

Polycom® KIRK® Wireless Server 300 & 6000

Provisioning Guide

14184650 Version 2

Copyright © Polycom, Inc.
All Rights Reserved

Catalog No. 14184650
Version 2.0

Proprietary and Confidential

The information contained herein is the sole intellectual property of Polycom, Inc. No distribution, reproduction or unauthorized use of these materials is permitted without the expressed written consent of Polycom, Inc. Information contained herein is subject to change without notice and does not represent commitment of any type on the part of Polycom, Inc. Polycom and Accord are registered trademarks of Polycom, Inc.

Notice

While reasonable effort was made to ensure that the information in this document was complete and accurate at the time of printing, Polycom, Inc., cannot assume responsibility for any errors. Changes and/or corrections to the information contained in this document may be incorporated into future issues.

Table of Contents

Provisioning Overview

Provisioning Architecture	-1
DHCP Server	-2
Provisioning Server	-2
Setting Up Provisioning on the KIRK Wireless Server	-3
Protocol	-4
Certificates for HTTPS	-4
Automatic Check for New Firmware and Configuration	-4
Polling	-4
SIP NOTIFY Check-sync	-5
Updating the Firmware	-5
Firmware Update	-5
Configuration Update	-7
User List Update	-7
Network Configuration	-8

Appendix A: Configuration XML File Reference

Appendix B: Configuration XML File Example

Appendix C: Users XML File Reference

Appendix D: Users XML File Example

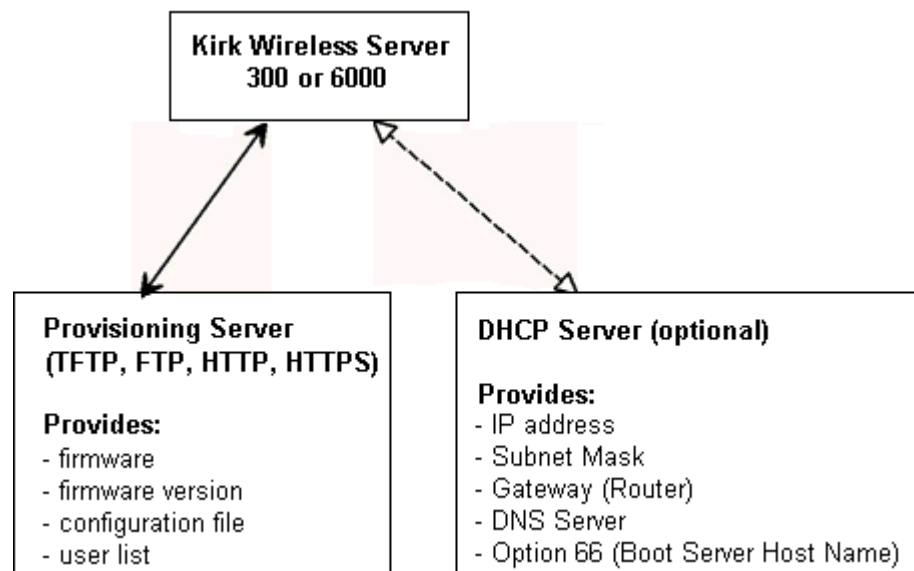
Provisioning Overview

Both Kirk Wireless Server 300 and Kirk Wireless Server 6000 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:

- kws300firmware.bin for Kirk Wireless Server 300
- kws6000firmware.bin for Kirk Wireless Server 6000

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

Firmware version file

A text file with text describing the current firmware version (e.g. "PCS03__18860"):

- kws300firmware.bin.ver for Kirk Wireless Server 300
- kws6000firmware.in.ver for Kirk Wireless Server 6000

The .ver file is included in the firmware package

Configuration file

An XML formatted file (see [Appendix B: Configuration XML File Example](#)):

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

User list file

An XML formatted file (see [Appendix D: Users XML File Example](#)):

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

Setting Up Provisioning on the KIRK Wireless Server

Figure -2 KWS300 Configuration -> Provisioning Page

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

This information is handled as URL in the format:

[<protocol>://[<username>:<password>@]]<host>[:<port>][/<path>]

Examples:

- 10.0.0.10 ; tftp used as default protocol
- 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 three 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.

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.

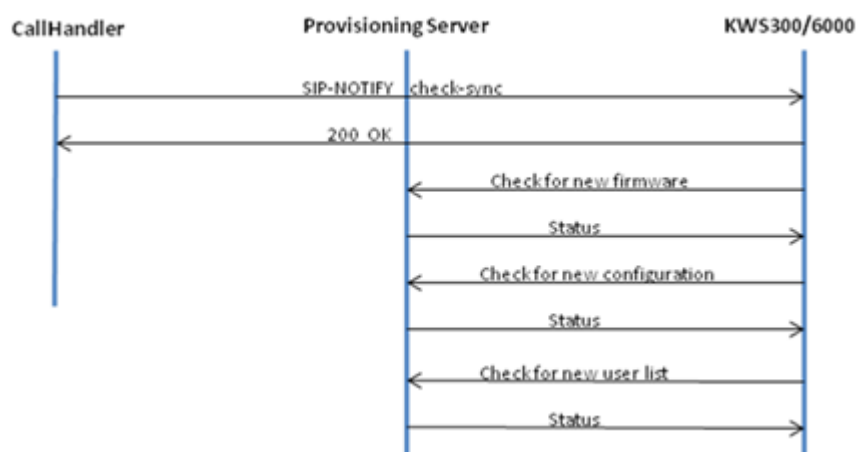
Polling

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/username handled by the Kirk Wireless Server, and when it is received the Kirk Wireless Server initiates a check for updates.

Figure -3 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

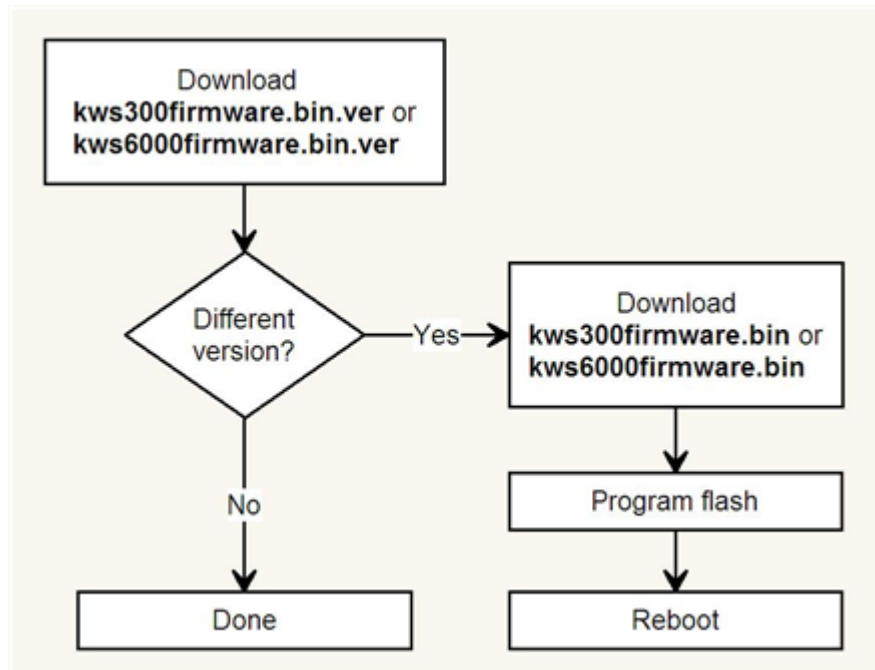
The firmware will be stored as a file on the provisioning server. Together with the firmware file, a firmware version file will be stored. This file is downloaded to determine the version of the firmware without actually downloading the firmware file in order to keep the network load to a minimum.

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

Table -1 Firmware files

File	Description
kws300firmware.bin	A binary file containing the firmware image.
kws300firmware.bin.ver	A text file with text describing the current firmware version. For example "PCS03_18860"

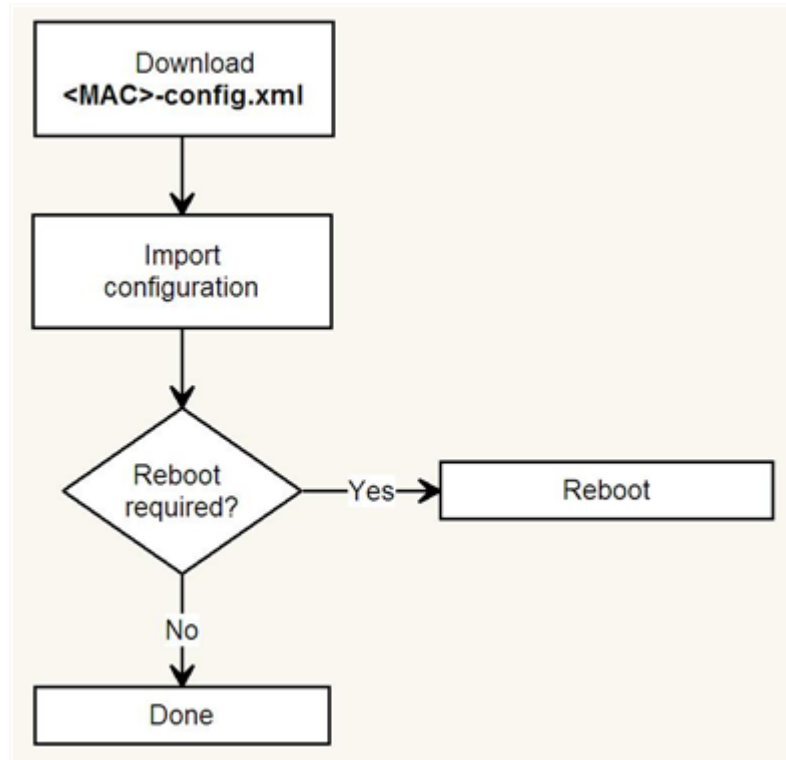
Figure -4 Firmware Update Process



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 -5 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 username field.

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

Network Configuration

Kirk Wireless Server 300 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.

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.

Appendix A: Configuration XML File Reference

The following tables list the configuration file parameters:

Table A-1 Application

Parameter	Description	Values
config.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
config.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
config.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
config.application.username	Specifies the username required for applications to log in.	Default: GW-DECT/admin

Parameter	Description	Values
config.application.password	Specifies the password required for applications to log in.	Default: "f621c2268a8df24955ef4052bffb80c" (password "ip6000" encrypted)

Table A-2 DECT

Parameter	Description	Values
config.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
config.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
config.dect.auto_create_users	config.dect.subscription_allowed	true - autocreat users false - disabled Default: false
config.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
config.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

Parameter	Description	Values
config.dect.subscription_allowed	Specifies if handset subscription is allowed	true - subscription allowed false - subscription disallowed Default: true

Table A-3 Features Codes

Parameter	Description	Values
config.feature_codes.enable	Enables/disables local handling of feature codes.	true/false Default: false
config.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*\$.
config.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#.

Table A-4 License

Parameter	Description	Values
config.license	Stores the license, if installed.	A comma separated list of licenses

Table A-5 Log

Parameter	Description	Values
config.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")
config.log.syslog.host	Specifies the remote syslog server host address.	Default: Empty

Parameter	Description	Values
config.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
config.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

Table A-6 Network

Parameter	Description	Values
config.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
config.network.dns1	Specifies the Primary DNS	Default: Empty
config.network.dns2	Specifies the secondary DNS	Default: Empty
config.network.domain	Specifies the name of the domain the system belongs to	Default: Empty
config.network.gateway	Specifies the IP address of the default gateway	Default: Empty
config.network.ipaddr	Specifies the IP address of the system	Default: 192.168.0.1
config.network.mtu	Specifies the Maximum Transmission Unit	Default: Empty
config.network.netmask	Specifies the network mask	Default: 255.255.255.0

Parameter	Description	Values
config.network.ntp	Specifies the address of the NTP server	Default: Empty
config.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
config.network.vlan	Specifies the VLAN to which the device belongs.	1-4094 Default: Empty

Table A-7 Phonebook

Parameter	Description	Values
config.phonebook.csv_number_fields	Specifies the indexes of the columns that contain dialable numbers. <i>Note: Available only on KWS6000.</i>	List of indexes of dialable columns. Default: 2 Example: 2,3
config.phonebook.encoding	Specifies the character encoding of the imported CSV file. <i>Note: Available only on KWS6000.</i>	utf-8 iso8859-1 windows-1252 Default - utf-8
config.phonebook.ldap_attributes	The LDAP attributes to retrieve and user <i>Note: Available only on KWS6000.</i>	Relevant attributes provided by the LDAP server.
config.phonebook.ldap_base	The base path where the users are located in the LDAP structure <i>Note: Available only on KWS6000.</i>	Base path from LDAP server.
config.phonebook.ldap_bind_password	Password used to login to the LDAP server. <i>Note: Available only on KWS6000.</i>	Valid LDAP password.
config.phonebook.ldap_bind_user	Username used to login to the LDAP server. <i>Note: Available only on KWS6000.</i>	Valid LDAP user name.

Parameter	Description	Values
config.phonebook.ldap_filter	The filter used for the LDAP query. The (objectClass=person) filter can be used successfully in most cases. <i>Note: Available only on KWS6000.</i>	A valid LDAP filter.
config.phonebook.ldap_names	The attribute names assigned to the Attributes specified, separated by a comma. <i>Note: Available only on KWS6000.</i>	Text strings.
config.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. <i>Note: Available only on KWS6000.</i>	Phone number(s) replace or strip. Default: "+=00" Example: "+45", "+=00"
config.phonebook.ldap_refresh_interval	The interval in seconds for querying the LDAP server for updates. <i>Note: Available only on KWS6000.</i>	A number of seconds.

Parameter	Description	Values
config.phonebook.ldap_number_attributes	Specifies the name of the LDAP attributes that contain dialable numbers. <i>Note: Available only on KWS6000.</i>	Dialable attributes provided by the LDAP server. Default: telephoneNumber,mobile Example:telephoneNumber, mobile
config.phonebook.source	The source of the phone book data. <i>Note: Available only on KWS6000.</i>	disabled - do not enable phone book. csv - import phone book from CSV file. ldap - query LDAP server for phone book data.
config.phonebook.ldap_uri	The URI of the LDAP server. <i>Note: Available only on KWS6000.</i>	A valid LDAP URI.

Table A-8 Provisioning

Parameter	Description	Values
config.provisioning.check.check_sync	Specifies how the KWS 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.
config.provisioning.check.interval	Specifies a checking interval for updates.	0 - do not check for updates periodically. >= 1 - interval in minutes Default: 0
config.provisioning.check.time	Specifies a certain checking time for each day. The format is HH:MM	00:00 - 23:59 Default: Empty
config.provisioning.users.check	Specifies if the KWS will try to download and import users from the provisioning server.	false – do not check for users. true – check for users. Default: false

Parameter	Description	Values
config.provisioning.server.method	Specifies how can the KWS obtain the provisioning server address.	dhcp static disabled Default: disabled
config.provisioning.server.url	Specifies the static provisioning server URL.	Example: ftp://boot.example.com/p/hones Default: Empty
config.provisioning.firmware.kws	Specifies the name of the firmware image to use for the KWS. The KWS will check for a version file and a binary file. They must be located as <URL>/<firmware>.bin.ver and <URL>/<firmware>.bin	Example: kws300-flash Default: Empty

Table A-9 Redundancy

Parameter	Description	Values
config.redundancy.failover_time	The time in seconds from a redundancy node, detects a failure until it initiates a failover operation. <i>Note: Available only on KWS6000.</i>	Default: 15
config.redundancy.peer	Specifies the hostname or IP address of the redundancy peer node. <i>Note: Available only on KWS6000.</i>	Default: none
config.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. <i>Note: Available only on KWS6000.</i>	Default: Randomly generated. Example: 6c71a688-23fc-4d54-845c-1b80172dd75e
config.redundancy.mode	Specifies the mode of the node: either a normal single node system, a master or a slave node in a redundant system. <i>Note: Available only on KWS6000.</i>	single/master/slave Default: single

Table A-10 Security

Parameter	Description	Values
config.security.allow_new_media_resource	Controls whether new media resources are allowed to connect to the KWS. Any media resource which is known by the KWS 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. <i>Note: Available only on KWS 6000</i>	true/false Default: true
config.security.allow_new_rfp	Controls whether new base stations are allowed to connect to the KWS. Any base stations which is known by the KWS 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. <i>Note: Available only on KWS 6000</i>	true/false Default: true
config.security.force_https	Specifies if the system should enforce remote access security using HTTPS (TLS)	true - force HTTPS (TLS) false - use HTTP Default: false
config.security.username	Username for the user who logs on to the web GUI	Default: admin
config.security.password	Password for the user who logs on to the web GUI	Default KWS300: kws300 Default KWS6000: ip6000

Parameter	Description	Values
config.security.srtp_rfp	<p>If enabled, it enforces the use of secure RTP for base station audio connections.</p> <p>If internal SRTP is enabled, the number of available voice channels on each base station is reduced from 12 to 6.</p> <p><i>Note: Available only on KWS 6000.</i></p>	<p>true/false</p> <p>Default: false</p>

Table A-11 SIP

Parameter	Description	Values
config.sip.auth.password	Specifies the default password for the handset authentication (if no specific handset authentication password is specified)	Default: Empty
config.sip.auth.username	Specifies the default username for the handset authentication (if no specific handset authentication username is specified)	Default: Empty
config.sip.callwaiting	Used to control whether Call Waiting is enabled.	<p>true/false</p> <p>Default: true</p>
config.sip.client_transaction_timeout	Specifies the timeout for client transactions. This controls timer B and F as specified in RFC3261.	<p>Milliseconds (1000-32000)</p> <p>Default: 4000</p>
config.sip.defaultdomain	Specifies the default domain for the handset (if no specific handset domain is mentioned)	Default: Empty

Parameter	Description	Values
config.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.
config.sip.dtmf.duration	Specifies the time length of the DTMF tones	Default: 270
config.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
config.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
config.sip.dtmf.rtp_payload_type	Specifies the payload type for RFC2833 in SDP offers	Default: 96
config.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
config.sip.localport	Specifies the SIP port	Default: 5060
config.sip.lync.enable	Enables Lync Server 2010 <i>Note: Available only on KWS 6000</i>	true/false Default: false

Parameter	Description	Values
config.sip.lync.domain	Specifies the domain of the Lync Server 2010 <i>Note: Available only on KWS 6000</i>	Default: Empty
config.sip.lync.servicename	Specifies the name of the DECT service user account. <i>Note: Available only on KWS 6000</i>	Default: Empty
config.sip.lync.password	Specifies the password of the DECT service user account. <i>Note: Available only on KWS 6000</i>	Default: Empty
config.sip.maxforwards	Specifies the maximum number of times the SIP messages can be forwarded	Default: 70
config.sip.media.codecs	Specifies the codec priority	Default: 1,2 (for KWS300) 1,2,1024,64,0,0 (for KWS6000)
config.sip.media.port	Specifies the start port for media	Default: 58000
config.sip.media.ptime	Specifies the packet duration for media (ms)	Default: 20
config.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.
config.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

Parameter	Description	Values
config.sip.media.sdp_ignore_version	Specifies whether to ignore the version information in incoming SDP received from remote endpoints.	true/false Default:false
config.sip.media.sdp_hold_null_connection	If this setting is true, the KWS will revert to the old way of signaling a hold.	true/false Default:false
config.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 KWS/media resource is reduced from 32 to 16, (if a codec card is used from 24 to 16).	true/false Default: false
config.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
config.sip.media.srtp.lifetime	Handles the RFC 4568 SRTP lifetime key parameter in SDP offers.	true/false Default: false
config.sip.media.srtp.mki	Handles the RFC 4568 SRTP Master Key Index Parameter in SDP offers.	true/false Default: false
config.sip.media.symmetric	Specifies if the RTP media should use symmetric port	true - use symmetric RTP false - do not use symmetric RTP Default: false
config.sip.media.tos	Specifies the media's TOS/Diffserv	Default: 184
config.sip.mwi.enable	Enables the MWI (Message Waiting Indicator)	true - MWI enabled false - MWI disabled Default: true

Parameter	Description	Values
config.sip.mwi.expire	Specifies the MWI subscription expiration time (s)	Default: 3600
config.sip.mwi.subscribe	Enables MWI subscription	true - MWI subscription enabled false - MWI subscription disabled Default: false
config.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
config.sip.pound_dials_overlap	Specifies if '#' should end overlap dialing	true - '#' ends overlap dialing false - '#' doesn't end overlap dialing Default: false
config.sip.proxy.domain config.sip.proxy.domain [1-3]	Specifies the SIP Proxy address	Default: Empty
config.sip.proxy.port config.sip.proxy.port[1-3]	Specifies the SIP Proxy port	Default: Empty
config.sip.proxy.priority config.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
config.sip.proxy.weight config.sip.proxy.weight [1-3]	Specifies the weight for using a proxy. If more proxies have the same priority the KWS will do load balancing using the weight to determine how much each proxy will be loaded.	0 -100 Default: 100

Parameter	Description	Values
config.sip.proxy.transport	<p>Deprecated. In release PCS07__, this setting is replaced by sip.transport & sip.dnsmethod.</p> <p>The KWS still understands this setting, but the new settings should be used.</p>	<p>UDPonly - use UDP and simple DNS for resolving IP addresses.</p> <p>DNSSrv - use UDP and DNS Srv for resolving IP addresses.</p> <p>Default: DNSSrv</p>
config.sip.registration_expire	Specifies the number of seconds before a SIP registration is renewed	Default: 3600
config.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.	<p>true/false</p> <p>Default: true</p>
config.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 KWS will terminate the dialog with a BYE request when acting as a transferor.	<p>true/false</p> <p>Default: true</p>
config.sip.send_to_current_registrar	Specifies if the system should send all the messages to the current registrar	<p>true - sends all the messages to the current registrar</p> <p>false - does not send all the messages to the current registrar</p> <p>Default: false</p>
config.sip.separate_endpoint_ports	Specifies if the endpoints should register on separate ports	<p>true - register endpoints on separate ports</p> <p>false - do not register endpoints on separate ports</p> <p>Default: false</p>
config.sip.showstatustext	Shows the information for the call status in the handset display (ring, hold etc)	<p>true: Show text</p> <p>false: Text is not shown</p> <p>Default: true</p>

Parameter	Description	Values
config.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
config.sip.tos	Specifies the SIP TOS/Diffserv	Default: 96
config.sip.transport	Specifies the transport mechanism used for SIP requests	UDP, TCP, TLS Default: UDP
config.sip.use_sips_uri	Normally, SIP communication on a TLS connection is using the SIPS: URI scheme. Disabling this option causes the KWS to use the SIP: URI scheme with a transport=tls parameter for TLS connections.	true/false Default: true

Table A-12 UPnP

Parameter	Description	Values
config.upnp.enable	Specifies if UPnP support is enabled. If enabled the device will respond to UPnP broadcasts.	true/false Default: true
config.upnp.broadcast	Specifies if UPnP announcements are broadcasted. If enabled the device will periodically broadcast announcements.	true/false Default: false

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.polycom.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=polycom,
      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.polycom.com</ldap_uri>
    <source>ldap</source>
```

```
</phonebook>
<security>
  <force_https>false</force_https>
  <password>XXXXXXXXXXXXXXXXXXXXXXXXXX</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 C-1 User XML References

Parameter	Description	Values
users.user.ipei	The DECT IPEI of the users handset	A valid IPEI in the format XXXXX XXXXXXX or empty.
users.user.accesscode	Access code required for subscribing the handset to the system	A number with 0-8 digits.
users.user.standbytext	The text displayed in the handset when idle	A text string.
users.user.username	The user name / extension used when communicating with the SIP server	A valid SIP user name. This field is required.
users.user.domain	The SIP domain for the user; used if the user has a different domain than the system default	A valid domain name.
users.user.displayname	The display name sent with SIP requests.	A valid SIP display name.
users.user.authuser	User name for authenticating the user.	A valid SIP authentication user name.
users.user.authpassword	Password for authenticating the user.	A valid SIP password.
users.user.disabled	Indicates if the user is disabled and unable to make calls.	true - user is disable. false - user is enabled.

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>
```

Tables

Table -1	Firmware files	-6
Table A-1	Application	A-1
Table A-2	DECT	A-2
Table A-3	Features Codes	A-3
Table A-4	License	A-3
Table A-5	Log	A-3
Table A-6	Network	A-4
Table A-7	Phonebook	A-5
Table A-8	Provisioning	A-7
Table A-9	Redundancy	A-9
Table A-10	Security	A-10
Table A-11	SIP	A-11
Table A-12	UPnP	A-17
Table C-1	User XML References	C-1

Figures

Figure -1	Provisioning Architecture	-1
Figure -2	KWS300 Configuration -> Provisioning Page	-3
Figure -3	Receiving SIP NOTIFY check-sync	-5
Figure -4	Firmware Update Process	-6
Figure -5	Configuration Update Process	-7