POLYCOM®

KIRK® IP Base Station

Firmware Version PCS10__
Q4, 2011

Table of Contents

1. Revision History

Date	Description
2008-06-16	First draft.
2008-09-24	Release Notes for PCS02A_
2008-11-13	Release Notes for PCS02B_ and PCS02C_
2009-06-10	Release Notes for PCS02D_
2009-09-09	Release Notes for PCS04__
2009-10-19	Release Notes for PCS04A_
2009-12-10	Release Notes for PCS05__
2010-01-27	Release Notes for PCS05A_
2010-03-31	Release Notes for PCS05B_
2010-06-21	Release Notes for PCS05C_
2010-09-15	Release Notes for PCS06__
2010-10-13	Release Notes for PCS06A_
2010-12-15	Release Notes for PCS07__
2011-03-08	Release Notes for PCS08__
2011-03-29	Release Notes for PCS08A_
2011-06-14	Release Notes for PCS09__
2011-09-14	Release Notes for PCS10__

2. General

2.1 Release

These release notes apply to released versions of the KIRK IP Base Station firmware. This version specifically applies to version PCS10__ of the KIRK IP Base Station. The release replaces the PCS09__ release as the latest generally available (GA) release.

2.2 References

KIRK Release Note: KWS6000 Firmware Version PCS10__ Q4 2011.

2.3 Important Notes

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

- The communication protocol between the KWS, the media resources and the base stations has been changed in PCS06A_ and it is not backward compatible starting with PCS06A_ of the KWS and PCS06A_ of the base station. This means that base stations or media resources with firmware version older than PCS06A_ will not connect to a KWS running firmware PCS06A_ or newer. To minimize downtime, update base stations, media resources and KWS6000 to firmware PCS06A_ before rebooting any of these. This will ensure that no pre-PCS06A_ firmware will try to connect to a PCS06A_ or newer firmware.

- The communication protocol between the KWS, the media resources and the base stations has been changed in PCS08__ and it is not backward compatible starting with PCS08__ of the KWS and PCS08__ of the base station. This means that base stations or media resources with firmware version older than PCS08__ will not connect to a KWS running firmware PCS08__ or newer. To minimize downtime, update base stations, media resources and KWS6000 to firmware PCS08__ before rebooting any of these. This will ensure that no pre-PCS08__ firmware will try to connect to a PCS08__ or newer firmware.

2.4 Feature License and Platform Limitations

None

2.5 System Requirements

Hardware Platform	Description
KIRK Base Station 12 HW PCS 10 or newer	KIRK IP Base Station 12

3. Distribution Files

Click here >> to find the firmware image of the KIRK IP Base Station.

4. Changes

4.1 Version PCS10__ – Q4, 2011

4.1.1 Added or Changed Features

- When used in a setup with KIRK Wireless Server redundancy, the storage of the primary and backup KIRK Wireless Server addresses has been improved. If major configuration changes were made to the redundancy setup (e.g. if the hostnames/IP-addresses of the primary and backup KIRK Wireless Server were changed and the roles were swapped i.e. the former primary KIRK Wireless Server was re-configured to be the secondary and vice versa), the base station could lose the correct hostnames/IP-addresses of the KIRK Wireless Server and a manual re-configuration was required to make the base station connect again.
- Set TOS correctly when connecting to the backup KIRK Wireless Server in a redundancy setup.
- The log daemon which collects messages and signaling for logging and debugging purposes has been improved. When sending a log entry to the listening clients, the log daemon does not give up on all the clients anymore if sending to one client fails.

4.1.2 Removed Features

- None.

4.1.3 Corrections

- Some potentially dangerous faulty error message formatting has been eliminated.
- An UPnP related issue has been fixed. A multicast packet missing the ST header could cause the administration process to restart.

4.1.4 Identified Issues

- None

4.1.5 Configuration File Parameter Changes

- None

4.2 PCS09__ – Q3, 2011

4.2.1 Added or Changed Features

- The product ID is now displayed in the Status General part of the web GUI for easy reference. Furthermore the product ID is included in a log dump (Status|Export Logs).

4.2.2 Removed Features

- None.

4.2.3 Corrections

- When the IP-cpu on the base station wanted to boot the BMC, the port used to do this was previously configured as an output port when initializing the bmc-driver kernel module and it was left that way. This made the signal level on the UART_TX from the BMC too low (close to the tolerance level). Some units started to have problems with the UART communication which revealed this problem. Now the direction of the port is set back to input after accessing the port.

4.2.4 Configuration File Parameter Changes

- None.

4.3 Version PCS08A_ – Q2, 2011

4.3.1 Added or Changed Features

- None.

4.3.2 Removed Features

- None.

4.3.3 Corrections

- Initialize Maxconnections to 6 or 12, otherwise the production cannot establish a connection in testmode.

4.3.4 Configuration File Parameter Changes

- None.

4.4 Version PCS08__ – Q2, 2011

4.4.1 Added or Changed Features

- Starting with PCS08__ the firmware is prepared for the Security Package license. If a Security Package license is installed, various security enhancing features become available.
  Encryption of external as well as internal media according to RFC 3711 (Secure RTP or SRTP) is possible. External media is the media stream between the KWS/media resource and the external endpoint/PBX. Internal media is the media stream between the KWS/media resource and the base station. This addresses DECT-143.

  Encryption of external media.
  External SRTP handling is supported in optional as well as required mode. Configuration of external SRTP is located in Configuration | SIP Media.
  If 'enabled', SRTP is supported and optional, and it must be negotiated with the remote endpoint. If 'enabled and required', the use of SRTP is mandatory, and if negotiation of SRTP with the other end is unsuccessful, call establishment will be aborted.

Handling of RFC 4568 SRTP lifetime key parameter and Master Key Index parameter in SDP offers are configurable.
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).

Encryption of internal media.
Configuration of internal SRTP is located in Configuration | Wireless Server.
The "Enable base station RTP encryption" setting will enforce 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.

- Media resources and base stations are allowed to connect to a KWS even in the case of incompatible protocol versions on the KWS and the media resource/base stations. This means that in future/upcoming releases it will be possible to update the firmware on base stations and media resources directly from the KWS even in the case where the KWS was updated to a newer (and potentially incompatible) firmware version and rebooted before the base stations/media resources.
- Support for VLAN tagging according to IEEE 802.1Q has been added.
  VLAN tagging is statically configured through the GUI or via provisioning. This addresses DECT-43.
- Support of reception of RTP packets with CSRCs.
  CSRCs are used for Contributing Sources. Previously the reception of RTP packets with CSRCs could potentially lead to faulty decoding of RTP packets and resulting noise/cracks in sound. This has been fixed.
- RTP stream handling improved.
  Previously an RTP stream would be reset if a call was put on hold, and a new stream would start when the call was resumed. Now the RTP stream is suspended when put on hold and resumed when the call is taken off hold. This eliminates some potential RTP synchronization issues which could lead to noise during on/off hold.
- The logic for handling RTP stream synchronization between local and remote ends is improved with regard to handling the scenario where the other end uses silence suppression.
- On the base station the reception of MAC layer page requests, connection indications and disconnect indications are logged with debug level. Previously these signals were not logged.
- Theoretically, the DECT-slot handling can go out of synchronization with the handset because the KWS "misses" a slot. If this situation occurs, it will now be automatically detected, logged as an error in the KWS and repaired. Previously, if this happened, the handsets would no longer be able to make and receive calls until the KWS was restarted. The situation has been seen to occur in a scenario with a very high load of multicast of large packets to the base station.

4.4.2 Removed Features

- When an IO handler is removed while IO is pending, it is recorded in the message log. Previously this was logged with level critical but is now decreased to debug. Specifically, this can happen with packet capture in admin.

4.4.3 Corrections

- On a base station the lower layer signaling between the IP-part and the radio part could be used before properly initialized which would sometimes result in prolonged boot time. This has been corrected.
- Corrected handling of MTU (network.mtu). In earlier versions of the firmware, the specified MTU was ignored and the MTU was always set to 1500 bytes. This has been corrected.

4.4.4 Configuration File Parameter Changes

File	Action	Parameter	Description
config.xml	Added	network.vlan	VLAN Identifier (VID) according to IEEE 802.1Q specifying the VLAN to which the device belongs. 4094 different VLANs are supported. Values: 1-4094 Default: Empty.

4.5 Version PCS07__ – Q1, 2011

4.5.1 Added or Changed Features

- The flash update process has been improved. It will no longer update the firmware if the new firmware is identical to the current firmware.
- Trigger dumps used to persist debug information in case of a fatal error have been rewritten. Previously the latest 10 trigger dumps were stored in the flash, but now only the first trigger dump made since last boot will be stored. This is to eliminate the possibility of excessive flash wear in the case of a repeated error scenario. Theoretically the former implementation could lead to flash corruptions.
- Status/debug information with regard to RTP handling has been added. When an RTP session is destroyed/closed, the current length of the RTP queue can now be logged.

4.5.2 Removed Features

- None.

4.5.3 Corrections

- None

4.5.4 Configuration File Parameter Changes

- None.

4.6 Version PCS06A_ - October 13, 2010

This release replaces the PCS05C_ release as the latest generally available (GA) release.

4.6.1 Added or Changed Features

- Base station side of KWS redundancy implemented.
  If a redundancy license is installed on the KWS it is now possible to configure a redundant setup of KWS. For more information refer to the application note regarding redundancy.
- Remote syslog improvements.
  It is now possible to send DEBUG messages via remote syslog. Furthermore it is possible to configure which log levels to send via remote syslog. All of the changes to the remote syslog can be made without restarting the KWS. This means that e.g. in a hosted environment the provider can increase or decrease the level of logging from a specific KWS without affecting the users of the KWS. In e.g. a trouble-shooting scenario the provider/administrator can increase the log level while debugging and subsequently decrease the level again.
- More robust flash upgrade process. Reboot is now handled centrally to ensure that the base station is not rebooted while flashing the firmware.
- Statistics is now handled locally in base stations.
- More elaborate logging concerning connection establishment towards KGAP(s). If problems are logged in the base station concerning the connection to the KWS (KGAP), it is now logged which KGAP it is (to handle a redundancy setup with several KGAPs).

4.6.2 Removed Features

- Removed debug log level from the message filter on the status logs page in the GUI. The debug messages were not available through the GUI anyway.
- If the rfp crashes a crash log is no longer written to the flash. This could in some rare conditions result in corruption of the flash file system.

4.6.3 Corrections

- RTP check that data is coming through the jitter buffer and if not reset the session. Addresses DECTESC-204 which is an issue with one-way voice in the second of two subsequent calls to the same number on an Aastra PBX.
- Bug fixed. May cause configuration daemon to crash if no network.domain is defined.
- Corrected error concerning handling of time zones on base station.

4.6.4 Configuration File Parameter Changes

- None

4.7 Version PCS05C_ Q3, 2010

4.7.1 Added or Changed Features

- Added ping and traceroute to the Web GUI (by popular demand from several customers).
  For network diagnostics, a ping and traceroute feature has been added. It is accessible through the Status menu.
- Added DHCP syslog server support.
  A syslog server can be assigned via DHCP option 7.

- Added reboot required banner to the Web GUI.
  When a configuration parameter requiring a reboot is changed, a yellow reboot required banner is shown until next reboot. This is to eliminate situations when administrators have updated configuration settings which require a reboot to become active and subsequently have forgotten to reboot the KWS.

4.7.2 Removed Features

None

4.7.3 Corrections

Removed RFPI scanner CSV file error from log.

4.7.4 Configuration File Parameter Changes

None

4.8 Version PCS05B_ Q2, 2010

4.8.1 Added or Changed Features

- NTP support: In earlier versions of the firmware, the base station retrieved time from the KWS when connected. The time from the KWS was not updated later on and the base station time could drift. It is now possible to use NTP to maintain a precise time. If no NTP server is configured, the base station will continue to retrieve time from the KWS.
  The NTP server can be configured either through the GUI or via DHCP option 42.
- Added syslog facility configuration: This makes it possible to configure the source facility used for syslog messages. The default is local0. For further details on remote syslog facilities refer to RFC5424.
- Reduced production time: Due to increasing demand and increasing amount of delivered devices the initial creation of an empty file system has been optimized. This only impacts the production process and has no impact on devices in the field.

4.8.2 Removed Features

None

4.8.3 Corrections

None

4.8.4 Configuration File Parameter Changes

config.xml	Added	log.syslog.facility	Used to specify the remote syslog facility used for log messages. Refer to RFC5424 for details. Values: The facility number to be used for the device. An integer between 0 and 23. Default: 16 ("local 0")

config.xml	Added	network.ntp	Specifies the hostname or IP address of the NTP server for retrieving time.
			Default: Empty

4.9 Version PCS05A_ January 27, 2010

4.9.1 Added or Changed Features
None

4.9.2 Removed Features
None

4.9.3 Corrections
Fixed problem that made the base station lock when flooded with DECT page requests from the KWS.

4.9.4 Configuration File Parameter Changes
None

4.10 Version PCS05_ Q1, 2010

4.10.1 Added or Changed Features
- Introduced remote syslog (RFC5424) via UDP. The remote syslog allows using a PC to receive messages/logging from the device.
- Added packet capture.
- When exporting logs, the message log is stored in clear text. The message log can now be read with standard software.
- Improve log export speed.
- Create a KSF log on RFP crash.

4.10.2 Removed Features
None

4.10.3 Corrections
- Fixed problem with device not falling back to static IP address when DHCP fails.
- Validate configuration keys when setting them. This avoids malforming the config.xml.
- Removed a few large buffers from the stack. These may have caused sporadic failures.
- Removed a lot of unnecessary writes to the flash. These induced unnecessary tear on the flash, especially during boot.
- Fixed bug that prevented enabling UPnP from the GUI.
- Fixed problem with UPnP UUID not being unique. If more devices on the network have the same UUID only one of them will be shown when UPnP devices are listed.

4.10.4 Configuration File Parameter Changes

config.xml	Added	log.syslog.host	Specifies the remote syslog server host address. Default: Empty
config.xml	Added	log.syslog.port	Used to specify the remote port of the syslog server. Values: The port number on a remote syslog server. Default: Empty which defaults to 514

4.11 Version PCS04A_ October 20, 2009

4.11.1 Added or Changed Features

None

4.11.2 Removed Features

None

4.11.3 Corrections

- Removed potential RFP problem present in firmware PCS04_.
  This problem would result in the loss of all active calls on the base station and a subsequent restart of the RFP process.
- Corrected handling of voice connection creation and termination.
  Creation and deletion of a voice connection could cause voice problems in other connections on the same base station.

4.11.4 Configuration File Parameter Changes

None

4.12 Version PCS04__ (Q4/2009)

4.12.1 Added or Changed Features

- 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.
  - o http[s]://<host>/config/get?<key> –
    http://192.168.0.1/config/get?sip.proxy.domain
  - o 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.

- 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 KWS6000 firmware version PCS04_ or higher.

4.12.2 Removed Features
None

4.12.3 Corrections
Drop RTP packages with unexpected payload without trying to play them.

4.12.4 Configuration File Parameter Changes

File	Action	Parameter	Description
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

*4.13 Version PCS02D_*

4.13.1 Added or Changed Features
None

4.13.2 Removed Features
None

4.13.3 Corrections
- BMC fix, allow dummy bearer setup in test mode (needed by production).

- Various bug fixes.

4.13.4 Configuration File Parameter Changes

None

4.14 Version PCS02D_ Q3, 2009

4.14.1 Added or Changed Features

None

4.14.2 Removed Features

None

4.14.3 Corrections

Various bug fixes

4.14.4 Configuration Parameter Changes

None

4.15 Version PCS02C_ Q1, 2009

4.15.1 Added or Changed Features

- Improved handling of lost sync. Rewrote synchronization over the air. Implemented new algorithm for handling loss of synchronization to make it more resilient towards a hostile rf-environment e.g. over-deployment and reflections.

- Added debug handles for synchronization over the air.

- BMC Allow dummy bearer on neighbor slot.

- BMC Do not scan RSSI - only move dummy bearer based on timer.

- BMC Do not ask RFP IP process for dummy bearer.

- BMC Added BMC/radio configuration.

4.15.2 Removed Features

None

4.15.3 Corrections

- BMC EEPROM read bug fixed.

- BMC Remove bug stopping dummy bearer.

- BMC Do not print from interrupt.

4.15.4 Configuration File Parameter Changes

None

4.16 Version PCS02A_ (Q4/2008)

4.16.1 Added or Changed Features

- Implemented support for DECT Frequency SWAP (license required, KWS6000 SW PCS 02A_ or later required).

- Implemented Type-of-Service/DiffServ handling. Replaced old Quality-of-Service approach with new Type-of-Service/DiffServ approach (KWS6000 SW PCS 02A_ or later required).

- Encrypt Admin GUI password

4.16.2 Removed Features

None

4.16.3 Corrections

None

4.16.4 Configuration File Parameter Changes

None

*4.17 Version PCS02_*

Initial KIRK IP Base Station release.

5. Outstanding Issues

The following issues will be fixed in a subsequent release

- None identified.