rfp_as_active		x	true/false	false	New base stations will become active when added. Otherwise they will have to be manually activated
	allow_new_media_resource_as_active		x	true/false	false	New media resources will become active when added. Otherwise they will have to be manually activated
	rfp_encryption		x	true/false	false	Require an encrypted connection with the base stations. Note: Not compatible with previous generation base stations.
	legacy_tls		x	true/false	false	Enabled legacy TLS versions 1.0 and 1.1 and SHA1 certificate signing support
	media_resource_encryption		x	true/false	false	Require an encrypted connection with the media resource. Note: Not compatible with previous generation media resources.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
	passwords_unexportable		x	true/false	false	Remove user passwords from exported files. Note: This will prevent full systems backups. Note: This setting can only be reset by a factory reset, removing all configuration and user data
	allow_http		x	true/false	false	Specifies if unencrypted HTTP request to the web GUI are allowed.
	password		x	-	admin	Password for the user who logs on to the web GUI.
	password_lifetime		x	0(forever), 30, 90 days	0	Specifies how many days the web GUI password is valid. Note: Can only be reset by a factory reset.
	strict_password		x	true/false	false	Specifies Controls if strict password quality rules are enabled. Note: Can only be disabled by a factory reset.
	username		x	-	admin	User name of the user who logs on to the web GUI.
*	srtp_rfp	x	x	true/false	false	If enabled, it enforces the use of secure RTP for base station audio connections. If internal SRTP is enabled, the number of available voice channels on each base station is reduced from 12 to 6
*redundancy	mode		x	master/slave/single	single	Specifies the mode of the node: either a normal single node system, a master or a slave node in a redundant system.
*	peer		x	-	-	Specifies the hostname or IP address of the redundancy peer node.
*	Peer→factoryid		x	String that consists of 16 hexadecimal numbers.	Empty	When the server is in redundant mode, this will contain the P-ID of the peer.
*	failovertime		x	sec	15 (8000) 10 (6500)	The time in seconds from a redundancy node, detects a failure until it initiates a failover operation.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
*	database_uuid		x	-	-	Represents the unique ID of the distributed database of the system which must match for replication to be performed. When reset on the master it is automatically generated and when reset on the slave, it is retrieved from the master. It must be reset when changing a master node to a slave node or when moving a slave node to another system.
*suota	load	x	x	medium, low, high	medium	Specifies the system load due to software update, i.e. the number of simultaneous uploads. IP-DECT 6500/400: Low: 1 handset at a time. Medium: 4 handsets per Media resource. High: 16 handsets per media resource. Example: 2 Media resources and High load gives 2*16 = 32 simultaneous updates. DECT 8000/2500: Low: 70% of total number of Base stations. Medium: 100% of total number of Base stations. High: 130% of total number of Base stations. Example: 10 base stations and Low load(70%) gives 7 simultaneous updates. Note: Only half of media resource capacity (32 channels/2 = 16 channels) can be used for SUOTA.
	start_time	x	x	immediately, hh:mm	immediately	Specifies when to perform the update, immediately or at a specific time within 24h.
	pcs_ignore	x	x	true/false	false	Specifies whether same or older software versions can be uploaded or only newer versions.
	incharger	x	x	true/false	false	Specifies if only handsets in a charger should be updated.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
	auto	x	x	true/false	false	Specifies if automatic update is enabled or disabled.
sip	allow_internal_routing		x	true/false	false	Specifies if internal routing should be used if connection cannot be established for any proxies.
	auth → password	x	x	-	-	Specifies the default password for the handset authentication (if no specific handset authentication password is specified).
	auth → realm	x	x	-	-	Realm used for SIP authentication. The realm is presented by the SIP server and is used for encrypting the SIP user password.
	auth → username	x	x	-	-	Specifies the default user name for the handset authentication (if no specific handset authentication user name is specified).
	blacklist_timeout	x	x	sec (5-600)	30	Specifies the blacklist timeout for SIP server blacklisting. (Used for redundant SIP server setups when loosing connection to a SIP proxy.)
	callwaiting	x	x	true/false	true	Used to control whether Call Waiting is enabled.
	client_transaction_timeout	x	x	Msec (1000 -32000)	16000	Specifies the timeout for client transactions. This controls timer B and F as specified in RFC3261.
	dect_detach_action	x	x	ignore/deregister	ignore	Specifies an action to perform when a handset is turned off.
	defaultdomain	x	x	-	example.com	Specifies the default domain for the handset (if no specific handset domain is mentioned).
	dnsmethod	x	x	arecord/dnssrv	arecord	Specifies the DNS method used to resolve host names for SIP requests.
	dtmf → duration	x	x	msec	270	Specifies the time length of the DTMF tones.
	dtmf → info	x	x	true/false	false	Specifies if the keypad signalling should be sent as SIP INFO.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
	dtmf → rtp	x	x	true/false	true	Specifies if the keypad signalling should be sent as RTP packets with DTMF code.
	dtmf → rtp_payload_type	x	x	refer to RFC2833	96	Specifies the payload type for RFC2833 in SDP offers.
	gruu	x	x	true/false	true	Specifies the use of Globally Routable UA URI (GRUU) which is an URI that routes to a specific UA instance. If enabled, a GRUU will be obtained from a server and communicated to a peer within a SIP dialog.
	hold_before_refer		x	true/false	true	Put all calls on hold before sending a REFER
	convert_sip_uri_to_phone		x	true/false	true	When enabled, the IP-DECT server will convert the callers SIP URI received from the PBX to a phone number, e.g. “SIP:1234@example.com” to “1234”. The phone number is then displayed in a DECT handset as the caller ID instead of the SIP URI. This makes the Call back functionality unusable for users on a different domain.
	localport	x	x	-	5060	Specifies the SIP port.
	maxforwards	x	x	-	70	Specifies the maximum number of times the SIP messages can be forwarded.
	media → codecs	x	x	0 = none 1 = G711U 2 = G711A 64 = G726_32 1024 = G729A (6500)	64,1,2,0,0,0	Specifies the codec priority.
*	media → default_relay	x	x	true/false	false	Specifies if the default address for TURN server should be used.
	media → ice → enable	x	x	true/false	false	Enable ICE support.
	media → port	x	x	-	58000	Specifies the start port for media.
	media → ptime	x	x	msec	20	Specifies the packet duration for media (ms).
*	media → rfc3489	x	x	true/false	true	Specifies if STUN is enabled or disabled.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
	media → sdp_answer_single	x	x	true/false	false	Specifies if the media handling must provide only a single CODEC in SDP answers.
	media → sdp_answer_with_preferred	x	x	true/false	false	Specifies if the media handling must ignore the remote SDP offer CODEC priorities. Note: Enabling this option, violates the RFC3264 SDP offer/answer model.
*	media → sdp_hold_attribute_sendonly	x	x	true/false	true	When putting a call on hold, the Spectralink IP-DECT Server or DECT Server sends sendonly. Configuring this setting as false, makes the Spectralink IP-DECT Server or DECT Server send inactive.
*	media → sdp_hold_null_connection	x	x	true/false	false	If this setting is true, the Spectralink IP-DECT Server or DECT Server will revert to the old way of signalling a hold.
	media → sdp_ignore_version	x	x	true/false	false	Specifies whether to ignore the version information in incoming SDP received from remote endpoints.
	media → tos	x	x	-	184 (0xb8)	Specifies the media's TOS/Diffserv.
	media → turn → enable	x	x	true/false	false	Enable TURN support.
	media → turn → password	x	x	-	-	Specifies the TURN server password. If left blank, the per-user authentication password will be used.
	media → turn → server	x	x	-	-	Specifies the TURN server address.
	media → turn → username	x	x	-	-	Specifies the TURN server user name. If left blank, the per-user authentication username will be used.
	media → vlan_cos	x	x	0 - 7	5	This setting controls the RTP 802.1p Class-of-Service Priority Code Point (PCP): A 3-bit field which refers to the IEEE 802.1p priority. It indicates the frame priority level. These values can be used to prioritize different classes of traffic (voice, video, data, etc.). The setting requires VLAN tagging to be enabled.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
*	media → srtp → enable	x	x	true/false	true	If enabled, external SRTP is supported and optional. It must be negotiated with the remote endpoint. If external SRTP is enabled the number of available voice channels on a Spectralink IP-DECT/DECT Server/media resource is reduced from 32 to 16, (if a codec card is used from 24 to 16).
*	media → srtp → required	x	x	true/false	false	If enabled, the usage of SRTP is required. If negotiation of SRTP with the other end is unsuccessful, call establishment is aborted).
*	media → srtp → lifetime	x	x	true/false	false	Handles the RFC 4568 SRTP lifetime key parameter in SDP offers.
*	media → srtp → mki	x	x	true/false	false	Handles the RFC 4568 SRTP Master Key Index Parameter in SDP offers.
	music_on_hold	x	x	true/false	false	Specifies if playing music on hold for the remote end is enabled or disabled.
	mwi → enable	x	x	true/false	true	Enables the MWI (Message Waiting Indicator).
	mwi → expire	x	x	sec	3600	Specifies the MWI subscription expiration time (s).
	mwi → subscribe	x	x	true/false	false	Enables MWI subscription.
	nat_keepalive		x	0 - 2	1	Specifies the type of NAT keepalive method. 0 = Disabled, 1 = CRLF, 2 = SIP OPTIONS
	nat_keepalive_interval		x	10, 20, 30	30	Specifies the NAT keepalive send interval in seconds.
	onholdtone	x	x	true/false	true	Specifies if the handset should hear the on-hold tone when put on-hold.
	pound_dials_overlap	x	x	true/false	false	Specifies if '#' should end overlap dialling.
	proxy → domain	x	x	-	-	Specifies the SIP Proxy address.
	proxy → domain2	x	x	-	-	-
	proxy → domain3	x	x	-	-	-
	proxy → domain4	x	x	-	-	-

Configuration parameter	Dect	IP-Dect	Options	Default	Description
proxy → port	x	x	-	0	Specifies the SIP Proxy port.
proxy → port2	x	x	-	0	-
proxy → port3	x	x	-	0	-
proxy → port4	x	x	-	0	-
proxy → priority	x	x	-	1	Specifies the priority for using a SIP proxy. Proxies with lowest priority will be preferred and higher priorities will be used for failover.
proxy → priority2	x	x	-	2	-
proxy → priority3	x	x	-	3	-
proxy → priority4	x	x	-	4	-
proxy → weight	x	x	-	100	Specifies the weight for using a proxy. If more proxies have the same priority the Spectralink IP-DECT Server or DECT Server will do load balancing using the weight to determine how much each proxy will be loaded.
proxy → weight2	x	x	-	100	-
proxy → weight3	x	x	-	100	-
proxy → weight4	x	x	-	100	-
registration_expire	x	x	sec	3600	Specifies the number of seconds before a SIP registration is renewed.
registration_max_pending		x	1-100	1	Specifies the maximum number of pending users attempting to register a SIP server.
send_to_current_registrar	x	x	true/false	false	Specifies if the system should send all the messages to the current registrar.
separate_endpoint_ports	x	x	true/false	false	Specifies if the endpoints should register on separate ports.
showstatustext	x	x	true/false	true	Shows the information for the call status in the handset display (ring, hold etc).

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
	tcp_contact_ephemeral_port	x	x	true/false	false	Enable this to add the TCP ephemeral port (the local TCP port of the outgoing connection) to the contact header used in outgoing SIP messages. Otherwise the local listening port is used.
	tls_allow_insecure	x	x	true/false	false	By default, UDP and TCP transports are disabled when TLS transport is the default. If this setting is true, UDP and TCP are allowed as fall back if TLS fails.
	tos	x	x	-	96 (0x60)	Specifies the SIP TOS/Diffserv.
	transport	x	x	udp/tcp/tls	udp	Specifies the transport mechanism used for SIP requests.
	use_sips_uri	x	x	true/false	true	Normally, SIP communication on a TLS connection is using the SIPS: URI scheme. Disabling this option causes the Spectralink IP-DECT Server or DECT Server to use the SIP: URI scheme with a transport=tls parameter for TLS connections.
*	vlan_cos	x	x	0 - 7	3	This setting controls the signalling 802.1p Class-of-Service Priority Code Point (PCP): A 3-bit field which refers to the IEEE 802.1p priority. It indicates the frame priority level. These values can be used to prioritize different classes of traffic (voice, video, data, etc.). The setting requires VLAN tagging to be enabled.
*	lync → enabled	x	x	true/false	false	Enable Microsoft Lync SIP mode.
*	lync → trusted	x	x	true/false	false	Enable Microsoft Lync trusted server for authenticating users.
snmp	enable		x	true/false	false	This enables SNMP and when enabled the device will respond to SNMP requests.
	community		x	-	public	The community string used for SNMP. The device will respond to requests for this community.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
	syscontact		x	-	-	The textual identification of the contact person for this host, together with information about how to contact them.
	syslocation		x	-	-	A descriptive text telling the physical location of the device.
	trapcommunity		x	-	-	The community used for sending traps.
	traphost		x	-	-	The host to which SNMP traps are sent.
system_event	auth_call (same as: dect → auth_call on 400/6500)	x		0x01 = Terminate Access Rights on Authentication error 0x02 = Create Authentication key at subscription 0x04 = Check Authentication when location registration is made 0x08 = Check Authentication on incoming voice calls 0x10 = Check Authentication on outgoing voice calls	0x07	Specifies if DECT authentication should be used when establishing calls.
	acustic_feedback_on_release	x		0,1,2 (acustic feedback, acustic feedback 3 sec timer, automatic release	0	Specifies if acoustic feedback should be sent to handsets.
	encrypt_voice_data (same as: dect → encrypt_voice_data 400/6500)	x		0 – DECT encryption is disabled. 1– DECT encryption is enabled. 2– DECT encryption is enforced and calls are terminated if the handsets do not support encryption.	0	Specifies if DECT encryption should be used for voice calls.
	internal_clip_presentation_ab	x		true/false	true	Only in analogue systems with analogue interface cards. If voice call is between internal DECT handsets, the local clip and presentation text is shown, in spite of external clip.

Configuration parameter	Dect	IP-Dect	Options	Default	Description
internal_switching_permits	x		bit 0: Allow internal switching between DECT-2-DECT and all types bit 1: Also when internal setup is used bit 2: Not used bit 3: When interface fails, Not implemented bit 4: Not used bit 5: Internal witching when possible bit 6 & 7: not used	0	Allow different user types (Analogue-, SIPand DECT to DECT users) to call each other without involving the (i)PBX, the Spectralink IP-DECT Server or DECT Server will switch the calls internally. Please notice, whenever a 'DECT to DECT' handset is involved in a call, transferrer/hold is not possible.
min_ringing_time	x		msec * 10 (units of 10ms) Minimum 40 (equal to 400 ms) Maximum 120 (equal to 1200 ms)	50	Only relevant when system_event.ringing_ mode=”E” and especially handsets newer than 40xx series. Insures the minimum hear able ringing time in the handset (Tip: If hear able ring time in handset is to short, then use ring tone 6 (Spectralink KIRK handsets).
msf_between_pp (same as: application → internal_messaging 400/6500)	x		true/false	false	Used to control if messaging between handsets is handled internally or by an external application. If enabled, messages will be handled internally.
outgoing_line_prefix	x		-	00	Only use full with Analogue users. The cipher(s) you need to get to the PSTN side of the PBX. Typically, prefixes are 0 or 9 but can contain up to 4 characters.
ringing_mode	x		0 = system 1 = exchange (pbx)	1	Choose if handset ringing shall follow PBX ringing cadence or internal handset ringing cadence.
send_date_time (same as: dect → send_date_time 400/6500)	x		true/false	true	Specifies if the date and time will be sent to the handsets.
sio_passwd	x		-	-	Password for the RS232 interface when used as EMD interface.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
	subscription_allowed (same as: dect → subscription_allowed 400/6500)	x		0, disallow. 2, allow . 3, wildcard (automatically create a subscribed user).	2	Specifies if handset subscription is allowed or allowed to add a new user when a DECT handset tries to subscribe to the system.
	system_access_code (same as: dect → accesscode 400/6500)	x		-	-	Specifies a system wide access code required to subscribe handsets to the system. The system wide access code can be overruled on a per user basis in the user settings.
TAP	shelf1 → card0 → port1 → CBNStart	x		Position, Start letter, First cipher	First cipher	Specifies the method used to find a call back number in a pager text. **First Cipher** in text is (start of) Call Back number: DECT Server will look though the text until it finds the first cipher and then extract the number. **Position in text:** DECT Server will look on position in text and if a number exist on that position, then it will extract the number. **Start letter** (just before the Call Back Number): DECT Server will though the text for a specific letter and if finds it, then it will look on the next position and extract a phone number if there is one.
	shelf1 → card0 → port1 → CBNprefix	x		-	-	Specifies the number to add in front a call back number.
	shelf1 → card0 → port1 → CBNsegmentReplaceStr	x		-	s	Specifies letters to be used as an extra cipher or a pause is needed as a replacement between the two parts of a call back number.
	shelf1 → card0 → port1 → CBNsegmentStr	x		-	E	Specifies letters to remove between two parts of a call back number. If Fist cipher in text is Call Back number, then this setting can be used to do some extra decoding so “Alarm 712E:5 Normal” result in number 7125 instead of just 712. If the letter(s) is followed by a ‘:’ then this will also be removed from number.
	shelf1 → card0 → port1 → DNorName	x		-	D	Not used.

Configuration parameter	Dect	IP-Dect	Options	Default	Description
shelf1 → card0 → port1 → EOL	x		0 = auto, 1 = CR 2 = LF 3 = CR/LF 4 = LF/CR	1	Specifies what end of line character to use.
shelf1 → card0 → port1 → ExtractCBN	x		true/false	true	Specifies if DECT Server should look into the text of TAP message for a phone number.
shelf1 → card0 → port1 → IgnoreCheckSum	x		0/1	0	Specifies it the checksum should be used for validation or not. Can be used for debugging.
shelf1 → card0 → port1 → LogMethod	x		0 = no online log, 1 = Send trace events (EMD & WEB), 2 = RS232 log printer, 3 = Send trace events & to log printer,	1	Specifies the method to use to log events.
shelf1 → card0 → port1 → LongMessage	x		-	-	Not used.
shelf1 → card0 → port1 → MaxSessionPerLogin	x		-	-	Not used.
shelf1 → card0 → port1 → MaxtimePerLogin	x		-	-	Not used.
shelf1 → card0 → port1 → N1	x		-	-	Not used.
shelf1 → card0 → port1 → N2	x		-	-	Not used.
shelf1 → card0 → port1 → N3	x		-	-	Not used.
shelf1 → card0 → port1 → NCReleaseCmd	x		-	*9	Specifies a Nurse care line release command. Some Nurse care systems require a special release sequence to end a voice call.
shelf1 → card0 → port1 → NoLogin	x		true/false	false	Specifies if the login procedure should be used. If enabled the DECT Server will require a response to “ID=” The expected text is “PG1” but can be changed with the SSTstring parameter.

Configuration parameter	Dect	IP-Dect	Options	Default	Description
shelf1 → card0 → port1 → PositionLetter	x		-	0	Specifies where to find a call back number in a pager text. **Position:** a number indicating the position. **Start letter:** An ASCII value of the start letter ex. 87 for 'W'.
shelf1 → card0 → port1 → RemoveCBNFromText	x		true/false	false	Specifies if a DECT Server shall remove the found phone number from the text before sending the Text to handset.
shelf1 → card0 → port1 → ResponseCodes	x		true/false	true	Specifies whether response codes should be used or not.
shelf1 → card0 → port1 → SMS_AlertPattern	x		0 = Not present, 1 = continuous tone, 2 = internal ringing in pp 3 = external ringing in pp, 4 = alarm in time defined by AlertTimeout	3	Specifies the type of alert pattern to use. This is handset specific.
shelf1 → card0 → port1 → SMS_AlertTmeout	x		0 – 127.5 sec	0	Specifies the timeout of alert.
shelf1 → card0 → port1 → SMS_AlertTone	x		0 = alerting off, 1..9 = tone 1..9, 10 = use tone chosen in pp	10	Specifies the alert tone to use. This is handset specific.
shelf1 → card0 → port1 → SMS_AlertVolume	x		0 - 9	3	Specifies the alert tone volume.
shelf1 → card0 → port1 → SMS_DispTimeout	x		0 – 127.5 sec	0	Specifies the Display timeout.
shelf1 → card0 → port1 → SMS_IconNo	x		0x00 - 0xFF	0	Specifies an icon to be displayed on a handset when receiving a message.

Configuration parameter	Dect	IP-Dect	Options	Default	Description
shelf1 → card0 → port1 → SMS_LedCtrl	x		0x00 None 0x01 Red 0x02 Green 0x04 Blue 0x03 Red, Green 0x05 Red, Blue 0x06 Green, Blue 0x07 Red, Green, Blue 0x08 Slow flashing 0x10 Fast flashing 0x18 Switch slow 0x20 Switch fast	0	Specifies the behaviour of an LED in a handset when receiving a message.
shelf1 → card0 → port1 → SMS_PriColour	x		0x00 Handset's default setting and no priority 0x01 Black text on white background 0x02 Black text on red background 0x03 Black text on yellow background 0x04 Black text on blue background 0x05 Black text on grey background 0x06 Black text on green background 0x07 White text on black background 0x08 White text on red background 0x09 White text on yellow background 0x0A White text on blue background 0x0B White text on grey background 0x0C White text on green background 0x10..0xF0 priority level 1..15	0	Specifies priority level of a message and the background and text colour displayed in a handset.

Configuration parameter	Dect	IP-Dect	Options	Default	Description
shelf1 → card0 → port1 → SMS_ResponseEnabler	x		-	0	Specifies if actions 0x81 to 0x87 are enabled or disabled. **0x01**: use of soft key “unable” will delete the task. **0x02**: accept by soft key (0x81). **0x04**: accept by hook key (0x82). **0x08**: unable by soft key(0x83). **0x10**: started on task(0x84). **0x20**: Nearly completed(0x85). **0x40**: Done(0x86). **0x80**: task can always be deleted.
shelf1 → card0 → port1 → SMS_SetupSpec1	x		-	39(0x27)	Specifies SMS setup specifications. SIS(0x01) – Save in stack. LV(0x02) – Use Local Alert Volume. AV(0x04) – Always Vibrate. IC(0x08) – Ignore SMS if PP in Charger. IIVC(0x010) – Ignore SMS if PP in Voice Call. SIC(0x020) – Silent if PP in Charger
shelf1 → card0 → port1 → SMS_action	x		-	0	Specifies how a DECT server shall handle a received TAP message.
shelf1 → card0 → port1 → SSTstring	x		-	PG1	Specifies a user name in a login procedure.
shelf1 → card0 → port1 → SmsMsf	x		DECT MSF = 0 DECT SMS (MSF III) = 1	0	Specifies if DECT MSF or DECT MSF III is used for messaging. Either DECT MSF or DECT SMS (MSF Format III) will end up as messages in handset. Supported on 74, 75, 76, 77 series handsets. DECT SMS will end up as task list in handset; supported on 7620, 7640, 7720 & 7740 handsets.
shelf1 → card0 → port1 → T1	x		-	2	Not used.
shelf1 → card0 → port1 → T2	x		-	1	Not used.
shelf1 → card0 → port1 → T3	x		-	10	Not used.
shelf1 → card0 → port1 → T4	x		-	4	Not used.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
	shelf1 → card0 → port1 → T5	x		-	8	Not used.
	shelf1 → card0 → port1 → TrailingDigitsLen	x		-	0	Specifies the number of trailing in/after pager ID number.
trace_event	level	x		0 – Disabled 1-Subscription requests are shown. 2 - Level 1 plus exceptional cases, startup and user maintenance (i.e. everything but normal operation). 3 -Level 2 plus call trace messages. 4 -Level 3 plus SIP signalling. 5 -All Trace messages + debug messages.	5	Trace message level
*tx_power	handset	x		1, 1.6, 2.5, 4, 6.3, 10, 16, 25, 40, 63, 100, 158, 250 (mW)	250	Specifies the output power of a base.
*	rfp	x		1, 1.6, 2.5, 4, 6.3, 10, 16, 25, 40, 63, 100, 158, 250 (mW)	250	Specifies the output power of a base.
threshold	basestation → calls		x	0 - 4294967295	250	Threshold of total calls from which the warning is calculated.
	basestation → dropcallrate		x	0 – 100%	1%	Threshold in percent of dropped calls rate from which the warning is calculated.
	basestation → droppedcalls		x	0 - 4294967295	50	Threshold of dropped calls from which the warning is calculated.
	basestation → handovercancelled		x	0 - 4294967295	50	Threshold of handover cancelled from which the warning is calculated.
	basestation → handoverrate		x	0 – 100%	20%	Threshold in percent of handover cancel rate from which the warning is calculated.
	basestation → handovertotal		x	0 - 4294967295	100	Threshold of handover total from which the warning is calculated.
	handset → calls		x	0 - 4294967295	100	Threshold of total calls from which the warning is calculated.

Configuration parameter	Dect	IP-Dect	Options	Default	Description
handset → dropcallrate		x	0 – 100%	1%	Threshold in percent of dropped calls rate from which the warning is calculated.
handset → droppedcalls		x	0 - 4294967295	10	Threshold of dropped calls from which the warning is calculated.
handset → handovercancelled		x	0 - 4294967295	10	Threshold of handover cancelled from which the warning is calculated.
handset → handoverrate		x	0 – 100%	20%	Threshold in percent of handover cancel rate from which the warning is calculated.
handset → handovertotal		x	0 - 4294967295	30	Threshold of handover total from which the warning is calculated.
site → calls		x	0 - 4294967295	300	Threshold of total calls from which the warning is calculated.
site → dropcallrate		x	0 – 100%	1%	Threshold in percent of dropped calls rate from which the warning is calculated.
site → droppedcalls		x	0 - 4294967295	30	Threshold of dropped calls from which the warning is calculated.
site → handovercancelled		x	0 - 4294967295	30	Threshold of handover cancelled from which the warning is calculated.
site → handoverrate		x	0 – 100%	20%	Threshold in percent of handover cancel rate from which the warning is calculated.
site → handovertotal		x	0 - 4294967295	100	Threshold of handover total from which the warning is calculated.
system → calls		x	0 - 4294967295	500	Threshold of total calls from which the warning is calculated.
system → dropcallrate		x	0 – 100%	1%	Threshold in percent of dropped calls rate from which the warning is calculated.
system → droppedcalls		x	0 - 4294967295	50	Threshold of dropped calls from which the warning is calculated.
system → handovercancelled		x	0 - 4294967295	50	Threshold of handover cancelled from which the warning is calculated.
system → handoverrate		x	0 – 100%	20%	Threshold in percent of handover cancel rate from which the warning is calculated.

	Configuration parameter	Dect	IP-Dect	Options	Default	Description
	system → handovertotal		x	0 - 4294967295	100	Threshold of handover total from which the warning is calculated.
	user → calls		x	0 - 4294967295	100	Threshold of total calls from which the warning is calculated.
	user → dropcallrate		x	0 – 100%	1%	Threshold in percent of dropped calls rate from which the warning is calculated.
	user → droppedcalls		x	0 - 4294967295	10	Threshold of dropped calls from which the warning is calculated.
	user → handovercancelled		x	0 - 4294967295	10	Threshold of handover cancelled from which the warning is calculated.
	user → handoverrate		x	0 – 100%	20%	Threshold in percent of handover cancel rate from which the warning is calculated.
	user → handovertotal		x	0 - 4294967295	30	Threshold of handover total from which the warning is calculated.
	zone → calls		x	0 - 4294967295	200	Threshold of total calls from which the warning is calculated.
	zone → dropcallrate		x	0 – 100%	1%	Threshold in percent of dropped calls rate from which the warning is calculated.
	zone → droppedcalls		x	0 - 4294967295	20	Threshold of dropped calls from which the warning is calculated.
	zone → handovercancelled		x	0 - 4294967295	20	Threshold of handover cancelled from which the warning is calculated.
	zone → handoverrate		x	0 – 100%	20%	Threshold in percent of handover cancel rate from which the warning is calculated.
	zone → handovertotal		x	0 - 4294967295	70	Threshold of handover total from which the warning is calculated.
upnp	enable	x	x	true/false	true	Specifies if UPnP support is enabled. If enabled the device will respond to UPnP broadcasts.
	broadcast	x	x	true/false	false	Specifies if UPnP announcements are broadcasted. If enabled the device will periodically broadcast announcements.

Configuration parameter	Dect	IP-Dect	Options	Default	Description
name	x	x	-	-	Specifies the friendly name for UPnP.

Appendix E: Acoustic Echo in Telephone System

Sometimes, when you speak in a telephone, you can hear your own voice coming back to you through the earpiece or the loudspeaker, sometimes with significant delay. If the delay exceeds app. 25 ms. it becomes audible to the speaker. The echo comes from the far-end microphone which picks up sound directly from a loudspeaker or sound reflected from walls, tables or something else in the room, where the microphone is and returned on the telephone line. Depending on the delay time and the volume of the echo, the problem can range from no problem to unbearable. There are different solutions to this problem. Just to mention 2 of the solutions, there are soft talk shift function and echo cancellation.

Handling Acoustic Echo

Acoustic echo can be handled in the following ways:

- Soft talk shift function

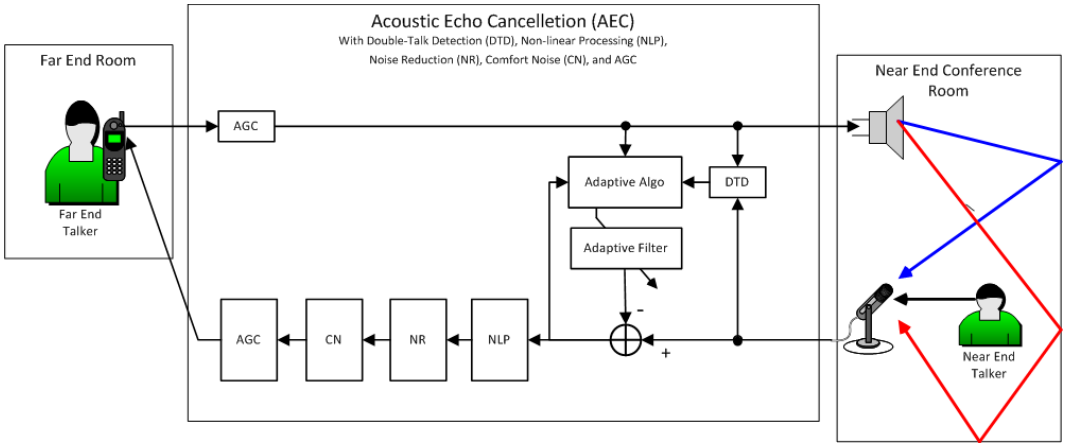
  Soft talk shift function is a simple way to handle acoustic echo. In soft talk shift function, the power of the receive signal and the power of the transmit signal is continuously measured, and the soft talk shift function decides either to open for the transmit signal and close for the receive signal, or to close for the transmit signal and open for the receive signal. The power level which causes switching can be adjusted. This system works, if you are in a quiet environment and the parties are not talking at the same time (No double talk). If you are in noisy environment, the continuous noise on the microphone will close for the received signal and the same will happen if there is double talk on the line.

  The bad behavior of the soft talk shift function is audible in your end of the connection.

- Echo cancellation

  The echo canceller is a much more complex functionality than soft talk shift function. The echo canceller works using the principle of spectral subtraction which means, that it converts both the received signal and the signal from the microphone into 12 different frequency bands, subtracts the rescaled received signals from the microphone signals to make 12 different frequency band signals, and then converts them back to 1 signal again to transmit out on the telephone line. The loudspeaker is not switched off at any time during conversation which means, that all what is received from the line is send to the loudspeaker.

  The result of using echo cancellation in the near end of the connection is audible in the far end of the connection.



Spectralink DECT Handset Handling of Acoustic Echo

Under the Settings Menu in the Spectralink DECT Handset, under Advanced> Echo canceller, you can define the echo canceller to be either off or on.

Note:

Only Spectralink DECT Handset 7202/7212, 7502, 7522/7532, 7622/7642 and 7722/7742 with firmware PCS 19K_ or newer support echo cancelling.

For more information about entering the handset menu, see the Handset User Guides.

- Echo canceller setting off

With the echo canceller setting off in the handset, you can activate or deactivate noisy environment. If noisy environment is deactivated, the soft talk shift function is enabled, which can give some bad performance in noisy environment and by double talk.

If noisy environment setting is activated, the soft talk shift function is disabled, which means that the sound on the loudspeaker is stable in that end of the connection, but echo can be received in the other end of the connection.

- Echo canceller setting on

With the echo canceller setting on, you can make understandable telephone calls to and from noisy environments, and even double talk can be handled.

If echo cancellation is enabled, then Noisy environment setting is ignored on ear speaker and wired headset. When echo cancellation is enabled, there are 2 additional volume steps on the ear speaker. If turning speakerphone on, the echo canceller setting is ignored. When turning speakerphone off, the echo canceller setting becomes valid again.

Note:

Enabling echo cancellation does not prevent you from hearing echo, but helps preventing the person you are talking with, from hearing an echo.

How Settings Influence on Spectralink DECT Handset

Settings				
Echo cancellation:	Disabled		Enabled	
Noisy environment:	Disabled	Enabled	Disabled	Enabled
Handset functions:				
Ear speaker/earpiece	Standard Difficulties by talking in noisy environment	Noisy Talk with possible echo in noisy environment	Cancellation Talk with minimal echo in noisy environment	Cancellation Talk with minimal echo in noisy environment
Handfree speaker:	Standard Difficulties by talking in noisy environment	Standard Difficulties by talking in noisy environment	Standard Difficulties by talking in noisy environment	Standard Difficulties by talking in noisy environment
Wireless handset	Wireless	Wireless	Wireless	Wireless
Wired handset	Standard Difficulties by talking in noisy environment	Noisy Talk with possible echo in noisy environment	Cancellation Talk with minimal echo in noisy environment	Cancellation Talk with minimal echo in noisy environment

Standard: The legacy functionality that have been in Spectralink DECT Handset 7202/7212, 7502, 7522/7532, 7622/7642 and 7722/7742 for years, which includes a soft talk shift function, when using the higher volume steps. Volume steps 1–8.

Noisy: Disable the soft talk shift function, and therefore gives a higher risk of echo. Volume steps 1–8.

Cancellation: Echo Cancellation is active. Volume steps 1–10 for ear speaker. Volume steps 1–8 for wired headset.

Wireless: Soft talk shift function and echo cancellation disabled. Performance depends of the selected wireless headset. Volume steps 1–8.

HAC enabled: To be compliant with the HAC standard, volume range is limited to step 3 to 8 if HAC enabled.

Recommended Echo Canceller Settings

Default setting in the Spectralink DECT Handset 7202/7212, 7502, 7522/7532, 7622/7642 and 7722/7742 is echo canceller off and noisy environment off in firmware PCS 19K_. Keep this setting if good voice quality.

Echo cancellation is recommended on sites with 1 or more noisy locations. If you start to use echo cancellation on a site, then it is highly recommended that echo cancellation is enabled on all handset.

*****END OF DOCUMENT*****