Spectralink IP-DECT Server 200/400/6500

Installation and Configuration Guide

14215700-IG, Edition 8.0
April 2018, Original document

Contact Information

US Location	UK Location	Denmark Location
+ 1 800-775-5330	+44 (0) 20 3769 9800	+45 75602850
Spectralink Corporation 2560 55th Street Boulder, CO 80301 USA	Spectralink Europe UK 329 Bracknell, Doncastle Road Bracknell, Berkshire, RG12 8PE United Kingdom	Spectralink Europe ApS Bygholm Søpark 21 E Stuen 8700 Horsens Denmark
info@spectralink.com	infoemea@spectralink.com	infoemea@spectralink.com

Contents

14215700-IG, Edition 8.0
April 2018, Original document

About This Guide

This guide is intended for qualified technicians who will install, configure and maintain the Spectralink IP-DECT Server 200/400/6500 solution. To qualify to install the Spectralink IP-DECT Server 400/6500 solution, you must have successfully completed the Spectralink IP-DECT Server 400/6500 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 DECT Media Resource (only Spectralink IP-DECT Server 6500)
- Spectralink IP-DECT Base Station (only Spectralink IP-DECT Server 400/6500)
- 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 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 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 are needed and where to place them. The site survery should also determine how many RF channels are needed.

Related Documentation

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

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

Regulatory information is available online at http://support.spectralink.com/products.

Subject	Documentation
Spectralink DECT Handset	For more information about the handset, refer to the user guide available online at http://support.spectralink.com/products.
Site Survey Function in Handset	For more information about the site survey function in handset, refer to the guide available online at http://support.spectralink.com/products.
Synchronization and Deployment	For more information about synchronization and deployment, refer to the guide available online at http://support.spectralink.com/products.
Provisioning	For more information about provisioning, refer to the guide available online at http://support.spectralink.com/products.
Spectralink Technical Bulletins	Available online at http://support.spectralink.com/products.
Release Notes	Document that describes software changes, bug fixes, outstanding issues, and hardware compatibility considerations for new software releases. Available online at http://support.spectralink.com/products.
Spectralink DECT Training material	In order 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.

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
ARI	Access Rights Identity - Wireless identity of the Spectralink IP-DECT/DECT Server.
CLI	Command Line Interface
CUCM	Cisco Unified Communications Manager
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 dependant on the deployment made - and, therefore, the survey performed.
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
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.
GAP	Generic Access Profile
Handover	A process initiated by the handset in which the speech 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

Term	Definition
LAN	Local Area Network
LAN synchronization	Method for synchronizing IP 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
MTU	Maximum Translation Unit
MWI	Message Waiting Indication
Ni-MH	Nickel -Metal Hydride
NIC	Network Interface Card
NTP	Network Time Protocol
PBX	Private Branch eXchange
PCS	Product Change Status (Edition)
PoE	Power over Ethernet
PP	Portable Parts - wireless handset
PTP	Precision Time Protocol (IEEE-1588v2)
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.
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

Term	Definition
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
Speech channel	A speech channel is used to carry communication between the handset and the base station or repeater.
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 base stations over Air (radio)
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TTL	Time To Live
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
VoIP	Voice over Internet Protocol
WLAN	Wireless Local Area Network
WRFP	Wireless Radio Fixed Part - Wireless Repeater

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: 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 phones, Bluetooth, microwave ovens and widely used Wi-Fi equipment.

Spectralink IP-DECT Server Solution

Types of Servers

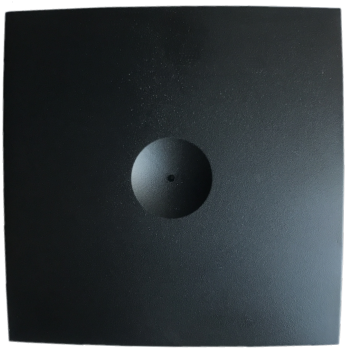
Following types of servers are available:

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

Note:

Besides the Spectralink IP-DECT Server 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 will be mentioned in "Spectralink Server Solution Overview and Comparison" on page 25.

Description - Spectralink IP-DECT Server 200



The Spectralink IP-DECT Server 200 is a single cell system (one built-in base station in the server) supporting SIP lines only.

The Spectralink IP-DECT Server 200 is designed with connector for External Antenna.

Up to 3 additional Spectralink DECT Repeaters can be added to the Spectralink IP-DECT Server 200.

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.

Description - Spectralink IP-DECT Server 400

The Spectralink IP-DECT Server 400 is in its basic edition 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 multicell functionality and to expand the covered area.

Note:

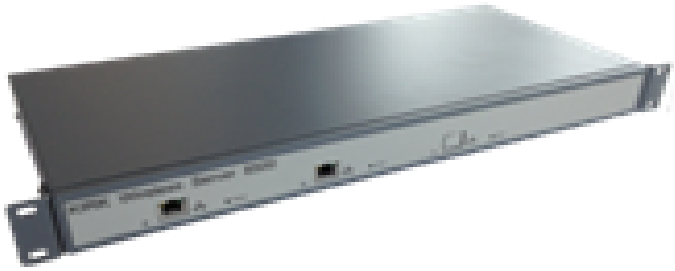
A license is required to enable the multicell function. For more information, see "Licenses for Spectralink IP-DECT Server 400/6500" on page 39.

All Spectralink IP-DECT Base Station models can be used. Up to 3 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 12 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.

Description - 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 an Spectralink IP-DECT Server 6500 with one Ethernet port and 32 on-board speech 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 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" on page 39.

Other Solution Components

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

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

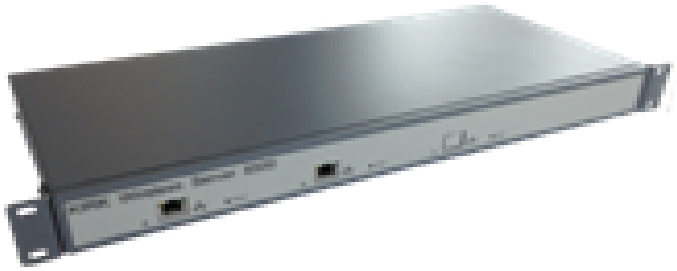
To handle the calls in the solution a call handler (IP-PBX SIP) is used.

Note:

For more information about system compatibility, see "Product Compatibility" on page 217.

For configuration overview, see "Total Configuration Overview" on page 26.

Description - Spectralink DECT Media Resource



The Spectralink DECT Media Resource is a print board that is placed within the same rack next to the Spectralink IP-DECT Server 6500 board. Up to 2 Spectralink DECT Media Resources can be placed in the same rack that houses the Spectralink IP-DECT Server 6500 board.

The Spectralink DECT Media Resource performs media conversion between the call handler and the Spectralink IP-DECT Server 6500 and is the media termination point for incoming and outgoing calls. Each Spectralink IP-DECT Server 6500 contains one built in media resource. The Spectralink IP-DECT Server 6500 can support a total of 32 Spectralink DECT Media Resources.

Each Spectralink 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. Depending on codec choice, the number of voice channels per Media Resource card can vary from 12 - 32.

G.726 allows for 32 duplex speech 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 speech channels on the Spectralink DECT Media Resource, lowering the number of speech 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. If using clusters, 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.

Description - Spectralink IP-DECT Base Station

The Spectralink IP-DECT Base Station is to be used with both Spectralink IP-DECT Server 400/6500 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 speech channels simultaneously.

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

Description - 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/DECT Base Stations/Spectralink IP-DECT Servers 200/400.

Note:

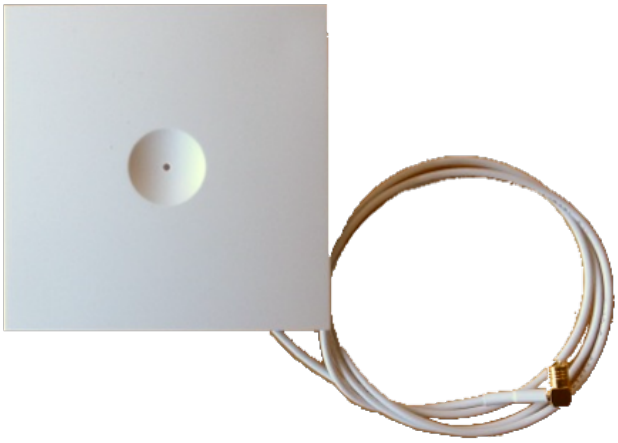
Both the Spectralink IP-DECT Server 200 and Spectralink IP-DECT Server 400 are Spectralink IP-DECT Servers with a built-in Spectralink IP-DECT Base Station.

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

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

Description - 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 the Spectralink IP-DECT Server 200/400 and Spectralink IP-DECT Base Station With External Antenna" on page 78.

For more information about using the repeater with external antenna, see "Using the Spectralink DECT Repeater With External Antenna" on page 76.

System Capacity Overview

Below you will find an overview of the system capacity of the Spectralink IP-DECT Server:

System Capacity - Servers

Description	IP-DECT Server 400	IP-DECT Server 6500
IP-DECT Servers	1	1
Media Resources	-	32
IP-DECT Base Stations	-	1024
Protocol supported	SIP	SIP
Max number of simultaneous SIP calls via license	12	1024 Up to 12 per Radio Base Station 32 per Media Resource
Codecs supported	G.711a, G.711u, G.726, G.729	G.711a, G.711u, G.726, G.729
Wireless DECT handsets	30	4096
Max number of base stations	3	1024
Repeaters per base station	3	3

System Capacity - Media Resources

Item	IP-DECT Server 6500 - Maximum Quantity
Media Resources	32
Protocol supported	SIP
Simultaneous calls	32 (depending on used codec)*
Codecs supported	G.711a, G.711u, G.726, G.729

* The available number of channels on a 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%.

Spectralink Server Solution Overview and Comparison

Product Overview

KWS (KIRK Wireless Server): IP-DECT Server 6500 / 400*) / 200*) 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 station 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 an Spectralink IP-DECT Base Station with up to 12 speech channels.

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

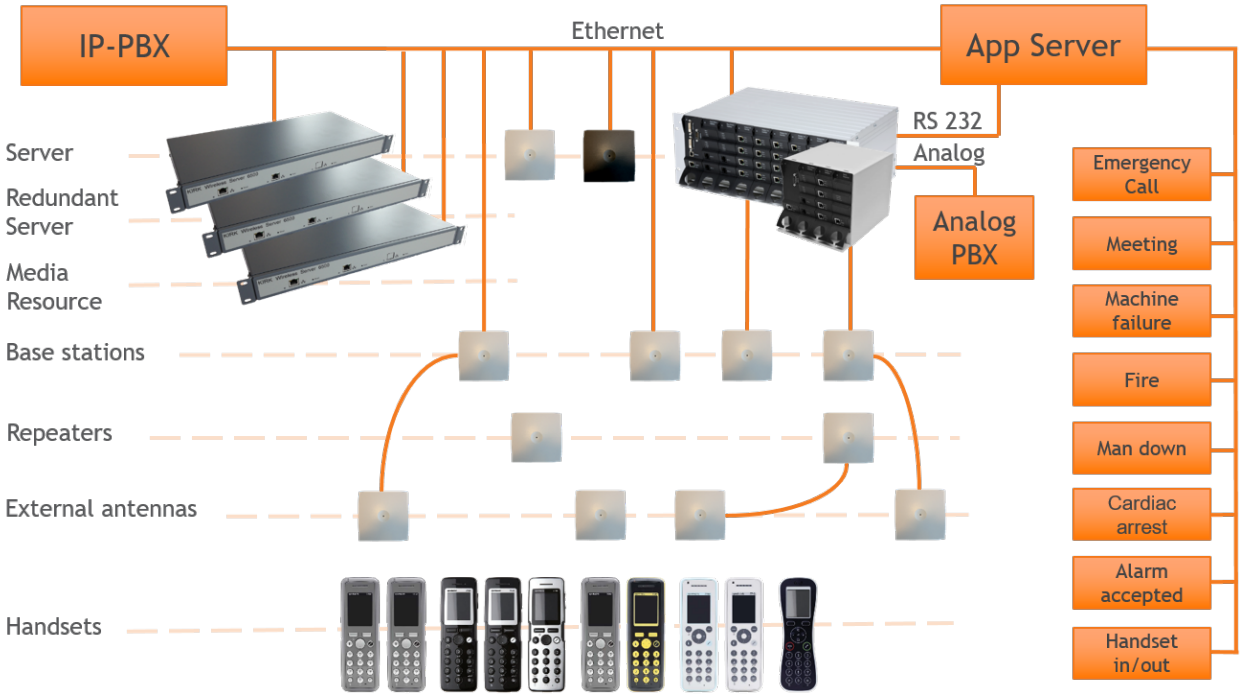
***) The external antenna is highly directional and used with RFP6 Spectralink Digital DECT Base Stations and Spectralink IP-DECT Base Stations or the Spectralink IP-DECT Server200/400 for added coverage in complex environments or to link up with remote areas. External antennas can also be used with 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" on page 27 and "Base Station Comparison Matrix" on page 29.

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	2500 Analog	2500 VoIP	8000 Analog	8000 VoIP
Market	SOHO	Small Business	Medium to large business	SMB	SMB	Medium to large business	Medium to large business
PBX Integration	IP (SIP)	IP (SIP)	IP (SIP)	Analog	IP (SIP)	Analog	IP (SIP)
Simultaneous calls	6	Up to 12	1024	32	32	1008	1024
DECT base stations	-	-	-	16/8 *)	16/8 *)	504/252 *)	512/256 *)
IP-DECT base stations	Itself **)	Itself **) +3	1024	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
Ext. antenna ***)	✓	✓	✓	✓	✓	✓	✓
Handsets (subscriptions)	12	30	4096	32	150	1008	4096

Server	200 VoIP	400 VoIP	6500 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.729, G.711 a-law & u-law	✓	✓	✓	-	-	-	-
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 an Spectralink IP-DECT Base Station with up to 12 speech 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.

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 Servers.

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		✓			
Tx power	100/250 mW	100/250 mW	100/250 mW	100/250 mW	100/250 mW
128Kb ISDN directly wired phantom power			✓	✓	✓ **)
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	Single slot	Single slot	Single/full slot

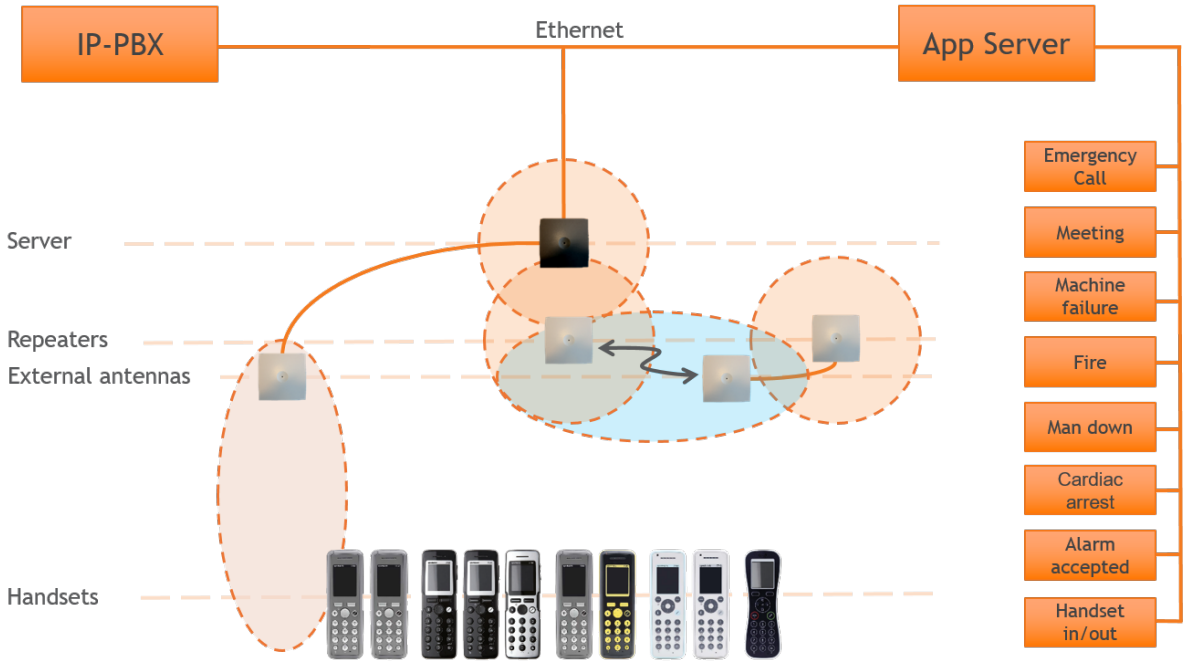
Base station	KIRK base station 12	IP-DECT base station	DECT base station (RFP4)	DECT base station (RFP5)	DECT base station (RFP6)
Use with repeaters	✓	✓	✓	✓	✓
Ext. Antenna support		✓			✓
Speech channels	11	11	4	4	4 or 8 *)
Synchronization	Over the air	Over the air	Via cable	Via cable	Via cable
LAN synchronization		✓			
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

Note:

It is possible to use LAN synchronization for Spectralink IP-DECT Base Station instead of Radio synchronization (Over The Air). This requires installation of a LAN Synchronization License. For more information, see "LAN Based Synchronization (License Required)" on page 131.

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 3rd party application server.

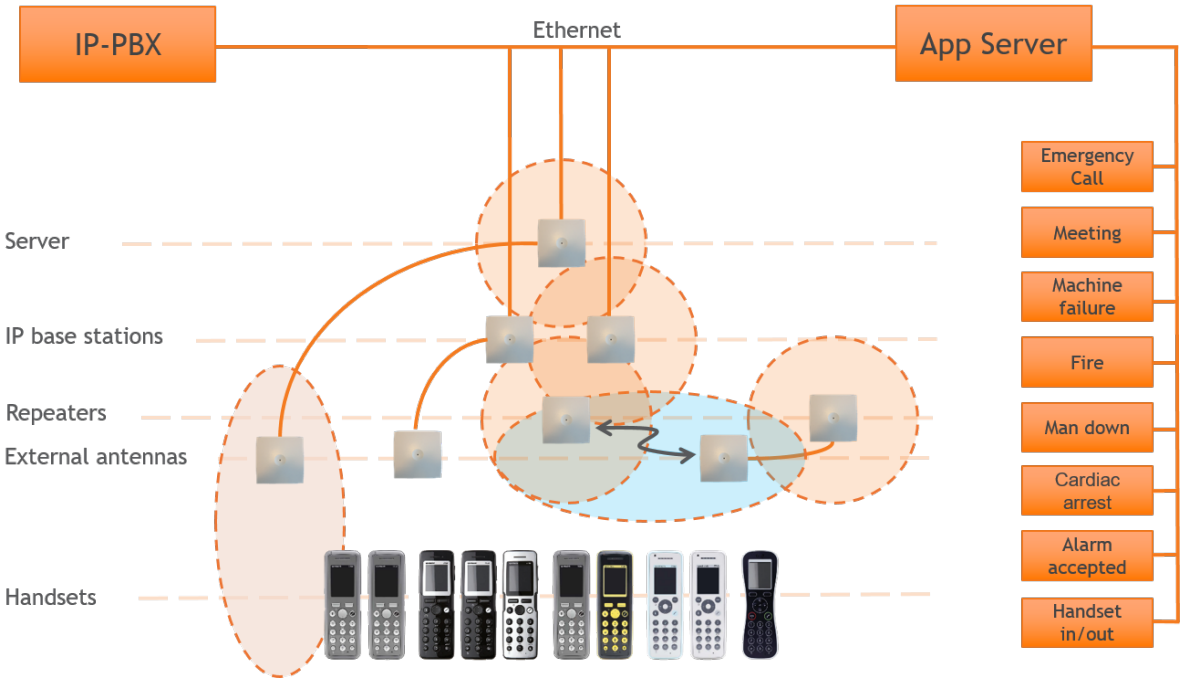
Optional wireless repeaters can be used to extend the coverage of the Spectralink IP-DECT Server 200. External directional antennas are also optional and can be used with the Spectralink IP-DECT Server 200 in physically complex environments which are challenging to cover with the built-in base station 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 3rd 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 3rd party application server. The optional Spectralink IP-DECT Base Stations are controlled by the Spectralink IP-DECT Server 400.

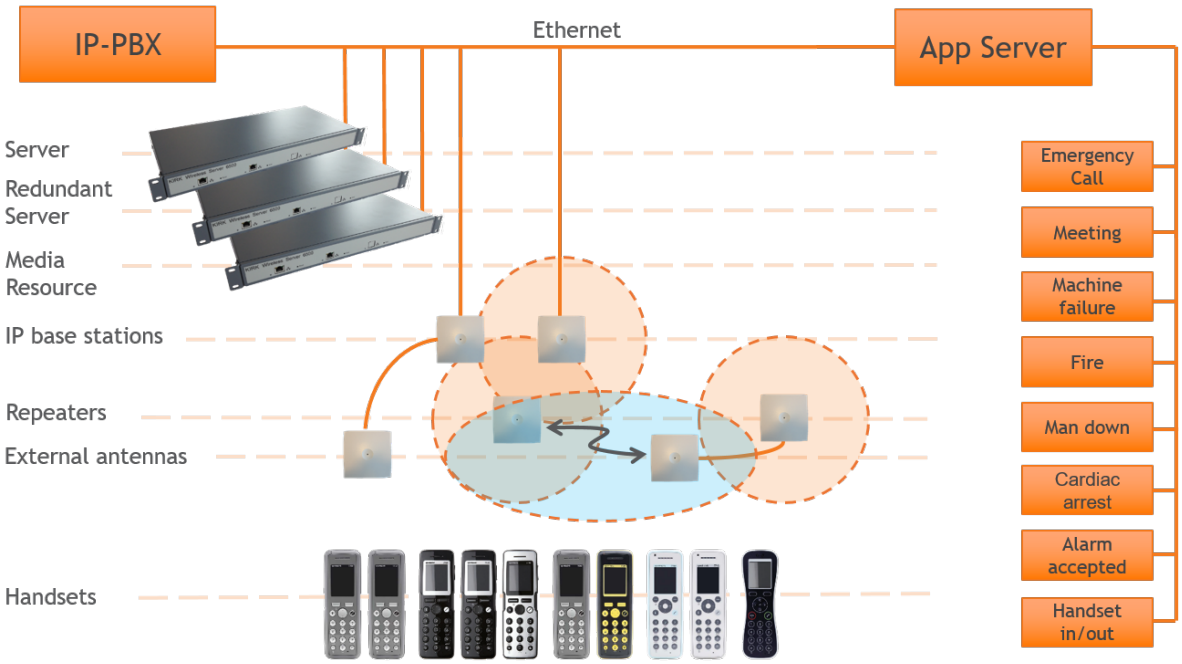
Optional wireless repeaters can be used to extend the coverage of the Spectralink IP-DECT Base Stations or the Spectralink IP-DECT Server 400 itself. External directional antennas are also optional and can be used with Spectralink IP-DECT Base Stations or the Spectralink IP-DECT Server 400 itself in 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 3rd 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 3rd party application can communicate over LAN with the Spectralink IP-DECT Server 6500.

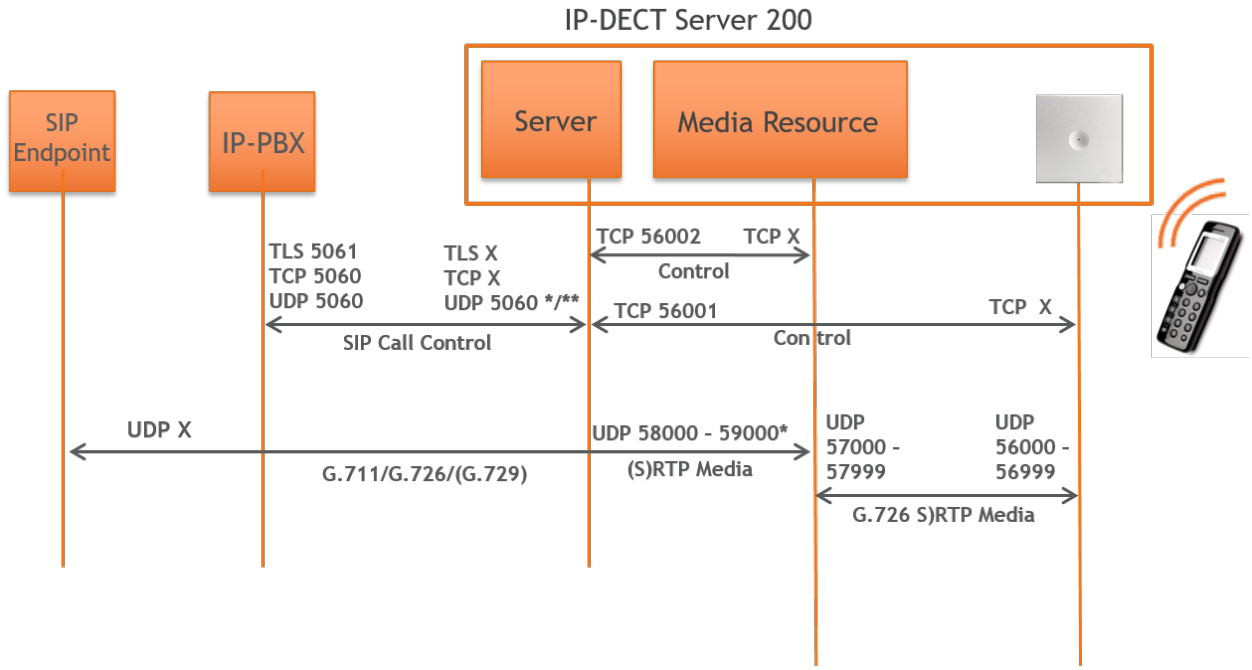
An optional Spectralink DECT Media Resource and Redundancy Spectralink IP-DECT Server 6500 can be added to the network in order to increase speech resources or share system load and maximize uptime.

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:

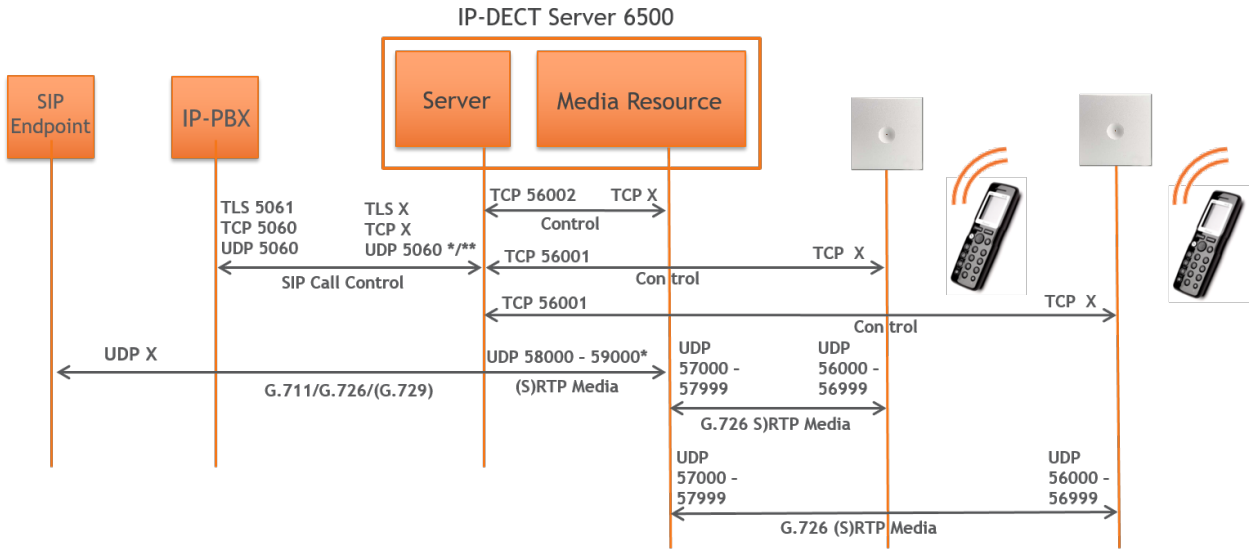
Use the communication port illustration as a reference when configuring your network for a Spectralink IP-DECT Server 200 solution.

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:

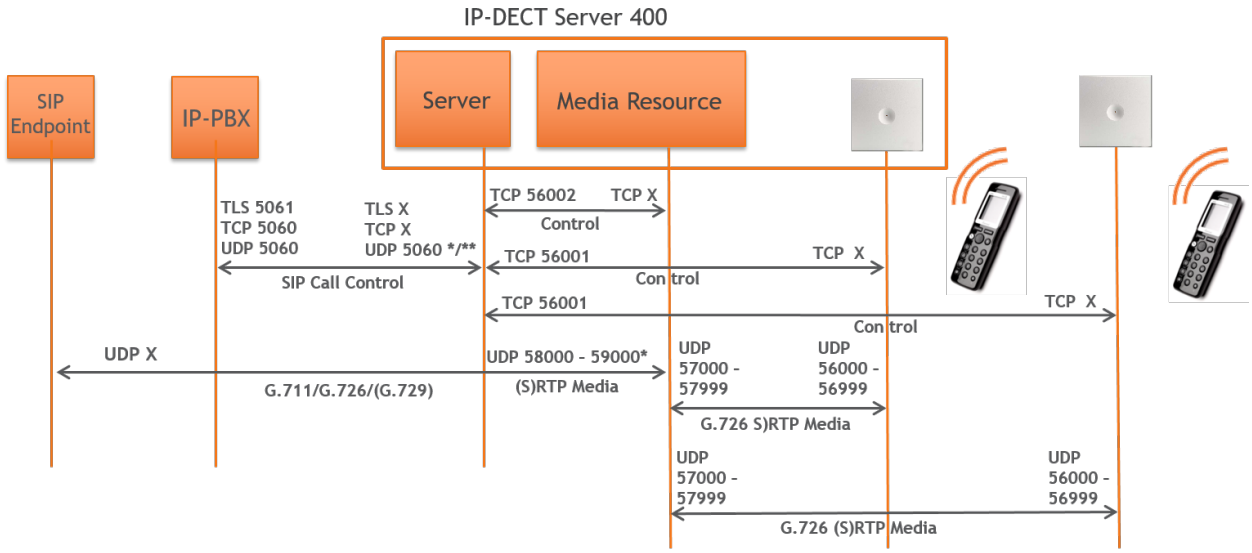


*) Default configurable

**) 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.

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 400/6500 solution.

Service Codes - Spectralink IP-DECT Server

It is possible to access the Spectralink IP-DECT Server 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 addres - enter ***999*01
- Server firmware ***999*02

Note:

If UPnP is enabled, all Spectralink IP-DECT Servers can be identified on the network by their serial number. For more information, see "Discovering the Spectralink IP-DECT Components via UPnP" on page 87.

The serial number can be found on the label on every Spectralink IP-DECT Server. For more information, see "Identifying ARI on Spectralink IP-DECT Server" on page 48.

Licenses

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

In the following you will find information about:

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

For more information about obtaining and loading licenses, see "Ordering Licenses" on page 43 and "Loading Licenses" on page 43.

Licenses for Spectralink IP-DECT Server 200

Licenses	Description	Server 200
Lync/SfB + Security (TLS, SRTP) | IP-DECT Server 200 (1407 5511)	Allows for integration with Microsoft Skype for Business and additional features. Includes Software Security Package (TLS + SRTP).	✓
Security (TLS, SRTP) | IP-DECT Server 200 (1407 5281)	Enables SRTP (Secure Real-time Transport Protocol) and TLS.	✓

Licenses for Spectralink IP-DECT Server 400/6500

Licenses	Description	Server 400	Server 6500
12 Channels + 30 Users | IP-DECT Server 400 (1407 5500)	Allows for up to 30 users and up to 6 speech channels. Increases the number of channels enabled from 6 to 12.	✓	-
12 Channels + 30 Users + Multicell | IP-DECT Server 400 (1407 5560)	Allows: Up to 30 users. Up to 3 additional base stations. Increases the number of channels enabled from 6 to 12.	✓	-
Lync/SfB +Security (TLS, SRTP) | IP-DECT Server 400 (1407 5510)	Allows for up to 12 users and 6 speech channels. Includes Software Security Package (TLS + SRTP).	✓	-
12 Channels + 30 Users + Lync/SfB + Security (TLS, SRTP) | IP-DECT Server 400 (1407 5540)	Allows: Up to 30 users. Increases the number of channels enabled from 6 to 12. Includes Software Security Package (TLS + SRTP).	✓	-
12 Channels + 30 Users + Lync/SfB + Security (TLS, SRTP) + Multicell | IP-DECT Server 400 (1407 5550)	Allows: Up to 30 users. Up to 3 additional base stations. Increases the number of channels enabled from 6 to 12. Includes Software Security Package (TLS + SRTP).	✓	-

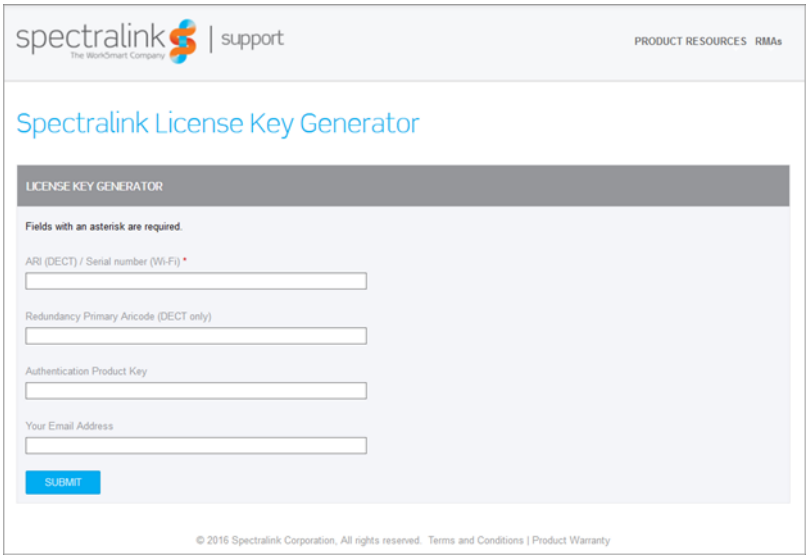
Licenses	Description	Server 400	Server 6500
Multicell | IP-DECT Server 400 (1407 5520)	Allows: Up to 12 users. Up to 3 additional base stations. Increases the number of channels enabled from 6 to 12.	✓	-
LAN Sync | IP-DECT Server 400 (1407 5600)	Allows base stations to be synchronized over LAN.	✓	-
Cisco Unified CM (Advanced Features) | IP-DECT Server 400 (1407 5490)	Allows for tighter integration with the Cisco Unified Communications Manager and additional features.	✓	-
Lync/SfB +Security (TLS, SRTP) | IP-DECT Server 6000/6500 (1407 5270)	Allows for integration with Microsoft Skype for Business and additional features. Includes Software Security Package (TLS + SRTP).	-	✓
LAN Sync | IP-DECT Server 6500 (1407 5610)	Allows base stations to be synchronized over LAN.	-	✓
Security (TLS, SRTP) | IP-DECT/DECT Servers 400/6000/6500/2500/8000 (1407 5280)	Enables SRTP (Secure Real-time Transport Protocol) and TLS.	✓	✓
Handset Sharing License | IP-DECT/DECT Servers 400/6500/2500/8000 (1407 5460)	Allows handsets to be shared among numbers and vice versa.	✓	✓
Frequency Swap | IP-DECT/DECT Servers 400/6500/2500/8000 (1407 5620)	Allows the active radio frequency to be changed in accordance to geographical locations.	✓	✓

Licenses	Description	Server 400	Server 6500
Cisco Unified CM (Advanced Features) | IP-DECT Server 6500 (1407 5495)	Allows for tighter integration with the Cisco Unified Communications Manager and additional features.	-	✓
Automatic Alarm Call | IP-DECT/DECT Servers 300/400/2500/6000/6500/8000 (1407 5450)	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 | IP-DECT Server 6000/6500 (1407 5260)	Allows adding a backup server to a system.	-	✓
Redundancy Master | IP-DECT Server 6000/6500 (1407 5250)	Allows adding a backup server to a system.	-	✓
30 Users | IP-DECT Server 6000/6500 (1407 5200)	Allows for up to 30 users.	-	✓
150 Users | IP-DECT Server 6000/6500 (1407 5210)	Allows for up to 150 users.	-	✓
500 Users | IP-DECT Server 6000/6500 (1407 5220)	Allows for up to 500 users.	-	✓
1500 Users | IP-DECT Server 6000/6500 (1407 5230)	Allows for up to 1500 users.	-	✓

Licenses	Description	Server 400	Server 6500
4096 Users | IP-DECT Server 6000/6500 (1407 5240)	Allows for up to 4096 users.	-	✓
Lync/SfB +Security (TLS, SRTP) | IP-DECT Server 6000/6500 (1407 5270)	Allows for integration with Microsoft Skype for Business and additional features. Includes Software Security Package (TLS + SRTP).	-	✓
Enhanced Provisioning Interface | IP-DECT Server 400 (1407 5701)	Allows for provisioning of firmware for: • IP-DECT base stations • Handsets	✓	-
Enhanced Provisioning Interface | IP-DECT Server 6500 (1407 5200)	Allows for provisioning of firmware for: • IP-DECT base stations • Media resources • Handsets	-	✓
Additional repeaters (up to 6 repeaters) | IP-DECT Server 400 1407 5570	Allows for use of up to 6 additional repeaters.	✓	-

Ordering Licenses

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.

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" on page 172.

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" on the next page.

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 and Spectralink DECT Media Resource, see "Installing the Spectralink IP-DECT Server 6500 and Spectralink DECT Media Resource" on page 55.

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 applies 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 environmentalair 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 the Spectralink IP-DECT Base Station" on page 62 and "Installing the Spectralink DECT Repeater" on page 68.

Note:

For more information about installing the Spectralink IP-DECT Server 200, see "Installing the Spectralink IP-DECT Server 200" on page 49.

For more information about installing the Spectralink IP-DECT Server 400, see "Installing the Spectralink IP-DECT Server 400" on page 54 and "Installing the Spectralink IP-DECT Base Station" on page 62.

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 Spectralink Maintenance Software

Software Requirements

The following is required to run the handset and repeater installation and maintenance tools.

- OS: Windows 7 or newer

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 or theIP-DECT Server 200 Deployment and Installation Configuration Guidedepending 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 Server (see label on the rear of the server unit)

  For more information, see "Identifying ARI on Spectralink IP-DECT Server" on the next page.
- Serial numbers for handsets.

  For more information, see "Identifying IPEI on Spectralink Handset" on the next page.
- 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 - 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.

About ARI and IPEI Identification

All Spectralink DECT Handsets and all Spectralink IP-DECT Servers have unique identification numbers.

This is needed in order for:

- The handsets to know which Spectralink IP-DECT Server installation they belong to.
- The Spectralink IP-DECT Server 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 Server.

A Spectralink IP-DECT Server 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 Server, the handset is subscribed. There is a record in the Spectralink IP-DECT Server holding information about all the handsets being subscribed to it. This record is subdivided in to 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" on page 139.

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 Server

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: From the web based Administration Page > **Status** > **Wireless Server**.

Installing the 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

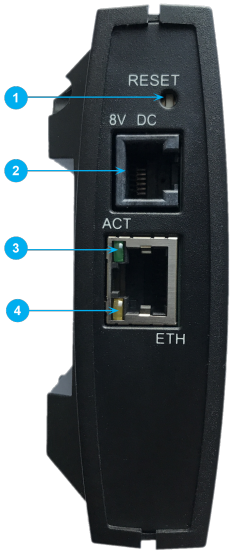
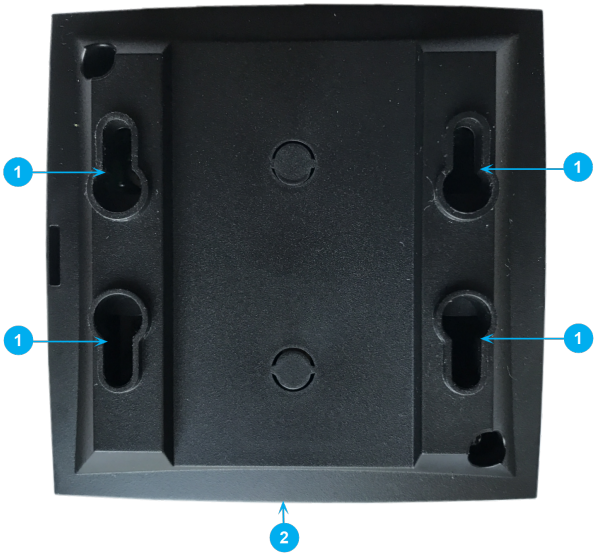
- Power over Ethernet (PoE 802.3af).
- Maximum power supply consumption is 3.0W (IEEE 802.3af class 1 device).

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.

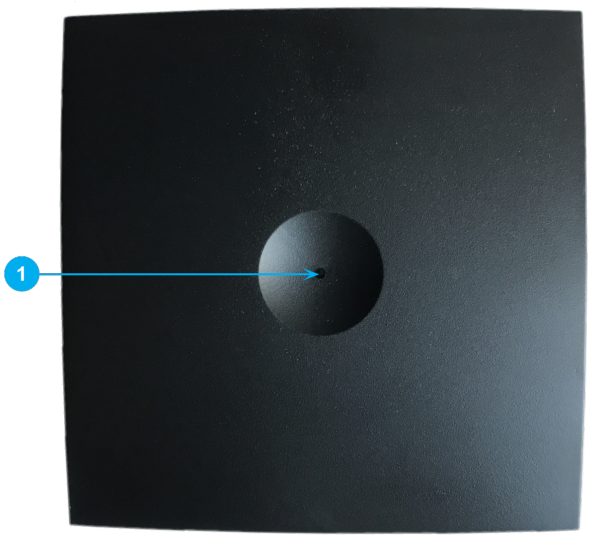
Use an 8V-DC power supply when using a port without PoE.

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 Server 200 - bottom	Spectralink IP-DECT Server 200 - rear
	
1. Reset button 2. DC 3. LINK/Activity Indicator 4. ETH port (power supply by PoE)	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 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.

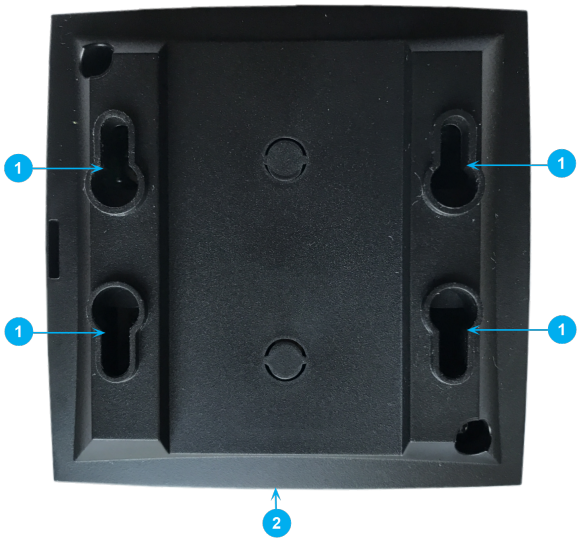
Wall-Mount and Power on the Spectralink IP-DECT Server 200

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.

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.

Installing the 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 the Spectralink IP-DECT Base Station" on page 62.

Note:

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

Installing the Spectralink IP-DECT Server 6500 and Spectralink DECT Media Resource

This section describes 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:

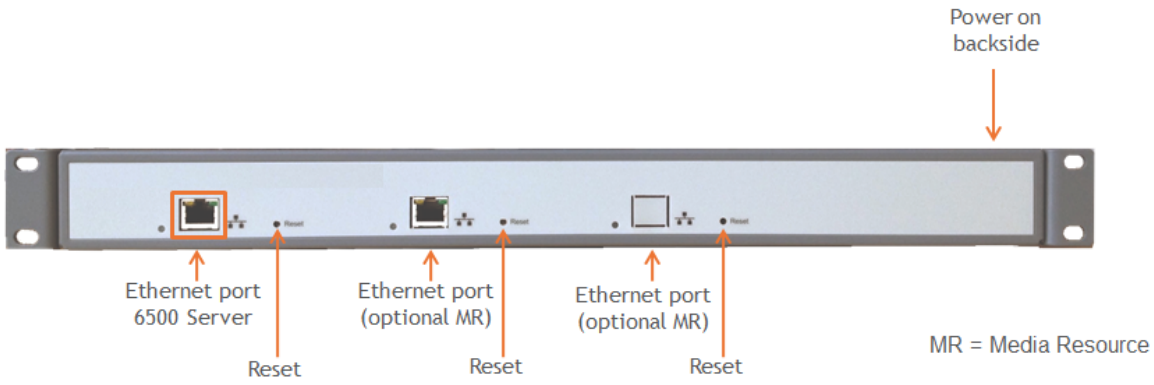
The installation of a Spectralink DECT Media Resource with the Spectralink IP-DECT Server 6500 is optional. Installation of a media resource will increase the number of simultaneous voice calls supported by a stand-alone server.

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

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:



Server 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.
Activity Indicator - green flashing	Activity

Server 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 and empty user data base) 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.

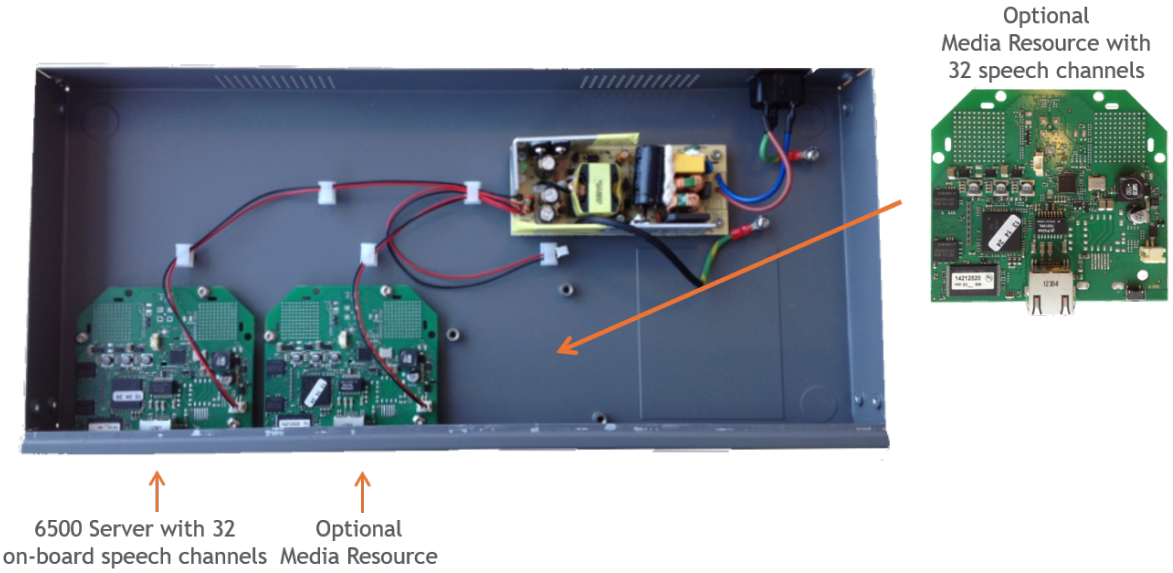
   All Spectralink IP-DECT Server 6500s and Spectralink DECT Media Resources must be connected to a switch port.

   Installed Spectralink DECT Media Resources must have their own switchport.
4. Connect the power on the back of the cabinet.

Adding Aditional 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 speech channels and is purchased seperately.

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.

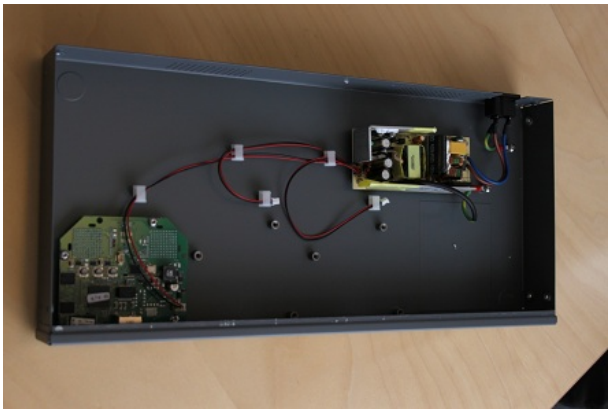


Note:

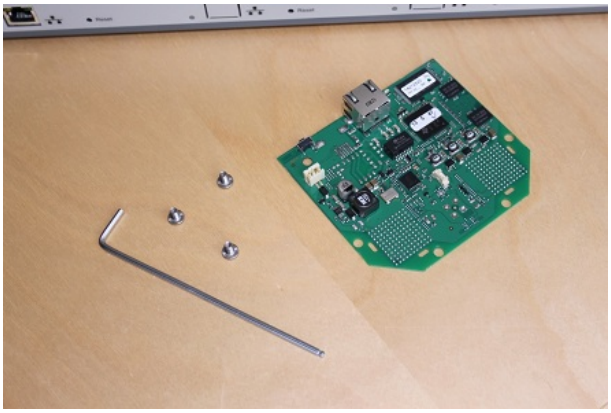
It is possible to have cabinets with Spectralink DECT Media Resources only, but they can only be used in conjunction with a Spectralink IP-DECT Server 6500.

How to Add a Spectralink DECT Media Resource

1. Remove the top cover from the cabinet.



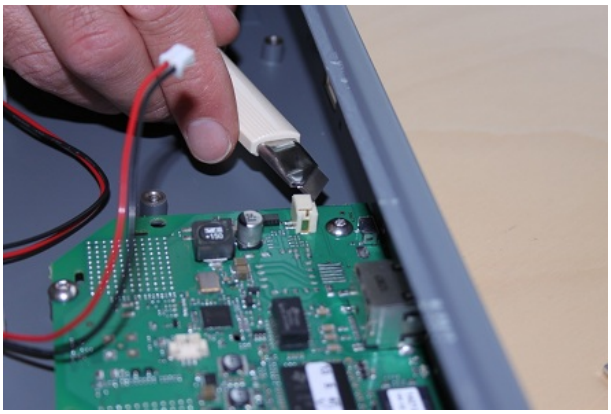
2. Unpack the media resource board.

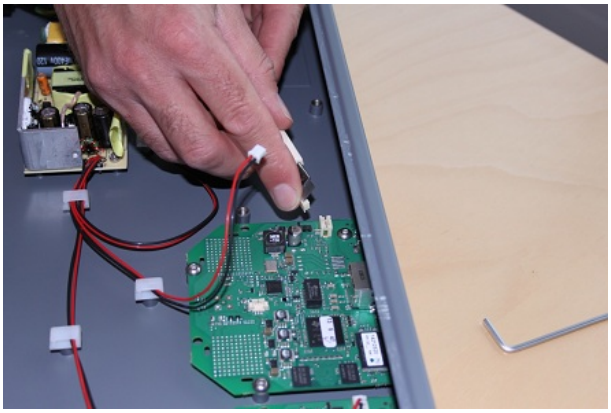


3. Cut a hole for the RJ45 network connector in the front foil of the cabinet.

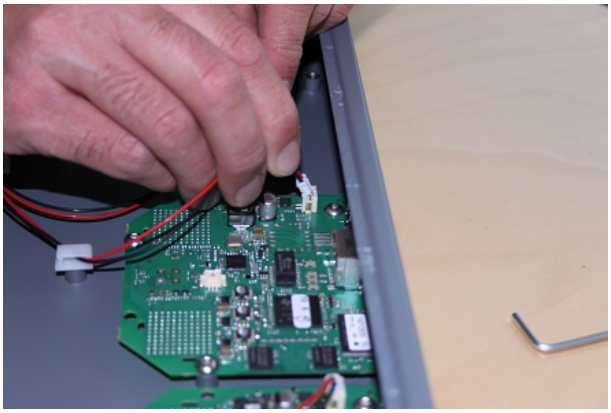
4. Mount the media resource board in the cabinet with three screws.

5. Prepare the media resource power connector.





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



7. Close the cabinet again.

Installing the 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 75 meters/245 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).

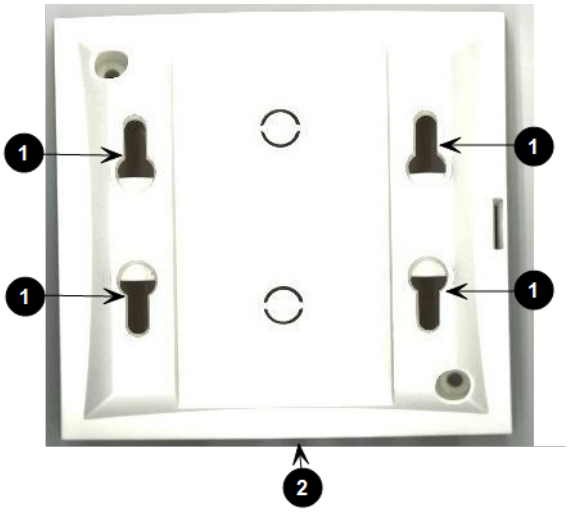
Use a standard PoE adapter or a PoE-enabled port on a switch adhering to PoE 802.3af when connecting the base station to a PoE power source.

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

Base Station Appearance and Components

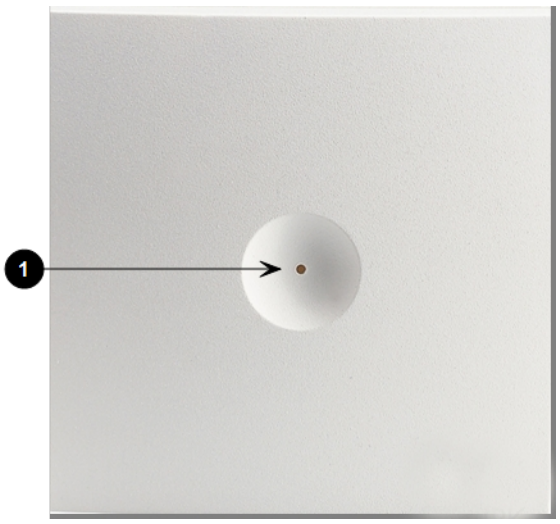
Below you will find a description of the base station appearance and components:

Spectralink IP-DECT Base Station - rear



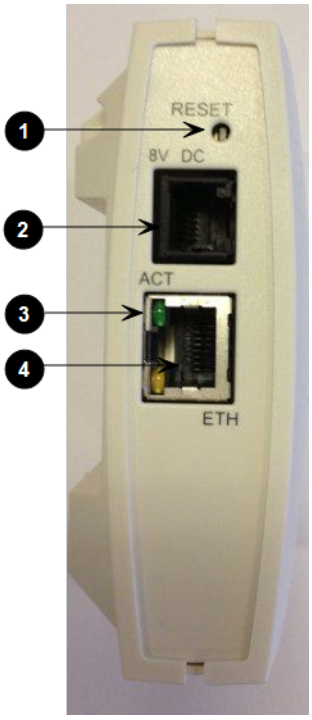
1. Holes for wall mounted screws
2. Connection to LAN

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.

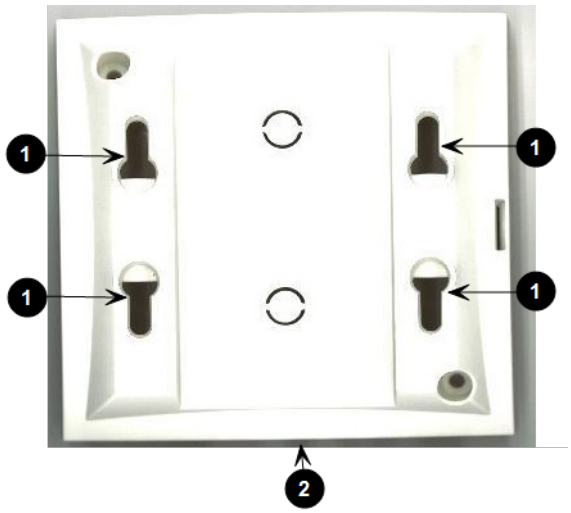
How to Wall Mount the Spectralink IP-DECT Base Station

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.

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 "Power Requirements for the Base Station" on page 62.

Installing the 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.

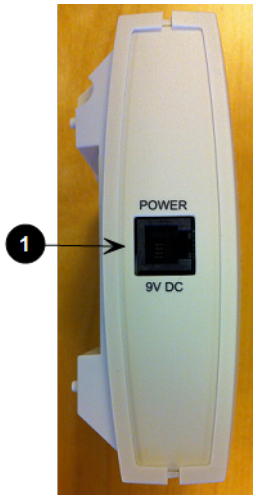
For installations, the following items should be present in every box containing a Spectralink DECT Repeater:

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

Repeater Appearance and Components

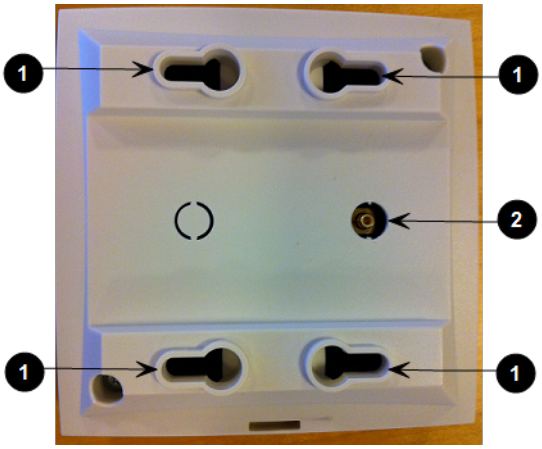
Below you will find a description of the repeater appearance and components:

DECT Repeater - bottom



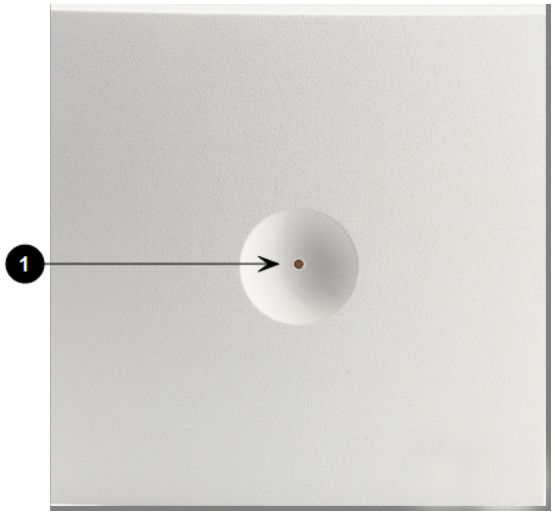
1. RJ9 port

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.
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 environmentalair 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

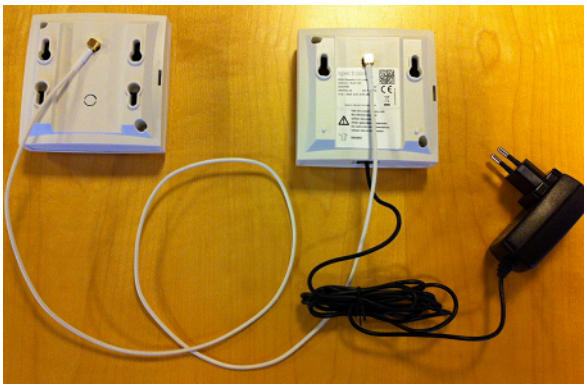
For best RF coverage, the device must be mounted vertically on walls.

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.

2. Mount the repeater on the wall using the anchors and screws accompanying the product.
3. After installing the repeater you need to power it up. The power supply for the repeater is 9VDC, 350mA.

Programming a Spectralink DECT Repeater with the Repeater Programming Kit

Content of the Spectralink Repeater Programming Kit

The Repeater Programming Kit (Part no. 0250 9210) consists of:

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

Set up of the Hardware for Repeater Programming

It is recommended that you carry out the set up in the following order:

1. Unplug the repeater power supply and insert the splitter.
2. Connect the repeater power supply to the splitter and the mains. LED flashes.
3. Connect the USB cable to the programming tool.
4. 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 it is possible to 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

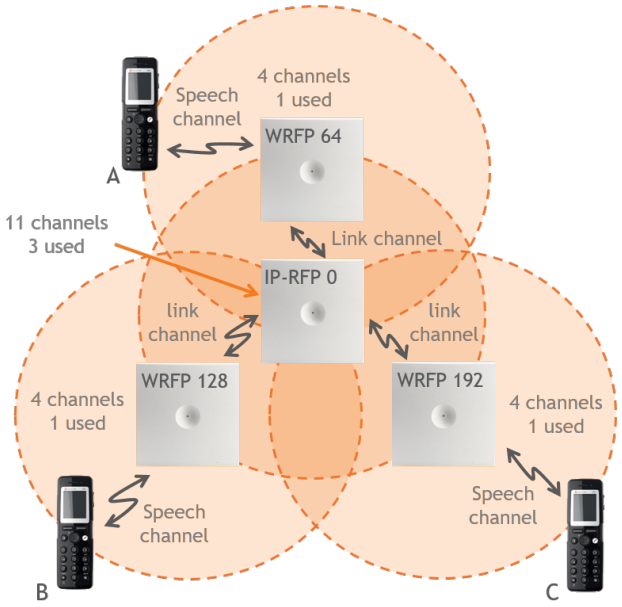
Second Repeater

- 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

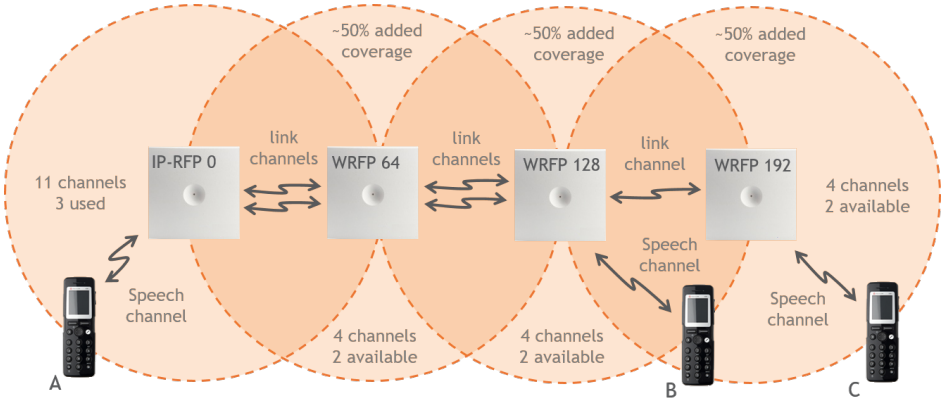
Second Repeater in Chain

- 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

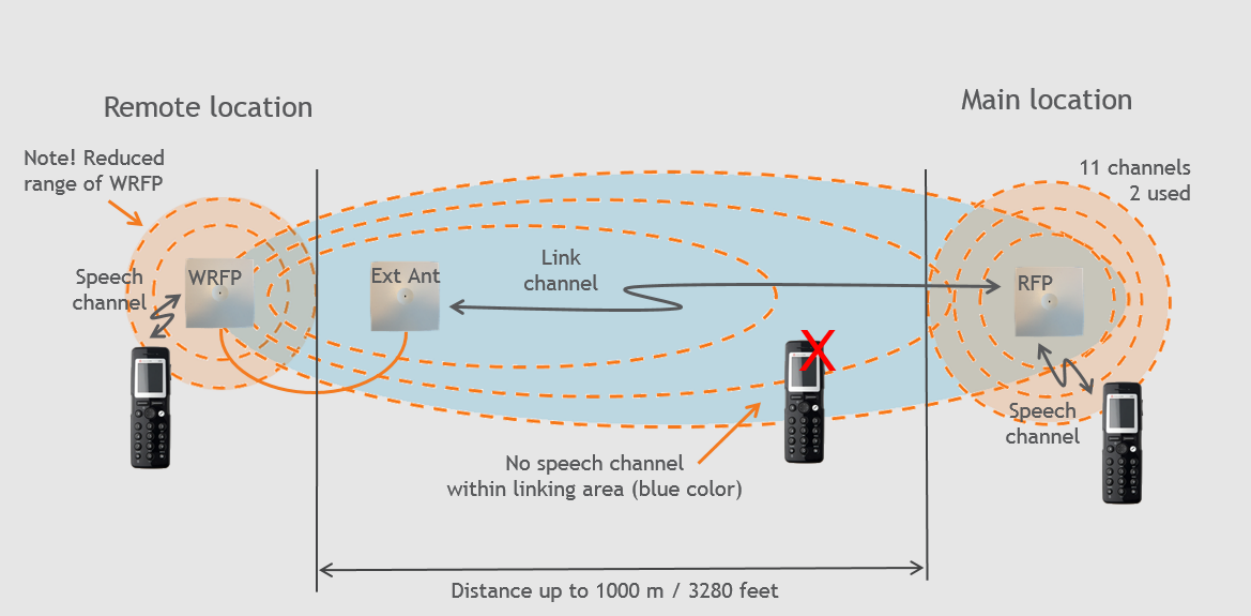
If coverage is needed in a remote area, synchronization can be established between the main system and a repeater by use of an external antenna. The external antenna establishes a radio link between the main system and a Spectralink DECT Repeater.

Note:

Only the Spectralink external antenna (part no. 0231 9705 - 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 3 m (part no. 1400 2704 and 7.5 m (part no. 1400 2706).

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.

Technical Specifications - External Antenna

Electrical Properties

- Frequency range: 1880-1930 MHz
- Impedance: 50 Ω (DC-path to ground)
- Polarization: RHCP
- Gain: 7.5 - 8.0 dB
- 3 dB beamwidth horizontal: > 62°
- 3 dB 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

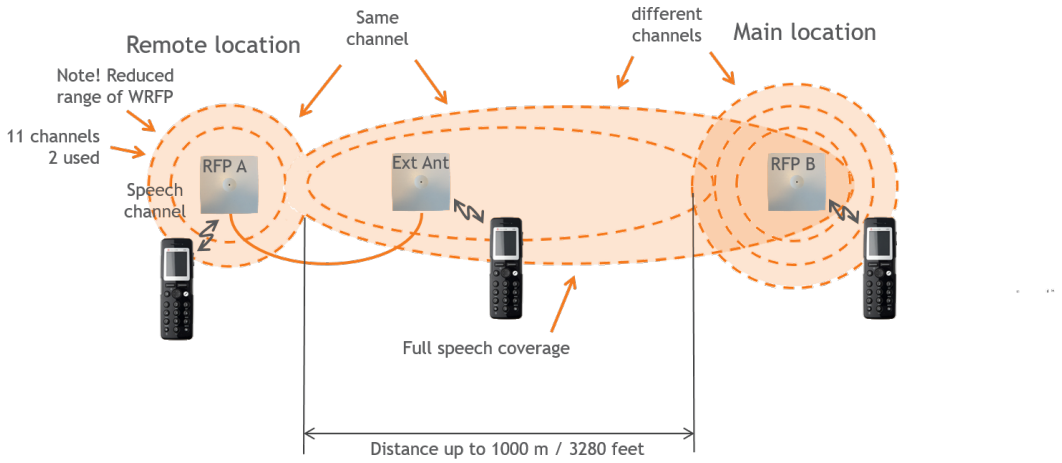
Using the Spectralink IP-DECT Server 200/400 and Spectralink IP-DECT Base Station With External Antenna

Note:

Only the Spectralink external antenna (part no. 0231 9705) 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 3 m (part no. 1400 2704 and 7.5 m (part no. 1400 2706).

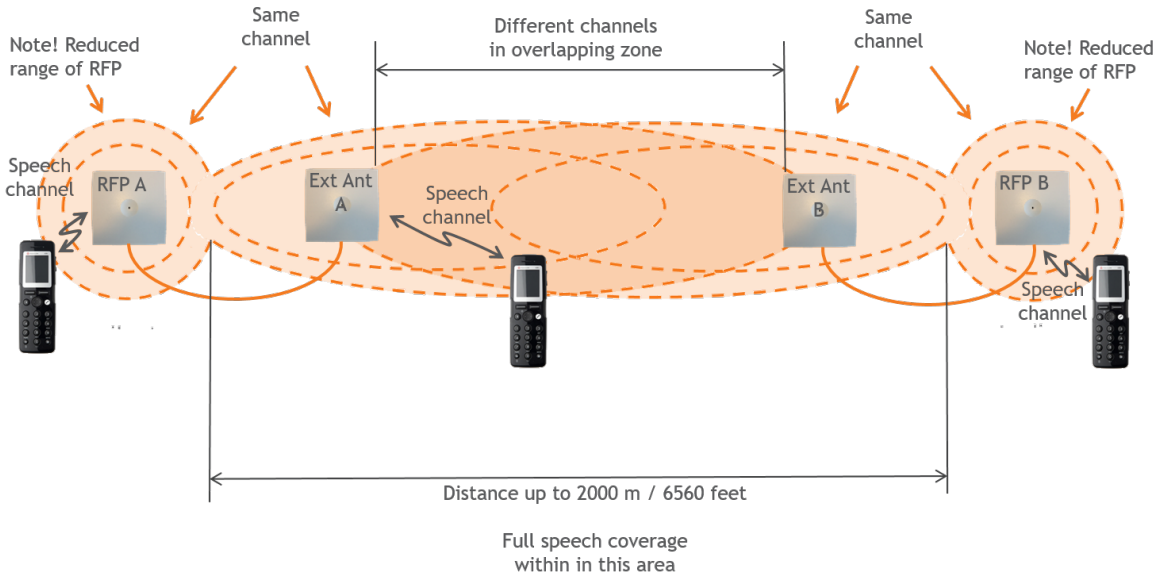
The devices are automatically configured to the external antenna when connected.

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

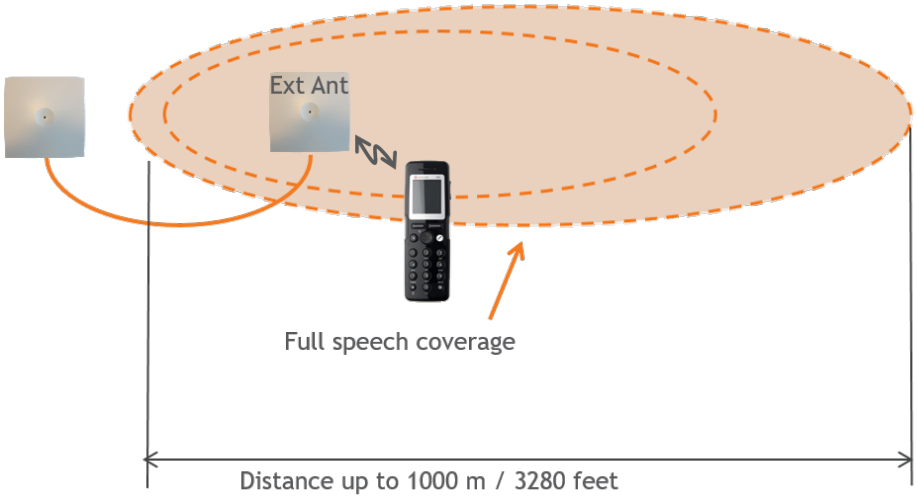


The 2 base stations are too far apart to maintain full speech coverage between them. An external antenna can be used on either side to create an overlap which allows for full speech coverage anywhere between the two base stations. Note that the range of RFP A is reduced when connected with an external 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.

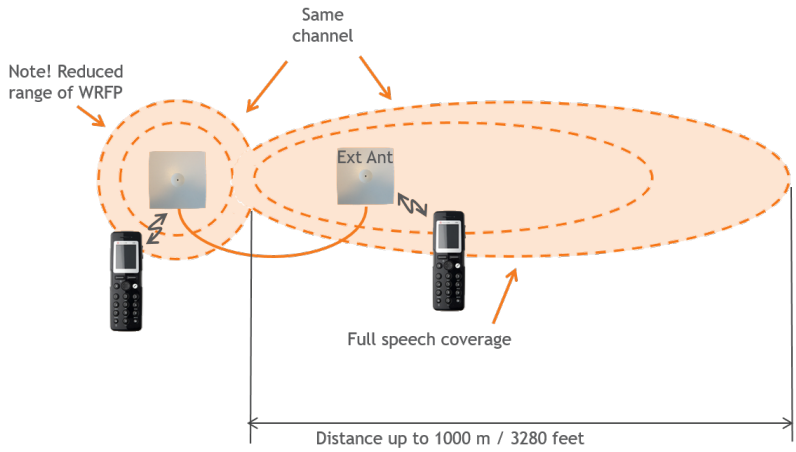
Second example (see illustration below) is an example of using Spectralink IP-DECT Base Stations, both having external antennas. This scenario allows for coverage over very long distances.



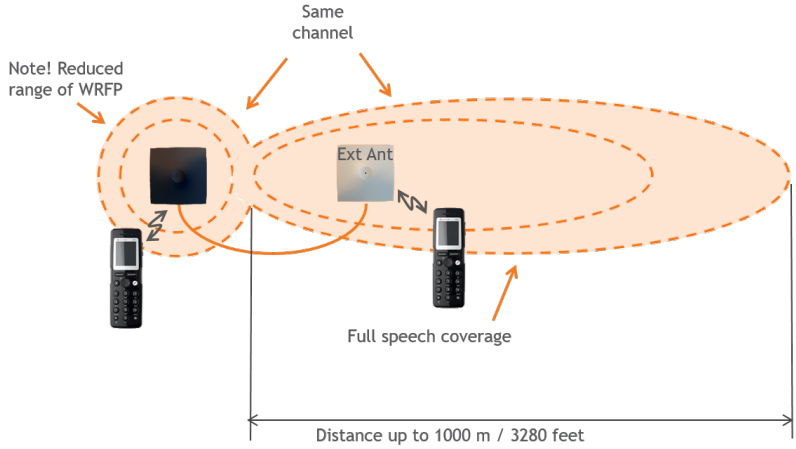
Third example (see illustration below) is an example of using external antenna only on a Spectralink IP-DECT Base Station or Spectralink IP-DECT Server 400 with built-in antenna turned off (requires Multicell | IP-DECT Server 400 License on the Spectralink IP-DECT Server 400).



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



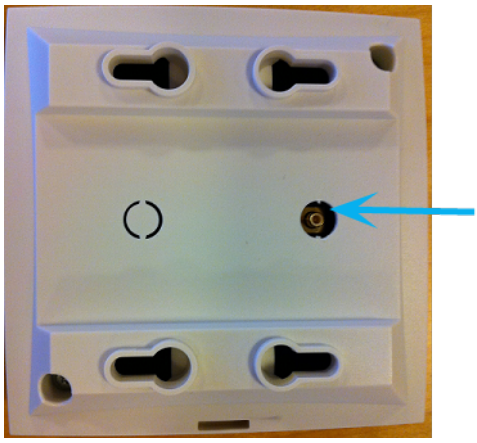
Fifth example (see illustration below) is an example of using a Spectralink IP-DECT Server 200 with external antenna.



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.

Configuration Steps Overview

Below is an overview of the steps to follow in order to configure the Spectralink IP-DECT Server 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 Server and Spectralink DECT Media Resource (if used).

   For more information, see "Installing the Spectralink IP-DECT Server 200" on page 49,"Installing the Spectralink IP-DECT Server 400" on page 54 and "Installing the Spectralink IP-DECT Server 6500 and Spectralink DECT Media Resource" on page 55 .

2. Change the IP address of the Spectralink IP-DECT Server.

   For more information, see "To Configure a Static IP Address and Other Network Settings" on page 93.

3. Power up the Spectralink IP-DECT Base Station.

   For more information, see "Installing the Spectralink IP-DECT Base Station" on page 62.

   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 "To Configure a Dynamic IP address" on page 92.

   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 Server.

   For more information, see "Assigning Server Address to Spectralink IP-DECT Base Station and Spectralink DECT Media Resource" on page 123.

   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" on page 101.

7. Register/create users and enter values for user name, authentication user and authentication password (depending on PBX type).

   For more information, see "Handset Management" on page 143.

8. Subscribe handset.

   For more information, see "Registering Users and Subscribing Spectralink DECT Handsets" on page 139.

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, clusters, redundancy server, handset sharing, phone book and MSF messaging can also be part of further configuration.

For more information, see:

- "Configuring Media Resource Settings" on page 115
- "Configuring Clusters" on page 118
- "Configuring Redundancy" on page 177
- "Configuration of Handset Sharing" on page 200
- "Configuring Corporate Phone Book/Directory " on page 193
- "Messaging Over MSF" on page 173

Configuring the Spectralink IP-DECT Server/Spectralink DECT Media Resource Solution

This section provides you with information on basic network configuration of the Spectralink IP-DECT Server 200/400/6500/Spectralink DECT Media Resource solution and the web based Administration Page.

Note:

Configuration of Spectralink DECT Media Resources and Clusters 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.

The web based Administration Page is used to configure the different components of the Spectralink IP-DECT Server 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 Server solution, Spectralink recommends doing it the following way:

- Spectralink IP-DECT Server 400/6500 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 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 need to use UPnP to discover the Wireless devices. In Windows Explorer the devices will appear under **Network** and **Other Devices** as “<device name>-<Serial number> “ (e.g. Spectralink IP-DECT Server 6500-8442621 or MR6500-84532341).

Note:

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

If the Spectralink IP-DECT Server solution is configured as recommended above, it is possible to assign options to the DHCP server making it extremely easy to configure all media resources and base stations. If the Spectralink IP-DECT Server 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 solution and the web based Administration Page.

You can provide information about the static IP address of Spectralink IP-DECT Server 400/6500 in the DHCP server through DHCP options. When defining the IP address of the Spectralink IP-DECT Server 400/6500 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 Server location in the Vendor Specific Information option (43), sub-option 43 encpapsulated as a string type parameter.

On a Windows Server 2012 DHCP Management Cosole, the following steps will configure the correct DHCP option:

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.

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 a 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:

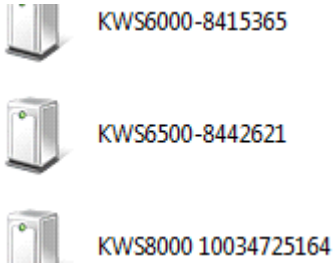
```
option space ipdect code width 1 length width 1;
option ipdect.server code 43 = text;
option vendor-ipdect code 43 = encapsulate ipdect;
class "vendor-classes" {
 match option vendor-class-identifier;
}
subclass "vendor-classes" "KIRK.IP6000" {
 vendor-option-space ipdect;
 option ipdect.server "192.168.1.10";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

Discovering the Spectralink IP-DECT Components via UPnP

The Spectralink IP-DECT Server is setup with DHCP enabled by default. Therefore, you must use UPnP to discover the Spectralink IP-DECT Server.

The Spectralink IP-DECT Server will appear under **Network** and **Other Devices** (using Windows Explorer) as "KWS6500 -<Serial number> ", e.g. KWS6500-8442621

Below is an example of using UPnP to discover Spectralink IP-DECT Server 6500.



- Double-click the icon to access the web based Administration Page of the Spectralink IP-DECT Server 6500.

Assigning DHCP Server Reservations

If the Spectralink IP-DECT Server/ Spectralink 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 Server, Spectralink 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 user name and password.

For more information, see "Discovering the Spectralink IP-DECT Components via UPnP" on the previous page.

Note:

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

Password

The Spectralink IP-DECT Server, Spectralink DECT Media Resources and Spectralink IP-DECT Base Stations are delivered with a default user name and password.

- Default user name 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 Server.

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 "Configuring Security Settings and Changing System Password" on page 99.

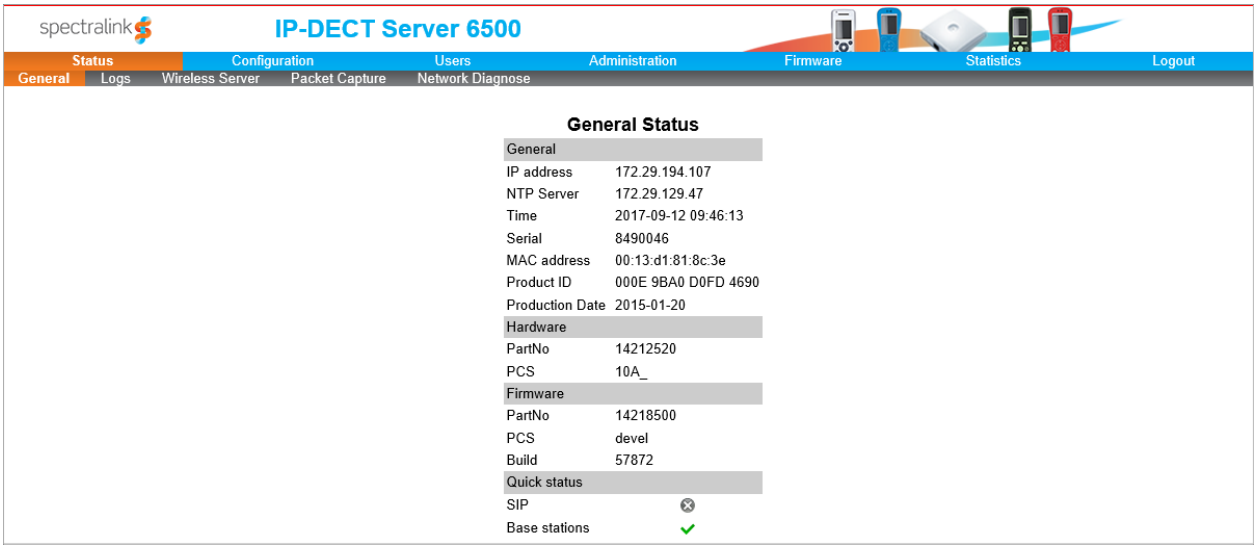
About the Main Page of the Web Based Administration Page

The main page of the web based Administration Page for the Spectralink IP-DECT Server, Spectralink 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 Server

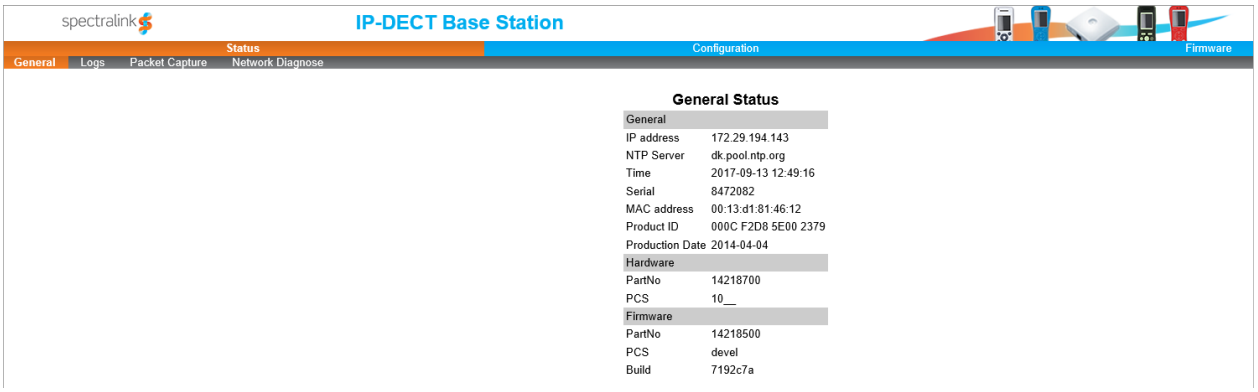
The web based Administration Page is used to configure the different solution components of the Spectralink IP-DECT Server. For an overview and description of parameters on the different pages, see "Parameter Overview" on page 223.



Spectralink IP-DECT Base Station

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

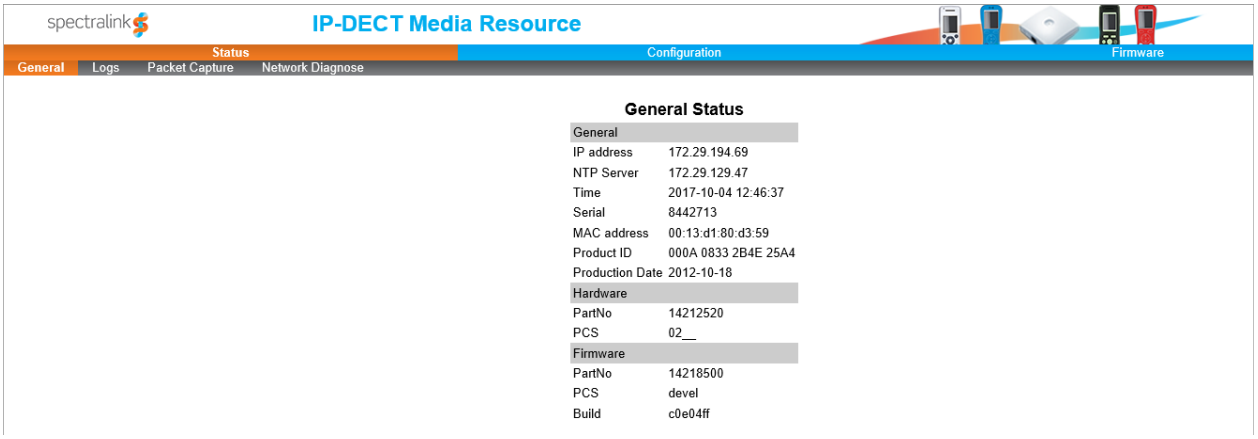
- Configuration - to specify to which Spectralink IP-DECT Server the Spectralink IP-DECT Base Station should connect.
- Status Information
- Firmware update



Spectralink DECT Media Resource

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

- Configuration - to specify to which Spectralink IP-DECT Server the Spectralink DECT Media Resource should connect.
- Status Information
- Firmware update



Configuring Network Settings

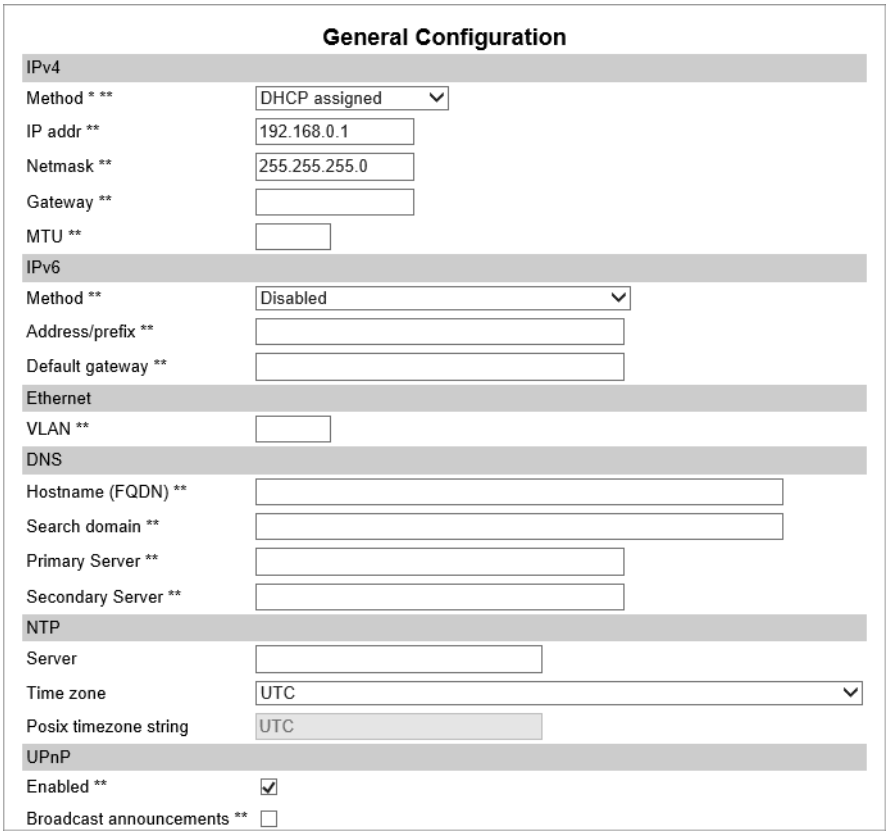
Through the web based Administration Page of the server, you can configure the network for the Spectralink IP-DECT Server components using a static IP address or a dynamic IP address (DHCP). For more information, see "Recommended Network Configuration" on page 85.

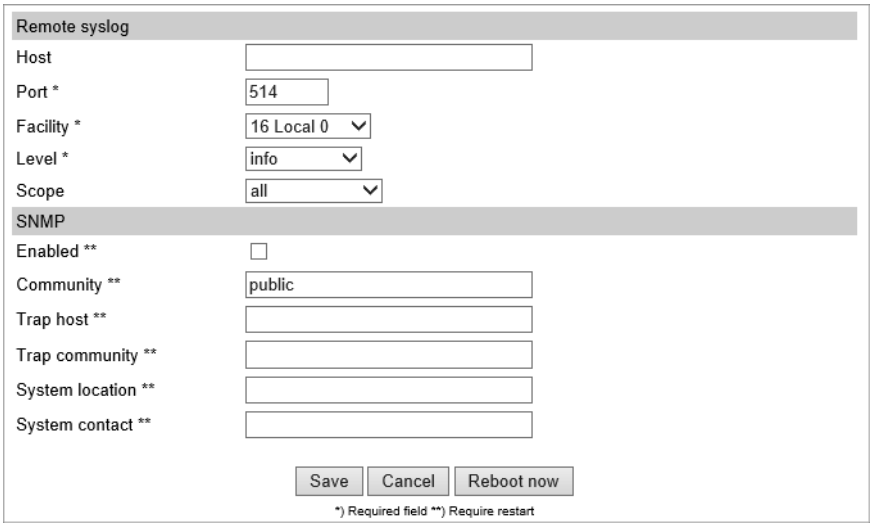
Note:

As the Spectralink IP-DECT Server 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 Server is the preferred method. If the device is configured using a static IP address, it is possible to 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).





To Configure a Dynamic IP address

It is recommended to use 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 Spectralink IP-DECT Server and Spectralink DECT Media Resource.

To configure IP address, DNS and NTP settings for the Spectralink IP-DECT Server and Spectralink DECT 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 also "Recommended Network Configuration" on page 85.
IP addr	Enter the IP address of the Spectralink IP-DECT Server.
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.

Field	Setting
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)	It is possible to 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)	It is possible to 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 Server 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.

Field	Setting
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 zones include day-light 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 dis-coverable. 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 Spec-tralink IP-DECT Server, Media resource and Base sta-tion will be present in **My Network Places**.
Broadcast announcements (Optional)	Specifies if UPnP announcements are broadcasted. If enabled, the device broadcasts announcements auto-matically.
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.

Field	Setting
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.

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 Servers, Spectralink 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
- SNMPv2
- IPV6
- UDP

In addition to the general information mentioned above, specific Spectralink DECT information is available on the Spectralink IP-DECT Server 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 server.
- dectGeneralStatisticsGroup

  Objects which provide general statistics about the IP-DECT server.
- dectUserInfoGroup

  Objects which provide information about users on the IP-DECT server.
- dectRfpInfoGroup

  Objects which provide information about base stations (RFP) configured on the IP-DECT server.
- dectMediaResourceInfoGroup

  Objects which provide information about media resources configured on the IP-DECT server.
- dectNotificationsGroup

  Notifications that are generated by the IP-DECT server.

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**.

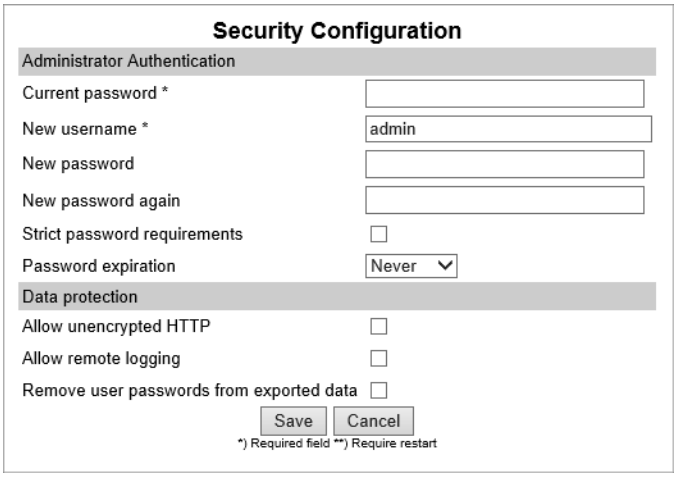
Configuring Security Settings and Changing System Password

It is recommended to change 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.
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" on the next page. **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.

Field	Setting
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 Server,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**.

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 signalling, 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 IP-DECT Server listens for incoming SIP-signalling. 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" on page 116.
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 Server 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.

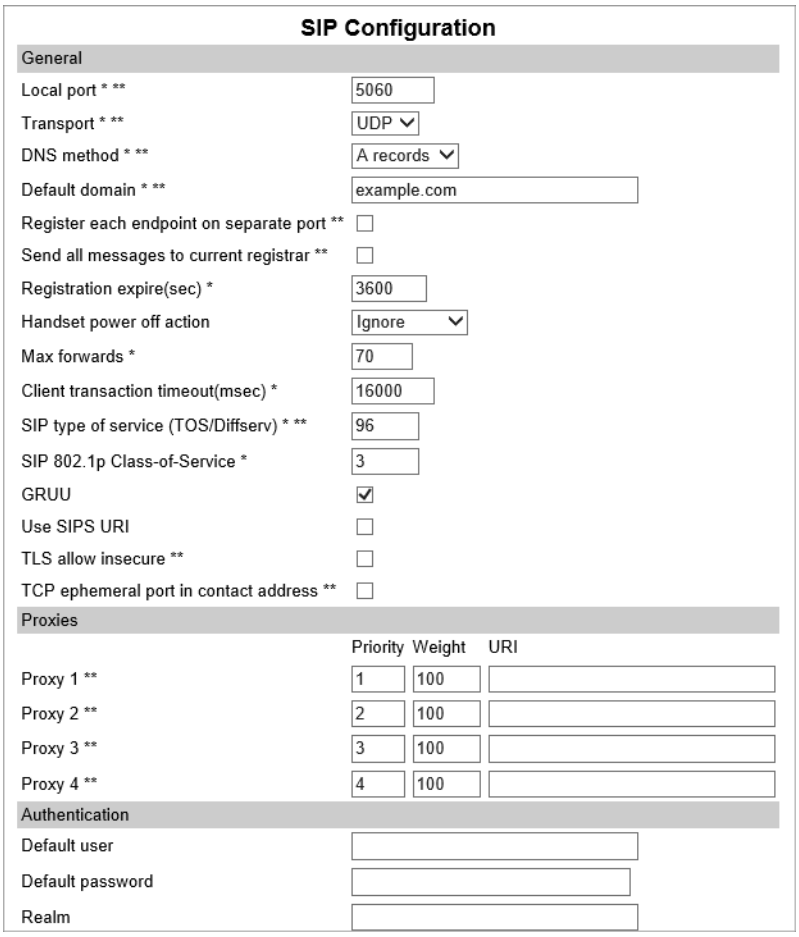
Field	Setting
Send all messages to current registrar (Optional)	If enabled, all non-REGISTER requests to the current registrar will be sent, when more proxies are available.
Registration expire(sec)	The maximum time between re-registrations. The registrar can signal a shorter time-out. Default value: 3600 sec
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)	Client transaction time-out. This controls timer B and F as specified in RFC3261. Increase this to eliminate time out errors or decrease it to reduce fail over time. Default value: 16000 msec
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

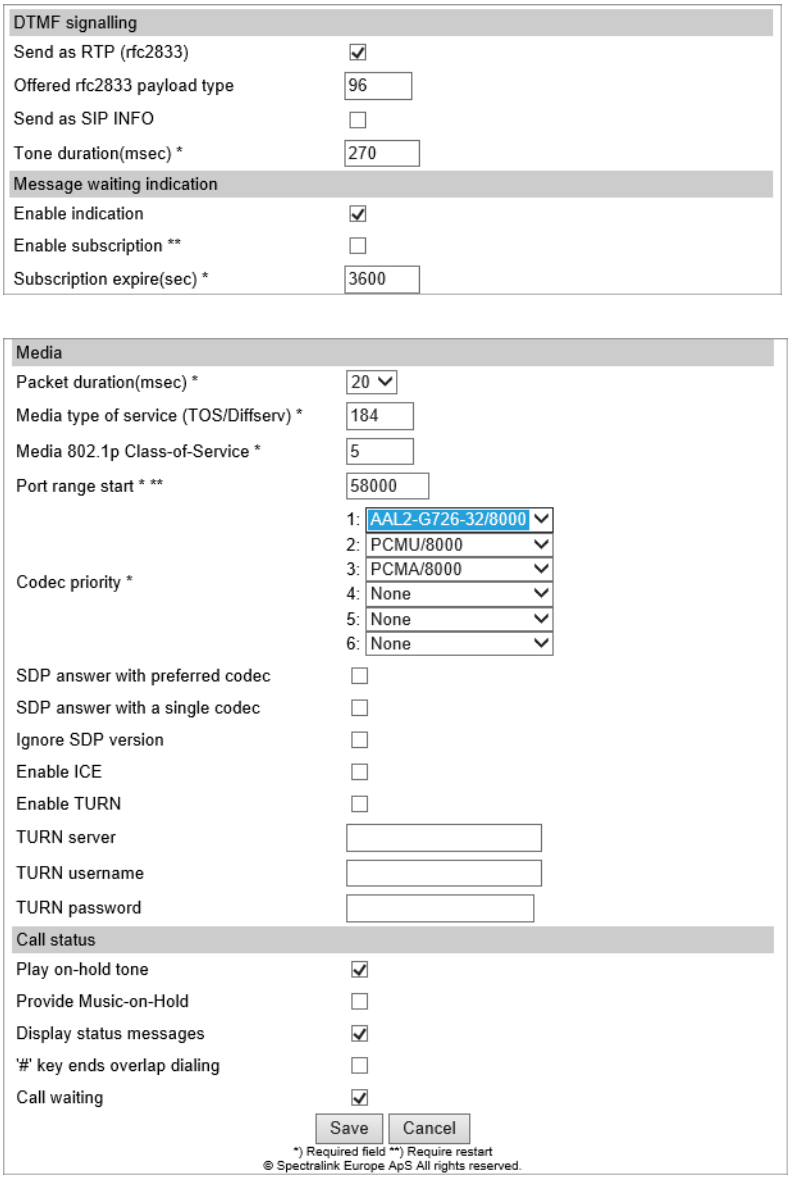
Field	Setting
TLS allow insecure (Optional)	By default, UDP and TCP transports are disabled when TLS transport is the default. If this setting is enabled, UDP and TCP are allowed as fallback if TLS fails. Default value: Disabled
TCP ephemeral port in contact address (Optional)	If enabled, the TCP ephemeral port (the local TCP port of the outgoing connection) to the contact header, used in outgoing SIP messages, is added.
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 user name used for SIP authentication. **Note**: If no handset specific authentication user name/-password is configured, handsets registered on theSpectralink IP-DECT/DECT Server will use the default user name/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 signalling	
Send as RTP (Optional)	If enabled, keypad signaling will be sent as RTP event codes.
Offered RFC2833 payload type	Default value: 96
Send as SIP INFO (Optional)	If enabled, keypad signalling will be sent as SIP INFO messages.

Field	Setting
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/Diff-serv)	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**.
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 end-points.

Field	Setting
Enable media encryption (SRTP) (Only visible if Security (TLS, SRTP) License is loaded) (Optional)	If enabled, external SRTP is supported and optional. It must be negotiated with the remote endpoint. **Note**: If external SRTP is enabled, the number of available voice channels on a Spectralink IP-DECT Server-/media resource is reduced from 32 to 16 (if a codec card is used from 24 to 16). Default value: Enabled
Require media encryption (SRTP) (Only visible if Security (TLS, SRTP) License is loaded) (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
Include lifetime in SDES offers (Only visible if Security (TLS, SRTP) License is loaded) (Optional)	Handles the RFC 4568 SRTP lifetime key parameter in SDP offers. Default value: Disabled
Include MKI in SDES offers (Only visible if Security (TLS, SRTP) License is loaded) (Optional)	Handles the RFC 4568 SRTP Master Key Index Parameter in SDP offers. Default value: Disabled
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 pass word. 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.

Field	Setting
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.




DTMF signalling
Send as RTP (rfc2833)
Offered rfc2833 payload type
96
Send as SIP INFO
Tone duration(msec) *
270
Message waiting indication
Enable indication
Enable subscription **
Subscription expire(sec) *
3600
Media
Packet duration(msec) *
20
Media type of service (TOS/Diffserv) *
184
Media 802.1p Class-of-Service *
5
Port range start * **
58000
Codec priority *
1: AAL2-G726-32/8000
2: PCMU/8000
3: PCMA/8000
4: None
5: None
6: None
SDP answer with preferred codec
SDP answer with a single codec
Ignore SDP version
Enable ICE
Enable TURN
TURN server
TURN username
TURN password
Call status
Play on-hold tone
Provide Music-on-Hold
Display status messages
'#' key ends overlap dialing
Call waiting
Save
Cancel
*) Required field **) Require restart
© Spectralink Europe ApS All rights reserved.

3. Click **Save**.

Configuring Wireless Server Settings

You must configure the Spectralink IP-DECT Server to allow for subscription. If the system does not allow subscription, it is not possible to subscribe handsets.

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	
Wireless Server Configuration - DECT	
Subscription allowed (Optional)	If enabled, it is possible to subscribe new handsets to the system.
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 **Enforced (non GAP)**. Default value: Disabled
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**: It is possible to define a TX power value for a specific base station (**Administration** > **Base Station**).

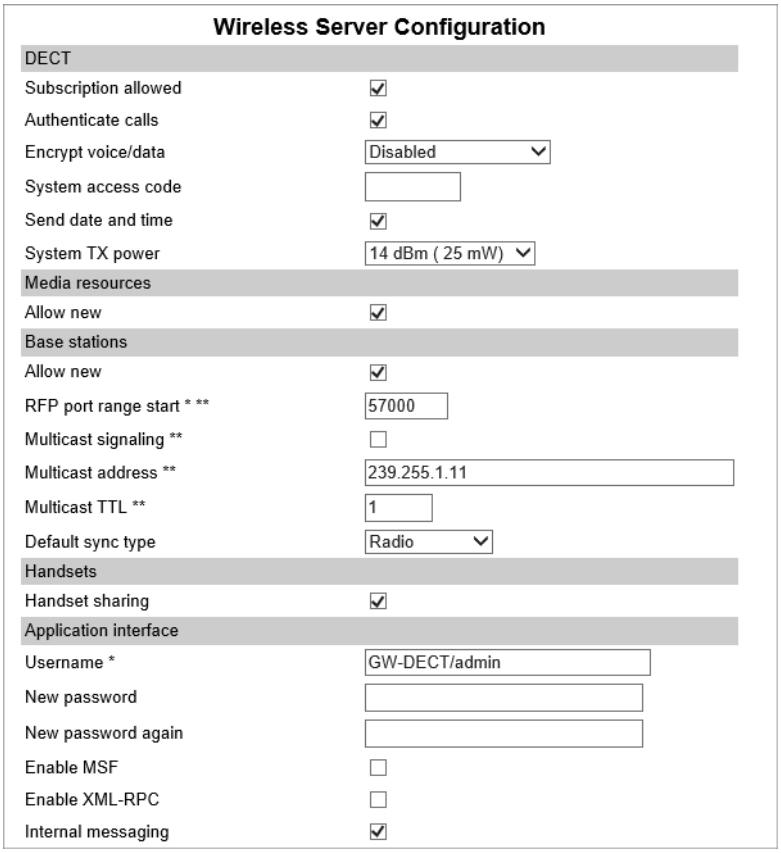
Field	
Wireless Server Configuration - Media resources (Not relevant to the Spectralink IP-DECT Server 200/400)	
Allow new (Optional)	If enabled, new media resources are allowed to connect to the server.
Add new as active (Optional)	If enabled, new media resources will become active when added. Otherwise they must be activated manually under **Administration** > **Media Resource** > **Media Resource** page.
Require encryption (Optional)	If enabled, the connection between the media resource and the Spectralink IP-DECT Server is required to be encrypted. **Note**: Enabling this, will only allow media resources with firmware PCS17Fa or newer to connect. 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.
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.
Require encryption (Optional)	If enabled, the connection between the base station and the Spectralink IP-DECT Server is required to be encrypted. **Note**: Enabling this, will only allow base stations with firmware PCS17Fa or newer to connect. If not enabled, the connection will be encrypted if the base station supports encryption.
RFP port range start	Port range start for RFP local RTP ports. Default value: 57000 **Note**: It is possible to change the value in case of conflicting ports.

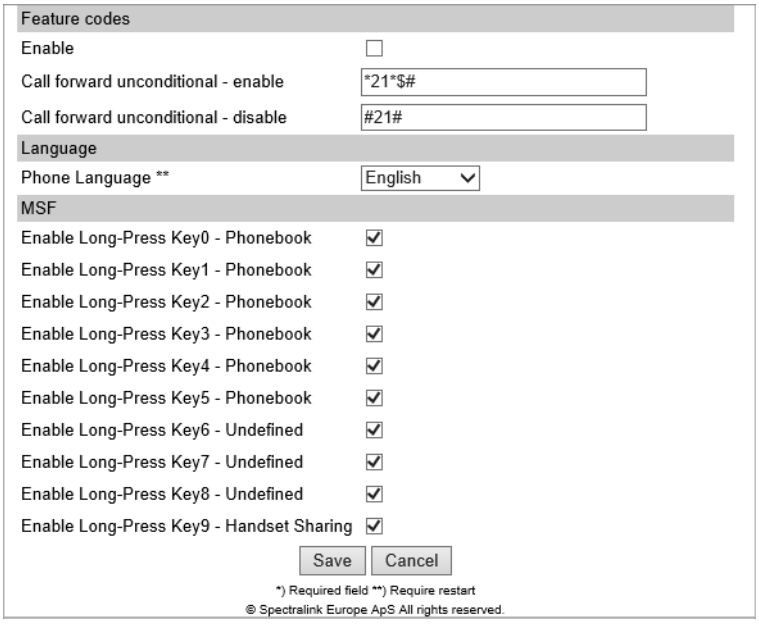
Field	
Multicast signaling (Optional)	Multicast signaling is optimal when having many base stations and is required with more than 256 base stations connected. If enabled, this will impose multicast support for the network. For more information, see "Using Multicast" on page 126.
Multicast address (Optional)	Multicast address used for signaling. Default value: 239.255.1.11 Please refer to RFC2365 and RFC4291 for details.
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 it is possible to change the value according to network topology. For more information, see vendor specific documentation.
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
LAN sync transport protocol (Only visible if license loaded)	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 (License Required)" on page 131.

Field	
LAN sync type of service (TOS/Diff-serv) (Only visible if license loaded)	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)
Wireless Server Configuration - Handsets (Not relevant to the Spectralink IP-DECT Server 200.	
Handset sharing (Optional) (Only visible if license loaded)	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" on page 197.
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 dependant). For more information, see "Configuring Handset Login" on page 202 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.

Field	
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 suported.
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***), including the desired extension. E.g.: ***21*$#** **Note**: It is possible to change the code *21* on the Spectralink IP-DECT Server 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 DECT Server to use this long key press for phone book.
Enable Long-Press Key1- Phonebook (Optional)	If enabled, allow DECT Server to use this long key press for phone book.

Field	
Enable Long-Press Key2 - Phone-book (Optional)	If enabled, allow DECT Server to use this long key press for phone book.
Enable Long-Press Key3 - Phone-book (Optional)	If enabled, allow DECT Server to use this long key press for phone book.
Enable Long-Press Key4 - Phone-book (Optional)	If enabled, allow DECT Server to use this long key press for phone book.
Enable Long-Press Key5 - Phone-book (Optional)	If enabled, allow DECT Server to use this long key press for phone book.
Enable Long-Press Key6 - Undefined (Optional)	If enabled, allow DECT Server to use this long key press.
Enable Long-Press Key7 - Undefined (Optional)	If enabled, allow DECT Server to use this long key press.
Enable Long-Press Key8 - Undefined (Optional)	If enabled, allow DECT Server to use this long key press.
Enable Long-Press Key9 - Hand-set Sharing (Optional)	If enabled, allow DECT Server to use this long key press for handset sharing. For more information, see "Handset Sharing" on page 197 and "User Sign-in/Sign-out" on page 201.


Wireless Server Configuration
DECT
Subscription allowed
Authenticate calls
Encrypt voice/data
Disabled
System access code
Send date and time
System TX power
14 dBm (25 mW)
Media resources
Allow new
Base stations
Allow new
RFP port range start * **
57000
Multicast signaling **
Multicast address **
239.255.1.11
Multicast TTL **
1
Default sync type
Radio
Handsets
Handset sharing
Application interface
Username *
GW-DECT/admin
New password
New password again
Enable MSF
Enable XML-RPC
Internal messaging


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**.

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	
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

3. Click **Save**.

Configuring Certificates

If using TLS as SIP transport method, it is necessary to import a CA certificate into the Spectralink IP-DECT/DECT Server from the web based Administration Page of the server. If using the trusted server functionality in a Lync/SfB environment or using TLS SIP transports in a Cisco Unified CM environment it is also necessary to import a host certificate.

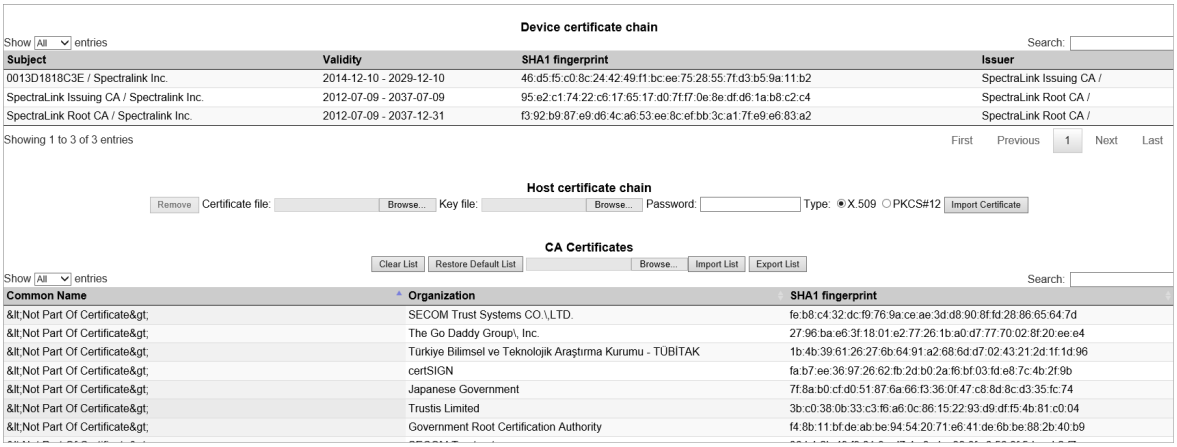
Installing a host certificate also eliminates browser security warnings when accessing the web based Administration Page.

Handling Host and/or CA Certificates

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

Field	
Certificates - Device certificate chain	
	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 certificate chain	
Certificate file	Click **Browse** to find the relevant host certificate file (*.crt file).
Key file	Click **Browse** to find the relevant key file (*.pem file).
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.
Certificates - CA certificates	
	Click **Browse** to find the relevant CA certificate file (*.pem file). E.g. a custom list of CA certificate files.

Field	
	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**).



3. Reboot the server.

For more information about use of TLS, import of certificates and callhandlers, see the relevant Interoperability Guides and Callhandler documentation.

Configuring Clusters

Note:

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

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, it is possible to create clusters (i.e. a cluster 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 cluster as the base station handling the call, avoiding unnecessary RTP traffic over e.g. a WAN connection.

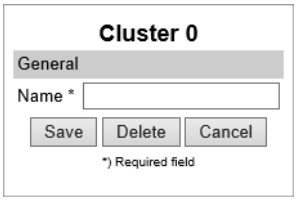
Though assigned to a cluster, the base stations are not forced to use that particular media resource only, it just takes priority over the other media resources in the system setup. If no media channels can be allocated on media resources in the local cluster, media resource from other clusters will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

Defining a Cluster for the Media Resource and Base Stations

Using clusters, you must as minimum define two cluster entities.

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

Field	
Cluster - General	
Name	Enter a name for the cluster. E.g. Site A, Site B, Site C.



4. Click **Save**.

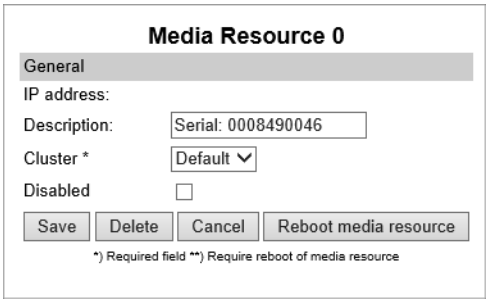
   You can now assign the base stations and media resources to use the relevant clusters.

Assigning Media Resources to Clusters

To make use of the created cluster entities, these must be assigned to the physical media resources and base stations. 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 Cluster field, select the desired cluster:

Field	
Media Resource - General	
IP address (Read only)	Current IP address of the media resource.
Description (Optional)	Enter a description. It is recommended to use a description of the physical location.
Cluster	Default value: Default It is possible to cluster devices that are located at the same location. To assign a cluster to the media resource, select the relevant cluster from the list. For information about defining clusters, see "Configuring Clusters" on the previous page.
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**.
5. Click **Reboot media resource**.

Assigning Base Stations to Clusters

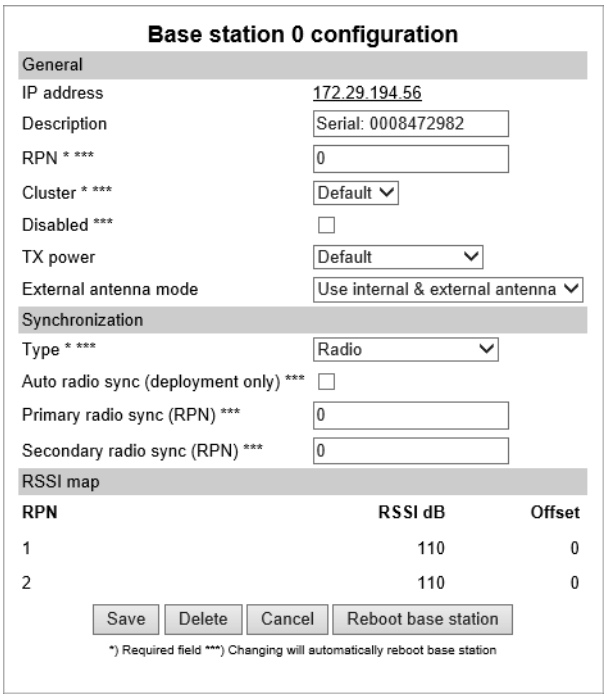
To make use of the created cluster entities, these must be assigned to the physical media resources and base stations. The devices can be both local and remote.

1. Click **Administration**, and then click **Base Station**.
2. On the **Base Stations** page, click on the relevant base station.
3. On the **Base Station** page, under **General** in the Cluster field, select the desired cluster:

Field	
Base Station - General	
IP address (Read only)	Current IP address of the base station.
Description (Optional)	Enter a description. It is recommended to use a description of the physical location.
RPN	Radio Part Number of the base station.
Cluster	Default value: Default It is possible to cluster devices that are located at the same location. To assign a cluster to the base station, select the relevant cluster from the list. For information about defining clusters, see "Configuring Clusters" on page 118.
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) **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	
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**: 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.

Field	
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**.
5. Click **Reboot base station**.

Assigning Server Address to Spectralink IP-DECT Base Station and Spectralink DECT Media Resource

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 through the web based Administration Page using either dynamic IP address (DHCP) or static IP address.

Note:

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

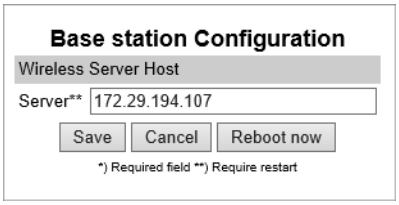
It is recommended that you configure the base station using DHCP. When using DHCP components should be discovered by UPnP. For more information, see "Discovering the Spectralink IP-DECT Components via UPnP" on page 87.

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 Server 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
Media Resource - Wireless Server Host	
Server	Enter the address of the Spectralink IP-DECT Server that the media resource must connect to.

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

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 ways 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 ways of the base station can be determined using one of the following 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)

  For more information about ordering and downloading a license, see "Ordering Licenses" on page 43 and "Loading Licenses" on page 43.

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 it is possible to 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, it is possible to:

- check the synchronization state of the of the base station. For more information, see "Checking Sync State of Spectralink IP-DECT Base Station" on page 138.
- check for loops in the synchronization chain. For more information, see "Checking for Loops" on page 138.

Using Multicast

Spectralink IP-DECT Base Stations will use IP multicast signaling in two different configurations; LAN based synchronization and if using more than 256 Spectralink IP-DECT Base Stations.

LAN Based Synchronization

- LAN Synchronisation 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.

Installation of more than 256 Spectralink IP-DECT Base Stations

When more than 256 Spectralink IP-DECT Base Stations is connected to a Spectralink IP-DECT 6500 Server, it is required to enable Multicast signaling.

- Multicast for more than 256 Spectralink IP-DECT Base Stations 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 256 base Spectralink IP-DECT Base Stations is designed for the scalability of large networks. Though multicast is required when using more than 256 Spectralink IP-DECT Base Stations it is also possible to use it on fewer Spectralink IP-DECT Base Stations.

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.

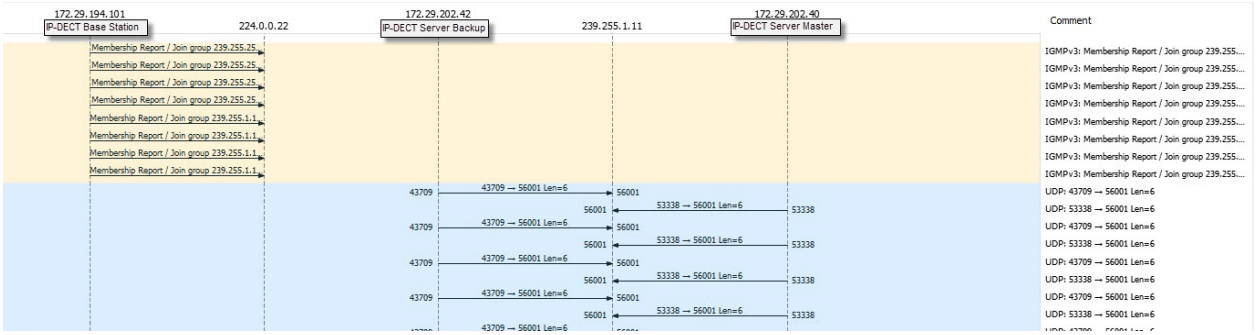
Note:

When using IGMP snooping for managing the multicast traffic in the network infra-structure, 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 Server 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 Server 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 signalling between server and base station.

When an incoming call is received in the Spectralink IP-DECT Server, 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 recive 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 Server. Hereafter, the call setup will be transmitted between server and base station as unicast traffic.

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" on page 123.

- Automatically when using DHCP and UpNP (recommended).

  For more information, see "Discovering the Spectralink IP-DECT Components via UPnP" on page 87.

Radio Based Synchronization

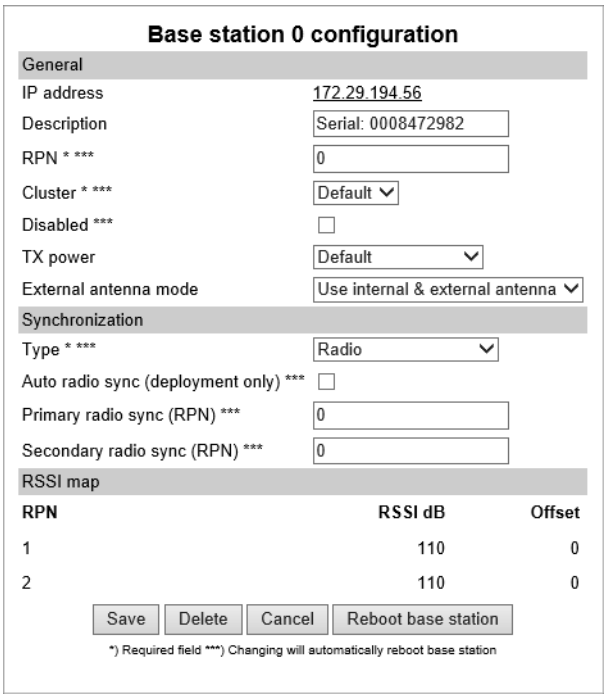
You define the sync. ways of the Spectralink IP-DECT Base Station through the web based Administration Page of the Spectralink IP-DECT Server.

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

Field	
Base Station - General	
IP address (Read only)	Current IP address of the base station.
Description (Optional)	Enter a description. It is recommended to use a description of the physical location.
RPN	Radio Part Number of the base station.
Cluster	Default value: Default It is possible to cluster devices that are located at the same location. To assign a cluster to the base station, select the relevant cluster from the list. For information about defining clusters, see "Configuring Clusters" on page 118.
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) **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	
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**: 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.

Field	
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**.

LAN Based Synchronization (License Required)

The LAN based synchronization has several advantages over synchronizing 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 Server are used to control base station synchronization via LAN.

To define system wide settings:

1. Click **Configuration**, 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	
Wireless Server Configuration - DECT	
Subscription allowed (Optional)	If enabled, it is possible to subscribe new handsets to the system.
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 **Enforced (non GAP)**. Default value: Disabled
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**: It is possible to define a TX power value for a specific base station (**Administration** > **Base Station**).
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.

Field	
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.
Require encryption (Optional)	If enabled, the connection between the media resource and the Spectralink IP-DECT Server is required to be encrypted. **Note**: Enabling this, will only allow media resources with firmware PCS17Fa or newer to connect. 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.
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.
Require encryption (Optional)	If enabled, the connection between the base station and the Spectralink IP-DECT Server is required to be encrypted. **Note**: Enabling this, will only allow base stations with firmware PCS17Fa or newer to connect. If not enabled, the connection will be encrypted if the base station supports encryption.
RFP port range start	Port range start for RFP local RTP ports. Default value: 57000 **Note**: It is possible to change the value in case of conflicting ports.

Field	
Multicast signaling (Optional)	Multicast signaling is optimal when having many base stations and is required with more than 256 base stations connected. If enabled, this will impose multicast support for the network. For more information, see "Using Multicast" on page 126.
Multicast address (Optional)	Multicast address used for signaling. Default value: 239.255.1.11 Please refer to RFC2365 and RFC4291 for details.
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 it is possible to change the value according to network topology. For more information, see vendor specific documentation.
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
LAN sync transport protocol (Only visible if license loaded)	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 (License Required)" on page 131.

Field	
LAN sync type of service (TOS/Diff-serv) (Only visible if license loaded)	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)
Wireless Server Configuration - Handsets (Not relevant to the Spectralink IP-DECT Server 200.	
Handset sharing (Optional) (Only visible if license loaded)	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" on page 197.
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 dependant). For more information, see "Configuring Handset Login" on page 202 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.

Field	
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 suported.
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***), including the desired extension. E.g.: ***21*$#** **Note**: It is possible to change the code *21* on the Spectralink IP-DECT Server 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 DECT Server to use this long key press for phone book.
Enable Long-Press Key1- Phonebook (Optional)	If enabled, allow DECT Server to use this long key press for phone book.
Enable Long-Press Key2 - Phonebook (Optional)	If enabled, allow DECT Server to use this long key press for phone book.

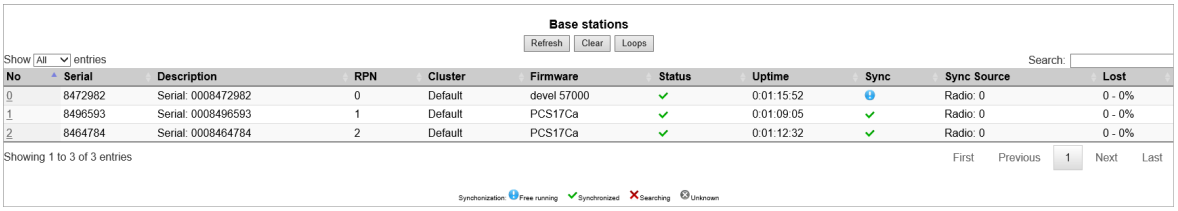
Field	
Enable Long-Press Key3 - Phone-book (Optional)	If enabled, allow DECT Server to use this long key press for phone book.
Enable Long-Press Key4 - Phone-book (Optional)	If enabled, allow DECT Server to use this long key press for phone book.
Enable Long-Press Key5 - Phone-book (Optional)	If enabled, allow DECT Server to use this long key press for phone book.
Enable Long-Press Key6 - Undefined (Optional)	If enabled, allow DECT Server to use this long key press.
Enable Long-Press Key7 - Undefined (Optional)	If enabled, allow DECT Server to use this long key press.
Enable Long-Press Key8 - Undefined (Optional)	If enabled, allow DECT Server to use this long key press.
Enable Long-Press Key9 - Hand-set Sharing (Optional)	If enabled, allow DECT Server to use this long key press for handset sharing. For more information, see "Handset Sharing" on page 197 and "User Sign-in/Sign-out" on page 201.

Click **Save**.

Checking Sync State of Spectralink IP-DECT Base Station

You can get information about the synchronization 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 Server. 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 for Loops

As part of troubleshooting it is possible to check if loops have accidently 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.

Registering Users and Subscribing Spectralink DECT 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.

  For more information about the handsets serial number, see "Identifying IPEI on Spectralink Handset" on page 48.

- 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.

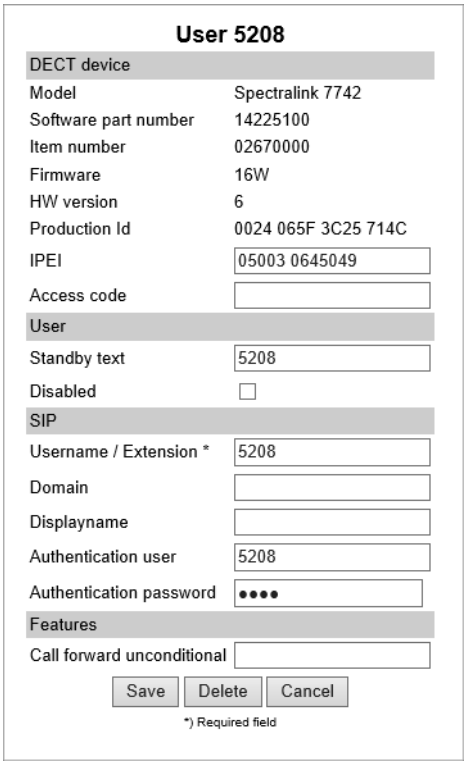
To Register/Create a New User

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	
Model	After registration of user and subscription of handset, this field will contain information about the handset model. E.g. Spectralink7742
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. PCSJA.

Field	Setting
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" on page 209.
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 phones may need an Access code to register to the Spectralink IP-DECT Server.
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" on page 201. See also Lync/Skype for Business Interoperability Guide.
Standby text (Optional)	Enter a standby text. 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.

Field	Setting
User - SIP	
Username/Extension	Must contain information used for SIP registration etc. E.g. the "user" in a SIP URI.
Domain (Optional)	Enter the domain part of a SIP URI. 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). 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 **5208**. **Note**: The user name 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. User name set for individual users
Authentication password (Optional)	Enter the digest credential of the end user. **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.



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 Server 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" on page 108.

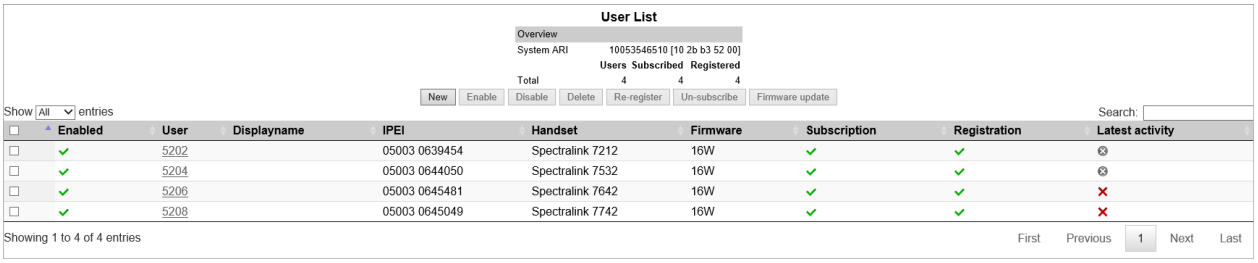
You subscribe a handset by creating a login (**Menu** > **Settings** > **Advanced** > **Login**).

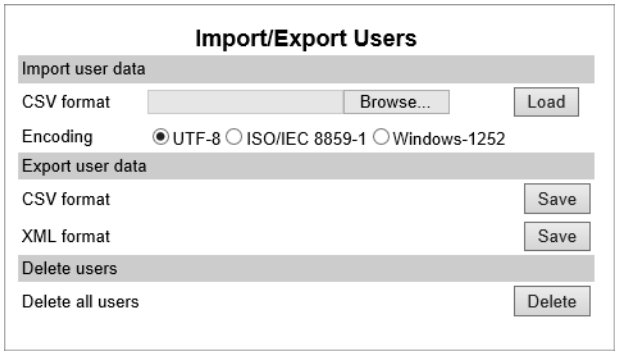
For more information, see the relevant Handset User Guides.

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**.
- Import and export of user data can be performed from **web based Administration Page** > **Users** > **Import/Export**.





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

User List Information

From the **User List** page it is possible to get an overview of the following:

- System ARI - the system the user is subscribed to.
- Enabled - if user/handset is enabled.
- User - SIP account user name/extension
- Displayname - 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 Server.
- 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
- Nodes (only relevant if using redundancy server) - indicates if handset is subscribed on the master server or backup server.

Note:

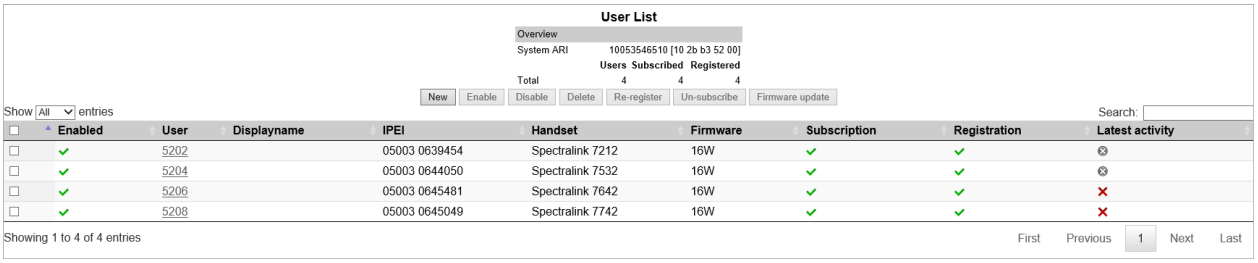
You can sort the information by clicking each header.

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
- search handset/user information
- enable/disable users
- delete users
- re-register users
- un-subscribe users
- update firmware in the handsets
- deregister a handset



Note:

You can also create users from the **User List**. For more information, see "Registering a User" on page 139.

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**.

   The list will show all entries as default. It is possible to search for information.

2. Click on the relevant user to change user configurations, such as the AC (authentication code). For more information, see "Registering Users and Subscribing Spectralink DECT Handsets" on page 139.
3. If changing user configuration settings, click **Save**.

To Search Handset/User Information

You can search for a registered handset/user in the system through the web based Administration Page.

1. Click **Users**, and then click **List Users**.
2. 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 Un-subscribe User

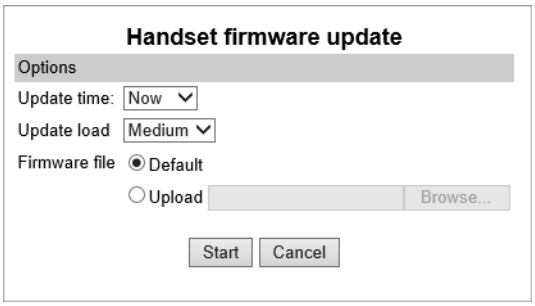
You can unsubscribe a handset from the system.

1. Click **Users**, and then click **List Users**.
2. On the **User List** page, select the relevant user(s) from the list.
3. Click **Un-subscribe**.
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**.



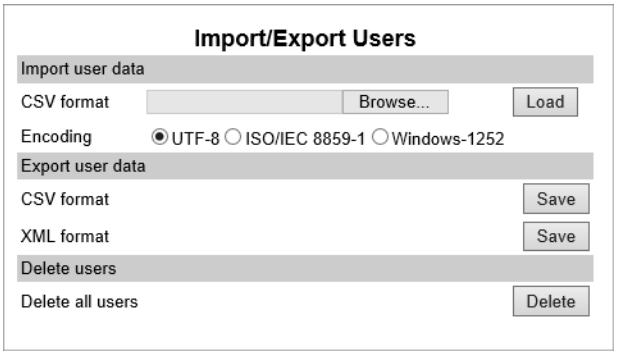
5. Click **Start**.

Import/Export of Users or Delete Users

From the **Import/Export** page it is possible to 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 "Example of Handset Registration Data - CSV Format" on the next page.
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**.



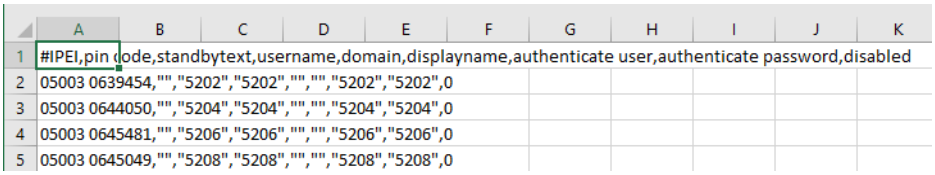
Example of Handset Registration Data - CSV Format

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" on page 147.

Note:

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

System Management

Through the web based Administration Page of the Spectralink IP-DECT Server it is possible to 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
- Import/Export configuration file
- delete license
- configure different system settings - for more information, see "Configuration Steps Overview" on page 82.

Note:

System software can also be updated through provisioning. Besides provisioning of the server configuration file, you can also provision firmware files for base stations, media resources and handsets. For more information, see Provisioning Guide.

Making a Back-Up and Restore of System

Through the web based Administration Page of the Spectralink IP-DECT Server it is possible to save the following data:

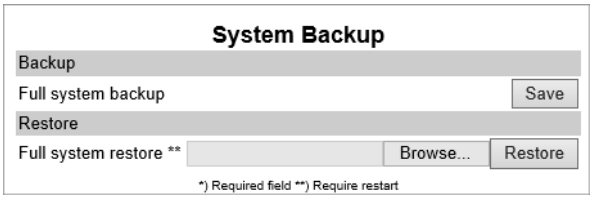
- configuration data of the Spectralink IP-DECT Server
- registration and subscription data of the users and handsets
- system information

When saving the configuration data, you have an overall overview of the Spectralink IP-DECT Server 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 Server, Spectralink IP-DECT Base Station and Spectralink DECT Media Resource firmware can be updated the following ways:

- Using the web based Administration Page of the Spectralink IP-DECT Server.
- Provisioning. For more information, see Provisioning Guide.

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 Server.
- 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.

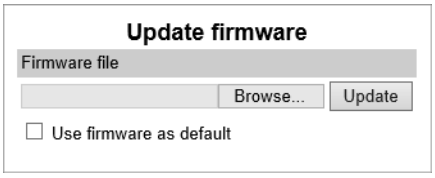
  For more information about the Handset Management Cradle and Handset and Repeater Management Tool, see Handset User Guides and Handset and Repeater Management Tool User Guide.
- Provisioning. For more information, see Provisioning Guide.

Note:

Before updating system software, always make a backup of the configuration. For more information, see "Making a Back-Up and Restore of System" on the previous page.

To Update Spectralink IP-DECT Server Firmware

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



2. On the **Update firmware** page, click **Browse** to find the relevant firmware file.

   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**.

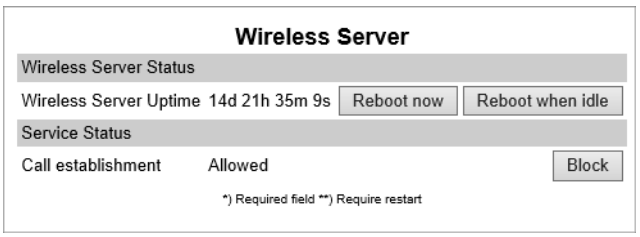
   Wait until the system has finished updating.

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.

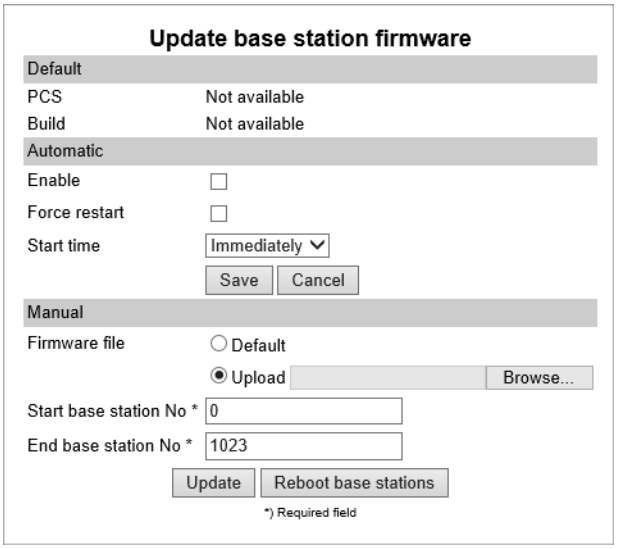
Note:

Base stations can use default firmware, if selected when server firmware is uploaded. For more information, see "To Update Spectralink IP-DECT Server Firmware" on the previous page.

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	
PCS	Information about default firmware file version (PCS) - if a firmware file has 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.
Build	Information about the build number of default firmware file - if a default firmware file has been uploaded.

Field	Setting
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**: 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. Select either **Default** or **Upload**.
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 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.

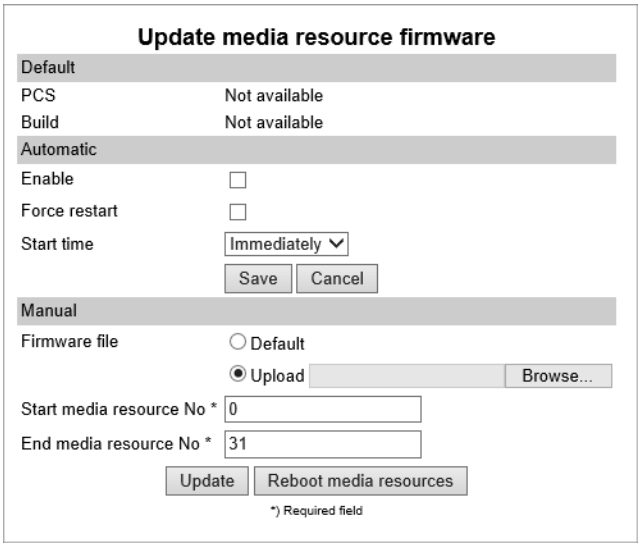
Note:

Media resources can use default firmware, if selected when server firmware is uploaded. For more information, see "To Update Spectralink IP-DECT Server Firmware" on page 153.

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	
PCS	Information about default firmware file version (PCS) - if a firmware file has 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.
Build	Information about the build number of default firmware file - if a default firmware file has been uploaded.

Field	Setting
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**.
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. Select either **Default** or **Upload**.
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 can be rebooted manually after they have been updated.

To Update Spectralink DECT Handset Firmware Over The Air (SUOTA)

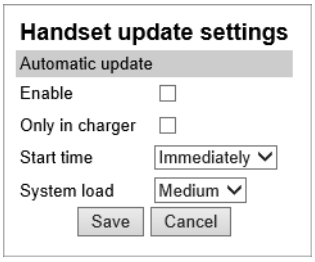
Note:

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.



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.

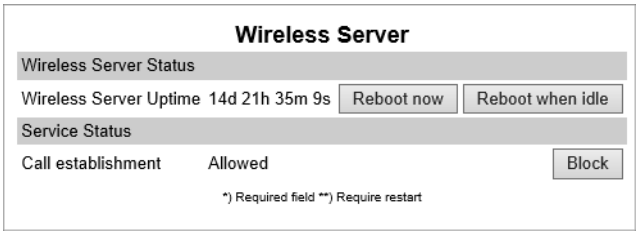
If battery level in handset is low, then the handset will refuse the update request.

Restarting System or Block Calls during Firmware Update

Through the web based Administration Page of the Spectralink IP-DECT Server it is possible to restart he Spectralink IP-DECT Server 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 Server it is possible to read the following system information:

- General status
- Logs Information
- Wireless Server Information

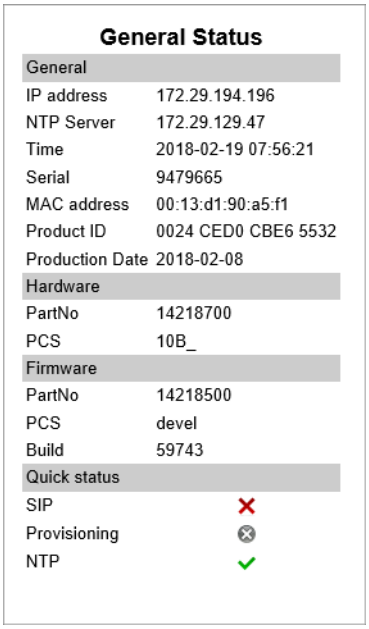
- Statistics (Wireless Server, Media Resource, Base Station, Active Calls, Abnormal Releases, Traffic Distribution)

General Status Information

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

1. Click **Status**, and then click **General**. The **General Status** page appears.

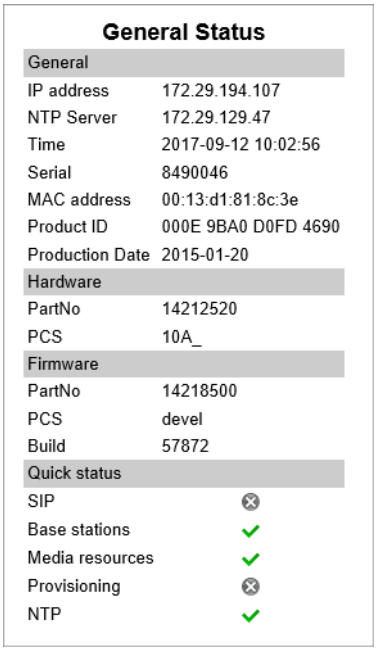
   Example from Spectralink IP-DECT Server 200:



General Status

General	
IP address	172.29.194.196
NTP Server	172.29.129.47
Time	2018-02-19 07:56:21
Serial	9479665
MAC address	00:13:d1:90:a5:f1
Product ID	0024 CED0 CBE6 5532
Production Date	2018-02-08
Hardware	
PartNo	14218700
PCS	10B_
Firmware	
PartNo	14218500
PCS	devel
Build	59743
Quick status	
SIP	✗
Provisioning	⊗
NTP	✓

   Example from Spectralink IP-DECT Server 6500:



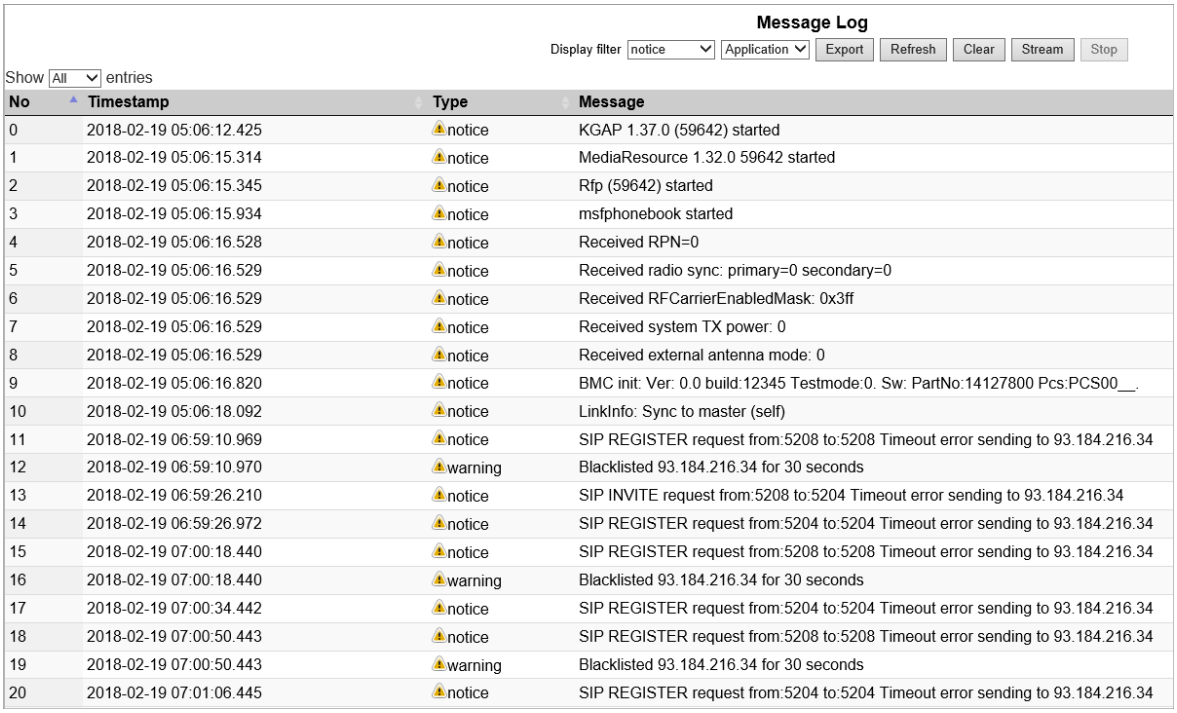
General Status

General	
IP address	172.29.194.107
NTP Server	172.29.129.47
Time	2017-09-12 10:02:56
Serial	8490046
MAC address	00:13:d1:81:8c:3e
Product ID	000E 9BA0 D0FD 4690
Production Date	2015-01-20
Hardware	
PartNo	14212520
PCS	10A_
Firmware	
PartNo	14218500
PCS	devel
Build	57872
Quick status	
SIP	⊗
Base stations	✓
Media resources	✓
Provisioning	⊗
NTP	✓

Logs Information

This page provides log information such as media resource connection, base station connection and different types of status.

1. Click **Status**, and then click **Logs**. The **Message Log** page appears.



Message Log

Display filter notice Application Export Refresh Clear Stream Stop

Show All entries

No	Timestamp	Type	Message
0	2018-02-19 05:06:12.425	notice	KGAP 1.37.0 (59642) started
1	2018-02-19 05:06:15.314	notice	MediaResource 1.32.0 59642 started
2	2018-02-19 05:06:15.345	notice	Rfp (59642) started
3	2018-02-19 05:06:15.934	notice	msfphonebook started
4	2018-02-19 05:06:16.528	notice	Received RPN=0
5	2018-02-19 05:06:16.529	notice	Received radio sync: primary=0 secondary=0
6	2018-02-19 05:06:16.529	notice	Received RFCarrierEnabledMask: 0x3ff
7	2018-02-19 05:06:16.529	notice	Received system TX power: 0
8	2018-02-19 05:06:16.529	notice	Received external antenna mode: 0
9	2018-02-19 05:06:16.820	notice	BMC init: Ver: 0.0 build:12345 Testmode:0. Sw: PartNo:14127800 Pcs:PCS00__.
10	2018-02-19 05:06:18.092	notice	LinkInfo: Sync to master (self)
11	2018-02-19 06:59:10.969	notice	SIP REGISTER request from:5208 to:5208 Timeout error sending to 93.184.216.34
12	2018-02-19 06:59:10.970	warning	Blacklisted 93.184.216.34 for 30 seconds
13	2018-02-19 06:59:26.210	notice	SIP INVITE request from:5208 to:5204 Timeout error sending to 93.184.216.34
14	2018-02-19 06:59:26.972	notice	SIP REGISTER request from:5204 to:5204 Timeout error sending to 93.184.216.34
15	2018-02-19 07:00:18.440	notice	SIP REGISTER request from:5208 to:5208 Timeout error sending to 93.184.216.34
16	2018-02-19 07:00:18.440	warning	Blacklisted 93.184.216.34 for 30 seconds
17	2018-02-19 07:00:34.442	notice	SIP REGISTER request from:5204 to:5204 Timeout error sending to 93.184.216.34
18	2018-02-19 07:00:50.443	notice	SIP REGISTER request from:5208 to:5208 Timeout error sending to 93.184.216.34
19	2018-02-19 07:00:50.443	warning	Blacklisted 93.184.216.34 for 30 seconds
20	2018-02-19 07:01:06.445	notice	SIP REGISTER request from:5204 to:5204 Timeout error sending to 93.184.216.34

2. 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.

Note:

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.

It is possible to clear the message log buffer for **Application** logs. The **Audit** log cannot be deleted - except when performing a factory reset.

It is possible to stream an **Application** log, whereas an **Audit** log cannot be streamed.

The different types of status are:

- emergency (errors causing the system to malfunction for all calls)
- critical (events that do not occur under normal operation, 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)

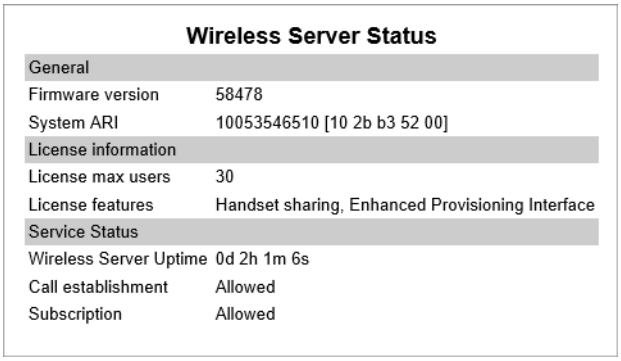
- notice info (events that occur under normal operation)

3. 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 Server.

1. Click **Status**, and then click **Wireless Server**. The **Wireless Server Status** page appears.



Wireless Server Status

General	
Firmware version	58478
System ARI	10053546510 [10 2b b3 52 00]
License information	
License max users	30
License features	Handset sharing, Enhanced Provisioning Interface
Service Status	
Wireless Server Uptime	0d 2h 1m 6s
Call establishment	Allowed
Subscription	Allowed

Statistics

On this page you can get an over all overview of how the system is running.

You can get statistics of the following:

- Wireless Server
- Media Resource
- Base Station
- Active Calls
- Abnormal Releases
- Traffic Distribution

Note:

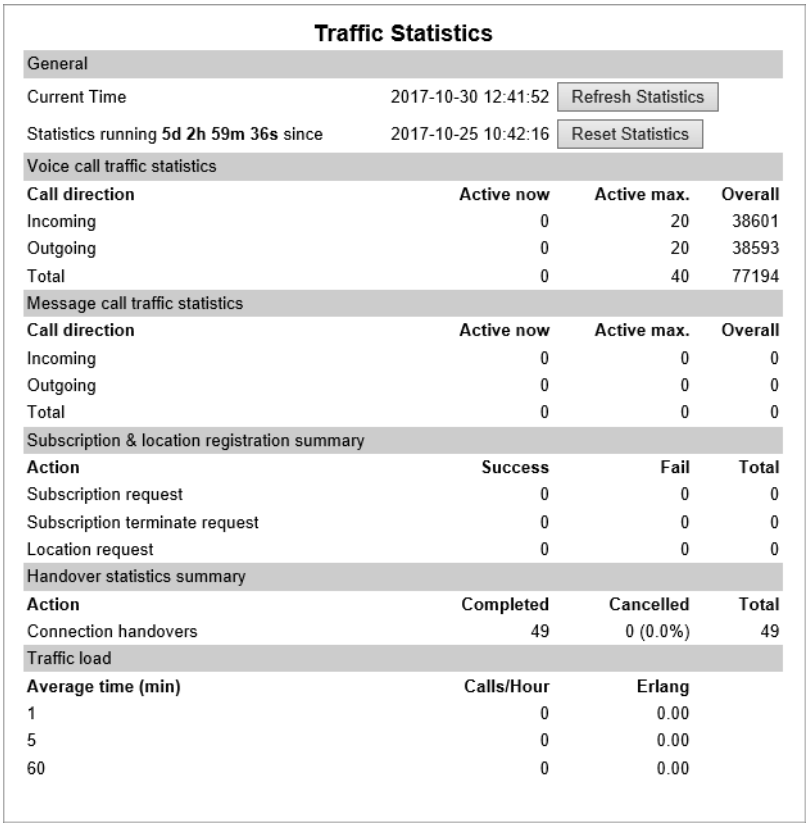
For more in depth information and to gain access to the Spectralink training material, you must attend training and become Spectralink Certified Specialist.

Please visit http://partneraccess.spectralink.com/training/classroom-training for more information and registration.

Statistics of Wireless Server

This page is useful to get information about traffic on the Spectralink IP-DECT Server 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 **Wireless Server**. The **Trafic Statistics** page appears.



Traffic Statistics

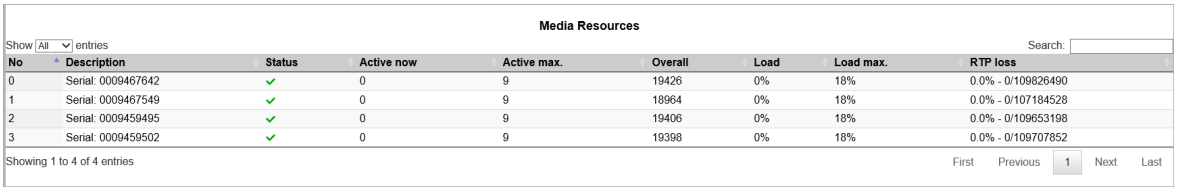
General			
Current Time	2017-10-30 12:41:52	Refresh Statistics	
Statistics running **5d 2h 59m 36s** since	2017-10-25 10:42:16	Reset Statistics	
Voice call traffic statistics			
Call direction	**Active now**	**Active max.**	**Overall**
Incoming	0	20	38601
Outgoing	0	20	38593
Total	0	40	77194
Message call traffic statistics			
Call direction	**Active now**	**Active max.**	**Overall**
Incoming	0	0	0
Outgoing	0	0	0
Total	0	0	0
Subscription & location registration summary			
Action	**Success**	**Fail**	**Total**
Subscription request	0	0	0
Subscription terminate request	0	0	0
Location request	0	0	0
Handover statistics summary			
Action	**Completed**	**Cancelled**	**Total**
Connection handovers	49	0 (0.0%)	49
Traffic load			
Average time (min)	**Calls/Hour**	**Erlang**	
1	0	0.00	
5	0	0.00	
60	0	0.00	

You can delete all statistic traffic information by clicking **Reset Statistics**.

Statistics of Media Resource

This page is useful to get statistical information about the media resource.

- Click **Statistics**, and then click **Media Resource**. The **Media Resources** page appears.



Media Resources

Show All entries Search:

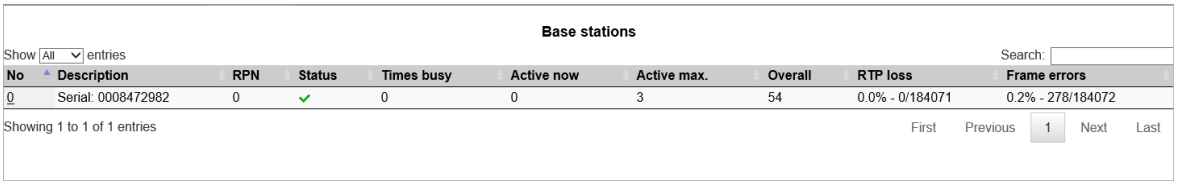
No	Description	Status	Active now	Active max.	Overall	Load	Load max.	RTP loss
0	Serial: 0009467642	✓	0	9	19426	0%	18%	0.0% - 0/109826490
1	Serial: 0009467549	✓	0	9	18964	0%	18%	0.0% - 0/107184528
2	Serial: 0009459495	✓	0	9	19406	0%	18%	0.0% - 0/109653198
3	Serial: 0009459502	✓	0	9	19398	0%	18%	0.0% - 0/109707852

Showing 1 to 4 of 4 entries First Previous 1 Next Last

Statistics of Base Station

This page is useful to get statistical information about the base station.

- Click **Statistics**, and then click **Base Station**. The **Base Stations** page appears.



Base stations

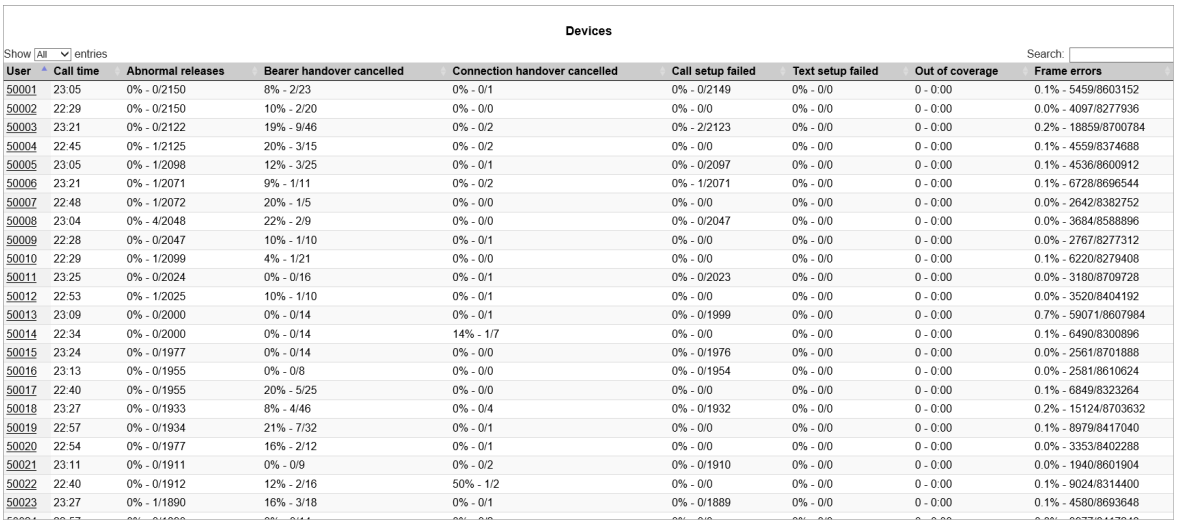
Show All entries Search:

No	Description	RPN	Status	Times busy	Active now	Active max.	Overall	RTP loss	Frame errors
0	Serial: 0008472982	0	✔	0	0	3	54	0.0% - 0/184071	0.2% - 278/184072

Showing 1 to 1 of 1 entries First Previous 1 Next Last

Statistics of Devices

- Click **Statistics**, and then click **Device**. The **Devices** page appears.



Devices

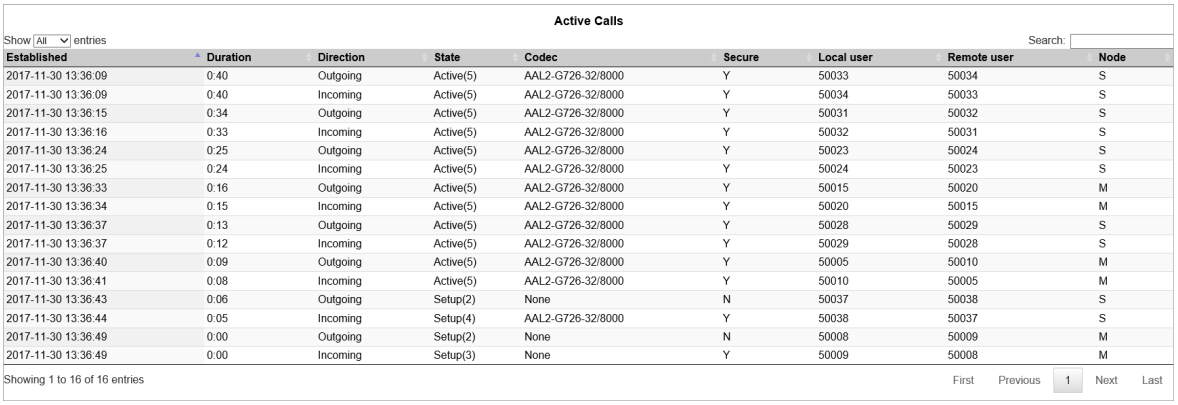
Show All entries Search:

User	Call time	Abnormal releases	Bearer handover cancelled	Connection handover cancelled	Call setup failed	Text setup failed	Out of coverage	Frame errors
50001	23:05	0% - 0/2150	8% - 2/23	0% - 0/1	0% - 0/2149	0% - 0/0	0 - 0:00	0.1% - 5459/8603152
50002	22:29	0% - 0/2150	10% - 2/20	0% - 0/0	0% - 0/0	0% - 0/0	0 - 0:00	0.0% - 4097/8277936
50003	23:21	0% - 0/2122	19% - 9/46	0% - 0/2	0% - 2/2123	0% - 0/0	0 - 0:00	0.2% - 18859/8700784
50004	22:45	0% - 1/2125	20% - 3/15	0% - 0/2	0% - 0/0	0% - 0/0	0 - 0:00	0.1% - 4559/8374688
50005	23:05	0% - 1/2098	12% - 3/25	0% - 0/1	0% - 0/2097	0% - 0/0	0 - 0:00	0.1% - 4536/8600912
50006	23:21	0% - 1/2071	9% - 1/11	0% - 0/2	0% - 1/2071	0% - 0/0	0 - 0:00	0.1% - 6728/8696544
50007	22:48	0% - 1/2072	20% - 1/5	0% - 0/0	0% - 0/0	0% - 0/0	0 - 0:00	0.0% - 2642/8382752
50008	23:04	0% - 4/2048	22% - 2/9	0% - 0/0	0% - 0/2047	0% - 0/0	0 - 0:00	0.0% - 3684/8588896
50009	22:28	0% - 0/2047	10% - 1/10	0% - 0/1	0% - 0/0	0% - 0/0	0 - 0:00	0.0% - 2767/8277312
50010	22:29	0% - 1/2099	4% - 1/21	0% - 0/0	0% - 0/0	0% - 0/0	0 - 0:00	0.1% - 6220/8279408
50011	23:25	0% - 0/2024	0% - 0/16	0% - 0/1	0% - 0/2023	0% - 0/0	0 - 0:00	0.0% - 3180/8709728
50012	22:53	0% - 1/2025	10% - 1/10	0% - 0/1	0% - 0/0	0% - 0/0	0 - 0:00	0.0% - 3520/8404192
50013	23:09	0% - 0/2000	0% - 0/14	0% - 0/1	0% - 0/1999	0% - 0/0	0 - 0:00	0.7% - 59071/8607984
50014	22:34	0% - 0/2000	0% - 0/14	14% - 1/7	0% - 0/0	0% - 0/0	0 - 0:00	0.1% - 6490/8300896
50015	23:24	0% - 0/1977	0% - 0/14	0% - 0/0	0% - 0/1976	0% - 0/0	0 - 0:00	0.0% - 2561/8701888
50016	23:13	0% - 0/1955	0% - 0/8	0% - 0/0	0% - 0/1954	0% - 0/0	0 - 0:00	0.0% - 2581/8610624
50017	22:40	0% - 0/1955	20% - 5/25	0% - 0/0	0% - 0/0	0% - 0/0	0 - 0:00	0.1% - 6849/8323264
50018	23:27	0% - 0/1933	8% - 4/46	0% - 0/4	0% - 0/1932	0% - 0/0	0 - 0:00	0.2% - 15124/8703632
50019	22:57	0% - 0/1934	21% - 7/32	0% - 0/1	0% - 0/0	0% - 0/0	0 - 0:00	0.1% - 8979/8417040
50020	22:54	0% - 0/1977	16% - 2/12	0% - 0/1	0% - 0/0	0% - 0/0	0 - 0:00	0.0% - 3353/8402288
50021	23:11	0% - 0/1911	0% - 0/9	0% - 0/2	0% - 0/1910	0% - 0/0	0 - 0:00	0.0% - 1940/8601904
50022	22:40	0% - 0/1912	12% - 2/16	50% - 1/2	0% - 0/0	0% - 0/0	0 - 0:00	0.1% - 9024/8314400
50023	23:27	0% - 1/1890	16% - 3/18	0% - 0/1	0% - 0/1889	0% - 0/0	0 - 0:00	0.1% - 4580/8693648

- Following columns contain important information about system performance:
  - Abnormal releases
  - Connection handover cancelled
  - Call setup failed
  - Frame errors

Statistics of Active Calls

- Click **Statistics**, and then click **Active Calls**. The **Active Calls** page appears.



Active Calls

Show All entries Search:

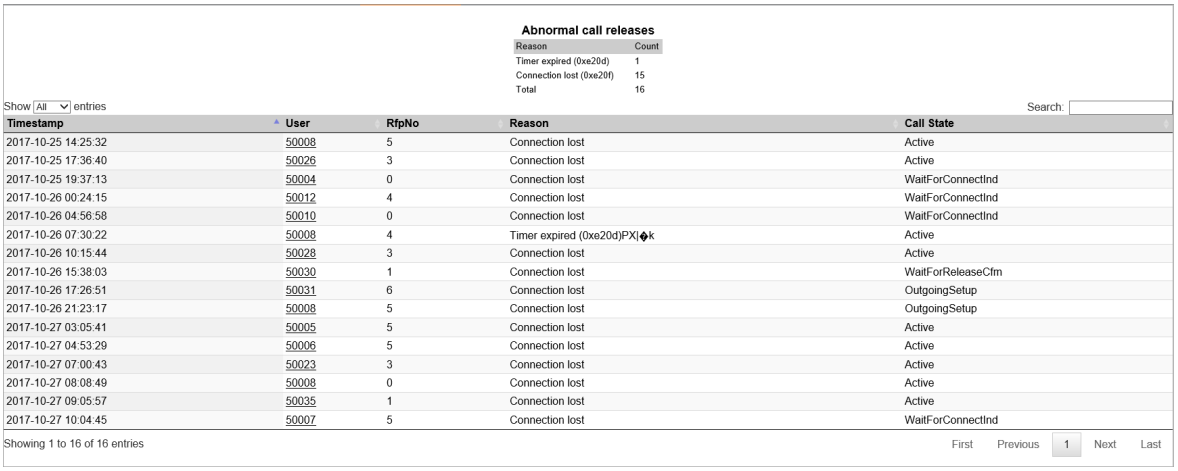
Established	Duration	Direction	State	Codec	Secure	Local user	Remote user	Node
2017-11-30 13:36:09	0:40	Outgoing	Active(5)	AAL2-G726-32/8000	Y	50033	50034	S
2017-11-30 13:36:09	0:40	Incoming	Active(5)	AAL2-G726-32/8000	Y	50034	50033	S
2017-11-30 13:36:15	0:34	Outgoing	Active(5)	AAL2-G726-32/8000	Y	50031	50032	S
2017-11-30 13:36:16	0:33	Incoming	Active(5)	AAL2-G726-32/8000	Y	50032	50031	S
2017-11-30 13:36:24	0:25	Outgoing	Active(5)	AAL2-G726-32/8000	Y	50023	50024	S
2017-11-30 13:36:25	0:24	Incoming	Active(5)	AAL2-G726-32/8000	Y	50024	50023	S
2017-11-30 13:36:33	0:16	Outgoing	Active(5)	AAL2-G726-32/8000	Y	50015	50020	M
2017-11-30 13:36:34	0:15	Incoming	Active(5)	AAL2-G726-32/8000	Y	50020	50015	M
2017-11-30 13:36:37	0:13	Outgoing	Active(5)	AAL2-G726-32/8000	Y	50028	50029	S
2017-11-30 13:36:37	0:12	Incoming	Active(5)	AAL2-G726-32/8000	Y	50029	50028	S
2017-11-30 13:36:40	0:09	Outgoing	Active(5)	AAL2-G726-32/8000	Y	50005	50010	M
2017-11-30 13:36:41	0:08	Incoming	Active(5)	AAL2-G726-32/8000	Y	50010	50005	M
2017-11-30 13:36:43	0:06	Outgoing	Setup(2)	None	N	50037	50038	S
2017-11-30 13:36:44	0:05	Incoming	Setup(4)	AAL2-G726-32/8000	Y	50038	50037	S
2017-11-30 13:36:49	0:00	Outgoing	Setup(2)	None	N	50008	50009	M
2017-11-30 13:36:49	0:00	Incoming	Setup(3)	None	Y	50009	50008	M

Showing 1 to 16 of 16 entries First Previous 1 Next Last

Statistics of Abnormal Releases

This page is useful to get statistical information about abnormal releases.

- Click **Statistics**, and then click **Abnormal Releases**. The **Abnormal call releases** page appears.



Abnormal call releases

Reason	Count
Timer expired (0xe20d)	1
Connection lost (0xe20f)	15
Total	16

Show All entries Search:

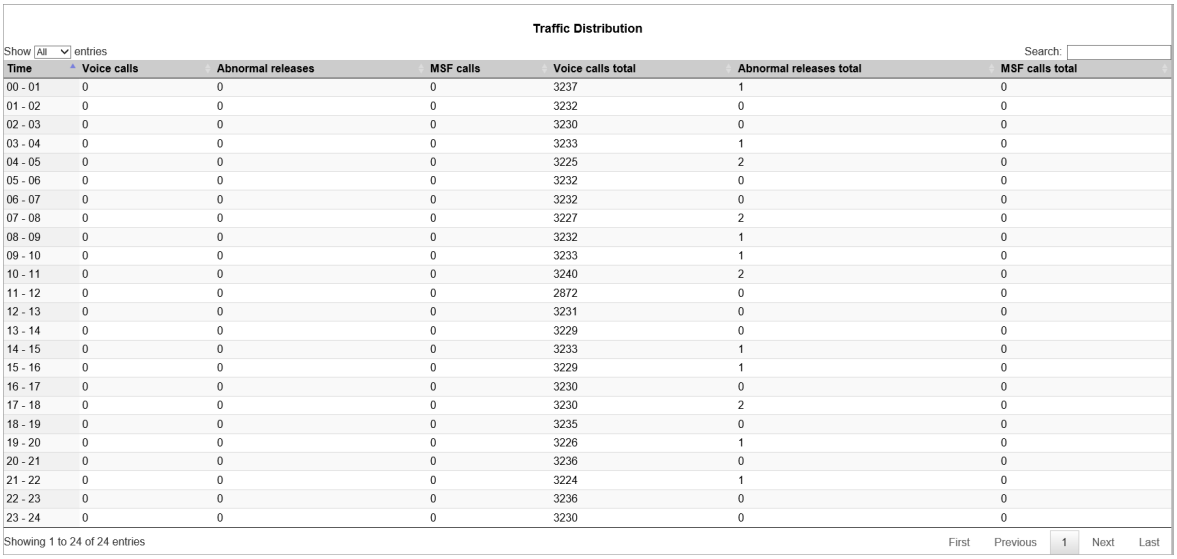
Timestamp	User	RfpNo	Reason	Call State
2017-10-25 14:25:32	50008	5	Connection lost	Active
2017-10-25 17:36:40	50026	3	Connection lost	Active
2017-10-25 19:37:13	50004	0	Connection lost	WaitForConnectInd
2017-10-26 00:24:15	50012	4	Connection lost	WaitForConnectInd
2017-10-26 04:56:58	50010	0	Connection lost	WaitForConnectInd
2017-10-26 07:30:22	50008	4	Timer expired (0xe20d)PXI$\blacklozenge$k	Active
2017-10-26 10:15:44	50028	3	Connection lost	Active
2017-10-26 15:38:03	50030	1	Connection lost	WaitForReleaseCfm
2017-10-26 17:26:51	50031	6	Connection lost	OutgoingSetup
2017-10-26 21:23:17	50008	5	Connection lost	OutgoingSetup
2017-10-27 03:05:41	50005	5	Connection lost	Active
2017-10-27 04:53:29	50006	5	Connection lost	Active
2017-10-27 07:00:43	50023	3	Connection lost	Active
2017-10-27 08:08:49	50008	0	Connection lost	Active
2017-10-27 09:05:57	50035	1	Connection lost	Active
2017-10-27 10:04:45	50007	5	Connection lost	WaitForConnectInd

Showing 1 to 16 of 16 entries First Previous 1 Next Last

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

Show All entries Search:

Time	Voice calls	Abnormal releases	MSF calls	Voice calls total	Abnormal releases total	MSF calls total
00 - 01	0	0	0	3237	1	0
01 - 02	0	0	0	3232	0	0
02 - 03	0	0	0	3230	0	0
03 - 04	0	0	0	3233	1	0
04 - 05	0	0	0	3225	2	0
05 - 06	0	0	0	3232	0	0
06 - 07	0	0	0	3232	0	0
07 - 08	0	0	0	3227	2	0
08 - 09	0	0	0	3232	1	0
09 - 10	0	0	0	3233	1	0
10 - 11	0	0	0	3240	2	0
11 - 12	0	0	0	2872	0	0
12 - 13	0	0	0	3231	0	0
13 - 14	0	0	0	3229	0	0
14 - 15	0	0	0	3233	1	0
15 - 16	0	0	0	3229	1	0
16 - 17	0	0	0	3230	0	0
17 - 18	0	0	0	3230	2	0
18 - 19	0	0	0	3235	0	0
19 - 20	0	0	0	3226	1	0
20 - 21	0	0	0	3236	0	0
21 - 22	0	0	0	3224	1	0
22 - 23	0	0	0	3236	0	0
23 - 24	0	0	0	3230	0	0

Showing 1 to 24 of 24 entries First Previous 1 Next Last

Changing Administration Password

From the web based Administration Page of the Spectralink IP-DECT Server it is possible to change the administration password.

For more information, see "Configuring Security Settings and Changing System Password" on page 99.

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.
New password (Optional)	Enter a new password.
New password again (Optional)	Enter the new password again to confirm.

Field	Setting
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 "Changing Administration Password" on the previous page. **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.
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 Server,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 Server it is possible to reset the Spectralink IP-DECT Server 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. For more information, see "Server and Media Resource Reset Button" on page 57.

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:

If you by mistake delete a license or perform a factory reset of the system (which will delete all loaded licenses), it is possible to retrieve the license(s) again by entering the ARI code of the Spectralink IP-DECT 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.

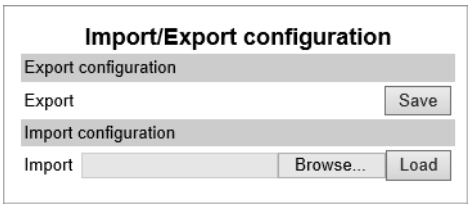
Exporting/Importing Configuration File

Through the web based Administration Page of the Spectralink IP-DECT Server it is possible to export and import configuration file.

To Import/Export Configuration File

1. Click **Configuration**, and then click **Import/Export**.
2. On the **Import/Export** configuration page, do the following:

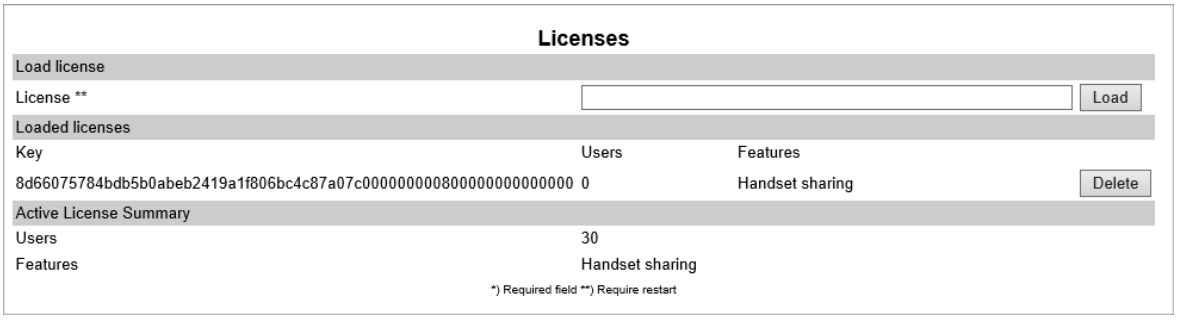
Field	
Import/Export - Export configuration	
Export	Click **Save**, if you want to export the configuration file. Save the configuration file.
Import/Export - Import configuration	
Import	Click **Browse**, if you want to search for a configuration file to be imported, select the relevant file, and then click **Load**.



3. Click **Reboot**.

Deleting Licenses

1. Click **Administration**, and then click **License**.
2. On the **Licenses** page, under **Loaded licenses**, click **Delete**, to delete the relevant license.



Note:

If you by mistake delete a license or perform a factory reset of the system (which will delete all loaded licenses), it is possible to retrieve the license(s) again by entering the ARI code of the Spectralink IP-DECT 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.

For information about loading a license, see "Loading Licenses" on page 43.

Messaging Over MSF

With the MSF messages function you can send text messages to any MSF compatible handset connected to the Spectralink IP-DECT Server.

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.

Redundant System Configuration

Note:

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

This section describes the redundancy feature in the Spectralink IP-DECT Server 6500. You will find a description of how to design, configure and administer a redundant Spectralink IP-DECT Server 6500 solution including a master and a backup server.

The redundancy feature of the Spectralink IP-DECT Server 6500 solution allows adding 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. Except for a few simple redundancy options, 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 entities, e.g. base stations, media resources and server.

Note:

If a third party application is connected to the Spectralink IP-DECT Server 6500, e.g. a messaging application or a nurse call application, this application must connect to the master Spectralink IP-DECT Server 6500.

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.

Firmware Compatibility (Redundancy)

For using a redundant server solution, it is required that the backup Spectralink IP-DECT Server has the same firmware revision and licensed features as the master Spectralink IP-DECT Server to be able to connect to the master.

In case a backup server tries to connect with a different firmware version or other licensed features than the master server, an error message will be logged and the backup server will be rejected.

For latest SW available, please go to http://support.spectralink.com/.

Note:

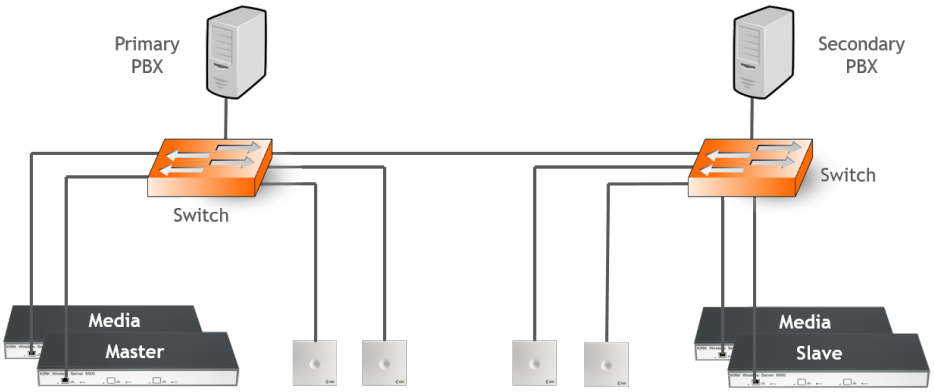
Provisioning of server firmware it not possible in a redundant setup.

Design of Redundant Server Solution

This section describes how to design a redundant server solution.

Designing a redundant Spectralink IP-DECT Server 6500 solution is very similar to designing any other redundant network service. In a redundant Spectralink IP-DECT Server 6500 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 (slave server).

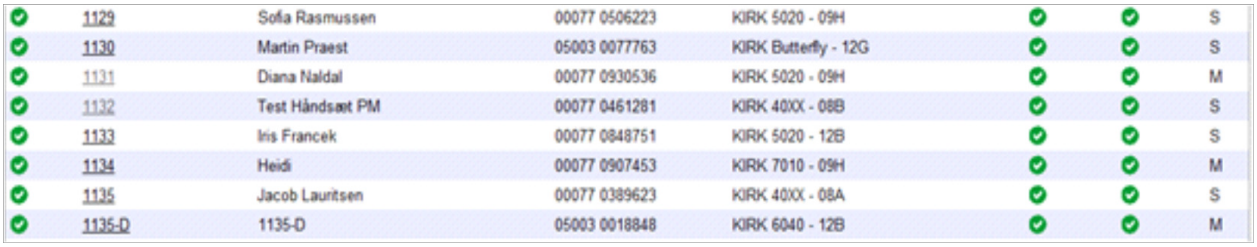


Note:

- Use separate switches, power groups and servers in a redundant setup.
- Master server and backup (slave) 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 50017 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 Server 6500 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):



✓	1129	Sofia Rasmussen	00077 0506223	KIRK 5020 - 09H	✓	✓	S
✓	1130	Martin Praest	05003 0077763	KIRK Butterfly - 12G	✓	✓	S
✓	1131	Diana Naldal	00077 0930536	KIRK 5020 - 09H	✓	✓	M
✓	1132	Test Håndsæt PM	00077 0461281	KIRK 40XX - 08B	✓	✓	S
✓	1133	Iris Francek	00077 0848751	KIRK 5020 - 12B	✓	✓	S
✓	1134	Heidi	00077 0907453	KIRK 7010 - 09H	✓	✓	M
✓	1135	Jacob Lauritsen	00077 0389623	KIRK 40XX - 08A	✓	✓	S
✓	1135-D	1135-D	05003 0018848	KIRK 6040 - 12B	✓	✓	M

The users will not always be on the same system. After a reboot of the Spectralink IP-DECT Servers 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:

In case you need to firmware upgrade to minimize downtime, update Spectralink IP-DECT Base Stations, Spectralink DECT Media Resources and Spectralink IP-DECT Servers 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.

Configuring Redundancy

Note:

Not relevant to the Spectralink IP-DECT Server 400.

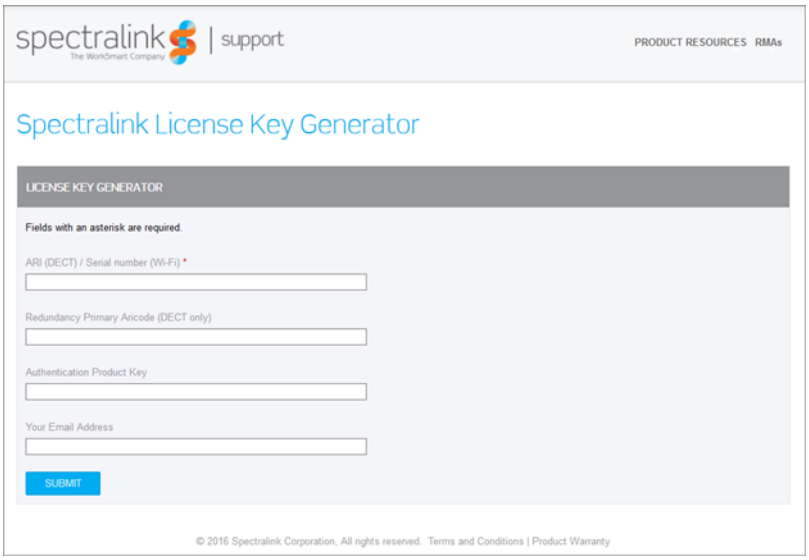
This section describes how to configure a redundant server solution:

- Configuration of the redundancy feature requires the acquisition of redundancy licenses.
- Configuration of setting is performed through the web based Administration Page of the Spectralink IP-DECT Server 6500 under **Configuration** > **Redundancy**.

Redundancy Licenses Generation

In the following you will find information about ordering redundancy licenses, Authentication Product Keys and final redundancy license key generation using the License Key Generator.

Authentication Product Keys are used to generate the final license using the License Key Generator on Spectralink Corporation's support portal: http://support.spectralink.com/keycode.



In the License Key Generator you bind the received Authentication Product Key to a specific Server ARI code.

Caution:

When an Authentication Product Key has been tied to an ARI code using the License Key Generator, the license has been used, a specific license cannot be untied from this ARI code again.

If a license has been tied to a wrong ARI code, please contact Technicalsupport@spectralink.com for help. In the worst case, it may be necessary to buy a new license.

Note:

If a license is installed on the master Spectralink IP-DECT Server 6500, a corresponding license with proper permissions must be installed on the backup Spectralink IP-DECT Server 6500 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 Generate License for Master IP-DECT Server

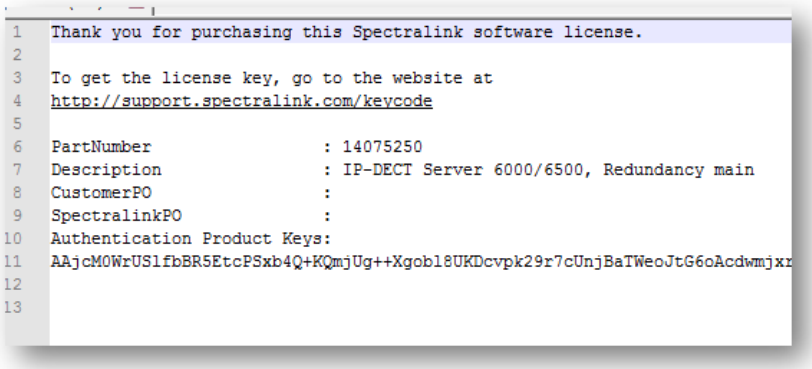
1. Order the license. Send your Purchase Order (PO) including the software part number and the number of licenses needed to Spectralink Order Management via (EMEA and APAC) emeaom@spectralink.com or (NALA) nalaom@spectralink.com .

   Note:

   - License required on the master:

     Redundancy Master | IP-DECT Server 6000/6500 (part no. 1407 5250)

2. When your order is processed, Order Management will send you an email including an Authentication Product Key for your software license. The e-mail contains a txt document called “License.txt” and looks like this:

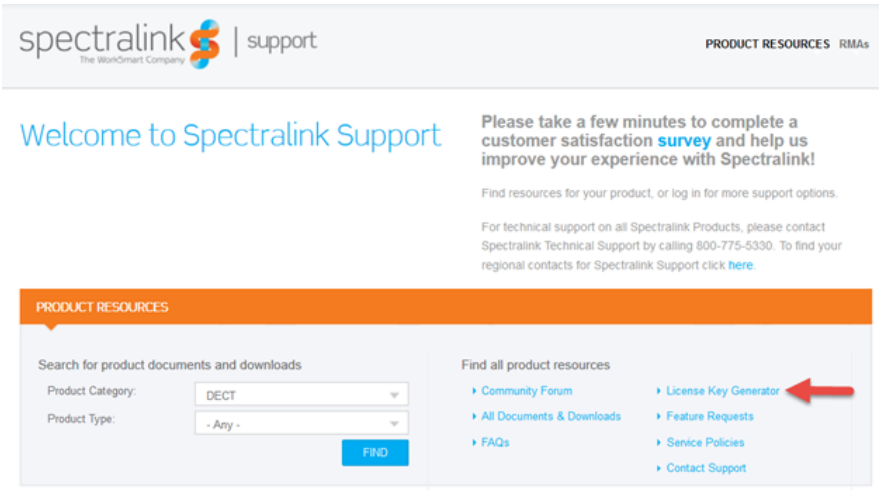


3. Find the System ARI Code for your master Spectralink IP-DECT Server6500 to be used in the License Key Generator. For more information, see "Identifying ARI on Spectralink IP-DECT Server" on page 48.

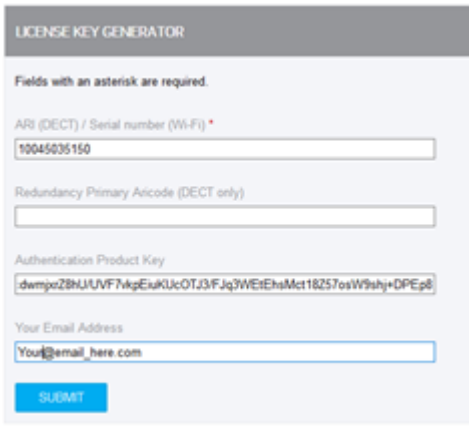
   Note:

   An ARI always start with 100 and then 8 number after, e.g. ARI: 10045035150.

4. Turn your browser to Spectralink Support portal http://support.spectralink.com/, and click the License Key Generator link to open the License Key Generator.



The following **Spectralink License Key Generator** screen appears:



5. Generate the license for the master Spectralink IP-DECT Server 6500 by doing the following:
   - In the **ARI (DECT) / Serial number (Wi-Fi)** field, enter the ARI of your master Spectralink IP-DECT Server.
   - In the **Authentication Product Key** field, enter the specific Authentication Product Key from the license.txt document received by e-mail (copy the key from the document and paste it in the field).
   - In the **Your Email Address** field, enter your email address.
   - Click **Submit**.
   - The webpage will output the license and an email with the new license code will be sent to

the e-mail you have entered.

6. Load the new license code using the web based Administration Page of the Spectralink IP-DECT Server.
   - 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.

How to Generate License for Backup IP-DECT Server

1. Order the licenses. 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 .

   Note:

   - License required on the backup:

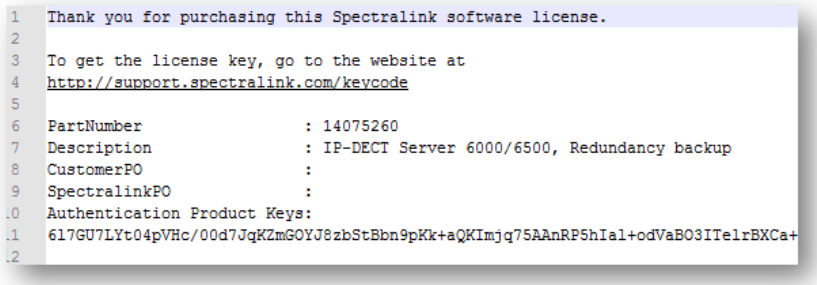
     Redundancy Backup | IP-DECT Server 6000/6500 (part no. 1407 5260)

   Note:

   The license for the backup Spectralink IP-DECT Server 6500 contains an ARI change license (also known as ARI swap license), which means that the Spectralink IP-DECT Server 6500 redundant solution only refers to the ARI code of the master Spectralink IP-DECT Server 6500, and not the ARI code of the backup Spectralink IP-DECT Server 6500.

   For more information, see "Administration Scenarios" on page 191.

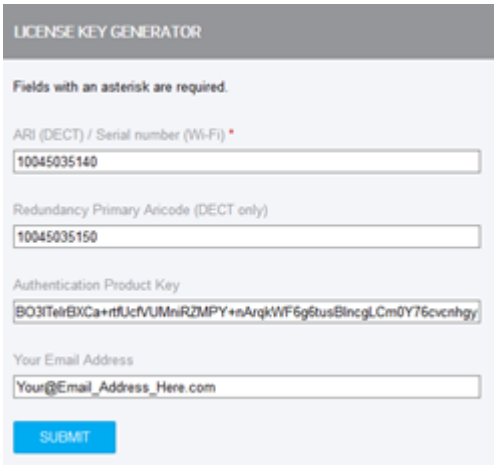
2. When your order is processed, Order Management will send you an email including an Authentication Product Key for your software license. The e-mail contains a txt document called “License.txt” and looks like this:



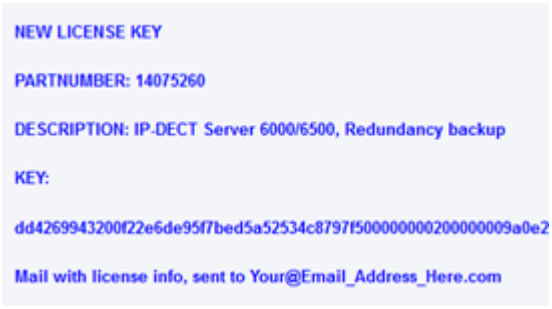
```
Thank you for purchasing this Spectralink software license.

To get the license key, go to the website at
http://support.spectralink.com/keycode

PartNumber                : 14075260
Description               : IP-DECT Server 6000/6500, Redundancy backup
CustomerPO                :
SpectralinkPO             :
Authentication Product Keys:
617GU7LYt04pVHc/00d7JqKZmGOYJ8zbStBbn9pKk+aQKImjq75AAnRP5hIal+odVaBO3ITelrBXCa+
```

3. Find the System ARI Code for your backup Spectralink IP-DECT Server6500 to be used in the License Key Generator. For more information, see "Identifying ARI on Spectralink IP-DECT Server" on page 48.
4. Turn your browser to Spectralink Support portal http://support.spectralink.com/, and click the License Key Generator link to open the License Key Generator.

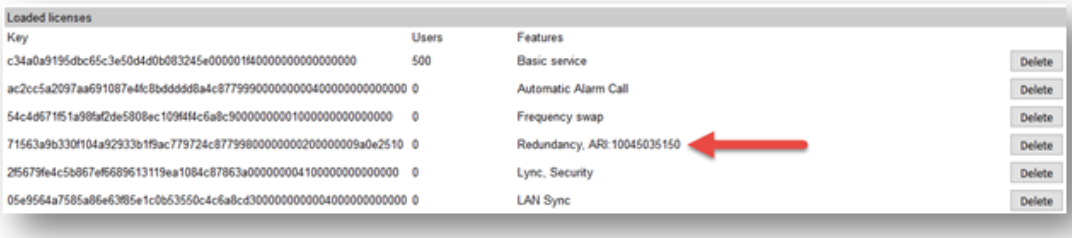
   The following **Spectralink License Key Generator** screen appears:



5. Generate the license for the backup Spectralink IP-DECT Server 6500 by doing the following:
   - In the **ARI (DECT) / Serial number (Wi-Fi)** field, enter the ARI of your backup Spectralink IP-DECT Server.
   - In the **Redundancy Primary Code (DECT only)** field, enter the ARI of your master Spectralink IP-DECT Server.
   - In the **Authentication Product Key** field, enter the specific Authentication Product Key from the license.txt document received by e-mail (copy the key from the document and paste it in the field).
   - In the **Your Email Address** field, enter your email address.
   - Click **Submit**.
   - The webpage will output the license and an email with the new license code will be sent to the e-mail you have entered.



6. Load the new license code using the web based Administration Page of the Spectralink IP-DECT Server.
   - 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.
7. Loaded licenses can be seen on the web based Administration Page > **Administration** > **Licenses** > **Loaded licenses**.

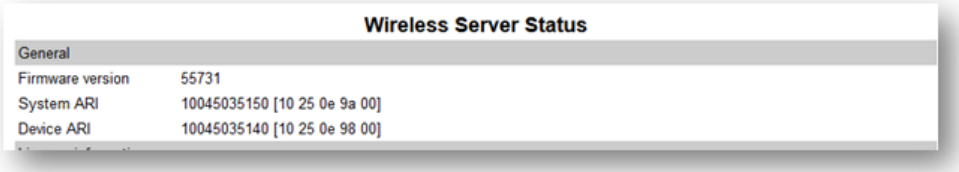


Note:

The Redundancy License had adopted the ARI code of the master Spectralink IP-DECT Server. This is done in the case of a failure of the master Spectralink IP-DECT Server, the backup Spectralink IP-DECT 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 Spectralink IP-DECT Server will look different after a Redundancy License has been installed, as the backup Spectralink IP-DECT Server adopts the ARI of the master Spectralink IP-DECT Server. The backup Spectralink IP-DECT Server will now have both a System ARI and a Device ARI.



Configuring a Master Spectralink IP-DECT Server 6500

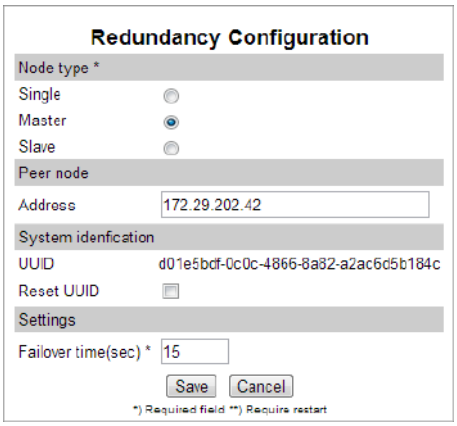
The master Spectralink IP-DECT Server 6500 must be configured as a normal single server solution with base stations, media resources and users as “normal” and it must be verified that the desired functionality is working before enabling the redundancy feature, and the backup Spectralink IP-DECT Server 6500 is added.

1. Ensure that the Redundancy License is installed, and that the master server is configured correctly.

   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. If backup server, enter the fixed IP address or hostname for the master Spectralink IP-DECT Server 6500.

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 is changed to a backup Spectralink IP-DECT Server 6500, or when a backup Spectralink IP-DECT Server 6500 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 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" on page 192.



4. Click **Save**.

Note:

Enabling or disabling the reduncancy funtion on a given server, will not require a reboot of the Spectralink IP-DECT Server(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

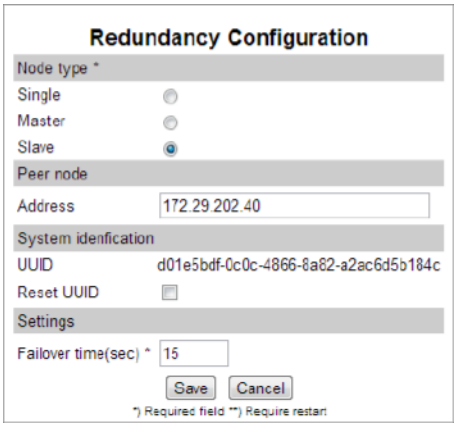
On the backup Spectralink IP-DECT Server 6500 only basic network settings and redundancy settings need to be configured. All other settings are retrieved from the master Spectralink IP-DECT Server 6500.

1. Ensure that the Redundancy License is installed, and configured with basic network settings.

   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. If backup server, enter the fixed IP address or hostname for the master Spectralink IP-DECT Server 6500.

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 is changed to a backup Spectralink IP-DECT Server 6500, or when a backup Spectralink IP-DECT Server 6500 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 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" on page 192.



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 internal corporate phone book feature on the Spectralink IP-DECT Server 6500 is to be used together with the redundancy feature, the corporate phone book needs to be configured for LDAP. For more information, see "To Get Phone Book Data through LDAP Server or CSV File" on page 193.

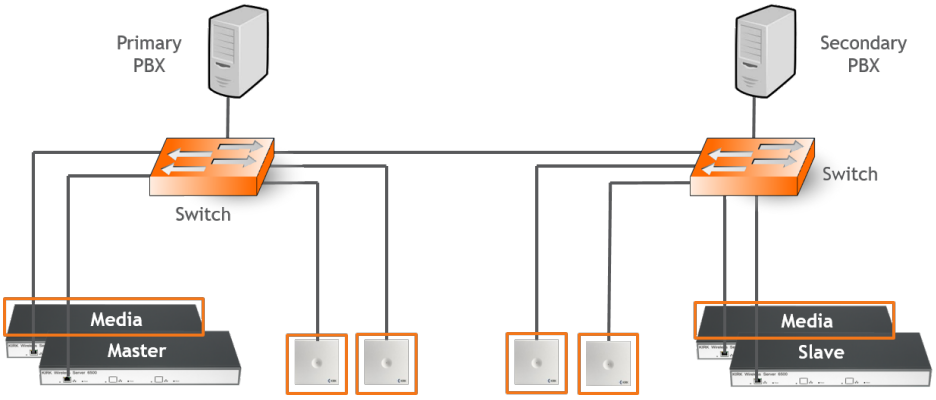
If the internal corporate phone book is configured to use a CSV file, it will not be compatible with the Spectralink IP-DECT Servers when running in failover mode.

Base Station and Media Resource Configuration

The base stations and media resource should be configured just as in a single Spectralink IP-DECT Server 6500 solution, and the server address should be set to the address of the master Spectralink IP-DECT Server 6500.

After connecting to the master Spectralink IP-DECT Server 6500, the base stations and media resource will automatically be configured to connect to the backup Spectralink IP-DECT Server 6500.

In the event that the master Spectralink IP-DECT Server 6500 fails, they will continue to provide service to the backup Spectralink IP-DECT Server 6500.



Note:

The license for the backup Spectralink IP-DECT Server 6500 contains an ARI change license (also known as ARI swap license), which means that the Spectralink IP-DECT Server 6500 redundant solution only refers to the ARI code of the master Spectralink IP-DECT Server 6500, and not the ARI code of the backup Spectralink IP-DECT Server 6500..

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 fails.

Upgrading an Existing Spectralink IP-DECT Server 6500 Solution into a Redundant Solution

When ordering a Redundancy License to an existing running Spectralink IP-DECT Server 6500 solution, please remember to inform about the existing Spectralink IP-DECT Server 6500 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 generates 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

In the case where the master Spectralink IP-DECT Server 6500 fails due to loss of power, network connection etc., the backup Spectralink IP-DECT Server 6500 will continue to provide service after a short failover time.

When the master Spectralink IP-DECT Server 6500 returns to operation, it will resume its normal operation in cooperation with the backup Spectralink IP-DECT Server 6500.

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

If the master Spectralink IP-DECT Server 6500 has been damaged, lost or had its data erased, it will have to be replaced by the backup Spectralink IP-DECT Server 6500 in order to return the system to normal operation mode. This is done by promoting the backup Spectralink IP-DECT Server 6500 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 Spectralink IP-DECT Server 6500.

Note:

Please be aware that if for some reason a repaired or replaced former master Spectralink IP-DECT Server 6500 is reinstated as master, it should be done very carefully.

First, it must be configured as a backup Spectralink IP-DECT Server 6500 in order to get the current user data and configuration from the acting master Spectralink IP-DECT Server 6500 (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 Spectralink IP-DECT Server 6500.

Failover time conditions

The default failover time is 15 seconds; however this may be adjusted in the Failover time setting (for more information, see "Configuring a Master Spectralink IP-DECT Server 6500" on page 185).

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

A failure of the backup Spectralink IP-DECT Server 6500 will induce a short service outage, and the master Spectralink IP-DECT Server 6500 will reestablish full operation as a single server solution.

If the backup Spectralink IP-DECT Server 6500 resumes its operation, it will automatically return to be part of the redundant system. In case the backup Spectralink IP-DECT Server 6500 has to be replaced, the new backup Spectralink IP-DECT Server 6500 must be added to the solution.

Configuring Corporate Phone Book/Directory

You can set up the corporate phone book/directory in the server. As default, the corporate phone book is disabled.

The server can be configured in two ways:

- Retrieving phone book data using LDAP server.

  Configuration of the LDAP based phone book in the Spectralink IP-DECT Server is carried out through the web based Administration Page of the server.
- Importing phone book data from a CSV file.

Note:

To access the corporate phonebook/directory from a Spectralink DECT Handset, the long key MSF Function must be enabled.

For information on setting up long key and using the corporate phone book/directory in the handset, see the relevant Handset User Guide.

To Get Phone Book Data through LDAP Server or CSV File

Configure the server to retrieve phone book data using LDAP server or by importing phone book data from a CSV file.

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.

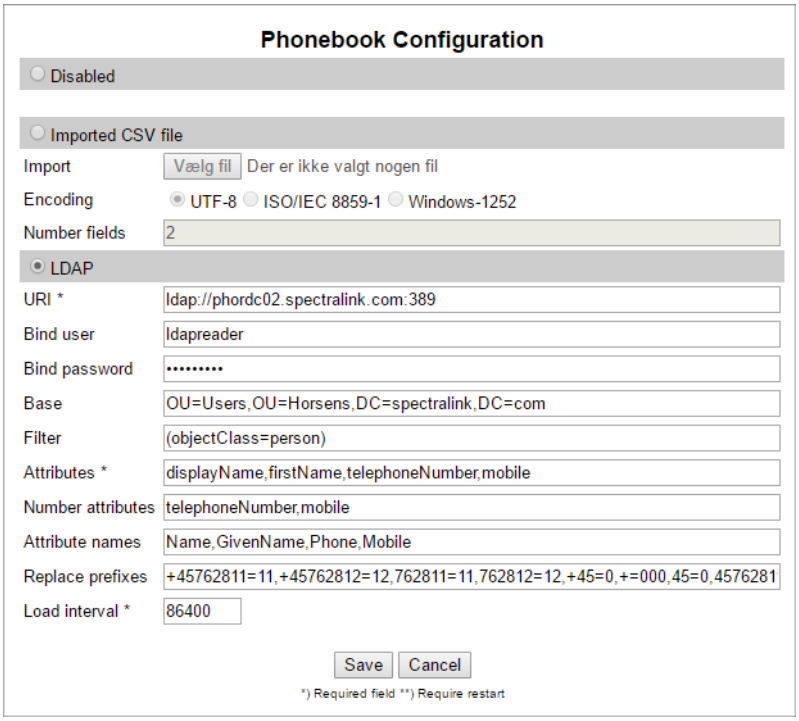
Field	Setting
Import	Browse for the CSV file to import. **Note**: The CSV file must contain correct format. For more information, see "Example of CSV File Format" on page 196.
Encoding	Select the correct encoding for the CSV file. You can choose between **UTF-8**, **ISO/IEC 8859-1** or **Windows-1252**. **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. For an example of LDAP configuation, see "Example of LDAP Configuration" on the next page.
URI	Enter the URI of the LDAP server. E.g. ldap://example.com
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 dialled, 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

3. Click **Save**.

   No restart is needed and the changes are accepted immediately.

Example of LDAP Configuration



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"

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 it is possible to 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 it is possible to let the 10 users share 4 devices for cost-saving

reasons.

To use the handset sharing feature, the following is needed:

- Acquisition of the Handset Sharing License | IP-DECT/DECT Servers 400/6500/2500/8000.

  For more information, see "Adding Handset Sharing License | IP-DECT/DECT Servers 400/6500/2500/8000 " on page 200.
- Firmware compatibility

  For more information, see "Handset Sharing - Firmware Compatibility" on the next page.
- Configuration of handset sharing, including:
  - Configuration of user sign-in/sign-out

    For more information, see "User Sign-in/Sign-out" on page 201.
  - Adding Devices to Server

    For more information, see "Adding Devices to Server" on page 209.
  - Adding Users to Servers

    For more information, see "Adding Users to Server" on page 212.
  - Handset Sharing and Provisioning

    For more information, see "Handset Sharing and Provisioning" on page 213.

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 PCS14_ or newer.
- The server must run firmware PCS12M_ 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 | IP-DECT/DECT Servers 400/6500/2500/8000

To enable handset sharing it is necessary to add a Handset Sharing License | IP-DECT/DECT Servers 400/6500/2500/8000 to the Spectralink IP-DECT Server.

For more information about ordering and loading license into the server, see "Ordering Licenses" on page 43 and "Loading Licenses" on page 43.

Note:

When a Handset Sharing License | IP-DECT/DECT Servers 400/6500/2500/8000 is loaded and the Spectralink IP-DECT/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 | IP-DECT/DECT Servers 400/6500/2500/8000 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 user, it is 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" on the next page.
- Adding Devices to Server

  For more information, see "Adding Devices to Server" on page 209.
- Adding Users to Servers

  For more information, see "Adding Users to Server" on page 212.
- Handset Sharing and Provisioning

  For more information, see "Handset Sharing and Provisioning" on page 213.

User Sign-in/Sign-out

Using a sign-in procedure, it is possible to 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 Server. 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 PCS17H 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 Server

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	
Wireless Server Configuration - DECT	
Subscription allowed (Optional)	If enabled, it is possible to subscribe new handsets to the system.
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 **Enforced (non GAP)**. Default value: Disabled
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**: It is possible to define a TX power value for a specific base station (**Administration** > **Base Station**).

Field	
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.
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.
Require encryption (Optional)	If enabled, the connection between the media resource and the Spectralink IP-DECT Server is required to be encrypted. **Note**: Enabling this, will only allow media resources with firmware PCS17Fa or newer to connect. 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.
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.
Require encryption (Optional)	If enabled, the connection between the base station and the Spectralink IP-DECT Server is required to be encrypted. **Note**: Enabling this, will only allow base stations with firmware PCS17Fa or newer to connect. If not enabled, the connection will be encrypted if the base station supports encryption.
RFP port range start	Port range start for RFP local RTP ports. Default value: 57000 **Note**: It is possible to change the value in case of conflicting ports.

Field	
Multicast signaling (Optional)	Multicast signaling is optimal when having many base stations and is required with more than 256 base stations connected. If enabled, this will impose multicast support for the network. For more information, see "Using Multicast" on page 126.
Multicast address (Optional)	Multicast address used for signaling. Default value: 239.255.1.11 Please refer to RFC2365 and RFC4291 for details.
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 it is possible to change the value according to network topology. For more information, see vendor specific documentation.
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
LAN sync transport protocol (Only visible if license loaded)	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 (License Required)" on page 131.

Field	
LAN sync type of service (TOS/Diff-serv) (Only visible if license loaded)	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)
Wireless Server Configuration - Handsets (Not relevant to the Spectralink IP-DECT Server 200.	
Handset sharing (Optional) (Only visible if license loaded)	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" on page 197.
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 dependant). For more information, see "Configuring Handset Login" on page 202 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.

Field	
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 suported.
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***), including the desired extension. E.g.: ***21*$#** **Note**: It is possible to change the code *21* on the Spectralink IP-DECT Server 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 DECT Server to use this long key press for phone book.
Enable Long-Press Key1- Phonebook (Optional)	If enabled, allow DECT Server to use this long key press for phone book.
Enable Long-Press Key2 - Phonebook (Optional)	If enabled, allow DECT Server to use this long key press for phone book.

Field	
Enable Long-Press Key3 - Phone-book (Optional)	If enabled, allow DECT Server to use this long key press for phone book.
Enable Long-Press Key4 - Phone-book (Optional)	If enabled, allow DECT Server to use this long key press for phone book.
Enable Long-Press Key5 - Phone-book (Optional)	If enabled, allow DECT Server to use this long key press for phone book.
Enable Long-Press Key6 - Undefined (Optional)	If enabled, allow DECT Server to use this long key press.
Enable Long-Press Key7 - Undefined (Optional)	If enabled, allow DECT Server to use this long key press.
Enable Long-Press Key8 - Undefined (Optional)	If enabled, allow DECT Server to use this long key press.
Enable Long-Press Key9 - Hand-set Sharing (Optional)	If enabled, allow DECT Server to use this long key press for handset sharing. For more information, see "Handset Sharing" on page 197 and "User Sign-in/Sign-out" on page 201.

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 **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.

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 user name and password. Entering the required credentials will allow the Spectralink IP-DECT Server 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 Server by specifying an IPEI or they can be automatically created when subscribed to the Spectralink IP-DECT Server.

Data are split in two categories.

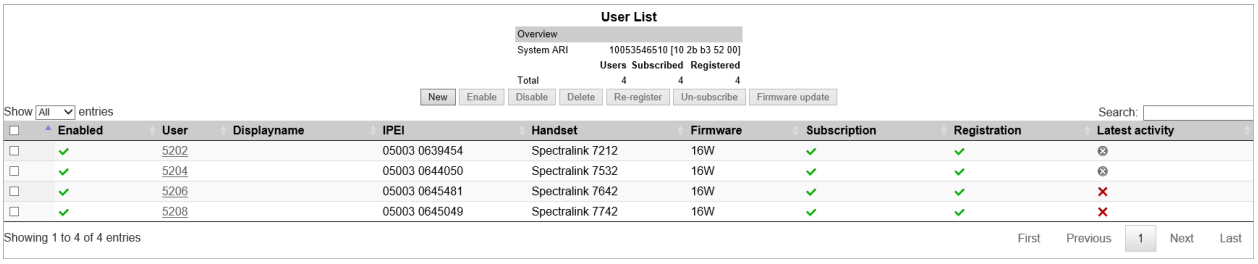
- Device data (handset)

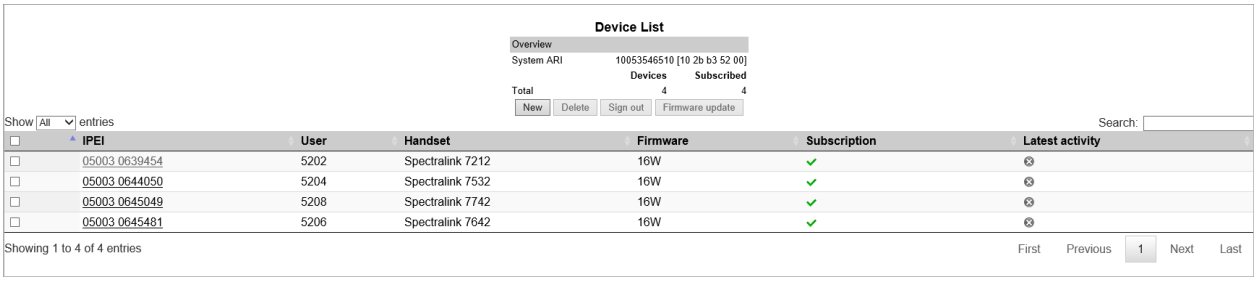
  Device specific data include an IPEI (mandatory) and an access code (optional). The access code is used for subscribing the device to the Spectralink IP-DECT Server.

- User data (username, standby text, display name etc.)

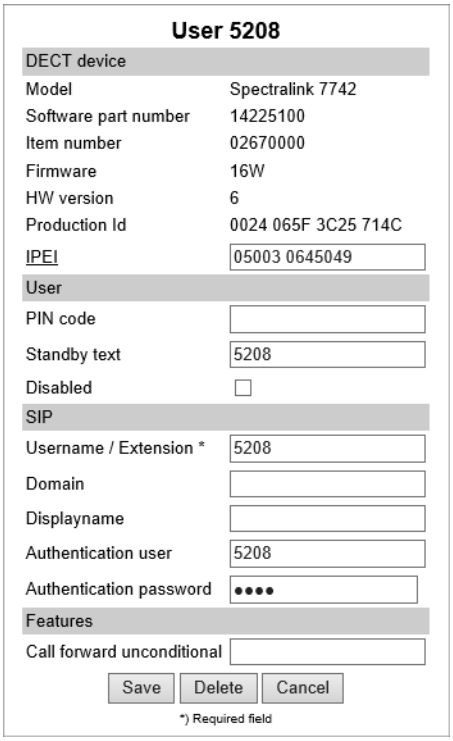
  If a user is signed in, it will be visible in the **Users** > **List Users** > **User List**. Editing the username will allow the administrator to “sign-in” a user to the device or alternatively to sign-out” a user.

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" on page 213.

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

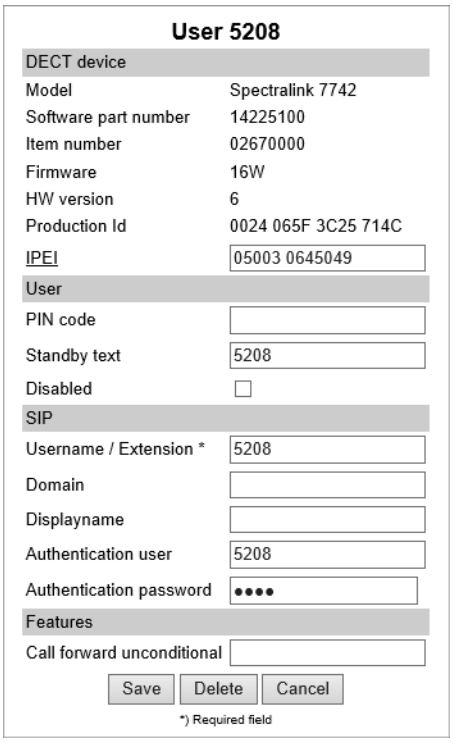
  User data are data specific to a specific user. The Standby text is displayed in the handset when the user is signed-in. If no user is currently signed in to a device the device will display “Signed out”. The user PIN code is used by the user to sign-in to a device.

- SIP

  The sip category consists of SIP data specific to the user.

- Features

  Features are user specific feature data.



Handset Sharing and Provisioning

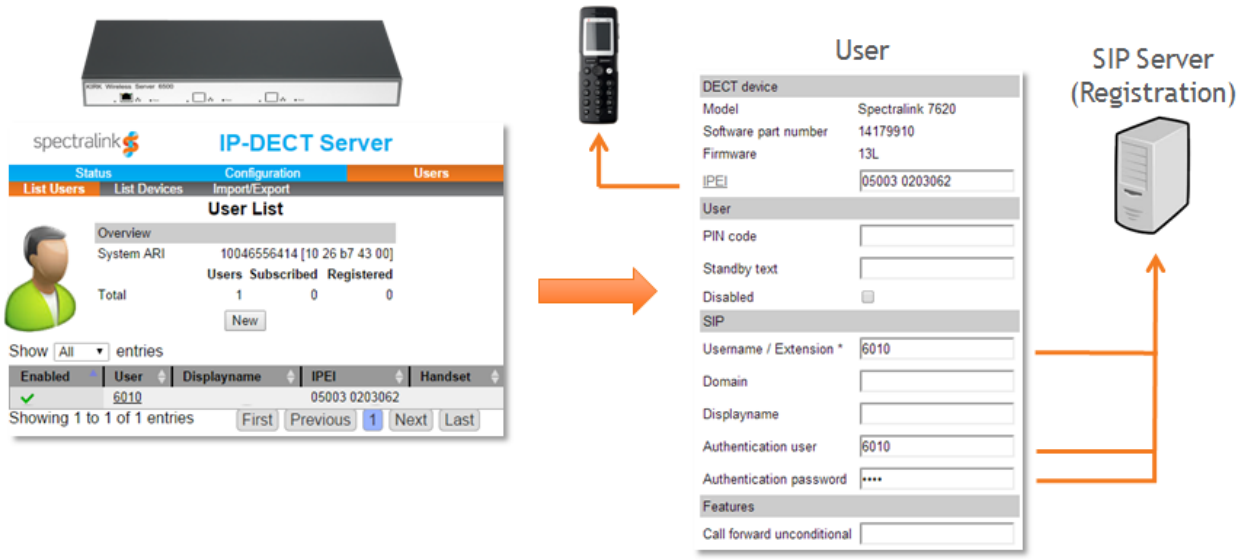
Handset sharing is used in combination with provisioning. Users can be provisioned via the <MAC>-users.xml file. Devices cannot be provisioned because the intention is that devices will be automatically created when they are subscribed.

It is recommended to provision users without an IPEI and let the user/device binding be handled by signing-in from the handsets.

Furthermore, it is recommended not to create the devices manually via the GUI but let the system automatically create them when subscribed. For security reasons it is recommended to restrict device subscription with a system access code.

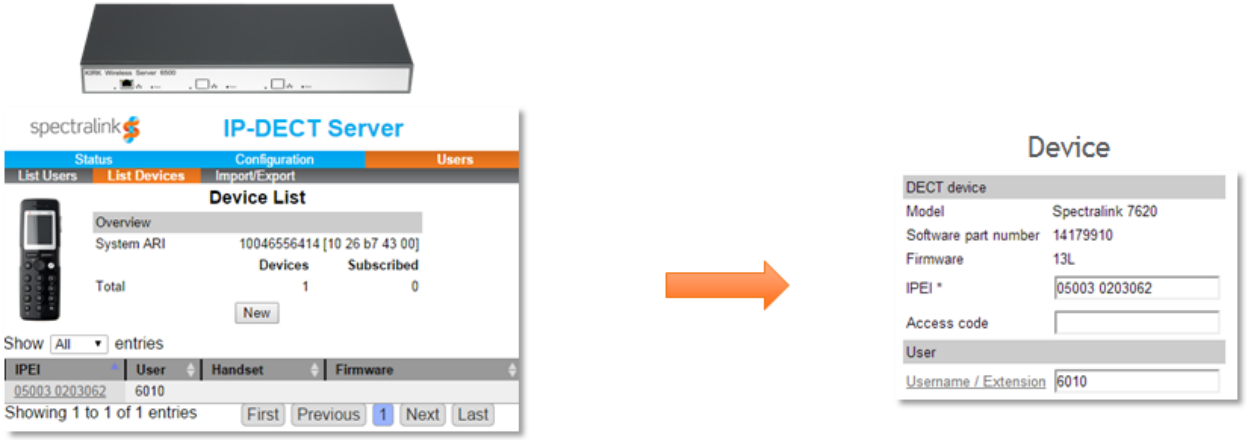
For more information about provisioning, see Provisioning Guide.

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 Server, 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

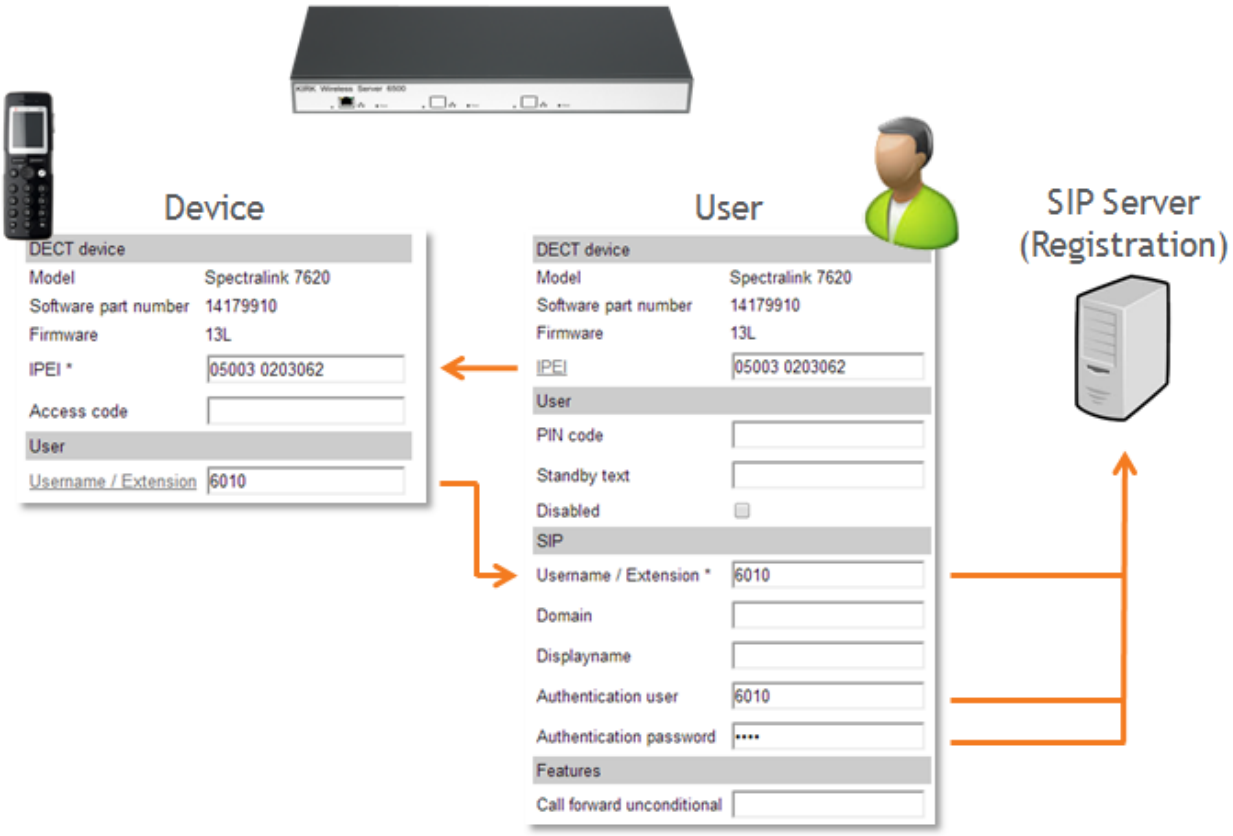
When clicking on an IPEI number under the **Device List** page, you see a **Device** profile which in essence is a unique handset, that has been subscribed to the Spectralink IP-DECT Server. The **Device** profile holds information about the handset's IPEI number and optional access code used, when the handset is subscribed to the Spectralink IP-DECT Server.

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.

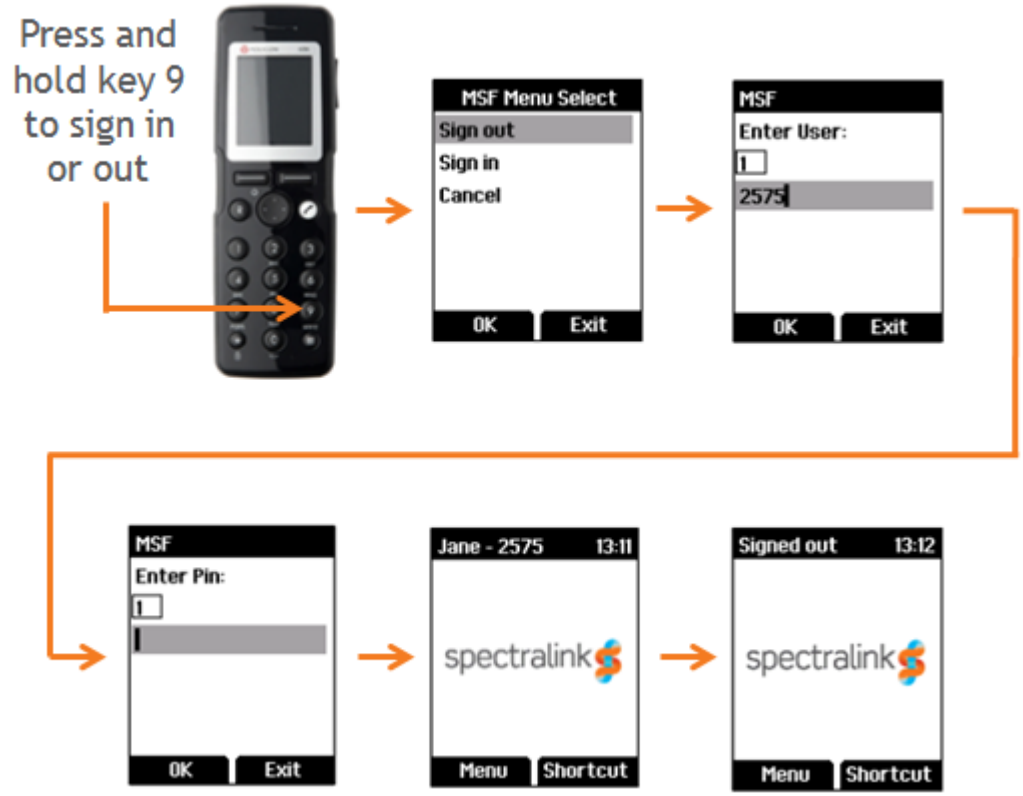
You can also work the other way around so that when creating a User you can choose to **link the user to an existing handset** by typing the IPEI. If the handset is already linked to another user, the handset will be released from that user and the handset will be linked with the user you are creating. For more information, see "Registering a User" on page 139.



- 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 License | IP-DECT/DECT Servers 400/6500/2500/8000 must be loaded to the Spectralink IP-DECT Server.
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.

Product Compatibility

If you have any questions about product compatibility, contact your system administrator.

You can use the Spectralink IP-DECT Server with other Spectralink products as identified by the type approval model ID and/or part number located on the label of the product.

Spectralink Server	
Spectralink IP-DECT Server 200	K005 (7234 5600/723 45601)
Spectralink IP-DECT Server 400	K005 (0234 4500/0234 4501)
Spectralink IP-DECT Server 6500	K006 (0235 0000)
Power Supply, 8.0V DC (only Server 200 and Server 400)	8464 2600
External Antenna (with 1 m connection cable) (only Server 200 and Server 400)	0231 9705
Connection cable for External Antenna, 3 m (only Server 200 and Server 400)	1400 2704
Connection cable for External Antenna, 7.5 m (only Server 200 and Server 400)	1400 2706

Spectralink Base Station	
Spectralink IP-DECT Base Station 1G8	K005
Spectralink IP-DECT Base Station 1G9	K005
Power Supply, 8.0V DC	8464 2600

Spectralink DECT Repeater	
Spectralink DECT Repeater 1G8, 2 channels, with connector for external antenna	K018B (0244 0000)
Spectralink DECT Repeater 1G9, 2 channels, with connector for external antenna	K018B (0244 1000)
Spectralink DECT Repeater 1G8, 2 channels, without connector for external antenna	K018 (0244 1100)
Spectralink DECT Repeater 1G9, 2 channels, without connector for external antenna	K018 (0244 1200)
Spectralink DECT Repeater 1G8, 4 channels, with connector for external antenna	K018 (0244 1600)
Spectralink DECT Repeater 1G9, 4 channels, with connector for external antenna	K018 (0244 0200)
Spectralink DECT Repeater 1G8, 4 channels, without connector for external antenna	K018C (0233 4601)
External Antenna (with 1 m connection cable)	0231 9705
Connection cable for External Antenna, 3 m	1400 2704
Connection cable for External Antenna, 7.5 m	1400 2706
Power Supply (9.0V DC, 350mA)	8464 2602
Repeater Programming Kit	0250 9210

Spectralink DECT Media Resource	
Spectralink DECT Media Resource (only Server 6500)	K006

Spectralink Server Licenses for 200	
Lync/SfB + Security (TLS, SRTP) | IP-DECT Server 200	1407 5511
Security (TLS, SRTP) | IP-DECT Server 200	1407 5281

Spectralink Server Licenses for Server 400	
12 Channels + 30 Users | IP-DECT Server 400	1407 5500
Lync/SfB +Security (TLS, SRTP) | IP-DECT Server 400	1407 5510
Multicell | IP-DECT Server 400	1407 5520
12 Channels + 30 Users + Lync/SfB + Security (TLS, SRTP) + Multicell | IP-DECT Server 400	1407 5550
12 Channels + 30 Users + Lync/SfB + Security (TLS, SRTP) | IP-DECT Server 400	1407 5540
12 Channels + 30 Users + Multicell | IP-DECT Server 400	1407 5560
Cisco Unified CM (Advanced Features) | IP-DECT Server 400	1407 5490
LAN Sync | IP-DECT Server 400	1407 5600
Enhanced Provisioning Interface | IP-DECT Server 400	1407 5701
Frequency Swap | IP-DECT/DECT Servers 400/6500/2500/8000	1407 5620
Handset Sharing License | IP-DECT/DECT Servers 400/6500/2500/8000	1407 5460
Automatic Alarm Call | IP-DECT/DECT Servers 300/400/2500/6000/6500/8000	1407 5450
Security (TLS, SRTP) | IP-DECT/DECT Servers 400/6000/6500/2500/8000	1407 5280
Additional repeaters (up to 6 repeaters) | IP-DECT Server 400	1407 5570

Spectralink Server Licenses for Server 6500	
30 Users | IP-DECT Server 6000/6500	1407 5200
150 Users | IP-DECT Server 6000/6500	1407 5210
500 Users | IP-DECT Server 6000/6500	1407 5220
1500 Users | IP-DECT Server 6000/6500	1407 5230
4096 Users | IP-DECT Server 6000/6500	1407 5240
Redundancy Master | IP-DECT Server 6000/6500	1407 5250
Redundancy Backup | IP-DECT Server 6000/6500	1407 5260
LAN Sync | IP-DECT Server 6500	1407 5610
Frequency Swap | IP-DECT/DECT Servers 400/6500/2500/8000	1407 5620
Cisco Unified CM (Advanced Features) | IP-DECT Server 6500	1407 5495
Lync/SfB +Security (TLS, SRTP) | IP-DECT Server 6000/6500	1407 5270
Enhanced Provisioning Interface | IP-DECT Server 6500	1407 5700
Handset Sharing License | IP-DECT/DECT Servers 400/6500/2500/8000	1407 5460
Automatic Alarm Call | IP-DECT/DECT Servers 300/400/2500/6000/6500/8000	1407 5450
Security (TLS, SRTP) | IP-DECT/DECT Servers 400/6000/6500/2500/8000	1407 5280

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

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.

Packet Capture

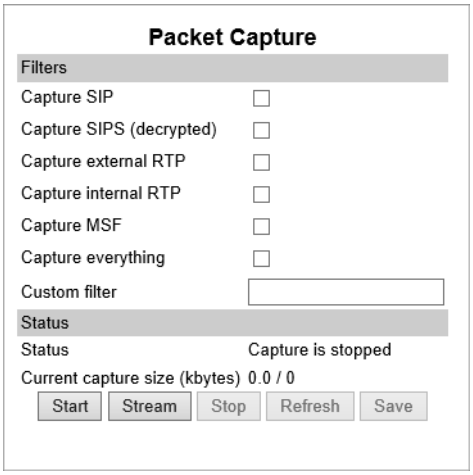
Spectralink Support can request a packet capture of the overall system status.

To make a packet capture from the web based Administration Page of the Spectralink IP-DECT Server:

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 signalling is captured.
Capture SIPS (decrypted) (Optional)	If enabled, decrypted SIPS (TLS) signalling 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 signalling 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.

Field	Setting
Packet Capture - Status	
Status	Shows the status of the capture progress.



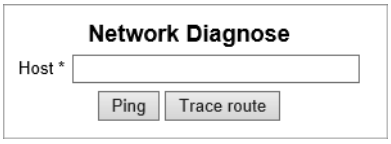
3. If you want to start capturing the network packets,click **Start**, click **Stop** after trying to reproduce the expected failure/behaviour, and then click **Save** to download and save the packet capture file.
4. If you want to stream a packet capture, click **Stream**. A pcap file is downloaded automatically.

Note:

The Spectralink IP-DECT Server has a packet capture size limit of 10 megabites. 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**.

Parameter Overview

Status - General

Field	
General Status - General	
IP address	IP address of the Spectralink IP-DECT Server.
NTP Server	IP address of the NTP Server.
Time	Time and date information.
Serial	Serial number of the Spectralink IP-DECT Server.
MAC address	MAC address of the Spectralink IP-DECT Server.
Product ID	Production ID of the Spectralink IP-DECT Server.
Production Date	Production Date of the Spectralink IP-DECT Server.
General Status - Hardware	
PartNo	Partnumber of the Spectralink IP-DECT Server hardware.
PCS	Hardware version
General Status - Firmware	
PartNo	Partnumber of the Spectralink IP-DECT Server 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.
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.

Field	
NTP (Network Time Protocol)	OK if the latest communication with the NTP server was successful.

Status - Logs

Field	
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 status 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. It is possible to clear the message log buffer for **Application** logs. The **Audit** log cannot be deleted - except when performing a factory reset. It is possible to stream an **Application** log, whereas an **Audit** log cannot be streamed.

Status - Wireless Server

Field	
Wireless Server Status - General	
Firmware version	Wireless Server firmware version. E.g. 59015
System ARI	E.g. 1005354651
Wireless Server Status - License information	
License max users	E.g. 30
License features	E.g. Handset sharing, Enhanced Provisioning Interface, Redundancy, Security, LAN Sync
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 signalling is captured.
Capture SIPS (decrypted) (Optional)	If enabled, decrypted SIPS (TLS) signalling 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 signalling 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.
Packet Capture - Status	
Status	Shows the status of the capture progress.

Status - Network Diagnose

Field	
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 - 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" on page 85.
IP addr	Enter the IP address of the Spectralink IP-DECT Server.
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.

Field	Setting
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)	It is possible to 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)	It is possible to 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 Server 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)	

Field	Setting
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 zones 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 Server, 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

Field	Setting
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	
Wireless Server Configuration - DECT	
Subscription allowed (Optional)	If enabled, it is possible to subscribe new handsets to the system.
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 **Enforced (non GAP)**. Default value: Disabled
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**: It is possible to define a TX power value for a specific base station (**Administration** > **Base Station**).
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.
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	
Require encryption (Optional)	If enabled, the connection between the media resource and the Spectralink IP-DECT Server is required to be encrypted. **Note**: Enabling this, will only allow media resources with firmware PCS17Fa or newer to connect. 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.
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.
Require encryption (Optional)	If enabled, the connection between the base station and the Spectralink IP-DECT Server is required to be encrypted. **Note**: Enabling this, will only allow base stations with firmware PCS17Fa or newer to connect. If not enabled, the connection will be encrypted if the base station supports encryption.
RFP port range start	Port range start for RFP local RTP ports. Default value: 57000 **Note**: It is possible to change the value in case of conflicting ports.
Multicast signaling (Optional)	Multicast signaling is optimal when having many base stations and is required with more than 256 base stations connected. If enabled, this will impose multicast support for the network. For more information, see "Using Multicast" on page 126.
Multicast address (Optional)	Multicast address used for signaling. Default value: 239.255.1.11 Please refer to RFC2365 and RFC4291 for details.

Field	
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 it is possible to change the value according to network topology. For more information, see vendor specific documentation.
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
LAN sync transport protocol (Only visible if license loaded)	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 (License Required)" on page 131.
LAN sync type of service (TOS/Diffserv) (Only visible if license loaded)	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)

Field	
Wireless Server Configuration - Handsets (Not relevant to the Spectralink IP-DECT Server 200.	
Handset sharing (Optional) (Only visible if license loaded)	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" on page 197.
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 dependant). For more information, see "Configuring Handset Login" on page 202 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 suported.
Wireless Server Configuration - Feature codes	
Enable (Optional)	If enabled, feature codes for controlling features from the handsets can be used.

Field	
Call forward unconditional - enable (Optional)	Enable call forward unconditional by dialing this code (***21***), including the desired extension. E.g.: ***21*$#** **Note**: It is possible to change the code *21* on the Spectralink IP-DECT Server 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 DECT Server to use this long key press for phone book.
Enable Long-Press Key1- Phonebook (Optional)	If enabled, allow DECT Server to use this long key press for phone book.
Enable Long-Press Key2 - Phonebook (Optional)	If enabled, allow DECT Server to use this long key press for phone book.
Enable Long-Press Key3 - Phonebook (Optional)	If enabled, allow DECT Server to use this long key press for phone book.
Enable Long-Press Key4 - Phonebook (Optional)	If enabled, allow DECT Server to use this long key press for phone book.
Enable Long-Press Key5 - Phonebook (Optional)	If enabled, allow DECT Server to use this long key press for phone book.
Enable Long-Press Key6 -Undefined (Optional)	If enabled, allow DECT Server to use this long key press.
Enable Long-Press Key7 - Undefined (Optional)	If enabled, allow DECT Server to use this long key press.
Enable Long-Press Key8 - Undefined (Optional)	If enabled, allow DECT Server to use this long key press.
Enable Long-Press Key9 - Handset Sharing (Optional)	If enabled, allow DECT Server to use this long key press for handset sharing. For more information, see "Handset Sharing" on page 197 and "User Sign-in/Sign-out" on page 201.

Configuration - Media Resource

Field	
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

Configuration - Security

Field	Setting
Security Configuration - Administrator Authentication	
Current password	Enter the current password.
New username	Enter a new username.
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" on page 223. **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.
Allow remote logging (Optional)	If enabled, remote logging is allowed. Remote logging allows for Spectralink debug tools to extract debug information from the unit.

Field	Setting
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 Server-,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	
Certificates - Device certificate chain	
	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 certificate chain	
Certificate file	Click **Browse** to find the relevant host certificate file (*.crt file).
Key file	Click **Browse** to find the relevant key file (*.pem file).
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.
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**).

Configuration - SIP

Field	Setting
SIP Configuration - General	
Local port	Enter the local port number. The local port is the port on which the Spectralink IP-DECT Server listens for incoming SIP-signalling. 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" on page 116.
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 Server 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.
Registration expire(sec)	The maximum time between re-registrations. The registrar can signal a shorter time-out. Default value: 3600 sec
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

Field	Setting
Max forwards	The maximum number of proxies outgoing messages are allowed to traverse. Default value: 70
Client transaction timeout(msec)	Client transaction time-out. This controls timer B and F as specified in RFC3261. Increase this to eliminate time out errors or decrease it to reduce fail over time. Default value: 16000 msec
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.

Field	Setting
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 user name used for SIP authentication. **Note**: If no handset specific authentication user name/-password is configured, handsets registered on theSpectralink IP-DECT/DECT Server will use the default user name/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 signalling	
Send as RTP (Optional)	If enabled, keypad signaling will be sent as RTP event codes.
Offered RFC2833 payload type	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.

Field	Setting
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/Diff-serv)	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**.
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 end-points.
Enable media encryption (SRTP) (Only visible if Security (TLS, SRTP) License is loaded) (Optional)	If enabled, external SRTP is supported and optional. It must be negotiated with the remote endpoint. **Note**: If external SRTP is enabled, the number of available voice channels on a Spectralink IP-DECT Server/media resource is reduced from 32 to 16 (if a codec card is used from 24 to 16). Default value: Enabled
Require media encryption (SRTP) (Only visible if Security (TLS, SRTP) License is loaded) (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
Include lifetime in SDES offers (Only visible if Security (TLS, SRTP) License is loaded) (Optional)	Handles the RFC 4568 SRTP lifetime key parameter in SDP offers. Default value: Disabled
Include MKI in SDES offers (Only visible if Security (TLS, SRTP) License is loaded) (Optional)	Handles the RFC 4568 SRTP Master Key Index Parameter in SDP offers. Default value: Disabled
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 pass word. 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.

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. If backup server, enter the fixed IP address or hostname for the master Spectralink IP-DECT Server 6500.
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 is changed to a backup Spectralink IP-DECT Server 6500, or when a backup Spectralink IP-DECT Server 6500 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.

Field	Setting
Redundancy Configuration - Settings	
Failover time(sec)	Enter value for failover time. Failure time is the time in seconds from the Spectralink IP-DECT Server 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" on page 192.

Configuration - Provisioning

Field	Setting
Provisioning Configuration - Server	
Method	The Spectralink IP-DECT/DECT Server must know the protocol and address of server containing the firmware and configuration. The Spectralink IP-DECT/DECT Server can use the following methods to obtain the provisioning server URL: • **Disabled** (The Spectralink IP-DECT/DECT Server 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

Field	Setting
URL	If using **Static** for obtaining the URL of the provisioning server, enter an URL. Accepted format of URL is: [<protocol>://[<user-name>:<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 For more information about protocols and , see "Protocol" on page 1.
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.
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 For more information about polling, SIP Notification Check-Sync method and "check-sync" events, see "Automatic Check for New Firmware and Configuration" on page 1.
Provisioning Configuration - Configuration	
Import	Enable. If enabled, this will make automatic update possible if a default firmware file is available.

Field	Setting
Provisioning Configuration - Users	
Import	Enable. If enabled, this will make automatic update possible.
Provisioning Configuration - Firmware	
Wirelesss 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)	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	
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 - List Users - User

Field	Setting
User - DECT device	
Model	After registration of user and subscription of handset, this field will contain information about the handset model. E.g. Spectralink7742
Software part number	After registration of user and subscription of handset, this field will contain information about the software partnumber. E.g. 14225100
Firmware	After registration of user and subscription of handset, this field will contain information about the firmware version. E.g. PCSJA.
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 sub-scribe. **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" on page 209.
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 phones may need an Access code to register to the Spectralink IP-DECT Server.
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" on page 201. See also Lync/Skype for Business Interoperability Guide.

Field	Setting
Standby text (Optional)	Enter a standby text. 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.
Domain (Optional)	Enter the domain part of a SIP URI. 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). 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 **5208**. **Note**: The user name 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. User name set for individual users
Authentication password (Optional)	Enter the digest credential of the end user. **Note**: The password will override the Default Password field under SIP Configuration.

Field	Setting
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.

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. Spectralink7742
Software part number	After registration of user and subscription of handset, this field will contain information about the software partnumber. 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 phones may need an Access code to register to the Spectralink IP-DECT Server .

Field	Setting
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. If the user is not linked to a handset, the link is inactive and there is no extension number in the text field.
Displayname (Optional)	After creation of user, this field will contain information about user name (e.g. caller ID). E.g. John Doe in John Doe<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 "Example of Handset Registration Data - CSV Format" on page 149.
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**.

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 alllowed. Click **Block**, if you want to block for new calls during firmware update.

Administration - License

Field	
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" on page 43.
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	
Media Resource - General	
IP address (Read only)	Current IP address of the media resource.
Description (Optional)	Enter a description. It is recommended to use a description of the physical location.
Cluster	Default value: Default It is possible to cluster devices that are located at the same location. To assign a cluster to the media resource, select the relevant cluster from the list. For information about defining clusters, see "Configuring Clusters" on page 118.
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	
Base Station - General	
IP address (Read only)	Current IP address of the base station.
Description (Optional)	Enter a description. It is recommended to use a description of the physical location.
RPN	Radio Part Number of the base station.
Cluster	Default value: Default It is possible to cluster devices that are located at the same location. To assign a cluster to the base station, select the relevant cluster from the list. For information about defining clusters, see "Configuring Clusters" on page 118.
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) **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	
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**: 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 - Clusters - Cluster

Field	
Cluster - General	
Name	Enter a name for the cluster. E.g. Site A, Site B, Site C.

Administration - Phonebook

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 "Parameter Overview" on page 223.
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. For an example of LDAP configuation, see "Parameter Overview" on page 223.
URI	Enter the URI of the LDAP server. E.g. ldap://example.com
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.

Field	Setting
Filter (Optional)	Enter the filter used for the LDAP query. The (objectClass-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 dialled, 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

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 - Wireless Server

Field	Setting
Update firmware - Firmware file	
	Click **Browse** to browse for the relevant firmware file. 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	
PCS	Information about default firmware file version (PCS) - if a firmware file has 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.
Build	Information about the build number of default firmware file - if a default firmware file has been uploaded.

Field	Setting
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**.
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. Select either **Default** or **Upload**.
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	
PCS	Information about default firmware file version (PCS) - if a firmware file has 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.
Build	Information about the build number of default firmware file - if a default firmware file has been uploaded.
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**: 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.

Field	Setting
	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. Select either **Default** or **Upload**.
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.