KIRK® Release Notes

KIRK® Wireless Server 6000

Firmware Version PCS10_._
Q4, 2011

Copyright © 2011 Polycom, Inc. All rights reserved.

Table of Contents

Copyright © 2011 Polycom, Inc.

Copyright © 2011 Polycom, Inc.

1. Revision History

Date	Description
2008-06-16	First draft.
2008-09-24	Release notes for PCS02A_
2008-11-04	Release notes for PCS02B_
2008-12-09	Release notes for PCS03__
2009-03-05	Release notes for PCS03A_
2009-06-10	Release notes for PCS03B_
2009-08-04	Release notes for PCS04__
2009-10-12	Release notes for PCS04A_
2009-10-19	Release notes for PCS04B_
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_
2010-07-13	Release notes for PCS05D_
2010-10-11	Release notes for PCS06A_
2010-12-15	Release notes for PCS07__
2011-03-08	Release notes for PCS08__
2011-05-29	Release notes for PCS08B_
2011-06-14	Release notes for PCS09__
2011-09-14	Release notes for PCS10__

Copyright © 2011 Polycom, Inc.

2. Introduction

2.1 Release

These release notes apply to released versions of firmware for the KIRK Wireless Server 6000 (hereinafter referred to as KWS6000). This version specifically applies to version PCS10__ of the KWS6000 firmware. The release replaces the PCS09__release as the latest generally available (GA) release.

2.2 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.

2.3 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
KWS Redundancy	License required
Security Package	License required
Microsoft Lync Interoperability	License required

2.4 System Requirements

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

Copyright © 2011 Polycom, Inc.

3. Distribution Files

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

4. Changes

4.1 Version PCS10__ – Q4, 2011

4.1.1 Added or Changed Features

- Handling of Calling Line Identification Presentation (CLIP) has been changed for incoming calls. If the call comes from an unknown or anonymous user, the “From URI” is suppressed and not used for CLIP display on the handset. Specifically, the following user names are suppressed: anonymous, unknown and null. This refers to DECTESC-283. Furthermore, incoming other party number is handled as digits even if parameters are added after the “number” with a semicolon. This fixes an issue reported in DECTESC-338. When running a firmware version later than PCS 06A in a setup with a Nortel CS1000, CLIP did not work as expected. When a handset received a call, "sip@[IP number]" was displayed on the handset instead of the caller ID. This has now been changed.
- Handling of CLIP in a setup with a KIRK Wireless Server connected to Microsoft Lync with an external gateway towards PSTN has been changed. In an outgoing call from a KIRK Wireless Server through the external gateway towards PSTN, the gateway previously presented the main number as caller id on the receiving phone instead of the local number from the calling handset. The KIRK Wireless Server now extracts its telephone number from Lync and presents it in the P-Preferred-Identity header. This is required to present the correct number when dialing to PSTN through the external gateway.
- Message Waiting Indication is now supported in a Microsoft Lync setup. I.e. if a voice mail is received it will be indicated on the handset.
- If a DECT Lync service user was configured, previous releases would initiate Kerberos signaling for authentication towards the Lync server even if Lync was not enabled. Now the KIRK Wireless Server will not start Kerberos signaling before Lync is enabled.
- In some failing outgoing call scenarios, the handset waits for the user to hang-up before disconnecting the call. One of these scenarios is calling a non existing/illegal number. Starting with this firmware the KIRK Wireless Server will disconnect the handset automatically after 10 seconds if outgoing call setup fails.
- Support for sending reliable provisional responses - 100rel has been added. This will make the KIRK Wireless Server able to handle incoming PRACK requests. Reliable provisional responses on the KIRK Wireless Server are currently not used. They will come into play when support for STUN/TURN/ICE will be launched for Microsoft Lync.
- Starting with this release, supported headers in outgoing SIP signaling will be added as separate headers instead of a list in a single header. This is currently required for Microsoft Lync support.
- When the KIRK Wireless Server indicates DTMF support in outgoing SDP offers, DTMF events 1-15 are indicated; previously 1-11 were indicated. The KIRK Wireless

Copyright © 2011 Polycom, Inc.

Server will actually send only 1-11 events. However CUCM 8.6.x apparently needs the offer to indicate 1-15 to be able to handle DTMF correctly.

- The Call-Id generation algorithm has been rewritten. The Call-Id is used to identify a call in SIP signaling. Previously, the Call-Id contained the IP-address of the KIRK Wireless Server. This has been changed for privacy reasons.
- The proxy port setting was previously required to be either 0 or between 1000 and 65535. Now the setting is allowed to be 0 – 65535 to enable connection to a Microsoft Lync Edge server.
- Handling of a second incoming (Call waiting) call while the user is on hold has been changed. In some PBX setups the following scenario could occur: if a handset is put on hold, and a new (Call Waiting) call is received, the second call will be indicated on the handset. If subsequently the second call is cancelled by the caller, the handset would not indicate this the right way. This behavior has now been changed.
- Simple handling of 305 Use Proxy response has been added (this was required by Coral UGW).
- Handling of several scenarios in a setup with KIRK Wireless Server Redundancy has been improved.
  It is now required that the backup KIRK Wireless Server to have the same firmware revision and licensed features as the master KIRK Wireless Server to be able to connect to the master. In case a backup tries to connect with a different firmware version or other licensed features than the master, an error message will be logged and the backup will be rejected. Furthermore, the logic to control the connection between the master and backup KIRK Wireless Server has been improved.
- 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 media resource could lose the correct hostnames/IP-addresses of the KIRK Wireless Server and a manual reconfiguration was required to make the media resource connect again.
- When acting as a media resource, set TOS correctly when connecting to the backup KIRK Wireless Server in a redundancy setup.
- The base station administration page on the WEB GUI has been improved:

  Previously a green icon indicated that the base station was synchronized to the primary synchronization source, and a yellow icon indicated that the base station was synchronized to the secondary synchronization source. The yellow icon has been removed and a green icon now indicates that the base station is synchronized.

  Furthermore, the Sync Changed column has been removed from the GUI. This is done to keep the GUI as clean and simple as possible. The number of times the synchronization source has changed does not affect the performance of the system and therefore this information is not relevant.

  The naming of synchronization sources has been made consistent. Now the secondary/alternative synchronization source is consistently denoted secondary. The current sync source is now printed in parentheses in the Prim/Sec column. Previously the current synchronization status was displayed even when the base

Copyright © 2011 Polycom, Inc.

station was disconnected. This was misleading and has been changed.

If a base station firmware is outdated this is now indicated by a yellow icon, (if a media resource firmware is outdated this is now also indicated by a yellow icon).

- More information is logged regarding DECT subscription of handsets. It is now logged with level info when a handset attempts to subscribe to the system. Furthermore it is logged if a subscription attempt fails because of timer expiry.
- When a handsets which is not in the subscription database contacts the system (e.g. performs a location registration), the KIRK Wireless Server will request the handset to delete the subscription. This is now logged with level notice.
  If a Location Registration is attempted with corrupt or missing subscription data, the subscription will be terminated on the handset. This is now logged.
- If a call attempt with missing or corrupt subscription data is made, it will cause the DECT subscription to be terminated. This is now logged. Furthermore, some additional textual representations of error codes are added.
- Handling of certificates has been made more user friendly. When a Certificate Authority (CA) bundle is loaded into the KIRK Wireless Server and an invalid or unsupported CA certificate is encountered, is now logged. Furthermore "(Certificate no:## in file)" is logged in order to locate the problematic certificate easier. The handling of invalid or unsupported CA certificates is improved. Invalid or unsupported certificates are listed in the GUI.
- For SIP over TLS, verify the server certificate against the proxy name instead of the request URI. This is required to make calls to another domain via a proxy. Such an example is federated calls in Microsoft Lync.
- Correctly handle TLS connection shutdown from the far end. Previously, some error scenarios with TLS connections have been seen to cause a high CPU-load. This could have been influencing SIP call handling. Furthermore, this may explain some problems encountered with HTTPS connections on some browsers.
- Use local media attributes to determine what RTP directions to enable.
- When putting a call on hold, send inactive instead of sendonly in the SDP. This is more correct because we do not send music-on-hold. This is configurable via sip.media.sdp_hold_attribute_sendonly which defaults to false. If this setting is true, old behavior is restored.
- The RTP profile, including crypto parameters is now persistent for the duration of a call. If e.g. SRTP is enabled and optional, the resulting RTP profile after negotiation with the other end is used throughout the call. Previously, re-INVITE scenarios e.g. when setting on hold would initiate a new negotiation and result in e.g. new crypto parameters. Some endpoints require the negotiated RTP profile to be persistent for the duration of the call. Such an example is Microsoft Lync clients.
- Log messages concerning SIP errors have been improved. Additional information about the state of the call as well as the state of the SIP endpoint has been added. Furthermore, the remote IP address on SIP connection failures is now logged for easier debugging of SIP related error scenarios.
- In the abnormal call release statistics more release codes have now a textual representation. E.g. "Authentication failed".
- A new timer concept has been added which drastically reduces the amount of timeout entries in the debug log.

Copyright © 2011 Polycom, Inc.

- When an unexpected event is received in response to a SIP SUBSCRIBE request, the name of the event is now logged.
- The log daemon which collects messages and signaling for logging and debugging purposes has been improved. When sending a log entry to listening clients, the log daemon no longer gives up on all clients if sending to one client fails.
- The default Certificate Authority (CA) bundle with trusted CAs has been updated. It was found that a Certificate Authority (CA) issued fraudulent HTTPS certificates. The compromised DigiNotar certificate has been removed, rendering any HTTPS certificates signed by that CA as untrusted.
- For the central phonebook, the LDAP search timeout has been increased from 5 to 15 seconds in order to wait for slow LDAP servers.

4.1.2 Removed Features

- None.

4.1.3 Corrections

- Sending DTMF signaling (key-presses) via SIP INFO in an early dialog could cause the KGAP to restart. This has now been corrected. This refers to DECTESC-340.
- A problem reported in DECTESC-323 has been fixed. The problem was caused by a call with a Cisco endpoint supporting both audio and video. The SDP answer received in the last ACK contained audio and video but with two different IP addresses in the c lines. The KIRK Wireless Server selected the audio but it selected the IP address from the video; as a result the KIRK Wireless Server sent RTP to the video address. This has now been fixed.
- Set local port for incoming SIP TCP connections. This makes the KIRK Wireless Server to use the correct source port when responding to a request sent directly to the KIRK Wireless Server, by passing the proxy.
- When DNS SRV and Use SIPS URI are enabled, the KIRK Wireless Server now requests SIPS from DNS SRV.
- If an incoming call is initially put on hold using IP address 0.0.0.0, the media is now correctly connected. This fixes DECTESC-344: no audio in incoming group call on Broadsoft R17.
- If a system running redundancy has more than 12 active calls and an active call list is requested from the WEB-GUI, a memory error will occur. This has now been fixed.
- Receiving too many A records from the DNS server previously triggered a buffer overflow. This has now been corrected. The first 10 A records are now handled and the rest are ignored.
- Some potential buffer overflows have been eliminated.
- Some potentially dangerous faulty error message formatting has been eliminated.
- Offset error in SRTP replay check has now been fixed.
- Always update Connection->General.LifeTime when sending TCP messages.
- If SIP signaling is received with an incoming Refer-To address without a user part, the KGAP could restart. As an example (probably rather theoretical) this can occur when transferring an active call to voicemail on Microsoft Lync. This has now been corrected.
- Previously, the KGAP could restart if a certificate with no names was received in a SIP TLS call. This has now been corrected.

Copyright © 2011 Polycom, Inc.

- Some small memory leaks in connection with handling illegal certificates have been removed.
- An unimportant state-event error which was issued when receiving a re-INVITE without SDP has been removed.
- An UPnP related issue has been fixed. A multicast packet missing the ST header could cause the administration process to restart.
- If auto creating a user failed (e.g. because of a wrong access code) the temporary user was not deleted. This has now been corrected.
- If auto assigning an IPEI to a user failed (e.g. because of a wrong access code), the temporary IPEI was not cleared. This has now been corrected.

4.1.4 Identified Issues

- In a Microsoft Lync setup ICE is sometimes necessary to establish calls between devices separated by firewalls. This is currently not supported. Support for this will be added in an upcoming release.

4.1.5 Configuration File Parameter Changes

File	Action	Parameter	Description
config.xml	Added	sip.media.sdp_hold_attribute_sendonly	When putting a call on hold the KIRK Wireless Server sends inactive (which is the more correct) instead of sendonly (which is old behavior). Configuring this setting as true restores old behavior. Values: true, false. Default: false

4.2 Version PCS09__ – Q3, 2011

No significant changes since PCS08B_. This is a GA version of the PCS08B_ firmware.

4.3 Version PCS08B_ – Q2, 2011

4.3.1 Added or Changed Features

- Microsoft Lync interoperability added.
- In scenarios where it is preferred that the user sends all SIP requests to the same proxy, the IP address of the proxy is now stored instead of the hostname when an OK is received for a REGISTER request. This will ensure that when a user is registered on a proxy it will use that proxy for all outgoing signaling, even in the case of a proxy name which resolves to multiple addresses.
  The above described behavior is enabled in the following scenarios:

Copyright © 2011 Polycom, Inc.

  - If “send_to_current_registrar” is enabled. This is typically used in Cisco Unified Call Manager scenarios.
  - If Microsoft Lync is enabled.

  With the above described behavior it is possible to have a setup with load sharing, while at the same time preventing that users potentially move from one proxy to another for every call.
- SIP proxy-handling and routing of SIP messages has been improved.
  If “dns method” is configured to DNS-SRV the KWS will attempt to resolve pre-configured proxies via DNS-SRV. If this fails they will still fall-back to A-records. Furthermore the KWS will no longer add any pre-configured proxy in a Route header for outbound requests outside a dialog.
- DNS A-records with multiple addresses are now handled and used like prioritized SRV records. Earlier if a DNS A-records answer with multiple addresses was received only the first address was used.
- If the KWS receives an INVITE or an UPDATE with an unknown Content-Type, it will Respond with “415 Unsupported Media Type”. This is a prerequisite for ad-hoc conferencing on Microsoft Lync.
- The KWS will no longer terminate the active call if a BYE is received for the held call while a REFER is pending for the active call. This resolves a problem introduced in PCS08__ which is known to cause problems with attended call transfer on Siemens OpenScape.
- 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).
- The KWS is now able to handle the release reason “MsfHandsetInCharger”. This release reason is only relevant for applications which enable this feature in the handset. The feature is supported by the KIRK 60- and 70- Handset Series.
- The handling of SIP SUBSCRIBE requests has been re-factored to enable a more robust handling of SUBSCRIBE requests.
- A warning will be issued to the Message Log if a DECT signal which is too long is sent to the protocol layers.
- The internal messaging protocol between the KWS and media resources is rewritten to make future protocol updates easier.
- An exponential back-off timer is now used for all kinds of REGISTER failures. Earlier if a SIP REGISTER failed due to a SIP error response e.g. 404 not found, the back-off timer was not used, now it is.
- The maximum allowed length of a SIP message is changed to 128kB on KWS6000 and 32kB on KWS300. This allows large presence XML documents from MS Lync to be handled.
- Messaging handling is changed. The KWS can now handle 24 character call back numbers and 72 characters text messages. Furthermore several potential buffer overflows were eliminated.
- Previously the reception of the SIP status responses: “181 Call Is Being Forwarded” and “199 Early Dialog Terminated” resulted in an entry in the message log: “INVITE unexpected response” with level NOTICE. This is no longer the case as these responses are perfectly legal and not unexpected.

Copyright © 2011 Polycom, Inc.

- If the KWS receives a SIP URI as callback number (a call back number starting with sip@ or sips@), the characters “p” and “s” will no longer be converted to 0x05 a pause-digit.
- When TLS domain verification fails the allowed domains and the failed domain are logged to the message log. This makes it easier to find and correct errors in the TLS configuration.
- An info message about re-registration is no longer logged every time a TCP connection is destroyed.
- If a packet capture is stopped or started it is now logged in the message log with level INFO. Furthermore it is logged if the packet capture is restarted due to overflow.
- The size of media resource messages is limited before they are sent.
- SIP TLS pcap trace messages are truncated to fit into UDP datagrams.
- If the “capture everything” setting is used in packet traces, decrypted SIP messages are included in the trace. Furthermore unencrypted SIP messages were previously potentially logged twice, this is corrected.

4.3.2 Removed Features

- None.

4.3.3 Corrections

- If the proxy uses strict routing the KWS would crash (this behavior was introduced in PCS07__). Support for strict routing is now restored. Specifically this addresses problems experienced when using a Toshiba CIX200 running software version MT4.1 together with KWS firmware PCS07 and PCS08. This fix addresses DECTESC-279.
- A SIP TCP buffer overflow crash and memory leak has been identified and corrected.
- If a reset device to default procedure is performed any custom ca-bundle installed will be removed and replaced by the default bundle. This was not the case in earlier releases.
- Changed handling of a SIP NOTIFY with a refer event. This results in a more correct call teardown in call transfer scenarios on some versions of Asterisk.
- For SRTP remember crypto attribute tag received in offer. This fixes a problem where the KWS used the wrong encryption key when more keys were available.

4.3.4 Identified Issues

- In a Microsoft Lync setup ICE is sometimes necessary to establish calls between devices separated by firewalls. This is currently not supported. Support for this will be added in an upcoming release.
- Issues have been identified in a Microsoft Lync setup with an external gateway towards PSTN or GSM.
  In an outgoing call from a KWS through a gateway to e.g. a PSTN phone, the gateway may present the main number as caller id on the receiving phone instead of the local number from the calling handset.

Copyright © 2011 Polycom, Inc.

- Presence status for a handset on a KWS will not be correct unless the Lync account for the handset has been activated at least one time from a presence enabled client, e.g. a Microsoft Lync client.
- Message Waiting Indication is currently not supported on Microsoft Lync.

4.3.5 Configuration File Parameter Changes

File	Action	Parameter	Description
config.xml	Added	sip.lync.enable	Enable Lync Server 2010 support. Values: true, false. Default: false
config.xml	Added	sip.lync.domain	The domain of the Lync Server 2010. Default: Empty
config.xml	Added	sip.lync.servicename	The name of the DECT service user account. Default: Empty
config.xml	Added	sip.lync.password	The password of the DECT service user account. Default: Empty

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).

Copyright © 2011 Polycom, Inc.

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.

- Handset display handling during SIP calls has been improved with respect to displaying other party username and display name.
  P-Asserted-Identity or Remote-Party-ID, INVITE and INVITE responses are used to update the handset display with other party username and display name.
  Specifically, this makes the handset update the display correctly during call transfer and call forwarding on several SIP servers including Cisco Unified Call Manager.
  Furthermore, this makes the display name of the other party update correctly in connection with group call pickup on a 3CX PBX.
- Putting calls on hold before performing an attended transfer.
  In previous versions of the firmware only one of the calls were put on hold. Now both calls are put on hold. This makes attended transfer work on some configurations of Cisco Unified Call Manager Express.
- Allow INVITE with a Replaces header for existing incoming early dialog.
  This makes semi-attended transfer work with Polycom SoundPoint and some SIP proxies, for example IPFx and OpenSer. This addresses DECTESC-266.
- 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.
- Quick status has been added by popular demand. The reasoning behind quick status is a wish to make it even easier to get an overview of the health of the system. This is accomplished by adding a status summary of different vital system components to the first webpage you see when logging in to the system. To get a more detailed status it is still necessary to go into the specific parts of the GUI.
  Quick status displays a status overview of the following system components:
  SIP:
  The SIP status is OK if all enabled SIP users are registered to the SIP server.

  KWS redundancy:
  KWS redundancy is OK if the connection to the redundancy peer is OK. The KWS redundancy status is not shown if redundancy is not installed on the KWS.

  Base stations:
  Base station status is OK if no synchronization loops are detected, auto synchronization is disabled for all base stations and all enabled base stations are connected and synchronized.

Copyright © 2011 Polycom, Inc.

Media resources:
Media resource status is OK if all enabled media resources are connected and at least one channel is available.

Provisioning:
Provisioning status is OK if the latest communication with the provisioning server was successful.

NTP:
NTP status is OK if the latest communication with the NTP server was successful.

- SIP user provisioning changed.
  Changing a SIP user setting using provisioning will have immediate impact. As an example changing the SIP display name or the SIP authentication password will be effective immediately without any issues. Some deployment configurations utilize this, e.g. for changing the display name automatically, for instance if a phone is shared between different users. One notable exception to the above is the SIP username of the user. The username is used as the key in the users.xml and therefore, changing the username was previously handled by deleting the old user and creating a new one. A result of this was that the handset was unsubscribed on the DECT side when the username was changed. Changing other fields would not cause this. Furthermore, changing the username through the GUI (and not using provisioning) would not cause this to happen.
  Now the user handling is rewritten to avoid deletion of users when their usernames are changed. For this to work, the user must have an IPEI in the users.xml file.
  With this new feature, it is now possible to implement a “hot-desking” feature where even the username used to call the user can change automatically controlled by provisioning. One use case is to have a device pool of handsets; when a user signs in at a shift, the user grabs any handset, calls a special number and enters an employee id. Subsequently, the provisioning framework configures the phone with the username, passwords, display name etc. without any manual interaction.
  This change addresses DECTESC-214.
- HTTP redirect in connection with provisioning allowed. If a provisioning server redirects a provisioning request with a 3xx redirection, this is now supported by the KWS.
- Backslash in SIP authentication user allowed. This is required for NTLM where the authentication user is typically entered as: *domain**user*.
- If an error response is received for a SIP transaction, the reason text, which in some cases is presented to the handset and logged in the message log, is now handled differently.
  Previously a reason text was derived from the status code, i.e. a 488 would always be converted to "Not Acceptable Here". Now the reason phrase is retrieved directly from the received SIP message. As an example an outgoing call attempt on a Microsoft Lync may result in a SIP 488 with a text like: "Encryption levels not compatible". Previously the message log would say: “Not acceptable here”, now it will say: "Encryption levels not compatible".
- License key handling has been updated. Previously 7 licenses were allowed, now up to 15 licenses can be loaded.

Copyright © 2011 Polycom, Inc.

- If TLS is used for SIP signaling and a TLS handshake failure is experienced, it will be logged as an error. Previously this was logged as an info.
- When using TLS for SIP signaling, the SIP signaling is encrypted. While increasing the security of the system, this also makes it very difficult to debug SIP signaling. The embedded packet capture functionality in the KWS now supports export of a decrypted version of the SIP signaling. This feature is controlled by the “Capture SIPS (decrypted)” checkbox on the KWS GUI in the packet capture menu.
- If a 301 Moved Permanently is received by the KWS as a response to a REGISTER requests, the KWS will now handle this and resend the REGISTER to the new destination.
  If the SIP setting “Send all messages to current registrar” (controlled by sip.send_to_current_registrar) is enabled, 301 Move Permanently will not work.
- When a SIP INFO request is received, the KWS responds with 200 OK. In previous firmware revisions, the KWS responded with 501 Not implemented. This addresses a problem reported in [DECTESC-254]. In a setup with an Aastra 5000 PBX, the PBX apparently uses SIP INFO for keep-alive signaling. If the Aastra did not receive a 200 OK, the call was terminated.
- 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.
- In an outgoing call the KWS now waits for RTP in early media before connecting the endpoint. This addresses the scenario where the other end signals early media e.g. for generating a ring-back tone and the early media has not been received. If the early media is not received, we now generate a local ring back tone until the actual RTP is received.
- The KWS now supports sending DTMF tones via rfc2833 in outgoing calls before the other end has answered the call. In some situations the user is required to enter a pin code before the call establishment can be completed. This is now handled by allowing DTMF transmission while early media is being received, and the 200 OK response is not yet received.
  This addresses DECTESC-263. The specific scenario is a user which has signed up for a carrier-based user authorization for long distance calls. When one of the users calls a long distance number, he will hear a beep and will then have to enter the authorization code to complete the call. In the scenario in question, the carrier side does not answer the call until the authorization code is validated.
- Corporate phonebook LDAP access has been improved. The allowed length of ldap_bind_user is increased from 64 to 256. This addresses DECTESC-268 which involves an LDAP bind user of 72 characters.

Copyright © 2011 Polycom, Inc.

- When new base stations or media resources are rejected due to actively disallowing them (controlled by security.allow_new_media_resource & security.allow_new_rfp), it is explicitly written in the message log that this is the cause of the rejection.
- Minor changes to the Kirk Wireless Server GUI.
  The following settings are now available from the web GUI on the KWS under Configuration|SIP general:
  - Enable Globally Routable User Agent URIs GRUU
  - Use SIPS URI
  - TLS allow insecure
- The base station configuration menu on the KIRK Wireless Server GUI which is available from Administration | Base station has been updated. Changing some of the fields in this menu would automatically reboot the base station. This is now emphasized.
  The Configuration | Media Resource menu on a KIRK Wireless Server applies to the internal media resource embedded in the KWS, this is now emphasized.
  Furthermore, hints are added to the media resource and base station central firmware update.
- 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

- Previously, if a SIP From header without username was received, it would in some cases result in a restart of the KWS and subsequent loss of active calls. This was reported in DECTESC-257 which describes a scenario with an incoming anonymous call on a Cisco Unified Call Manager. This has been corrected.
- XML-RPC default password problem introduced in PCS07__ is fixed. If the default password was never changed or saved, the XML-RPC interface in firmware PCS07__ would not allow login.
- Allow SIPS URI in Refer-To header of REFER. Previously this was not handled correctly and would sometimes cause call transfers to fail (e.g. on Kameilio) if SIP over TLS was used.
- When using HTTPS for provisioning, the HTTPS connection in some cases was not established correctly due to a bug in the TLS handling. This has been corrected.
- If a TLS connection (either for provisioning or for SIP over TLS) was closed by the other end during handshake, this would in some cases cause a restart of the administration or the call handling process. This has been corrected.
- Port numbers are no longer inserted on GRUUs. This fixes some potential routing problems when GRUU is used.

Copyright © 2011 Polycom, Inc.

- Previously the following error message was logged in some cases: “Unknown configuration key, rtp.* setting changed.” This log message was not an error and has been removed.
- Previously a reboot was required if either of the settings: sip.media.sdp_answer_single and/or sip.media.sdp_answer_with_preferred were disabled. 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.
config.xml	Added	security.srtp_rfp	Enabling this 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. Values: true/false Default: false.
config.xml	Added	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). Values: true/false Default: false.

Copyright © 2011 Polycom, Inc.

config.xml	Added	sip.media.srtp.required	If enabled, the use of SRTP is required. If negotiation of SRTP with the other end is unsuccessful, call establishment is aborted. Values: true/false Default: false.
config.xml	Added	sip.media.srtp.lifetime	Handling of RFC 4568 SRTP lifetime key parameter in SDP offers. Values: true/false Default: false.
config.xml	Added	sip.media.srtp.mki	Handling of RFC 4568 SRTP Master Key Index parameter in SDP offers. Values: true/false Default: false.

4.5 Version PCS07__ – Q1, 2011

4.5.1 Added or Changed Features

- Support for using TCP as transport protocol for SIP signaling has been added.
- Support for using TLS as transport protocol for SIP signaling has been added. Be aware that TLS is supported only for outbound connections. Using TLS will allow for encryption of SIP call signaling. If TLS is enabled, UDP and TCP connections will be disabled by default to increase security.
- Provisioning using HTTPS is now supported. With the possibility to use HTTPS for provisioning of users and configuration data, it is now possible to increase the level of security with regard to remote management of KWS solutions.
- Added support for certificate handling. A certificate is required to be able to use HTTPS provisioning or SIP over TLS. The KWS is delivered with a Certificate Authority (CA) bundle with common Certificate Authorities. This means that the KWS will accept certificates issued by for example Verisign out-of-the-box. In addition to the CA-bundle the GUI allows for installing a local CA certificate bundle if a certificate is generated by a local authority (e.g. a service provider or the local IT department). A certificate bundle in PEM-format may be imported.
- 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.
- Port numbers for separate, individual SIP signaling ports have been changed. Previously, port number 5060 – (5060 + number of users) was used. Now, port numbers 15061 – (15061 + number of users) is used.
  This is relevant only when the KWS is configured to use separate individual SIP signaling ports.

Copyright © 2011 Polycom, Inc.

- Configuration key sip.proxy.transport has been replaced by the keys sip.transport and sip.dnsmethod. That way the SIP transport and the DNS method are separate making it easier to understand how these are configured. The KWS still understands the key sip.proxy.transport, but it is recommended to use sip.transport and sip.dnsmethod.
- When the KWS requests to put the remote end on hold, the KWS sends an INVITE with a SDP message indicating that the call must be put on hold. Previously this SDP had the media attribute 'sendonly', and the IP address of the connection was set to 0.0.0.0. Now only the media attribute 'sendonly' is used to signal that the call is on hold. This change has been made because some SIP implementations do not allow the 0.0.0.0 IP address. Setting sip.media.sdp_hold_null_connection=true returns to the previous behavior (not RFC compliant).
- Globally Routable User Agent URI (RFC5627) support has been implemented. A Globally Routable UA URI (GRUU) is an URI which 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. With GRUU support the KWS can handle more advanced transfer scenarios, provided it is supported by the SIP server.
- An Universal Unique ID, UUID, has been added to the user data. The UUID is used for GRUU and is generated automatically by the KWS.
- user=phone has been added to header in outgoing SIP signaling. This is required by e.g. Microsoft OCS.
- Support added for SIP URIs in called/calling party numbers. If for example an incoming call with calling party number consisting of a SIP URI (e.g. sip:alice@example.org) is received, the SIP URI can be stored in the redial-stack in the handset. To utilize this, it needs to be supported in the DECT handsets. For KIRK 50-, 60- and 70-Handset Series this will be supported starting with the following releases:

Handset	**Firmware version**
5020- and 5040-Handset Series	PCS08Na (or newer) released 2011-Q1
6020- and 6040-Handset Series	PCS07Ea (or newer) released 2011-Q1
7010-, 7020- and 7040-Handset Series	PCS07Ea (or newer) released 2011-Q1

- Support P-Preferred-Identity and P-Asserted-Identity headers (RFC3325). These headers allow trusted parties to assert the identity of authenticated users.
- Sending BYE immediately after REFER has been made configurable. During a call transfer the existing SIP dialog can be terminated by either the transferor or the transferee. Per default the KWS will terminate the dialog with a BYE request when acting as a transferor. If sip.send_bye_with_refer is set to false, the KWS will not send BYE when acting as transferor but rely on the transferee to send the BYE.
- Added support for SDP message sessions. Now SIP-servers/endpoints which use an INVITE to establish an instant-messaging session are supported by the KWS. This can be used for instant messaging towards the DECT endpoints on the KWS.
- Added option for ignoring the version information in incoming SDP received from remote endpoints. The default setting is sip.media.sdp_ignore_version=false. With the default setting, the version information in the incoming SDP will be honored. If the version is not changed, any change in incoming SDP will be ignored. This option

Copyright © 2011 Polycom, Inc.

can be controlled via the GUI on the Configuration|SIP page and through the setting: sip.media.sdp_ignore_version. If the other end changes the SDP without changing the SDP version, this setting should be true (not RFC compliant).
- When logging an abnormal call release, add a textual interpretation of the error code (if available). This addresses a feature request reported in DECTESC-236.
- If the process of allocating a voice channel on a media resource for a new call fails, the reason for the failed allocation is now logged, e.g. no media resource connected or no free channels.
- Logging of failure to allocate a voice channel on a media resource is demoted from CRITICAL to NOTICE.
- Status/debug information with regard to RTP handling has been added. When a 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

- If the configuration setting media_resource.enabled is changed, the local media resource will be stopped if the setting is false. All other values will result in the start of the media resource, e.g. true or empty (default). This solves DECTESC-226.
- An error in reboot-on-idle functionality has been corrected. Since provisioning is using the reboot-on-idle functionality as of PCS06A_, this correction will make provisioning able to reboot the device.
- If the KWS receives a 423 (Interval Too Brief) response to a SIP REGISTER, it will now honor the expiration interval within the Min-Expires header field of the 423 response. This means that subsequent SIP REGISTER requests will be sent with an interval as specified by the registrar even if this interval is greater than the registration expire setting of the KWS.
- DNS SRV priorities with the value 0 are now allowed. Previously the value 0 was regarded as no priority.
- The negotiated ptime while sending DTMF via RFC2833 is respected.
- The free (12/30) users are not lost when only a feature license is loaded.
- Monotonic clock is used within SIP transaction timer handling. This means that SIP transactions will not be affected by “jumps” in local time, e.g. due to NTP corrections to the time.
- CSV file import of users has been fixed, line ending is handled correctly. Furthermore, the line number in the following error message has been corrected: "CSV import line # - Wrong number of fields expected #".
- IPEI is printed correctly on auto created users.

4.5.4 Configuration File Parameter Changes

File	Action	Parameter	Description
config.xml	Added	sip.media.sdp_ignore_version	Specifies whether to ignore the version information in incoming SDP received from

Copyright © 2011 Polycom, Inc.

			remote endpoints. Values: true/false. Default: false.
config.xml	Added	sip.media.sdp_hold_null_connection	If this setting is true, the KWS will revert to the old way of signaling a hold. Values: true/false. Default: false.
config.xml	Deprecated	sip.proxy.transport	Deprecated. In release PCS07__, this setting is replaced by sip.transport & sip.dnsmethod. The KWS still understands this setting, but the new settings should be used.
config.xml	Added	sip.dnsmethod	Specifies the DNS method used to resolve host names for SIP requests. Values: arecord/ dnssrv. arecord: Use simple DNS A records to resolve host names. Basically A records are used to translate a hostname to an IP-address. dnssrv: 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.xml	Added	sip.transport	Specifies the transport mechanism used for SIP requests. Values: UDP, TCP, TLS. Default: UDP.

Copyright © 2011 Polycom, Inc.

config.xml	Added	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. Values: true/false Default: true.
config.xml	Added	sip.rfc3325	This setting controls support of RFC3325 P-Asserted-Identity and P-Preferred-Identity headers. These headers allow trusted parties to assert the identity of authenticated users. Values: true/false Default: true.
config.xml	Added	sip.send_bye_with_refer	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. Values: true/false Default: true.
config.xml	Added	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. Values: true/false Default: true.

Copyright © 2011 Polycom, Inc.

config.xml	Added	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. Values: true, false. Default: false

4.6 Version PCS06A_ - October 13, 2010

This release replaces the PCS05D_ release as the latest generally available (GA) release.

4.6.1 Added or Changed Features

- KWS redundancy available.
  If a redundancy license is installed it is now possible to configure a redundant setup of KWS. For more information refer to the application note regarding redundancy.
- Major upgrade of the provisioning handling including several enhancements to address the scenarios where a KWS is hosted by a service provider.
  Earlier local changes made through the web GUI would not be reverted by provisioning. This would make provisioning server settings and local settings inconsistent. Now the provisioning server settings, user data and firmware always take precedence over any local changes. I.e:
  - The config.xml file on the provisioning server takes precedence over settings on the KWS.
  - The users.xml file on the provisioning server takes precedence over user data on the KWS.
  - The firmware.bin file on the provisioning server takes precedence over the version on the KWS. A side effect of this is that provisioning (if activated) will revert firmware if updated via the GUI. I.e. if provisioning is configured and someone upgrades (or downgrades) the firmware from the version that is on the provisioning server, the provisioning process will revert the firmware version to the one available on the provisioning server.
- Added provisioning configuration merge functionality. This means amongst other things that provisioning will only initiate a reboot if a setting is changed that requires a reboot to become active. In previous releases any change to the configuration files located on the provisioning server would initiate a reboot.
- Eliminated several reboot scenarios. Some settings that previously required a reboot before a change would become active do no longer require a reboot to become active.
  Do not require a reboot to enable/disable XML-RPC.
  Do not require a reboot to enable/disable MSF.
  Do not require a reboot to enable/disable local media-resource.
  Do not require a reboot for provisioning method, URL, interval and time.
- Do not store default values in config.xml. This means that any setting which is left at the default value will not be saved in the config.xml file. Furthermore empty

configuration keys are deleted from the file, thus the config.xml file has become much smaller and radically easier to read.

- More robust flash upgrade process. Reboot is now handled centrally to ensure that the KWS is not rebooted while flashing the firmware.
- Add Reboot when idle function. This way it is now possible to schedule a reboot to take place when no calls are active on the system.
- 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.
- License handling changed to support cumulative licenses. I.e. several licenses can be installed on the KWS independently of each other.
- Store licenses in config.xml.
  The license was stored outside the configuration but is now moved into config.xml. This makes it possible to handle the license via provisioning.
- Distinguish between transport and timeout errors when displaying error messages in the handset.
  In earlier firmware versions all transport and timeout errors were reported as being transport errors. Now the transport and timeout errors are reported separately. A transport error is when a request cannot be delivered to the destination due to for example failed DNS lookup. A timeout error is when a response is not received within a reasonable time.
- Make SIP client transaction timeout configurable. Increase this time to eliminate timeout errors towards the SIP Provider or decrease it to reduce fail over time if you have several SIP proxies configured. If you have a “not-so-reliable” connection to your SIP provider/IPBX, it may be an advantage to increase this value. The value specifically controls timer B and F as specified in RFC3261.
- Prolonged the time a KWS waits for a response from a DHCP-server during boot before start-up. This addresses an issue where a KWS is configured for DHCP assigned IP-address and the KWS is deployed on certain Cisco switches (e.g. Catalyst 3560). On these switches the network link establishment is delayed which could result in a situation where the SIP User Agent Server is started before the KWS has received a DHCP assigned IP-address. Previously the KWS would wait 30 s before starting the KWS without a DHCP-assigned IP-address, this is now prolonged to 60 s.
- Statistics is now handled locally in media resources and base stations. This means e.g. that connection statistics for media resources and base stations will not be reset when a KWS restarts. If a manual statistics reset is performed on the KWS the connection statistics counters will however be cleared.
- Log (with level notice) when settings are changed either from the GUI or using provisioning. Indicate whether the change requires a reboot.
- Added support for RFC 3326 Reason header. This allows the PBX to control if the handset will display “Missed call” when part of a ring group. As an example if 2 handsets are part of a ring group an INVITE is sent to both handset. If handset 1

Copyright © 2011 Polycom, Inc.

answers the call, the PBX can send a CANCEL with reason header “Call Completed Elsewhere” to handset 2, which will result in the fact that no missed call indication will be displayed on handset 2. This is supported by e.g. Asterisk 1.6.
Support for this is expected to become available in the 50xx, 60xx and 70xx series handset Q1 2011.

- Allow "+" in outgoing B-no. If. e.g. "+45123456" is received as a calling party number a redial from the handset will now be allowed.
  Support for this is expected to become available in the 50xx, 60xx and 70xx series handset Q1 2011.
- Add broadcast of 60xx & 70xx series handset XML-RPC messages SMSSetupReq and ExtendedHwReq.
- Handling of SIP registrations improved. A new queuing technique allows for faster SIP registering of endpoints. In connection with e.g. reboots SIP registrations of many users is now handled faster.
- If problems are logged in the Media Resource concerning the connection to the KWS, it is now logged which KWS (which KGAP) it is (to handle a redundancy setup with several KGAPs).
- When the media resource logs messages, the message is prepended with MR (serial:####) to distinguish media resource logging from KWS (KGAP) logging. Furthermore shutdown connection to KGAP, and establish connection to KGAP is logged.
- More elaborate logging on the KGAP concerning connection establishment towards media resources.
- More verbose when ping or traceroute fails.
- It is now possible to allow/disallow new media resources or base stations to connect to a KWS. This can be controlled via the web GUI at Configuration|Wireless Server or through provisioning. Any media resource / base station 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/base stations will not be allowed to connect if set to disallow. The default setting is allow.
- LogMessage "HL_ME_U_PLANE_ind Me-Instance null. (Pmid:xxxxxx)" downgraded from warning to debug because it is misleading. The warning is logged before an abnormal release but is caused by the abnormal release.
- LogMessage "Users download complete" downgraded from info to debug.
- LogMessage "Configuration download complete" downgraded from info to debug.
- LogMessage "Firmware version download complete" downgraded from info to debug.
- Added info LogMessage "Firmware check complete".
- LogMessage "Provisioning reboot requested" upgraded from info to notice.
- Log a message if someone is trying to access XML-RPC while it is disabled.

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.
- The Derived Cipher Key which is used for encryption of voice data in the air is no longer stored at each handset location registration. It is stored at handset subscription and not subsequently. If authentication of calls is enabled a new derived Cipher Key will be calculated at each call. The only reason for storing the Derived

Copyright © 2011 Polycom, Inc.

Cipher Key after each location registration was to support the scenario where authentication of calls is disabled while encryption of calls is enabled. This scenario is no longer supported, to prevent problems with mismatching Derived Cipher Keys between PP and FP, authentication of calls is no longer optional if encryption is activated. This ensures that a new Derived Cipher Key is generated at every call.

4.6.3 Corrections

- Handle UPDATE requests correctly for incoming calls. This fixes an issue with some call transfer scenarios encountered on a CUCM and on an Avaya Aura™ Session Manager.
- Always set to-tag in SIP responses except 100. This fixes an issue encountered in interoperability testing against Avaya Aura™ Session Manager version 6.0, regarding handling of call forwarding (302 Moved Temporarily).
- 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.
- Do not crash when Referred-By header is missing in REFER, DECTESC-207 Avaya IPOffice.
- For outgoing calls only check the ARI and not the RPN, fixes problem with DistyBox 300 reported in DECTESC-208.
  When a handset performs an outgoing call the ARI of the system is sent to the system and checked. This failed for DistyBox 300 because the RPN was included in the ARI.
- Send BYE from transferor if transfer target does not send BYE.
  Addresses DECTESC-215 where a PBX does not send a BYE in an attended transfer scenario causing a hanging call on the PBX. The scenario was identified on an IPECS Call Server.
- Bug fixed. May cause configuration daemon to crash if no network.domain is defined.
- Disabling MSF did not work, this is now corrected.
  MSF was reported as disabled but was still active.
- Shutdown uPnP properly if disabled.
- Pressing save in the web-GUI for a user in the user list would initiate a new SIP register even in the case where nothing was changed for the user in question. This is corrected.
- Indicate “reboot required” for endpoint separate local ports (a setting on the Configuration | SIP page of the web GUI). This setting requires a reboot and this was not indicated in earlier releases.
- Fixed javascript problem in Firefox with auto sync. warning.
- Do not truncate the last character of a broadcast request sent via XML-RPC.
- Fix bug not allowing CLMS to a single handset via MSF.
- Fix group number in CLMS via XML-RPC. Previously it was interpreted as hexadecimal, now it is interpreted as decimal.
- Only write DNS configuration when we have something to put in it - avoid overwriting DHCP.
- If HTTP request line contains a full url, strip scheme and host part.

Copyright © 2011 Polycom, Inc.

4.6.4 Configuration File Parameter Changes

File	Action	Parameter	Description
config.xml	Added	redundancy.failover_time	The time in seconds from a redundancy node detects a failure until it initiates a failover operation. Default: 15.
config.xml	Added	redundancy.peer	The hostname or IP address of the redundancy peer node Default: none.
config.xml	Added	redundancy.database_uuid	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
config.xml	Added	redundancy.mode	The mode of the node: Either a normal single node system, a master or a slave node in a redundant system. Values: "single", "master", "slave". Default: “single”
config.xml	Added	sip.client_transaction_timeout	Specifies the timeout for client transactions. This controls timer B and F as specified in RFC3261. Values: Milliseconds (1000-32000). Default: 4000.
config.xml	Added	license	Storing of licenses if installed.

Copyright © 2011 Polycom, Inc.

			Values: A comma separated list of licenses. Default: Empty
config.xml	Added	security.allow_new_media_resource	This setting 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. Values: true, false. Default: true
config.xml	Added	security.allow_new_rfp	This setting controls whether new base stations are allowed to connect to the KWS. Any base station 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. Values: true, false. Default: true

4.7 Version PCS05D_ July 13, 2010

4.7.1 Added or Changed Features

- None

4.7.2 Removed Features

- None

4.7.3 Corrections

- Provisioning: Do not handle SIP NOTIFY check-sync events while updating the firmware.

If a SIP NOTIFY check-sync event was received while provisioning was updating the firmware, the device could reboot. This could make the device unable to start up afterwards.
This is only a problem if the firmware is updated via provisioning and SIP NOTIFY check-sync events are used.

4.7.4 Configuration File Parameter Changes

- None

4.8 Version PCS05C_ Q3, 2010

4.8.1 Added or Changed Features

- Added base station radio synchronization loop detection.
  It is of major importance that the configuration of the synchronization of the base stations does not contain loops. To ease the configuration of the system, automatic loop detection is added. The configuration is tested for loops at boot up when a base station configuration is saved and when the Loops button is clicked on the base station administration page.
  Be aware that the loop detection might be unable to detect loops correctly if the configuration contains duplicate RPNs or repeaters are involved.
- Implemented auto-answer feature which can be used for intercom and loudspeaker call. If an INVITE with an Alert-Info header, a Call-Info header or an Answer-Mode header is received, it is possible to make a Polycom handset automatically answer the call, mute the microphone and turn on speakerphone.
  The reason for handling several headers for activating this feature is that different SIP-PBXs have different default implementations. The following list of headers will activate auto answer:
  - Alert-Info: Auto Answer
  - Alert-Info: info=alert-autoanswer
  - Alert-Info: Ring Answer
  - Alert-Info: info=RingAnswer
  - Alert-Info: Intercom (*This is the default setting on Trixbox*)
  - Alert-Info: info=intercom
  - Call-Info: =\;answer-after=0
  - Call-Info: ;answer-after=0
  - Answer-Mode: Auto (*This is according to RFC 5373*)

  The feature is implemented in the 50-, 60- and 70-Handset series (except 7010 which does not have speakerphone). The feature requires a recent firmware for the handsets.

Handset	**Firmware version**
5020 and 5040 series handsets	PCS08Ja (or newer) released 2010-Q3
6020 and 6040 series handsets	PCS06Da (or newer) released 2010-Q3
7020 and 7040 series handsets	PCS06Da (or newer) released 2010-Q3

Please note that the Alert-Info header can also be used to control external/internal ring pattern. This feature is not affected by the addition of the loudspeaker call

feature. The following Alert-Info headers can be used to enable internal ringing (external ringing is default).

- Alert-Info: <internal>
- Alert-Info: <alert-internal>
- Alert-Info: internal
- Alert-Info: alert-internal

- Central phonebook: Increase the maximum number of records from 10,000 to 40,000. It should be noted that while retrieving phonebook data from a remote LDAP-server, the phonebook will be inaccessible. This means that the refresh interval (the interval at which the central phonebook data is being copied from the LDAP to the KWS) should be chosen with care. The combination of a slow LDAP-server/slow LDAP-server connection and a high number of entries in the corporate phonebook (> 10,000) should be configured with a long refresh interval, e.g. once-a-day.
- Central phonebook: Add support for more dialable numbers per record.
  This allows for dialling for example business and mobile phone via the central phonebook. The configuration parameter phonebook.ldap_number_attributes lists the LDAP attributes containing phone numbers, and the parameter phonebook.csv_number_fields contains CSV columns containing phone numbers.
- Central phonebook: Extended strip number feature to include replace number feature.
  This allows for more advanced number manipulation. See the configuration parameter phonebook.ldap_prefixes for details.
- 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.
- SIP UPDATE support (RFC3311).
  The KWS is able to receive and handle SIP UPDATE requests.
- Added DHCP syslog server support.
  A syslog server can be assigned via DHCP option 7.
- Added DHCP NTP server support for KWS6000.
  A NTP server can be assigned via DHCP option 42.
- 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.
- Export of rfps.xml and statistical data as part of the exported log for better diagnostics.
- More verbose logging when malformed SIP messages are received.
- User's CSV import is now more verbose on failure. Errors are listed in the log.
- Revised handling of SIP authentication credentials.
  The implementation of SIP authentication credentials varies significantly across different platforms and providers. To accommodate this, the SIP authentication credentials handling is made a lot more flexible.

Copyright © 2011 Polycom, Inc.

The authentication user is selected with these priorities:
1. Per user authentication user
2. Default authentication username
3. Per user username.

The authentication password is selected with these priorities:
1. Per user authentication password
2. Default authentication password.

All scenarios which were possible before are still possible for example the most restrictive (and most cumbersome to implement), i.e. using a per user authentication user and per user authentication password. However, it is now also possible to skip entering an authentication user in which case the username will be used as authentication username, and combining this with either a per user authentication password or a default authentication password.

- Added tooltips to the SIP configuration and edit user Web pages.
- Implemented Connected Line Identification Presentation.
  Shows returned display name in handset display for outgoing calls.
  If the To header in the 200 OK responses received for an INVITE contains a display name, this is displayed in the handset.
- Return of display name to caller for incoming calls.
  The display name is added to the 200 OK responses sent for an INVITE.
- More pedantic provisioning parsing of config.xml and users.xml to avoid that an incorrect file deletes users or configuration.
- Added SW PCS to SIP User-Agent header.
- More verbose display of SIP errors in handset.
  If a textual error message exists for a SIP error code, this is displayed.
- Added support for sending History-Info (RFC4244) used for call forward loop detection.
  This can be used to avoid problems when users are making a loop by forwarding calls to each other in a ring. For instance 2000 is forwarding to 2010 which is forwarding to 2020 which is forwarding to 2000.
- For incoming calls with no CODEC match, the response with error 488 is earlier.
  Sends the error before the handset starts to alert and terminates the call.
- XML-RPC: endpoint_base_stations() function added.
  This function allows for querying a Polycom handset for its base station map. This can be used for positioning of the handset. See the XML-RPC SDK version 1.4 for further details.
  The feature is implemented in the 50-, 60- and 70-Handset series. The feature requires a recent firmware for the handsets.

Handset	**Firmware version**
5020 and 5040 series handsets	PCS08Ja (or newer) released 2010-Q3
6020 and 6040 series handsets	PCS06Da (or newer) released 2010-Q3
7020 and 7040 series handsets	PCS06Da (or newer) released 2010-Q3

Copyright © 2011 Polycom, Inc.

- Added settings for sending callees preferred CODEC in SDP answers and for only sending a single CODEC in SDP answers. See configuration parameters sip.media.sdp_answer_with_preferred and sip.media.sdp_answer_single.

4.8.2 Removed Features

None

4.8.3 Corrections

- Fixed problem with auto creating maximum users.
  When auto create users was enabled, it was not possible to auto create the last user of the maximum users.
- Fixed hanging call waiting status when handset was released while waiting for a re-INVITE response (on/off hold).
  This made the KWS unable to handle call waiting for that particular handset until a reboot.
- Fixed wrong dialog handling for call waiting that made the To-tag change between the 180 and the 200 response.
  This caused some SIP servers to handle the responses as they were sent from forked calls. The issue was identified to cause problems on for example Shoretel.
- Pressing the alarm button on a subscribed Bosch D6000 handset caused system failure and required a reboot.
- Removed RFPI scanner CSV file error from log.

4.8.4 Configuration File Parameter Changes

File	Action	Parameter	Description
config.xml	Added	phonebook.csv_number_fields	The indexes of columns that contain dialable numbers. Values: List of indexes of dialable columns. Default: 2 Example: 2,3
config.xml	Added	phonebook.ldap_number_attributes	The names of the LDAP attributes that contain dialable numbers. Values: Dialable attributes provided by the LDAP server. Default: telephoneNumber,mobile Example: telephoneNumber,mobile
config.xml	Changed	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

Copyright © 2011 Polycom, Inc.

			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. Values: Phone number(s) to replace or strip. Default: "+=00" Example: "+45,+=00 "
config.xml	Added	sip.media.sdp_answer_with_preferred	Specifies if the media handling must ignore the remote SDP offer CODEC priorities. Values: true, false. True - ignores remote CODEC priorities. False - honours remote CODEC priorities. Default: false Comment: Enabling this option violates the RFC3264 SDP offer/answer model.
config.xml	Added	sip.media.sdp_answer_single	Specifies if the media handling must provide only a single CODEC in SDP answers. Values: true, false. True - provides only a single CODEC. False - provides all matching CODECs. Default: false

4.9 Version PCS05B_ Q2, 2010

4.9.1 Added or Changed Features

- Support handling of pauses in phone numbers: This makes is possible to include pauses in dialed phone numbers. If pauses are added in a phone number the part before the first pause is send in an INVITE and the KWS will wait for a 200 OK

before sending the pauses and the rest of the number via DTMF. Typical applications for this feature are nurse call system integration or voicemail applications. As an example it is now possible to store the following number in the phonebook/speed dial.
"5555pp8888#" where
- 5555 could be the number to the voice mail application.
- pp would indicate two pauses (this would give the voicemail application time to send out a new dial tone and be ready to receive an access code.
- 8888# would be the access code.
Phone numbers including pauses can be entered on the handset or received as call back numbers via the XML-RPC application interface or MSF application interface (a comma "," or a p "p" can be used to denote a pause in a call-back number).

- 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.

- Only reset media resource DSP on re-INVITE when needed: If a re-INVITE was received very early in a call it could potentially cause one-way-voice.

- The internal messaging feature added in firmware PCS05__ has been improved: Previously, internal messages were echoed on the XML-RPC application interface, this is removed.

- 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.

4.9.2 Removed Features

None

4.9.3 Corrections

- Fixed problem with local call forward in a setup with local call forward enabled and call waiting disabled.
  In this setup if a user is in an active call, and a second call is received the system previously would send busy to the second caller. This is now corrected so a second caller will be forwarded.
- Fixed not working NTP on media resource.
- Mask DECT high priority bit to remove problem with subscribing some Bosch handsets
- Removed memory leak when failing to decode SIP replaces header.

4.9.4 Configuration File Parameter Changes

File	Action	Parameter	Description
config.xml	Added	log.syslog.facility	Used to specify the remote syslog facility used for log messages. Refer to RFC5424 for

Copyright © 2011 Polycom, Inc.

			details. Values: The facility number to be used for the device. An integer between 0 and 23. Default: 16 (“local 0”)

4.10 Version PCS05A_ Jan. 27, 2010

4.10.1 Added or Changed Features

- Disable reboot button in KWS base station edit when base station is off line.
- Do not generate an error when an off-line base station is edited and saved.
- Save XML-RPC SMS on the handset stack when sent using endpoint_sms(). This makes it work the same way as handset-to-handset SMS.
- Do not send DECT pages to base stations that are not in sync. They are unable to handle them.
- Handle DECT page limiter signals from the base stations.
- Send a XML-RPC endpoint_broadcast event as a response to the endpoint_broadcast() function.
- Improved MSF buffer handling.

4.10.2 Removed Features

None

4.10.3 Corrections

- Removed fault causing restart when MSF buffer is full.
- Limit Message Waiting Indication (MWI) rate to not overload the infrastructure when many MWI are received.
- Removed a NULL pointer dereference when deleting a user and MWI is disabled.

4.10.4 Configuration File Parameter Changes

None

4.11 Version PCS05__ Q1, 2010

4.11.1 Added or Changed Features

- Call waiting is now supported. It must be enabled to be active (default on). Call waiting is supported on the whole range of Polycom DECT Handsets. However due to differences in keyboard layout, audio processing capabilities and display types, the appearance (audio as well as visual) differs between the different handsets. The solution implemented is a trade-off between back-ward compatibility and appearance. Note: The 5020 and 5040 handsets require firmware PCS_08Ca or newer.
  Accepting a new call: If call waiting is enabled a second call can be accepted by pressing “R”, in which case the other end will be set on hold and a connection will be established to the new/call waiting caller.
  Rejecting a new call: Pressing left arrow/ok button will reject the call waiting call.

Ending the old call and taking the new call: Pressing on-hook while the second call (the call waiting call) is alerting, will terminate the old call and the handset will start/continue ringing. It is now possible to answer the new call.
Ending an established call (if two calls are active):
- If two calls are established due to call transfer pressing on-hook will complete a call transfer.
- If two calls are established due to an incoming Call Waiting which is accepted, pressing on-hook will terminate both calls.

Toggling between two active calls: Pressing “R” will toggle between two active calls.

Ending the active call if two calls are present: Pressing left arrow/ok button will terminate the current call (but not the second call).

- Add Message Waiting Indication (MWI) for the 2010 handset. With this addition Message Waiting Indication is supported on the complete range of Polycom DECT handsets.
- Local call forward (unconditional) is now supported. Number to forward to is configurable from the web-GUI as well as directly from the handset. Using the web-gui the Local Call Forward number can be viewed/edited directly from the user entry of the user in question. The feature code for enabling/disabling local call forward from the handset can be configured from the “Configuration|Wireless Server” menu. The default code is “*21*$#” where “$” denotes the number to forward to. If a handset has call forward enabled the standby text will be pre-pended with (CFU) to give the user an indication that the handset is forwarded.
- It is now possible to disconnect the active call if two calls are active (either due to an attended call transfer, or due to an accepted call waiting call). If two calls are active pressing left-arrow will disconnect the active call (without disconnecting the in-active call).
- Increased string lengths for SIP parameters.
  - Default domain 32 -> 256.
  - User name 32 -> 64.
  - User domain 32 -> 64.
  - User authentication 32 -> 64.
- Introduced remote syslog (RFC5424) via UDP. The remote syslog allows for using a PC to receive messages/logging from a KWS.
- Added internal messaging for sending text messages between handsets without requiring an external application.
  The feature is enabled per default but can be disabled if it interferes with an external application.
- Failure to read ARI is now logged as EMERGENCY (was KSF_CRITICAL).
- MSF/XML-RPC: Release DECT connection immediately when a PP_STATUS_ind initiated by the handset is received.
- Support for advanced messaging features introduced. This includes MSF_SMS_SETUP_req (MSF format 3) and support for MSF_SMS_RESPONSE_ind & ExtenHwReq/Cfm. These features will become available with the release of the upcoming next-generation handset series (the 60xx and 70xx series). The advanced features include alarm buttons, tear-off cord, multicolour LED controllable from an application and motion sensor etc.
- Do not send XML-RPC/MSF messages to a handset while messages are queued for the handset.

Copyright © 2011 Polycom, Inc.

- Added XML-RPC endpoint_release event.
- Provisioning improved detection of firmware version inconsistency to avoid problems if firmware is updated manually.
- Provisioning is made more verbose. Download of users, firmware and configuration from a provisioning server is now logged to the message log.
- Also log line number when failing to parse users.xml.
- Do not stop user import if displayname or standby text is invalid or too long - just skip or truncate and log a message.
- Do not abort provisioning process when one of the steps fails.
- When exporting logs, the message log is stored in clear text. The message log can now be read with standard software.
- Improved logging of SIP failures.
- Improve log export speed.
- Attended transfer: Send the REFER to inactive dialog instead of active. This is required by Siemens HiPath and Toshiba.
- Create a KSF log on media resource crash.

4.11.2 Removed Features

None

4.11.3 Corrections

- Add double-quotes to SIP display names to allow special characters and international letters. This is required by the RFC and e.g. Cisco Call Manager.
- Fixed problem with provisioning polling interval. This could result in the fact that the device stopped polling for updates.
- Increase SIP dialog local cseq when a request is re-send. This solves a problem with mid-dialog authentication of requests. The problem was originally seen with a Nortel IPBX (DECT-142).
- Does not require that a SIP dialog is established when 180 Ringing is received. Fixes problem with missing dialog parameters for Aastra and Splicecom.
- Fixed resolver CNAME problem. DNS CNAME records now supported.
- Handles a comma(,) in the username part of the URI in a Refer-To header (DECTESC-167).
- Removed a lot of unnecessary writes to the flash. These induced unnecessary tear on the flash, especially during boot.
- Changing sip.media.symmetric setting would issue an error in the message log: “Unknown SIP configuration key: sip.media.symmetric”, this is fixed.
- XML-RPC: Fixed problem with zero length data in PP_STATUS_ind.
- Removed a few large buffers from the stack. These may have caused sporadic failures.
- Minor NTP client improvement which reduces the amount of “NTP failed” errors in the log.
- XML-RPC/MSF: Handle PP_STATUS_req/ind in more states.
- Report SIP transaction failed if decoding the unauthorized header fails.
- Re-classified some log messages.
- Removed memory leak when receiving a SIP MESSAGE.

Copyright © 2011 Polycom, Inc.

- Validate configuration keys when setting them. This avoids malforming the config.xml.
- Improved logging of failures in connection with the DNS resolver.
- A "No license available" notice message was written to the log even if no license was required, this is corrected.
- MSF: Handle XML escaped characters correctly for incoming messages.
- XML-RPC/MSF: Clean up release reasons to comply with the documentation. Normal release reasons (0x00) are unchanged but the values of other release reasons have changed. For XML-RPC refer to the XML-RPC SDK version 1.1 or later for details.
- 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.
- Does not require a default gateway for UPnP to work.

4.11.4 Configuration File Parameter Changes

File	Action	Parameter	Description
config.xml	Added	log.syslog.host	Specifies the remote syslog server host address. Default: Empty
config.xml	Added	log.syslog.port	Specifies the remote port of the syslog server. Values: The port number on a remote syslog server. Default: Empty which defaults to 514
config.xml	Added	feature_codes. enable	Used to enable/disable local handling of feature codes. Values: true/false Default: false
config.xml	Added	feature_codes.call_forward.unconditional.enable	Specifies the feature code used for enabling unconditional call forward (CFU). Values: The feature code users must dial to enable unconditional call forward. Default: *21*$#
config.xml	Added	feature_codes.call_forward.unconditional.disable	Specifies the feature code used for disabling unconditional call forward (CFU). Values: The feature code users must dial to disable unconditional call forward. Default: #21#
config.xml	Added	application.internal_messaging	Used to control if messaging between handsets is handled internally or by an external application. If enabled messages will be handled

			internally. Values: true/false Default: true
Config.xml	Added	sip.callwaiting	Used to control whether Call Waiting is enabled. Values: true/false Default: true

4.12 Version PCS04B_ October 20, 2009

4.12.1 Added or Changed Features

- None

4.12.2 Removed Features

- None

4.12.3 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.

4.12.4 Configuration File Parameter Changes

- None

4.13 Version PCS04A_ October 12, 2009

4.13.1 Added or Changed Features

- None

4.13.2 Removed Features

- None

4.13.3 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.

4.13.4 Configuration File Parameter Changes

- None

4.14 Version PCS04_ Q4/2009

4.14.1 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.

Copyright © 2011 Polycom, Inc.

- 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.

4.14.2 Removed Features

- None

4.14.3 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.

4.14.4 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

Copyright © 2011 Polycom, Inc.

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

4.15 Version PCS03B_ (Q3/2009)

4.15.1 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.

Copyright © 2011 Polycom, Inc.

- Added timestamp and synchronization statistics duration to rfps.xml.
- If SIP registration fails, re-register within a short time and then wait.

4.15.2 Removed Features

- None

4.15.3 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.

Copyright © 2011 Polycom, Inc.

4.15.4 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)

4.16 Version PCS03A_ (Q2/2009)

4.16.1 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.

4.16.2 Removed Features

- None

4.16.3 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.

Copyright © 2011 Polycom, Inc.

- 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.

4.16.4 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

4.17 Version PCS03_ (Q1/2009)

4.17.1 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.

Copyright © 2011 Polycom, Inc.

- 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.

4.17.2 Removed Features

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

4.17.3 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.

4.17.4 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

Copyright © 2011 Polycom, Inc.

File	Action	Parameter	Description
config.xml	Added	provisioning.check.interval	Specifies an interval for checking for updates. 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

Copyright © 2011 Polycom, Inc.

File	Action	Parameter	Description
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
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.

Copyright © 2011 Polycom, Inc.

4.18 Version PCS02A_ (Q4/2008)

4.18.1 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.

4.18.2 Removed Features

None

4.18.3 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.

Copyright © 2011 Polycom, Inc.

*4.19 Version PCS02_*

Initial KWS6000 version.

5. Outstanding Issues

The following issues will be fixed in a subsequent release

- None identified.

Copyright © 2011 Polycom, Inc.