KIRK Release Note

KWS6000

Firmware Version PCS04B_
October 20/2009

Table of Contents

1. General

This release note applies to released versions of the KWS6000 Firmware. This version specifically applies to version PCS04B_of the KWS6000 Firmware. This release replaces the PCS04A_ release as the latest generally available (GA) release.

1.1 Important Notes

Some features require specific versions of the firmware loaded into the base stations or media resources.

1.2 Feature License and Platform Limitations

The following table summarizes features that require a particular hardware platform and / or a license key for activation.

Feature	**Comment**
DECT frequency swap	License required.

1.3 System Requirements

Hardware Platform:	**Description**
KWS6000 HW PCS 3C or newer	KWS6000 Server
Media Resource 6000 HW PCS 3C or newer	Media Resource 6000

2. Terms and Definitions

WCAG Web Content Accessibility Guidelines. W3C Recommendation. These guidelines explain how to make Web content accessible to people with disabilities.

3. Distribution Files

Click here >> to find the firmware image of the KWS6000.

4. Changes

4.1 Version PCS04B_ - October 20, 2009

4.1.1 Added or Changed Features

- None

4.1.2 Removed Features

- None

4.1.3 Corrections

- Removed potential media resource problem present in firmware PCS04__ and PCS04A_.

This problem would result in the loss of all active calls on the media resource and a subsequent restart of the media resource.

- Removed delay in the media stream after re-configuring media with re-INVITE.
  For example, after placing a call on and off hold a delay was introduced in the voice stream.

4.1.4 Configuration File Parameter Changes

- None

4.2 Version PCS04A_ October 12/2009

4.2.1 Added or Changed Features

- None

4.2.2 Removed Features

- None

4.2.3 Corrections

- Corrected provisioning check at specific time.
  If the device was configured to check for updates at a specific time each day, the device would only check for updates twice.
- XML-RPC application interface: The method end_call_display() ignored the setupspec1 parameter.
- Removed memory leak related to DECT encryption.
  After handling 2,000,000 calls with DECT encryption, the device will run out of memory.

4.2.4 Configuration File Parameter Changes

- None

4.3 Version PCS04__ Q4/2009

4.3.1 Added or Changed Features

- Added support for entering more SIP proxies for failover and load balancing.
  This feature is relevant in a setup with more than one SIP proxy. In this case it is now possible to manually enter the SIP URI of the proxies, in earlier releases this could only be done with DNS-SRV.
- Added UPnP for discovery of devices.
  UPnP is an acronym for Universal Plug and Play. If for some reason, the IP-address of the device is unknown (e.g. forgotten or DHCP-assigned), UPnP can be utilized to easily identify the IP-address of the device. If “My Network Places” in Windows is setup to show icons for networked UPnP devices, every KWS300/6000, Media-resource, and Base station will be present in “My Network Places”.
- Added method for manipulating settings by requesting an URL.

  - http[s]://<host>/config/get?<key> – http://192.168.0.1/config/get?sip.proxy.domain
  - http[s]://<host>/config/set?<key>=<value> – http://192.168.0.1/config/set?sip.proxy.domain=example.com
- Improved jitter buffer.
  The sound quality on IP-connections experiencing jitter issues is improved considerably.
- Improved the user interface for managing base stations, media resources, clusters and users.
  Several improvements are made based upon customer feedback. Previously when e.g. manually editing or adding e.g. users, after pressing "Save" the GUI would present a new screen acknowledging that the user was edited/added ok. On this screen the user had to press "OK". This is now changed so that after pressing save the user is returned to the list. A dialog screen is only presented to the user if something goes wrong. As a result, the number of mouse-clicks required to do repetitive tasks with regard to editing/creating items in a list has been reduced.
- Improved the user interface for central firmware update.
  After making a central firmware upgrade of e.g., media-resources and base station, the media-resources/base stations need to be re-booted before the new firmware is active. The system will continue to run the previous firmware until a reboot of the devices. This allows for a non-intrusive firmware upgrade, which can be done on the system without affecting normal operation. However, this also means that if the devices are not rebooted the system will continue to run on the old firmware. The user interface has been updated to clarify this.
- Improved the user interface with respect to the auto-sync feature of base stations.
  The auto-sync feature for base stations is only for usage while deploying the system. This was not clear in the user-interface. A more descriptive text has been added and a warning is issued if auto-sync is enabled.
- Added XML-RPC application interface.
  The new XML-RPC based application interface uses open standards and is easy to use. This interface gives access to the same functionality as the existing MSF interface but is not based on a Microsoft Windows API. The existing MSF interface will not be affected.
- Added HTTP/1.1 persistent connections support to the built-in HTTP server. This is mainly done to increase performance on the XML-RPC interface when using HTTPS.
- Improved security measures. Formerly every time a dect device would enter the range of the system (making a location registration) the device was authenticated. Starting with this release additional authentication is performed every time a call is established. Furthermore it is now possible to enable dect encryption of voice sent over the air. In previous firmware revisions all dect communication in the air is scrambled, enabling encryption will additionally encrypt voice with an encryption key. A new key will be calculated for each new call.
  IMPORTANT NOTICE!! If dect encryption is enabled it is NOT possible to use repeaters on the system.
  IMPORTANT NOTICE!! If dect encryption is enabled it requires base station firmware version PCS04__ or higher.
- Removed unnecessary warning: HL_ME_RESOURCE_ALLOCATE_req resource already allocated.

- Changed the User-Agent name for the provisioning HTTP client.

4.3.2 Removed Features

- None

4.3.3 Corrections

- Dialog event package – notify dialog terminated when a call is rejected.
- Drop RTP packages with unexpected payload without trying to play them.
- Do not crash with high load of MSF and message waiting indication (MWI) traffic.
- Fixed problem where the maximum CLMS broadcast data length was reduced with one byte.
- Do not show 0kB captured when less than 1kB is captured by the packet capture function.
- Fixed a bug not allowing the user to enter POSIX time zones via the GUI.
- Do not crash when using DNS SRV and deleting a user.
- When users are controlled via provisioning – do not indicate users as changed when the handset has reported a firmware version. This caused the system to report the user data as changed when auto provisioning users even with no changes.
- Removed crash when attempting to change the standby text for non-KIRK handset.
- Handle international characters better in phonebook. The matched part of a search was not displayed correctly when international letters was part of the match.
- Make phonebook stop logging a warning when LDAP server is slow.

4.3.4 Configuration File Parameter Changes

File	Action	Parameter	Description
config.xml	Added	application.enable_rpc	Specifies if the XML-RPC application interface is enabled. true – The XML-RPC interface is enabled and applications can connect. false – The XML-RPC interface is disabled. Default: false
config.xml	Added	dect.auth_call	Specifies if DECT authentication should be used when establishing calls. true – DECT authentication is required when establishing calls. false – DECT authentication of calls is disabled. Default: true
config.xml	Added	dect.encrypt_voice_data	Specifies if DECT encryption should be used for voice calls. 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.
config.xml	Added	sip.proxy. domain[2-4]	Specifies domain/host name for additional SIP proxies. Default: Empty
config.xml	Added	sip.proxy.port[2-4]	Specifies port for additional SIP proxies. Default: Empty
config.xml	Added	sip.proxy.priority sip.proxy.priority[2-4]	Specifies the priority for using a SIP proxy. Proxies with lowest priority will be preferred and higher priorities will be used for failover. Values: 1-4 Default: 1, 2 , 3, 4
config.xml	Added	sip.proxy.weight sip.proxy.weight[2-4]	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. Values: 0-100 Default: 100
config.xml	Added	upnp.enable	Specifies if UPnP support is enabled. If enabled the device will respond to UPnP broadcasts. Values: true/false Default: true
config.xml	Added	upnp.broadcast	Specifies if UPnP announcements are broadcasted. If enabled the device will periodically broadcast announcements. Values: true/false Default: false

4.4 Version PCS03B_ (Q3/2009)

4.4.1 Added or Changed Features

- DECT-97: Add service codes to read system information via handset. Initiated by typing codes and then pressing off hook from the handset. This information can be read from the system.

    - IP address: ***999*00
    - MAC address: ***999*01
    - Server Firmware: ***999*02

- Allow custom posix timezone specification strings.
    - It is now possible to configure the system to show "½-hour time zones", by entering a posix string
- Add revision to User Agent string.
    - Firmware version can be obtained from traces, inspecting the User Agent field
- Include DNS traffic when capturing SIP.
- Allow custom capture filters.
    - Customize the captured data to a trace by entering a filter in pcap format.
- DECT-63: New and improved NTP client.
    - Improved error recovery.
    - Information for the NTP client included in the log file.
- Add user/password and enable/disable options to MSF.
    - It is possible to change login username and password for MSF applications (text messaging interface)
    - MSF functionality can be enabled/disabled
- Send unregister and unsubscribe when deleting an endpoint.
    - Inform the PBX when a DECT handset is deleted.
- Clean out parameters in user names received from some PBX'es.
- Handle "302 Multiple Choices" - for now just pick the first choice.
- Handle SDP in multipart body.
- Added timestamp and synchronization statistics duration to rfps.xml.
- If SIP registration fails, re-register within a short time and then wait.

4.4.2 Removed Features

- None

4.4.3 Corrections

- Fixed problem with authentication on some PBX'es.
- Fixed problem with wrong answer to SDP update offers.
- Fixed timer problem that might break provisioning.
- MSF callback number length increased.
- Check for required SIP headers before creating a dialog.
- Handle timeout for SUBSCRIBE requests.
    - Retry if SIP subscription fails.
- Skip local media resource in central firmware update.

  - If media resource firmware is updated, the KWS6000 server is not affected even if it acts as local media resource.
- Remove require 100rel header from PRACK as this is wrong according to RFC3262.
- Improved CODEC card DTMF handling.
- DECT-111: Handle MSF timestamps.
- Does not crash in some rare call transfer scenarios.

4.4.4 Configuration File Parameter Changes

File	Action	Parameter	Description
config.xml	Added	application.enable_msf	Specifies if the MSF application interface is enabled. true – The MSF interface is enabled and applications can connect. false – The MSF interface is disabled. Default: true
config.xml	Added	application.username	Specifies the username required for applications to log in. Default: “GW-DECT/admin”
config.xml	Added	application.password	Specifies the encrypted password required for applications to log in. Default: “f621c2268a8df24955ef4052bfbb80cf” (password “ip6000” encrypted)

4.5 Version PCS03A_ (Q2/2009)

4.5.1 Added or Changed Features

- Retrieving a big file from the internal web server no longer blocks the server.
- Retain any existing other call when a REFER triggered INVITE fails, otherwise release the handset.
- Do not require username in URI in REFER.
- Handle "423 Interval to brief" REGISTER response.
- Default log level in the GUI increased from INFO to NOTICE.
- Add support for international letters using UTF-8.
- DECT-83: If no protocol is specified in the provisioning URL then default to TFTP.
- DECT-81: Do not repeatedly program flash if version and binary firmware files are inconsistent.
- Log an error if configuration XML contains invalid XML.
- Add support for keep-alive used by version 18 or later of MSF.DLL.
- Send "unknown op" error when an unknown operation is requested via MSF.

4.5.2 Removed Features

- None

4.5.3 Corrections

- Fixed bug in Refer-To handling.
- Fixed bug in Record-Route handling.
- Fixed bug that made the DTMF duration being rounded down to N*80.

- Fixed handling of too long dialled numbers.
- DECTESC-75: Fixed bug making it impossible to save Wireless Server Configuration.
- Disable unsupported media lines correctly.
- Parse remote SDP ptime attribute correctly.
- Do not send SDP with new version if remote SDP version has not changed.
- Only check for remote SDP version changes if remote SDP was received earlier.
- Fixed problem with one-way voice when a call is answered during a handover.
- Fix bug not allowing MSF multi-byte status requests – required for RTLS.
- Handle MSF call release without call record correctly.

4.5.4 Configuration File Parameter Changes

File	Action	Parameter	Description
config.xml	Changed	provisioning.server.url	Specifies the static boot server URL from where the KWS will retrieve configuration information. The format is [<protocol>://[<user>:<password>@]]<host>[/<path>]. Protocol can be either tftp, ftp or http. It is optional to specify a protocol. If the protocol is not specified the KWS will default to tftp. Example: ftp://kws:ip6000@boot.example.com/phones or 192.168.0.1 Default: Empty

4.6 Version PCS03_ (Q1/2009)

4.6.1 Added or Changed Features

- Optional individual ports per handsets for SIP signaling. Extend support to SIP PBXs using per port registration.
- Cisco Unified Call Manager 6.1 support.
- Provisioning: Possible to centralize configuration and maintenance.
- Users export to XML and CSV format: Decrease installation and maintenance cost.
- Allow adding users with unspecified IPEI: Option of adding handsets without knowing the IPEI of the handset. Decrease installation and maintenance cost by allowing field subscription of handset(s) and possibility for remote configuration.
- Added system wide DECT access code: Possible to create a default DECT access code for all users – instead of per user (access code in user will overrule the system default value).
- Added automatic standby text update. When the standby text is updated (either through the GUI or through auto-provisioning) the change appears instantly on the handset (no power-cycle of the handset is needed).

- In overlap dialing send digits when # is pressed. Optional: Default is disabled.
- When a user is deleted, unsubscribe the handset: When user is deleted, the handset removes the subscription to the system.
- Added RFC3896 Referred-By handling.
- Offered rfc2833 payload type (DTMF payload type) can now be configured default is 96.
- Add refresh and clear button in base station administration.
  CLI / Name display for complete call duration for incoming calls.
- Base station lost sync. Ratio / percentage added.
- Added BMC/radio configuration.

4.6.2 Removed Features

- No longer possible to use local number – the SIP user name is now used for MSF.

4.6.3 Corrections

- Fix base station lost sync. ratio calculation.
- Fix DTMF payload type.
- Fix order in route sets for SIP dialogs.
- Fix statistics for failed MSF calls.
- Fix handling of escaped SIP URI parameters.
- Pass all parameters and headers from REFER to the sent INVITE.
- Remove http server crash when downloading rfps.xml.
- Remove crash on re-INVITE when collecting digits.
- Remove crash on INVITE with long From header.

4.6.4 Configuration File Parameter Changes

File	Action	Parameter	Description
config.xml	Added	provisioning.server .method	Specifies how the KWS6000 will obtain the boot server address. • dhcp – obtain from DHCP option 66. • static – use static configured. • disabled – do not check for updates. Default: dhcp
config.xml	Added	provisioning.server .url	Specifies the static boot server URL from where the KWS6000 will retrieve configuration information. The format is <protocol>://[<user>:<password>@]<host>/<path>. Protocol can be either tftp, ftp or http. Example: ftp://kws:ip6000@boot.example.com/phones Default: Empty
config.xml	Added	provisioning.check. interval	Specifies an interval for checking for updates.

File	Action	Parameter	Description
			0 – do not check for updates periodically. >1 – interval in minutes. Default: 0
config.xml	Added	provisioning.check.time	Specifies a specific time for checking each day. The format is HH:MM. 00:00 – 23:59 Default: Empty
config.xml	Added	provisioning.check.check_sync	Specifies how the KWS6000 will react to SIP NOTIFY check-sync events. • disabled – do nothing if a check-sync event is received. • reboot – reboot and check for updates. • update – check for updates and reboot if necessary. Default: disabled
config.xml	Added	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
config.xml	Added	provisioning.firmware.kws	Specifies the name of the firmware image to use for the KWS6000. The KWS6000 will check for a version file and a binary file. They must be located as <URL>/<firmware>.ver and <URL>/<firmware> Example: kws300-flash.bin Default: Empty
config.xml	Added	sip.send_to_current_registrar	Specifies how requests outside a dialog are sent if a list of SIP servers is received via DNS SRV. • false – perform a DNS SRV lookup for each request and determine the destination from this. • true – send each request to the server currently holding the registration. Default: false

File	Action	Parameter	Description
config.xml	Added	sip.separate_endpoint_ports	Specifies if each user should use an individual UDP for its signaling or all users should use the local port defined in the SIP configuration. • false – use one UDP port for all users. • true – use individual UDP ports for each user. Default: false
config.xml	Added	sip.pound_dials_overlap	Specifies if pressing # while off hook dialing will dial the entered extension. • false – do not dial when # is pressed. • true – dial when # is pressed. Default: false
config.xml	Added	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.xml	Added	Sip.dtmf.rtp_payload_type	Offered rfc2833 payload type (DTMF payload type) default is 96.

4.7 Version PCS02A_ (Q4/2008)

4.7.1 Added or Changed Features

- Added cluster handling. This is only relevant for de-centralized installations.
- Added support for DECT frequency swap (requires license and base station with firmware PCS02a_ or later.
- Added phonebook application. This feature offers a centralized phonebook. The formats supported for the phonebook is csv-file and LDAP.
- Added enable/disable send date and time to handsets. This feature makes it possible to select whether the date/time should be visible in the handset or not.
- Add distinctive alerting by interpreting the Alert-Info SIP header. Use external ring tone as default. If distinctive ring is supported by the IP PBX, different ring tones can be set for the handset to differ between internal and external calls.
- Update MWI when a handset subscribes or makes a location registration.

- Always respond with 200 OK when a MWI NOTIFY is received. This is done to avoid terminating an existing MWI subscription.
- Added automatic MWI retransmission.
- Allow for special characters like &_ in SIP authentication user/password.
- Allow alphanumeric SIP username.
- Implement RFC4235 Dialog state event package. Used for e.g. call pickup support.
- Allow for receiving asymmetric RTP (optional, requires media resource with firmware PCS02A_ or later). This is required to operate with e.g. a Mitel NuPoint voice mail server.
- Detect merged invites after a fork and respond with “482 Loop Detected”.
- Added full system backup facility. Instead of separate backups of configuration, users etc. everything is now in one backup and it is optional how much is restored.
- Standby text length increased from 16 to 24 characters.
- Implemented Type-of-Service/DiffServ. Replaced old Quality-of Service approach with new Type-of-Service approach.

4.7.2 Removed Features

None

4.7.3 Corrections

- Corrected error in subscription statistics (subscriptions which failed due to e.g. wrong or missing DECT access code was logged as a success).
- Release MSF-call correctly when no CR is assigned.
- Fix reversed time zones. GMT time zones were reversed – GMT+2 meant GMT-2. This has now been fixed.

*4.8 Version PCS02_*

Initial KWS6000 version.

5. Outstanding Issues

The following issues will be fixed in a subsequent release

- None identified.

