Spectralink Kirk Wireless Server 400, 6500, 2500 and 8000

Provisioning Guide

14184650 version 4.0
April 2013

Copyright Notice

Notice

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

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

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

Spectralink Corporation,
2550 55th Street,
Boulder CO 80301,
USA

Spectralink Europe ApS,
Langmarksvej 34,
8700 Horsens,
Denmark

Table of Contents

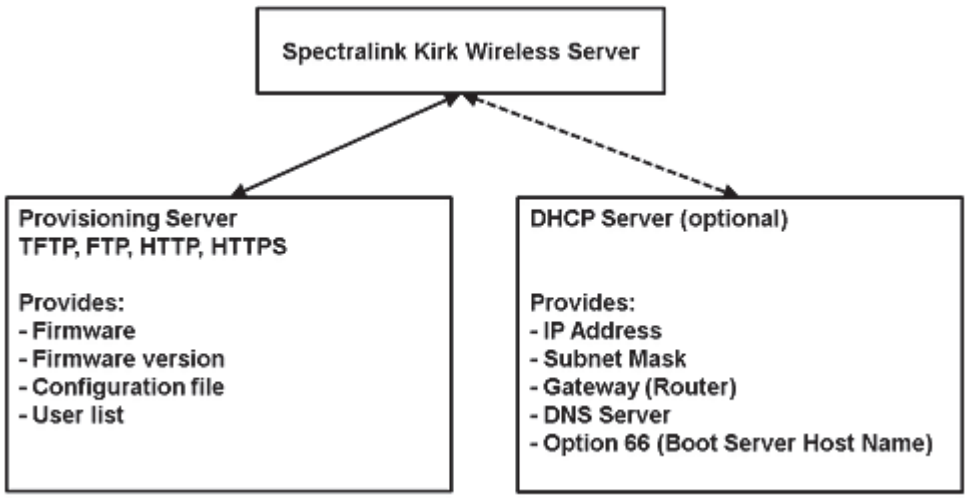
Chapter 1: Provisioning Overview

Both KIRK Wireless Server 400/6500 and KIRK Wireless Server 2500/8000 use a common method for provisioning.

Provisioning Architecture

When the KIRK Wireless Server is powered and configured to use DHCP provisioning, it contacts the DHCP server to obtain the network parameters. If a provisioning server is specified, it contacts the provisioning server to check/update its firmware, configuration and user list.

Figure 1 *Provisioning Architecture*



DHCP Server

When using DHCP, option 66 (TFTP server name) is used to provide the provisioning server URL. This is a string type option configured on the DHCP server of the network.

Provisioning Server

A central provisioning server keeps the firmware and configuration files for the devices. The firmware and configuration is pulled from the provisioning server by the devices using FTP, TFTP, HTTP or HTTPS.

The central provisioning server provides the following files to the KIRK Wireless Server:

Firmware file

A binary file containing the firmware image:

- kws400firmware.bin for KIRK Wireless Server 400
- kws6500firmware.bin for KIRK Wireless Server 6500
- kws8000firmware.bin for KIRK Wireless Server 2500/8000

The filename can be defined in the XML configuration file or it can be typed in the Provisioning -> Firmware -> KIRK Wireless Server field in the web interface.

Firmware version file (.ver)

A text file with text describing the current firmware version (for example, "PCS03__ 18860"):

- kws400firmware.bin.ver for KIRK Wireless Server 400
- kws6500firmware.bin.ver for KIRK Wireless Server 6500
- kws8000firmware.bin.ver for KIRK Wireless Server 2500/8000

The .ver file is included in the firmware package

Configuration file

An XML formatted file (see Appendix B:):

- <KWS MAC address>- config.xml
  example: 0013d1800032-config.xml

User list file

An XML formatted file (see Appendix D:):

- <KWS MAC address>- users.xml
  example: 0013d1800032-users.xml

Chapter 2: Setting Up Provisioning on the KIRK Wireless Server

The KIRK Wireless Server needs to know the protocol and address of the provisioning server containing the firmware and configuration.

Figure 1 *KIRK Wireless Server 400 Configuration -> Provisioning Page*

This information is handled as URL in the format:
`[<protocol>://[<username>:<password>@]]<host>[:<port>][/<path>]`

Examples:

- 10.0.0.10
- tftp://provisioning.test.com
- ftp://192.168.0.1
- ftp://user:password@provisioning.example.com
- http://server.example.com/boot.
- https://server.example.com:10443/boot

The URL can be obtained through the configuration file or through DHCP.

The KIRK Wireless Server can use the following methods to obtain the provisioning server URL:

- Disabled (The KIRK Wireless Server will not use provisioning)
- Static (The administrator must manually specify the URL of the provisioning server)
- DHCP Option 66 (default)

If no provisioning server is configured or obtained, the KIRK Wireless Server will not use auto provisioning.

Protocol

To download the firmware and configuration there are four available protocols: TFTP, FTP, HTTP and HTTPS. All the protocols are available at the target and no additional software is required. Within the provisioning server URL it is specified what protocol to use.

Certificates for HTTPS

When HTTPS is used, the KIRK Wireless Server requires the provisioning server to present a server certificate that can be verified using a known CA certificate. The KIRK Wireless Server firmware is shipped with a bundle of known CA certificates. It is preferred to use a server certificate signed by one of these certificate authorities.

If this is not suitable, a custom CA bundle can be imported into the KIRK Wireless Server via the GUI -> Configuration -> Certificates. The bundle must be in PEM format.

Updated Certificate Authority

As of December 4th 2012, the deliveries of the KIRK Wireless Server 400 and 6500 have an updated SpectraLink Certificate Authority (CA) enclosed. Only the company name has been changed in the CA. When a KIRK Wireless Server 400 or 6500 has been in for repair, they will be returned with an updated SpectraLink CA even though they originally were returned with a Polycom CA.

Use the following link to download the new hosted CA: http://pki.spectralink.com/ aia

Automatic Check for New Firmware and Configuration

When a new firmware or configuration is available, the KIRK Wireless Server must download it. In order to do this, the KIRK Wireless Server needs to know when the data is available. There are two methods supplied for this: Periodic polling and SIP notifications.

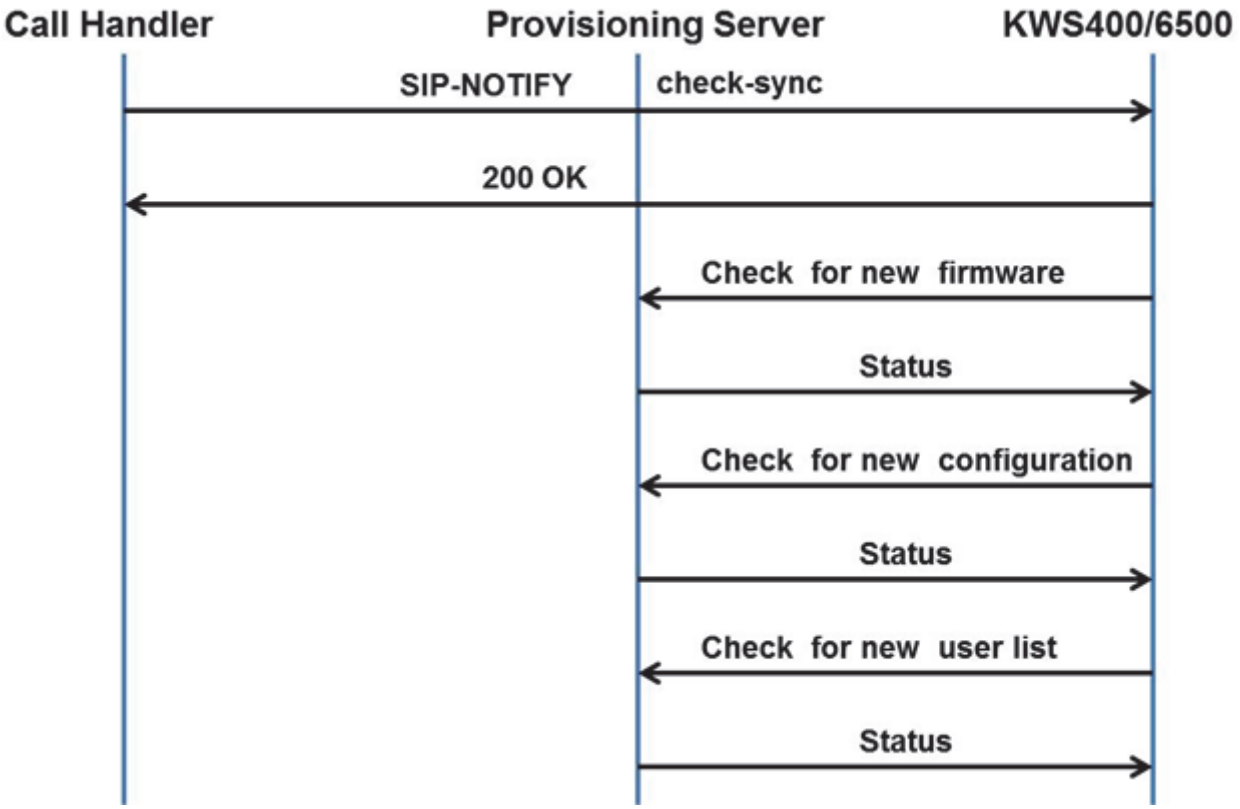
Polling

When polling is selected, the server will automatically initiate a check for updates. The check will be performed at a specified interval or at a specific time.

SIP NOTIFY Check-sync

The optimum way to handle updates is by notifying the KIRK Wireless Server that updates are available. This is done using SIP NOTIFY method with the event "check-sync". A "check-sync" event is sent to one of the extensions/user names handled by the KIRK Wireless Server, and when it is received the KIRK Wireless Server initiates a check for updates.

Figure 2 *Receiving SIP NOTIFY check-sync*



Updating the Firmware

The KIRK Wireless Server will be able to automatically download firmware, configuration and users from a provisioning server. This section provides detailed information about Firmware Update, Configuration Update and User List Update.

Firmware Update

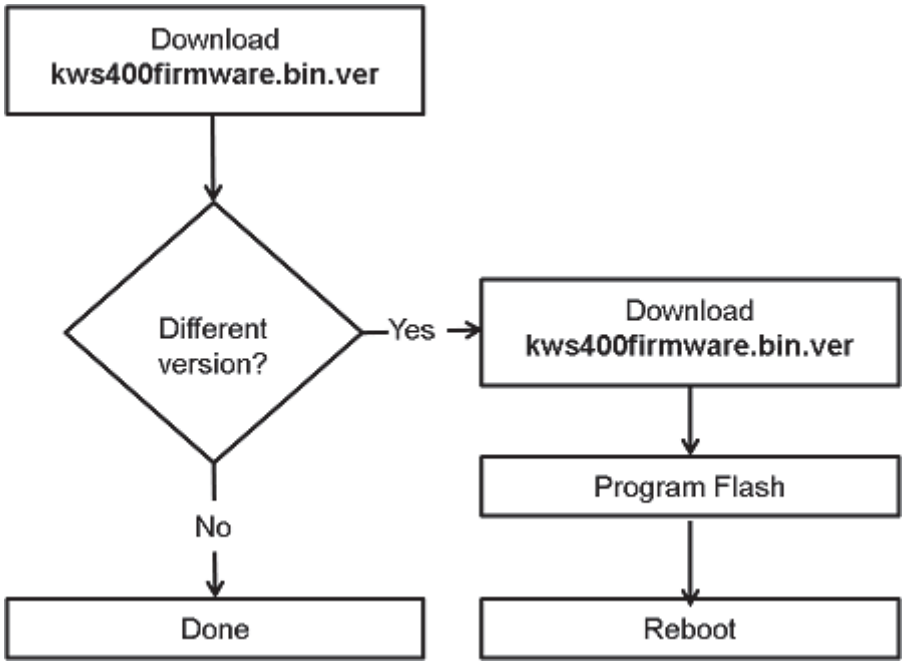
The firmware will be stored as a file on the provisioning server. Together with the firmware file, a firmware version file will be stored. This file is downloaded to determine the version of the firmware without actually downloading the firmware file in order to keep the network load to a minimum.

For flexibility, the name of the firmware file is stored in the XML configuration.

Table 1 *Firmware files*

File	Description
xxxfirmware.bin	A binary file containing the firmware image.
xxxfirmware.bin.ver	A text file with text describing the current firmware version. For example “PCS03_18860

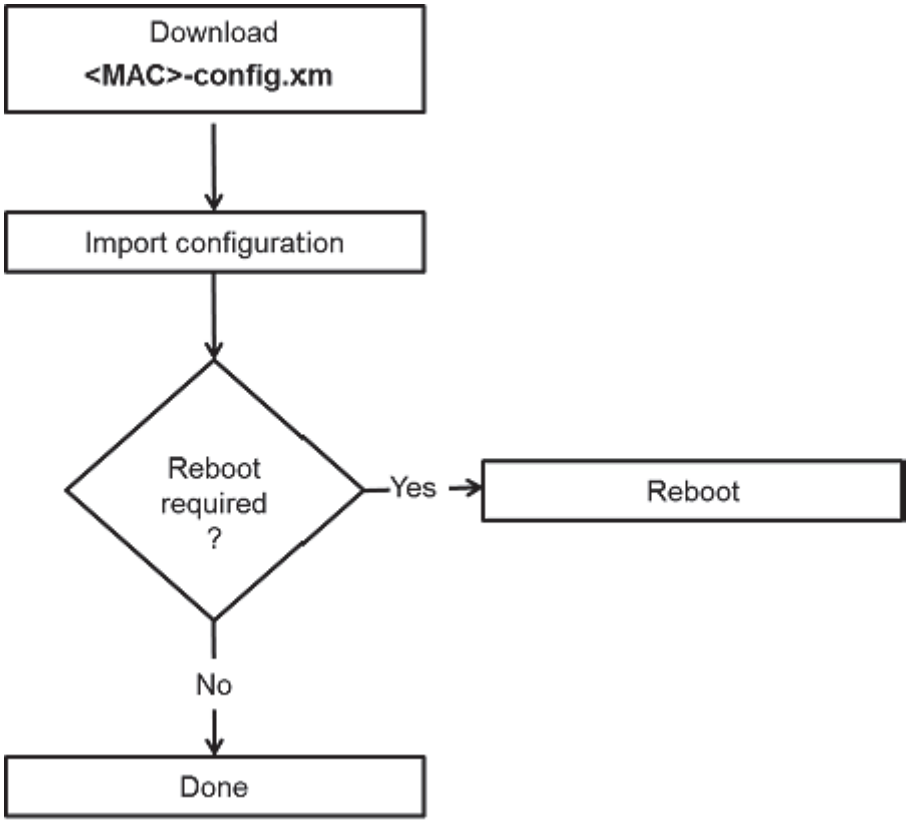
Figure 3 *Example of The Firmware Update Process*



The firmware version specified in the ".ver" file is compared with the firmware version that is currently executed. To avoid problems with different firmware versions being executed and program flash, the KIRK Wireless Server is rebooted immediately after the firmware is updated.

Configuration Update

Figure 4 *Configuration Update Process*



The XML configuration file is downloaded and imported into the KIRK Wireless Server configuration by replacing the existing data.

This guarantees that the data located on the provisioning server and on the DECT server are identical.

User List Update

The users are stored in a separate "<MAC>-users.xml" file. In an existing KIRK Wireless Server installation, the user list file can be retrieved by clicking Users -> Import/Export -> Save XML format.

Each record must have at least a user name field.

Changes in the "<MAC>-users.xml" file do not require a reboot of the system.

Chapter 3: Network Configuration

KIRK Wireless Server requires the network configuration to be part of the config.xml.

Note

If the network configuration is invalid/missing, the device will not be able to boot.

To keep it simple, every configuration parameter is in the <MAC>-config.xml file. The user/administrator does not need to worry about how the provisioned <MAC>-config.xml is merged into the device configuration because it gets updated automatically. Therefore, the configuration is 100% controlled by the provisioning server.

Configuration Example

Here is an example of a sufficient network configuration for DHCP:

```
<network>
  <bootproto>dhcp</bootproto>
</network>
```

This way it is not necessary to configure the network configuration in the provisioning.

Chapter 1: Appendix A

Configuration XML File Reference

The following tables list the configuration file parameters:

Table 1 *Application*

Parameter	Description	Values	KIRK Wireless Server
application.enable_rpc	Specifies if the XML-RPC application interface is enabled.	true/false true – The XML-RPC interface is enabled and applications can connect. false – The XML-RPC interface is disabled. Default: false	400, 6500 2500, 8000
application.enable_msf	Specifies if the MSF application interface is enabled.	true/false true – The MSF interface is enabled and applications can connect. false – The MSF interface is disabled. Default: true	400, 6500
application.internal_messaging	Controls if messaging between handsets is handled internally or by an external application. If enabled messages will be handled internally.	true/false Default: true	400, 6500
application.username	Specifies the user name required for applications to log in.	Default: GW-DECT/admin	400, 6500 2500, 8000
application.password	Specifies the password required for applications to log in.	Default: kws400/kws6500 “f621c2268a8df249 55ef4052bfbb80cf” (password “ip6500” encrypted) Default: kws2500/kws8000 “8e49ea4c7249f802a983ad c7d50375f1”(password “kws8000” encrypted)	400, 6500 2500, 8000

Table 2 *DECT*

Parameter	Description	Values	KIRK Wireless Server
dect.accesscode	Specifies a system wide DECT access code required for subscribing handsets. The access code is from 0 to 8 decimal digits. Access codes assigned for specific users will override this setting.	Example: 1234 Default: Empty	400, 6500
dect.auth_ call	Specifies if DECT authentication should be used when establishing calls.	true/false true – DECT authentication is required when establishing calls. false – DECT authentication of calls is disabled. Default: true	400, 6500
dect.auto_ create_users	config.dect.subscription_allowed	true - autocreat users false - disabled Default: false	400, 6500
dect.encrypt_voice_data	Specifies if DECT encryption should be used for voice calls.	disabled/enabled/inforced Disabled – DECT encryption is disabled. Enabled – DECT encryption is enabled. Enforced – DECT encryption is enforced and calls are terminated if the handset do not support encryption. Default: disabled	400, 6500

Parameter	Description	Values	KIRK Wireless Server
dect.ng_call_control	Controls whether the new context sensitive handset user interface is enabled. If disabled, even handsets which support the context sensitive user interface will operate in standard mode.	true/false Default: true	400, 6500
dect.send_date_time	Specifies if the date and time should be sent to the handsets.	true - send date & time false - do not send date & time Default: true	400, 6500
dect.subscription_allowed	Specifies if handset subscription is allowed.	true - subscription allowed false - subscription disallowed Default: true	400, 6500

Table 3 *Features Codes*

Parameter	Description	Values	KIRK Wireless Server
feature_codes.enable	Enables/disables local handling of feature codes.	true/false Default: false	400, 6500 2500, 8000
feature_codes.call_forward.unconditional.enable	Specifies the feature code used for enabling unconditional call forward (CFU).	The feature code users must dial to enable unconditional call forward. Default: *21*$#.	400, 6500 2500, 8000
feature_codes.call_forward.unconditional.disable	Specifies the feature code used for disabling unconditional call forward (CFU).	The feature code users must dial to disable unconditional call forward. Default: #21#.	400, 6500 2500, 8000

Table 4 *License*

Parameter	Description	Values	KIRK Wireless Server
license	Stores the license, if installed.	A comma separated list of licenses	400, 6500 2500, 8000

Table 5 *Log*

Parameter	Description	Values	KIRK Wireless Server
log.syslog. facility	Specifies the remote syslog facility used for log messages. Refer to RFC5424 for details.	The facility number to be used for the device. An integer between 0 and 23. Default: 16 (“local 0”)	400, 6500
log.syslog. host	Specifies the remote syslog server host address.	Default: Empty	400, 6500
log.syslog. level	Used to specify what log levels to send via syslog. All log messages that have a higher level than the one specified will be sent.	debug/info/notice/ warning/error/critical/ emergency Default: info	400, 6500
log.syslog. port	Specifies the remote port of the syslog server.	The port number on a remote syslog server. Default: Empty which defaults to 514	400, 6500

Table 6 *Network*

Parameter	Description	Values	KIRK Wireless Server
network.bootproto	Specifies if the IP configuration is provided by DHCP or static.	dhcp - get IP config using DHCP static - the IP config is statically defined Default: static	400, 6500 2500, 8000
network.dns1	Specifies the Primary DNS.	Default: Empty	400, 6500 2500, 8000
network.dns2	Specifies the secondary DNS.	Default: Empty	400, 6500 2500, 8000
network.domain	Specifies the name of the domain the system belongs to.	Default: Empty	400, 6500 2500, 8000
network.gateway	Specifies the IP address of the default gateway.	Default: Empty	400, 6500 2500, 8000
network.ipaddr	Specifies the IP address of the system.	Default: 192.168.0.1	400, 6500 2500, 8000
network.mtu	Specifies the Maximum Transmission Unit.	Default: Empty	400, 6500
network.netmask	Specifies the network mask.	Default: 255.255.255.0	400, 6500 2500, 8000
network.ntp	Specifies the address of the NTP server.	Default: Empty	400, 6500 2500, 8000
network.timezone	Specifies the time zone in Posix timezone string format.	Default: CET-1CEST-2,M3.5.0/02:00 :00,M10.5.0/03:00:00	400, 6500 2500, 8000
network.vlan	Specifies the VLAN to which the device belongs.	1-4094 Default: Empty	400, 6500

Table 7 *Phonebook*

Parameter	Description	Values	KIRK Wireless Server
phonebook.csv_number_ fields	Specifies the indexes of the columns that contain dialable numbers.	List of indexes of dialable columns. Default: 2 Example: 2,3	6500 2500, 8000
phonebook.encoding	Specifies the character encoding of the imported CSV file.	utf-8 iso8859-1 windows-1252 Default - utf-8	6500 2500, 8000
phonebook.ldap_attributes	The LDAP attributes to retrieve and user.	Relevant attributes provided by the LDAP server.	6500 2500, 8000
phonebook.ldap_base	The base path where the users are located in the LDAP structure.	Base path from LDAP server.	6500 2500, 8000
phonebook.ldap_bind_password	Password used to login to the LDAP server.	Valid LDAP password.	6500 2500, 8000
phonebook.ldap_bind_ user	user name used to login to the LDAP server.	Valid LDAP user name.	6500 2500, 8000
phonebook.ldap_filter	The filter used for the LDAP query. The (objectClass=person) filter can be used successfully in most cases.	A valid LDAP filter.	6500 2500, 8000
phonebook.ldap_names	The attribute names assigned to the Attributes specified, separated by a comma.	Text strings.	6500 2500, 8000

Parameter	Description	Values	KIRK Wireless Server
phonebook.ldap_prefixes	The phone number prefixes to replace or strip, separated by a comma. For example if the phone number is +45678912345 and the user must dial the 12345 extension, then “+456789” is specified in the strip prefixes field. If a "=" is added, the prefix will be replaced instead of stripped. For example if the phone number is +4576280001 and the user must dial the 004576280001 extension, then “+=00” is specified in the strip prefixes field.	Phone number(s) replace or strip. Default: “+=00” Example: “+45”, “+=00”	6500, 2500, 8000
phonebook.ldap_refresh_ interval	The interval in seconds for querying the LDAP server for updates.	A number of seconds.	6500, 2500, 8000
phonebook.ldap_number_attributes	Specifies the name of the LDAP attributes that contain dialable numbers.	Dialable attributes provided by the LDAP server. Default: telephoneNumber,mobile Example:telephoneNumber, mobile	6500, 2500, 8000
phonebook.source	The source of the phone book data.	disabled - do not enable phone book. csv - import phone book from CSV file. ldap - query LDAP server for phone book data.	6500, 2500, 8000
phonebook.ldap_uri	The URI of the LDAP server.	A valid LDAP URI.	6500, 2500, 8000

Table 8 *Provisioning*

Parameter	Description	Values	KIRK Wireless Server
provisioning.check.check_sync	Specifies how the KIRK Wireless Server will react to SIP NOTIFY check-sync events.	disabled - do not react. reboot - reboot and check for updates update - check for updates and reboot if necessary. Default: disabled.	400, 6500 2500, 8000
provisioning.check.interval	Specifies a checking interval for updates.	0 - do not check for updates periodically. >= 1 - interval in minutes Default: 0	400, 6500 2500, 8000
provisioning.check.time	Specifies a certain checking time for each day. The format is HH:MM.	00:00 - 23:59 Default: Empty	400, 6500 2500, 8000
provisioning.users.check	Specifies if the KIRK Wireless Server will try to download and import users from the provisioning server.	false – do not check for users. true – check for users. Default: false	400, 6500 2500, 8000
provisioning.server.method	Specifies how can the KIRK Wireless Server obtain the provisioning server address.	dhcp static disabled Default: disabled	400, 6500 2500, 8000
provisioning.server.url	Specifies the static provisioning server URL.	Example: ftp://boot.example.com/phones Default: Empty	400, 6500 2500, 8000
provisioning.firmware.kws	Specifies the name of the firmware image to use for the KIRK Wireless Server. The KIRK Wireless Server will check for a version file and a binary file. They must be located as <URL>/<firmware>.bin.ver and <URL>/<firmware>.bin	Example: kws400-flash Default: Empty	400, 6500 2500, 8000

Table 9 *Redundancy*

Parameter	Description	Values	KIRK Wireless Server
redundancy.failover_time	The time in seconds from a redundancy node, detects a failure until it initiates a failover operation.	Default: 15	6500
redundancy.peer	Specifies the hostname or IP address of the redundancy peer node.	Default: none	6500
redundancy.database_ uuid	Represents the unique ID of the distributed database of the system which must match for replication to be performed. When reset on the master it is automatically generated and when reset on the slave, it is retrieved from the master. It must be reset when changing a master node to a slave node or when moving a slave node to another system.	Default: Randomly generated. Example: 6c71a688-23fc-4d54-845c-1b80172dd75e	6500
redundancy.mode	Specifies the mode of the node: either a normal single node system, a master or a slave node in a redundant system.	single/master/slave Default: single	6500

Table 10 *Security*

Parameter	Description	Values	KIRK Wireless Server
security.allow_new_media_resource	Controls whether new media resources are allowed to connect to the KIRK Wireless Server. Any media resource which is known by the KIRK Wireless Server i.e. has been connected before, is allowed to connect regardless of this setting; however new (unknown) media resources will not be allowed if this setting is false.	true/false Default: true	6500
security.allow_new_rfp	Controls whether new base stations are allowed to connect to the KIRK Wireless Server. Any base stations which is known by the KIRK Wireless Server i.e. has been connected before, is allowed to connect regardless of this setting; however new (unknown) base stations will not be allowed if this setting is false.	true/false Default: true	6500
security.force_https	Specifies if the system should enforce remote access security using HTTPS (TLS).	true - force HTTPS (TLS) false - use HTTP Default: false	400, 6500

Parameter	Description	Values	KIRK Wireless Server
security.username	User name of the user who logs on to the web GUI.	Default: admin	400, 6500
security.password	Password for the user who logs on to the web GUI.	Default KIRK Wirless Server 400: kws400 Default KIRK Wireless Server 6500: ip6000	400, 6500
security.srtp_rfp	If enabled, it inforces the use of secure RTP for base station audio connections. If internal SRTP is enabled, the number of available voice channels on each base station is reduced from 12 to 6.	true/false Default: false	6500

Table 11 *SIP*

Parameter	Description	Values	KIRK Wireless Server
sip.auth.password	Specifies the default password for the handset authentication (if no specific handset authentication password is specified).	Default: Empty	400, 6500 2500, 8000
sip.auth.realm	Realm used for SIP authentication. The realm is presented by the SIP server and is used for encrypting the SIP user password.	A string Default: Empty	400, 6500
sip.auth.username	Specifies the default user name for the handset authentication (if no specific handset authentication user name is specified).	Default: Empty	400, 6500 2500, 8000
sip.callwaiting	Used to control whether Call Waiting is enabled.	true/false Default: true	400, 6500 2500, 8000

Parameter	Description	Values	KIRK Wireless Server
sip.client_transaction_timeout	Specifies the timeout for client transactions. This controls timer B and F as specified in RFC3261.	Milliseconds (1000 -32000) Default: 4000	400, 6500 2500, 8000
sip.defaultdomain	Specifies the default domain for the handset (if no specific handset domain is mentioned).	Default: Empty	400, 6500 2500, 8000
sip.dnsmethod	Specifies the DNS method used to resolve host names for SIP requests.	arecord/dnssry arecord: Use simple DNS A records to resolve host names. Basically A records are used to translate a hostname to an IP-address. dnssry: Use DNS SRV records to determine host addresses.Refer to RFC3263. DNS SRV records can be used to specify multiple servers with different priorities and/or multiple servers for load-balancing. Default: arecord.	400, 6500 2500, 8000
sip.dtmf.duration	Specifies the time length of the DTMF tones.	Default: 270	400, 6500 2500, 8000
sip.dtmf.info	Specifies if the keypad signaling should be sent as SIP INFO.	true - send as SIP INFO false - do not send as SIP INFO Default: false	400, 6500 2500, 8000
sip.dtmf.rtp	Specifies if the keypad signaling should be sent as RTP packets with DTMF code.	true - send as RTP false - do not send as RTP Default: true	400, 6500 2500, 8000
sip.dtmf.rtp_payload_type	Specifies the payload type for RFC2833 in SDP offers.	Default: 96	400, 6500 2500, 8000

Parameter	Description	Values	KIRK Wireless Server
sip.gruu	Specifies the use of Globally Routable UA URI (GRUU) which is an URI that routes to a specific UA instance. If enabled, a GRUU will be obtained from a server and communicated to a peer within a SIP dialog.	true/false Default: true	400, 6500
sip.localport	Specifies the SIP port.	Default: 5060	400, 6500 2500, 8000
sip.lync.enable	Enables Lync Server 2010.	true/false Default: false	6500
sip.lync.domain	Specifies the domain of the Lync Server 2010.	Default: Empty	6500
sip.lync.servicename	Specifies the name of the DECT service user account.	Default: Empty	6500
sip.lync.password	Specifies the password of the DECT service user account.	Default: Empty	6500
sip.maxforwards	Specifies the maximum number of times the SIP messages can be forwarded.	Default: 70	400, 6500 2500, 8000
sip.media.codecs	Specifies the codec priority.	Default: 1,2 (for KIRK Wireless Server 400) 1,2,1024,64,0,0 (for KIRK Wireless Server 6500)	400, 6500 2500, 8000
sip.media.port	Specifies the start port for media.	Default: 58000	400, 6500 2500, 8000
sip.media.ptime	Specifies the packet duration for media (ms).	Default: 20	400, 6500 2500, 8000

Parameter	Description	Values	KIRK Wireless Server
sip.media.sdp_answer_ with_preffered	Specifies if the media handling must ignore the remote SDP offer CODEC priorities.	true/false True - ignores remote CODEC priorities. False - honors remote CODEC priorities. Default: false Note: Enabling this option, violates the RFC3264 SDP offer/answer model.	400, 6500
sip.media.sdp_answer_ single	Specifies if the media handling must provide only a single CODEC in SDP answers.	true/false True - provides only a single CODEC. False - Provides all matching CODECs Default: false	400, 6500
sip.media.sdp_hold_attribute_sendonly	When putting a call on hold, the KIRK Wireless Server sends sendonly. Configuring this setting as false, makes the KIRK Wireless Server send inactive.	true/false Default: true	400, 6500
sip.media.sdp_ignore_ version	Specifies whether to ignore the version information in incoming SDP received from remote endpoints.	true/false Default:false	400, 6500
sip.media.sdp_hold_null_ connection	If this setting is true, the KIRK Wireless Server will revert to the old way of signaling a hold.	true/false Default:false	400, 6500

Parameter	Description	Values	KIRK Wireless Server
sip.media.srtp.enable	If enabled, external SRTP is supported and optional. It must be negotiated with the remote endpoint. If external SRTP is enabled the number of available voice channels on a KIRK Wireless Server/media resource is reduced from 32 to 16, (if a codec card is used from 24 to 16).	true/false Default: false	400, 6500
sip.media.srtp.required	If enabled, the usage of SRTP is required. If negotiation of SRTP with the other end is unsuccessful, call establishment is aborted).	true/false Default: false	400, 6500
sip.media.srtp.lifetime	Handles the RFC 4568 SRTP lifetime key parameter in SDP offers.	true/false Default: false	400, 6500
sip.media.srtp.mki	Handles the RFC 4568 SRTP Master Key Index Parameter in SDP offers.	true/false Default: false	400, 6500
sip.media.symmetric	Specifies if the RTP media should use symmetric port.	true - use symmetric RTP false - do not use symmetric RTP Default: false	400, 6500 2500, 8000
sip.media.tos	Specifies the media's TOS/Diffserv.	Default: 184	400, 6500 2500, 8000
sip.mwi.enable	Enables the MWI (Message Waiting Indicator).	true - MWI enabled false - MWI disabled Default: true	400, 6500 2500, 8000
sip.mwi.expire	Specifies the MWI subscription expiration time (s).	Default: 3600	400, 6500 2500, 8000

Parameter	Description	Values	KIRK Wireless Server
sip.mwi.subscribe	Enables MWI subscription.	true - MWI subscription enabled false - MWI subscription disabled Default: false	400, 6500 2500, 8000
sip.onholdtone	Specifies if the handset should hear the on-hold tone when put on-hold.	true - on-hold tone enabled false - on-hold-tone disabled Default: true	400, 6500 2500, 8000
sip.pound_dials_overlap	Specifies if '#' should end overlap dialing.	true - '#' ends overlap dialing false - '#' doesn't end overlap dialing Default: false	400, 6500 2500, 8000
sip.proxy.domain sip.proxy.domain[1-3]	Specifies the SIP Proxy address.	Default: Empty	400, 6500 2500, 8000
sip.proxy.port sip.proxy.port[1-3]	Specifies the SIP Proxy port.	Default: Empty	400, 6500 2500, 8000
sip.proxy.priority sip.proxy.priority[1-3]	Specifies the priority for using a SIP proxy. Proxies with lowest priority will be preferred and higher priorities will be used for failover.	1-4 Default: 1, 2 , 3, 4	400, 6500 2500, 8000
sip.proxy.weight sip.proxy.weight[1-3]	Specifies the weight for using a proxy. If more proxies have the same priority the KIRK Wireless Server will do load balancing using the weight to determine how much each proxy will be loaded.	0 -100 Default: 100	400, 6500 2500, 8000

Parameter	Description	Values	KIRK Wireless Server
sip.proxy.transport	Deprecated. In release PCS07__, this setting is replaced by sip.transport & sip.dnsmethod. The KIRK Wireless Server still understands this setting, but the new settings should be used.	UDPonly - use UDP and simple DNS for resolving IP addresses. DNSsrv - use UDP and DNS Srv for resolving IP addresses. Default: DNSSrv	400, 6500 2500, 8000
sip.registration_expire	Specifies the number of seconds before a SIP registration is renewed.	Default: 3600	400, 6500 2500, 8000
sip.rfc3325	Controls the support of RFC3325 P-Asserted-Identity and P-Preferred-Identity headers. These headers allow trusted parties to assert the identity of authenticated users.	true/false Default: true	400, 6500
sip.send_bye_with_refer	Deprecated. During a call transfer, the existing SIP dialog can be terminated by either the transferor or the transferee. When set to true, the KIRK Wireless Server will terminate the dialog with a BYE request when acting as a transferor.	true/false Default: true	400, 6500
sip.send_to_current_registrar	Specifies if the system should send all the messages to the current registrar.	true - sends all the messages to the current registrar false - does not send all the messages to the current registrar Default: false	400, 6500 2500, 8000

Parameter	Description	Values	KIRK Wireless Server
config.sip.separate_endpoint_ports	Specifies if the endpoints should register on separate ports.	true - register endpoints on separate ports false - do not register endpoints on separate ports Default: false	400, 6500 2500, 8000
sip.showstatustext	Shows the information for the call status in the handset display (ring, hold etc).	true: Show text false: Text is not shown Default: true	400, 6500
sip.tls_allow_insecure	By default, UDP and TCP transports are disabled when TLS transport is the default. If this setting is true, UDP and TCP are allowed as fallback if TLS fails.	true/false Default: false	400, 6500
sip.tos	Specifies the SIP TOS/Diffserv.	Default: 96	400, 6500 2500, 8000
sip.transport	Specifies the transport mechanism used for SIP requests.	UDP, TCP, TLS Default: UDP	400, 6500
sip.use_sips_uri	Normally, SIP communication on a TLS connection is using the SIPS: URI scheme. Disabling this option causes the KIRK Wireless Server to use the SIP: URI scheme with a transport=tls parameter for TLS connections.	true/false Default: true	400, 6500

Table 12 *System Event*

Parameter	Description	Values	KIRK Wireless Server
system_event.msf_between_pp	Used to control if messaging between handsets is handled internally or by an external application. If enabled, messages will be handled internally.	enable– Messages send between handsets are handled internally. disable – All messages are send via an external application. Default: disable	2500, 8000
system_event.internal_clip_presentation_ab	Only in analogue systems with analogue interface cards. If voice call is between internal DECT handsets, the local clip and presentation text is shown, in spite of external clip.	true -enables internal clip (still using clip info from pbx if call is external) false- disables internal clip (using clip info from pbx if available) Default: true	2500, 8000
system_event.ringing_mode	Choose if handset ringing shall follow PBX ringing cadency or internal handset ringing cadency.	1 – follow Exchange(PBX) ringing cadency. 0 – follow System(handset) internal generated ringing cadency. Default: 1	2500, 8000
system_event.min_ringing_time	Only relevant when system_event.ringing_mode=”E” and especially handsets newer than 40xx series. Insures the minimum hear able ringing time in the handset (Tip: If hear able ring time in handset is to short, then use ring tone 6 (Spectralink KIRK handsets).	(units of 10ms) Minimum 40 (equal to 400 ms) Maximum 120 (equal to 1200 ms) Default: 50	2500, 8000
system_event.outgoing_line_prefix	Only use full with Analogue users. The cipher(s) you need to get to the PSTN side of the PBX. Typically prefixes are 0 or 9.	Prefix can contain up to 4 charaters, but is typically only one characters (0-9). Default: Empty	2500, 8000

Parameter	Description	Values	KIRK Wireless Server
system_event.internal_switching_permits	Allow different user types (Analogue-, SIP- and DECT to DECT users) to call each other without involving the (i)PBX, the KIRK Wireless Server will switch the calls internally. Please notice, whenever a 'DECT to DECT' handset is involved in a call, transferrer/hold is not possible.	0 - Only Between DECT to DECT. 3 - Between DECT to DECT and all types of local users. 15 - Internal Setup from PP will result in local switched call. 63 - All local calls. Default: 0	2500, 8000
system_event.system_access_code	Specifies a system wide access code required to subscribe handsets to the system. The system wide access code can be overruled on a per user basis in the user settings.	Empty or 1-8 digits. Default: Empty	2500, 8000
system_event.send_date_ time	Specifies if the date and time will be sent to the handsets.	true – send date & time false – do not send date & time Default: true	2500, 8000
system_event.subscription_allowed	Specifies if handset subscription is allowed or allowed to add a new user when a DECT handset tries to subscribe to the system.	0 - subscription disallowed 1 - subscription allowed 2 – Wildcard (automatically create a subscribed user) Default: 2	2500, 8000

Parameter	Description	Values	KIRK Wireless Server
system_ event.auth_call	Specifies if DECT authentication should be used when establishing calls.	31 – DECT authentication is required when establishing calls. 7 – DECT authentication of calls is disabled. Default: 7	2500, 8000
system_event.sio_passwd	Password for the RS232 interface when used as EMD interface.	Default: Empty	2500, 8000
system_event.encrypt_voice_data	Specifies if DECT encryption should be used for voice calls.	0 – DECT encryption is disabled. 1– DECT encryption is enabled. 2– DECT encryption is enforced and calls are terminated if the handsets do not support encryption. Default:0	2500, 8000

Table 13 *Trace*

Parameter	Description	Values	KIRK Wireless Server
trace_event.level	Trace message level	0 – Disabled 1-Subscription requests are shown. 2 - Level 1 plus exceptional cases, startup and user maintenance (i.e. everything but normal operation). 3 -Level 2 plus call trace messages. 4 -Level 3 plus SIP signaling. 5 -All Trace messages + debug messages. Default:0	2500, 8000

Table 14 *UPnP*

Parameter	Description	Values	KIRK Wireless Server
upnp.enable	Specifies if UPnP support is enabled. If enabled the device will respond to UPnP broadcasts.	true/false Default: true	400, 6500 2500, 8000
upnp.broadcast	Specifies if UPnP announcements are broadcasted. If enabled the device will periodically broadcast announcements.	true/false Default: false	400, 6500 2500, 8000

Appendix B:

Configuration XML File Example

```
  <?xml version="1.0" standalone="yes" ?>
<config>
   <dect>
      <auto_create_users>true</auto_create_users>
      <send_date_time>true</send_date_time>
      <subscription_allowed>true</subscription_allowed>
   </dect>
   <media_resource>
       <enabled>true</enabled>
   </media_resource>
   <network>
       <bootproto>static</bootproto>
       <dns1>172.29.129.5</dns1>
       <domain>emea.spectralink.com</domain>
       <gateway>172.29.192.1</gateway>
       <ipaddr>172.29.202.1</ipaddr>
       <mtu>0</mtu>
       <netmask>255.255.240.0</netmask>
       <ntp>172.29.129.5</ntp>
       <timezone>GMT-1</timezone>
   </network>
   <phonebook>
       <encoding>utf-8</encoding>
       <ldap_attributes>displayName, telephoneNumber</ldap_attributes>
       <ldap_base>OU=Brugere,OU=Horsens,DC=emea,DC=spectralink,
         DC=com</ldap_base>
       <ldap_bind_password>XXXX_XXXX</ldap_bind_password>
       <ldap_bind_user>ldapreader</ldap_bind_user>
       <ldap_filter>(objectClass=person)</ldap_filter>
       <ldap_names>Name, Phone</ldap_names>
       <ldap_prefixes>+4576281,76281,+45</ldap_prefixes>
       <ldap_refresh_interval>3600</ldap_refresh_interval>
       <ldap_uri>ldap://phor1s03.emea.spectralink.com</ldap_uri>
       <source>ldap</source>
   </phonebook>
   <security>
        <force_https>false</force_https>
        <password>XXXXXXXXXXXXXXXXXXXXXXXX</password>
        <username>admin</username>
   </security>
```

```
    <sip>
        <auth>
            <password>1234</password>
            <username>someone</username>
        </auth>
        <defaultdomain>kirktelecom.com</defaultdomain>
        <dtmf>
            <duration>270</duration>
            <info>false</info>
            <rtp>true</rtp>
            <rtp_payload_type>96</rtp_payload_type>
            <rtp_payloadtype>96</rtp_payloadtype>
        </dtmf>
        <localport>5060</localport>
        <maxforwards>70</maxforwards>
        <media>
            <codecs>1,2,0,0,0,0</codecs>
            <port>58000</port>
            <ptime>20</ptime>
            <symmetric>true</symmetric>
            <tos>0</tos>
        </media>
        <mwi>
            <enable>true</enable>
            <expire>3600</expire>
            <subscribe>false</subscribe>
        </mwi>
        <onholdtone>true</onholdtone>
        <pound_dials_overlap>true</pound_dials_overlap>
        <proxy>
            <domain>172.29.200.250</domain>
            <port>5060</port>
            <transport>UDPonly</transport>
        </proxy>
        <registration_expire>3600</registration_expire>
        <send_to_current_registrar>false</send_to_current_registrar>
        <separate_endpoint_ports>false</separate_endpoint_ports>
        <showstatustext>true</showstatustext>
        <tos>0</tos>
    </sip>
</config>
```

Appendix C:

Users XML File Reference

Table 1 *User XML References*

Parameter	Description	Values	KIRK Wireless Server
user.ipei	The DECT IPEI of the users handset	A valid IPEI in the format XXXXX XXXXXXX or empty.	400, 6500 2500, 8000
user.accesscode	Access code required for subscribing the handset to the system	A number with 0-8 digits.	400, 6500 2500, 8000
user.standbytext	The text displayed in the handset when idle	A text string.	400, 6500 2500, 8000
user.username	The user name / extension used when communicating with the SIP server	A valid SIP user name. This field is required.	400, 6500 2500, 8000
user.domain	The SIP domain for the user; used if the user has a different domain than the system default	A valid domain name.	400, 6500 2500, 8000
user.displayname	The display name sent with SIP requests.	A valid SIP display name.	400, 6500 2500, 8000
user.authuser	User name for authenticating the user.	A valid SIP authentication user name.	400, 6500 2500, 8000
user.authpassword	Password for authenticating the user.	A valid SIP password.	400, 6500 2500, 8000
user.disabled	Indicates if the user is disabled and unable to make calls.	true - user is disable. false - user is enabled.	400, 6500 2500, 8000
user.lid	Line IDentifier is only supposed to be used with analogue interface cards. xxyyzzzz xx is shelf number yy is card number in shelf zzzz is line number on analogue card	xx - (01 – 08) yy – (01-08) zzzz – (0000 - 0015) empty or leave out if user is not assigned to a analogue interface card.	2500, 8000

Parameter	Description	Values	KIRK Wireless Server
user.linetype	Type of interface the handset is subscribed to.	D : DECT to DECT S : SIP interface A : Analgue interface	2500, 8000
user.presentationtext	Presentation text can be shown on the display of the handset(only for handsets subscribed to an analogue interface) which makes a local call. (system_event.internal_clip_presentation_ab)	true : show presentation text false : Don NOT show presentation text. Default: false	2500, 8000
user.name	Typically the name of the function or user who is using the handset.	A text string	2500, 8000
user.localno	Localno is typically the same as user.username. But in case of difference the localnumber (DN) can be used for addressing the handset when sending text messages.	Max 12 characters, local number (DN) is mandatory.	2500, 8000
user.tx_gain	Adding gain to the handsets transmit path. Not possible to add gain for DECT to DECT users.	From -12 to 12 dB Default :0	2500, 8000
user.rx_gain	Adding gain to the handsets receive path. Not possible to add gain for DECT to DECT users..	From -12 to 12 dB Default :0	2500, 8000

Appendix D:

Users XML File Example

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<users>
  <user>
    <ipei>00077 0000001</ipei>
    <accesscode></accesscode>
    <standbytext>2639 </standbytext>
    <username>2639</username>
    <domain></domain>
    <displayname>Morten Mortensen</displayname>
    <authuser>2639</authuser>
    <authpassword>1234</authpassword>
    <disabled>true</disabled>
  </user>
  <user>
    <ipei>00077 0000002</ipei>
    <accesscode></accesscode>
    <standbytext>2638 </standbytext>
    <username>2638</username>
    <domain></domain>
    <displayname>Ole Olsen</displayname>
    <authuser>2638</authuser>
    <authpassword>1234</authpassword>
    <disabled>true</disabled>
  </user>
</users>
```

Figures

Tables