Versionsreport Firmware

# COMfortel WS-400 IP/Multi, WS-650 IP, WS-Base

**Version: 18Ba (Q2 2018)**

**Hinzugefügte oder geänderte Leistungsmerkmale**

- Sortieren von CSV oder LDAP Telefonbüchern wurde bisher nur aufgrund von englischer Buchstabenreihenfolge gemacht. Das Sortieren erfolgt nun basierend auf der lokalen Sprache auf dem Server. Mit dieser Information im Hinterkopf macht es noch mehr Sinn, die Sprache des Servers auch auf die Sprache zu setzen, die im Telefonbuch benutzt wird.
- Der G.729 Codec mit niedriger Bitrate ist nun nicht mehr eine Kaufoption, sondern frei erhältlich.
- Die maximale Anzahl der unterstützten Cluster ist nun 1024.
- Es ist nun möglich, ein CSRF Token für Scripting über das Web-Interface zu erhalten.
- Es ist nun möglich, gesperrte Basisstationen und Media-Ressources von getrennten zu unterscheiden.

**Korrekturen**

- TLS-Algorithmen ohne explizite Hash-Funktion (z. B. AEAD-Algorithmen) wurden in TLS-DSK deaktiviert. Dadurch wird die TLS-DSK-basierte Authentifizierung korrigiert, wenn das Skype for Business-Frontend unter Windows Server 2016 ausgeführt wird (DECTESC-841)
- Wenn die Verbindung über eine langsame Verbindung hergestellt wurde oder der IP-DECT-Server überlastet ist, konnte der interne Sendepuffer in den Basisstationen und Medienressourcen überlaufen und das Gerät hängenbleiben oder nicht mehr reagieren (DECTESC-849).
- ICE-Kandidatenprioritäten, die von dem entfernten Endpunkt empfangen werden, werden nicht länger als einzigartig angenommen. Dies beseitigt einen Fehler in den ICE-Implementierungen von Polycom-Endpunkten, der dazu führt, dass die Schaltfläche zum Halten / Übertragen des Menüs nicht angezeigt wird. (DECTESC-845).
- Es wurde ein Problem behoben, bei dem, wenn ein SUOTA-Versuch fehlschlug, nachfolgende Sprachanrufe zufällig getrennt werden konnten, bis die SUOTA-Instanz beendet oder abgebrochen wurde (DECTESC-846).
- Wenn die Basisstation die IP-DECT-Serveradresse über DHCP empfangen hat, wurde fälschlicherweise angezeigt, dass sie in der Web-GUI neu gestartet werden musste (DECTESC-851).
- Eine Race Condition zwischen dem Löschen eines Benutzers und dem Ausführen der Anmeldung von einem Mobilteil könnte dazu führen, dass die Benutzerdatenbank einen inkonsistenten Geräteeintrag erstellt, der die Erstellung neuer Benutzer verhindert (DECTESC-852).
- Ein Remote-Endpunkt, der viele reflexive Peer-Kandidaten erzeugt, könnte dazu führen, dass bei der Mediaressource eine interne Tabelle überläuft und abstürzt.
- Fehlerberichte vom internen http-Client wurden verbessert.
- Es wurde ein Fehler in der Webschnittstelle behoben, der beim Importieren einer CSV-Datei mit demselben Namen einen internen 500 Fehler zurückgab.
- In einer Cisco Unified Communication Manager-Umgebung wird SRTP jetzt optional unterstützt, sodass es in einer Mixed Mode-Einstellung sowohl mit SRTP-aktivierten als auch regulären Endpunkten funktioniert (DECTESC-836).
- Wenn die Verbindung mit einem sehr langsamen oder angehaltenen Client hergestellt wurde, konnte die Web-GUI blockieren und nicht mehr reagieren. Die Web-GUI trennt nun solche Clients (DECTESC-828).

**Bekannte Einschränkungen**

- Der IP-DECT-Server ist nicht mehr kompatibel mit den Asterisk Releases vor 1.2.

**Version: 18Aa (Q1 2018)**

**Hinzugefügte oder geänderte Leistungsmerkmale**

- Die Verbindung zwischen dem IP-DECT-Server und den Basisstationen/Medienressourcen ist jetzt vollständig verschlüsselt, wenn beide Enden dies unterstützen. Optional kann die Verschlüsselung im Menü Konfiguration / Wireless-Server als obligatorisch festgelegt werden.
- Wenn neue Basisstationen und Medienressourcen mit dem Server verbunden sind, werden sie jetzt standardmäßig im deaktivierten Zustand hinzugefügt, um eine bessere Kontrolle darüber zu ermöglichen, welche Geräte mit dem Server verbunden sind. Dieses Verhalten kann im Menü Konfiguration / Wireless-Server geändert werden.
- Das Server-Web-GUI enthält jetzt einen CSRF-Schutz (Cross Site Request Forgery) auf allen Seiten, der Änderungen am Server verursachen kann.
- Die Namen, der auf dem Server erstellten Dateien (Protokolle, Paketerfassung, Backups) enthalten jetzt die Seriennummer des Geräts sowie das aktuelle Datum und die aktuelle Uhrzeit.
- Es ist jetzt möglich, Benutzerkennwörter und andere vertrauliche Daten daran zu hindern, in Dateien exportiert zu werden. Hinweis: Wenn Sie dies aktivieren, wird bei Systembackups die Benutzerdatenbank ausgeschlossen. Hinweis: Wenn diese Option aktiviert ist, kann sie nur durch Zurücksetzen auf die Werkseinstellungen deaktiviert werden, wobei alle Konfigurations- und Benutzerdaten entfernt werden.

**Korrekturen**

- Die Benutzererfahrung in Bezug auf die manuelle Aktualisierung der Firmware wurde verbessert. Beim Aktualisieren von Medienressourcen und IP-Basisstationen war es zuvor zwingend erforderlich, die Version manuell einzugeben und die Nummer der Firmware zu erstellen. Ab dieser Firmware werden die Informationen direkt aus der Binärimage-Datei extrahiert.
- Wenn Server, Medienressourcen und IP-Basisstations-Firmware über Provisioning aktualisiert werden (Medienressource und IP-Basisstation erfordern eine erweiterte Bereitstellungslizenz), musste der Benutzer zuvor den Dateinamen für alle 3 Firmware-Arten (Server, Medienressource und IP-Basisstation) eingeben. Da Spectralink empfiehlt, auf allen Geräten dieselbe Firmware zu verwenden, wurden die drei Namensfelder auf eine reduziert (siehe Provisioning-Dokumentation im Support-Portal).
- DECTESC-829: Die Verknüpfung mit den Benutzerdaten von der Seite mit den Gerätestatistiken war möglicherweise auf Systemen, auf denen zuvor die Mobilteilfreigabe aktiviert war, nicht korrekt.
- DECTESC-833, DECTESC-845: Anrufe zwischen IP-DECT-Systemen und Polycom VVX-Telefonen wurden aufgrund eines Fehlers im Polycom ICE-Stapel manchmal nach 10 Sekunden getrennt. Diese Version fügt eine Problemumgehung für den IP-DECT-Server hinzu, die durch Setzen von sip.media.polycom_ice_bug_workaround auf true in der Konfiguration aktiviert wurde. Hinweis: Das Aktivieren dieser Einstellung kann sich auf die Kompatibilität mit OCS / 2007-Endpunkten auswirken.
- DECTESC-834: Benutzer, die über die Skype for Business-PIN-Authentifizierung angemeldet sind, können aufgrund einer fehlenden Aktualisierung des Authentifizierungstokens in regelmäßigen Abständen keine Anrufe tätigen oder empfangen.
- DECTESC-839: Es konnten keine SIP-Nummern aus einem mit LDAP abgerufenen Telefonbuch gewählt (und anzeigt) werden. Zuvor wurden nur Nummern 0-9 und "+" in einem Nummernfeld akzeptiert. Jetzt wird auch eine Zahl akzeptiert, die mit "sip:" beginnt.
- Das Timing zwischen NTP-Zeiteinstellung und Dienststart wurde angepasst, sodass alle Zeitstempel in den Protokollen die korrekte Uhrzeit verwenden sollten, wenn ein NTP-Server konfiguriert ist.
- Spezielle SIP-URI-Parameter werden in der aktiven Anrufliste entfernt.

**Bekannte Einschränkungen**

- Der IP-DECT-Server ist nicht mehr kompatibel mit den Asterisk Releases vor 1.2.

## Version: 17Ea (Q4 2017)

**Hinzugefügte oder geänderte Leistungsmerkmale**

- Support für die Suche im Telefonbuch mit mehreren Tastendrücken (mit mehr als einem Buchstaben). Bisher konnte der Anwender nur 1 Buchstaben zurzeit eingeben und musste dann auf die Anzeige des Ergebnisses warten, um erst dann den nächsten Buchstaben eingeben zu können.
- Support für Türkisch bei M-210/310.
- Support für das erweiterte Provisionieren. Bisher konnte Nebenstelle, Konfiguration und Firmware nur vom Provisionierung-Serverempfangen werden. Jetzt ist es auch möglich, Firmware mit einer Media Ressource, einer IP-Basis und Handteilen (M-210/310) zu empfangen. Dieses automatische Update ist auch bis zu einem gewissen Grad über das Web-UI verfügbar. Erweitertes Provisionieren erfordert eine extra Lizenz.
- Es ist nun möglich, direkt SIP-URLs an den Handteilen zu wählen.

**Korrekturen**

- Wenn ein eingehender Ruf zu früh abgebrochen wird (z.B. vor dem Klingeln), versucht der IP-DECT-Server nun erneut, den Ruf zuzustellen. Dies betrifft DESCTESC-777.
- Wenn Wartemusik aktiviert ist, wird diese nicht weiter gespielt beim Anrufenden während eines Vermittlungsvorgangs. Es wird nicht mehr der Mediendatenstrom einfach abgeschnitten wie in vorherigen Versionen. Dies betrifft DESCTESC-778.
- Der SIP-Reregistrierungsprozess wurde optimiert bei der Nutzung der TLSDSK-Autorisierung.
- Wenn ein eingeloggtes Handteil ausgeschaltet wird oder die ID deaktiviert wird über das Web-Interface, wurde das Handteil nicht aus der Datenbank entfernt. Dies betrifft DESCTESC-812.
- Der Lifetime-Parameter von SRTP in SDP-Nachrichten wird nicht länger hinzugefügt, wenn diese Einstellung deaktiviert ist. Dies betrifft DESCTESC-817.
- Wenn ein zweiter, eingehender Ruf zu einer Wettlaufssituation führte, wurde dieser Ruf auf beiden Seiten beendet. Dies betrifft DESCTESC-749 und -799).
- Es wurde immer die SyslogServer-Einstellungen an die MR/RFP, auch wenn kein Server konfiguriert war. Dies betrifft DESCTESC-798.
- Eine Anzahl von Cross-Site-Scripting-Angriffen im Web-UI konnte bereinigt werden.
- Basisstationen können nun via XML-RPC neu gestartet werden.
- Es ist nun möglich, sich bei den Basisstationen und Media-Ressourcen vom Web-UI auszuloggen.
- Die Zeichen ,;?/ wurden den erlaubten Zeichen in SIP-Benutzernamen hinzugefügt, um die komplette SIP RFC3261 zu erfüllen.
- Es wurde ein Problem beseitigt, dass bei schlechten Netzwerk-Konditionen zu einem Systemabsturz führte. Dies betrifft DESCTESC-820.
- Es wurde ein Workaround hinzugefügt für Endgeräte von Drittanbietern, die nicht ICE Verbindungscheck anstoßen konnten.
- Es wird nicht mehr das Fehlerlog mit immer derselben Fehlermeldung geflutet, wenn die interne Media-Ressource deaktiviert war auf einem IP-DECT-Server. Dies betrifft DESCTESC-813.
- Es wurde ein Problem bei WS-400 IP beseitigt, bei dem die lokale UDP-Port-Zuweisung fehlschlug. Dies betrifft DESCTESC-765, -787, -802 und -803.
- Es wurde ein Problem beseitigt, bei dem der Sync-Status inkorrekt an redundante Systeme gemeldet wurde. Dies betrifft DESCTESC-792.

**Bekannte Einschränkungen**

- Der IP-DECT-Server ist nicht mehr kompatibel zu Asterisk-Versionen vor 1.2.

## Version: 17C (Q3 2017)

### Hinzugefügte oder geänderte Leistungsmerkmale

- Support für die neue Nutzung des zentralen Telefonbuchs im Handset. Dieses Leistungsmerkmal erfordert M-210/310-Handteile mit der Firmware PCS17J oder neuer. Um eine Rückwärtskompatibilität zu gewährleisten, ist die alte Schnittstelle weiterhin vorhanden.

### Korrekturen

- Wenn der SIP Servicetyp in der SIP-Konfiguration geändert wurde machte die Basisstation einen Neustart. Nun wird die Änderung ohne Neustart übernommen.

### Bekannte Einschränkungen

- Der IP-DECT-Server ist nicht mehr kompatibel zu Asterisk-Versionen vor 1.2.

## Version: 17B (Q2 2017)

### Hinzugefügte oder geänderte Leistungsmerkmale

- Zusätzlich zur Authentifikation mit vertrauenswürdigem Server und Benutzername/Passwort unterstützt der IP-DECT-Server nun auch Telefonnummer/PIN für die Anmeldung in Skype for Business-Umgebungen, wenn dies auf dem Frontend-Server aktiviert ist und die CertProvURL-Option vom DHCP-Server angeboten wird.
- Die TLS-DSK SIP-Authentifizierungsmethode wurde hinzugefügt für den Gebrauch bei Skype for Business-Servern.
- Ein neuer Benutzerverwaltungsmodus wurde als Alternative zu „vertrauenswürdiger Server“ für Skype für Business-Installationen hinzugefügt.
- Support für Skype for Business E911 wurde hinzugefügt.
- Der IP-DECT-Server und die Handteile benutzen nun einen speziellen Klingelton und Displayanzeige bei einem Gespräch über Skype for Business private line. Dies erfordert im Handteil die Firmware PCS17H oder neuer.
- Support für SIP dialog recovery bei Skype for Business wurde hinzugefügt.
- Der IP-DECT-Server unterstützt nun IPv6 in Skype for Business-Umgebungen komplett, sowohl für SIP- als auch für RTP-Übertragung.
- Der IP-DECT-Server hält nun ein persistentes Protokoll der Systemereignisse:
    - User login/logout
    - Systemneustart
    - Konfigurationsänderungen
    - Nutzeränderungen

  Dieses Protokoll kann nur durch das Zurücksetzen in den Auslieferzustand gelöscht werden.
- Die Sicherheit des Web-UI vom IP-DECT-Server wurde deutlich verbessert.
    - HTTP Digest Authentifizierung wurde ersetzt durch eine Lösung mit Profilen und Cookies, die das Speichern der zufälligen Passwörter nicht erlaubt.
    - Der IP-DECT-Server kann so konfiguriert werden, dass bestimmte Regeln eingehalten werden müssen, wenn das Passwort geändert wird. Die folgenden Regeln müssen dann beachtet werden:
        - Minimale Länge: 8 Zeichen
        - Es müssen mindestens zwei der folgenden Zeichenklassen enthalten sein: Großbuchstabe, Kleinbuchstabe, Nummern und Sonderzeichen
        - Keine einfachen Wörter wie im Wörterbuch
        - Ungleich den letzten drei Passworten
        - Darf nicht mehr als zwei gleiche, aufeinander folgende Zeichen enthalten

      Wenn die strikten Passwort-Anforderungen aktiviert sind, kann dies nur durch das Zurücksetzen in den Auslieferzustand gelöscht werden.

  - Nach 20 Minuten Leerlauf wird der Anwender automatisch ausgeloggt.
  - Es kann konfiguriert werden, dass das Passwort nach 30 oder 90 Tagen die Gültigkeit verliert. Bitte beachten: Dies kann nur durch das Zurücksetzen in den Auslieferzustand gelöscht werden.
  - Nach fünf erfolglosen Login-Versuchen ist das Web-UI des IP-DECT-Servers für fünf Minuten verriegelt.
  - HTTPS wird standardmäßig forciert. HTTP kann im Menü Configuration/Security aktiviert werden (WARNUNG: Das Aktivieren von HTTP führt dazu, dass Passwörter und andere sensitive Daten im Klartext über das Netzwerk transportiert werden.)

  Bitte beachten: Ein Downgrade auf eine Firmware vor PCS17Ba setzt das Passwort auf den Defaultwert zurück.

- Die RFPI-Scanner-Funktionalität, die es in früheren Firmware-Versionen gab, wurde auf die aktuelle Version portiert.
- Die Handhabung der Kommunikation mit Basestations und Media Resources wurde umgearbeitet um robuster zu arbeiten; speziell in Netzwerken mit Fehlern und in Situationen mit ausfallenden Geräten.
- Wenn ein Handteil für ein Update vorgesehen ist, das außerhalb der Reichweite ist, wird nur einmal protokolliert, dass es nicht erreichbar ist. Das Protokoll wird nicht mit diesen Meldungen aufgefüllt.
- Eine SIP TCP Verbindung gilt nun als tot, wenn ein Rückmeldungspaket nicht innerhalb von 10 Sekunden nach der Sendung empfangen wird. Hierdurch wird eine schnellere Ausfallsicherung erreicht in Situationen, in denen der Server nicht antwortet.
- Der Linux-Kernel wurde upgedated auf Version 4.4.52.
- Update des Standard-CA-Pakets. Dies erneuert die Liste der Certificate Authorities, die dem DECT-Server bekannt sind. Dadurch werden dem Server neue Zertifikate zugänglich und unsichere wurden entfernt.

**Entfernte Leistungsmerkmale**

- Keine

**Korrekturen**

- Die Liste der Geräte- und Host-Zertifikate wird nicht mehr sortiert. Dies erlaubt die Darstellung in der korrekten Reihenfolge.
- Parsing von SIP-Nachrichten, die verschachtelte Multipart-Bodies enthalten, wird nun unterstützt. Dies repariert ein Problem bei Skype for Business Gruppenrufen.
- Wenn ein SIP-Request nochmal gesendet wird und ein anderer Request für den selben User gesendet wird, enthielt der Request eine falsche Sequenznummer.
- Bei der Nutzung von SRV-Datensätzen wurde nur ein Datensatz mit der vorgegebenen Priorität genutzt, auch wenn mehrere verfügbar waren. Nun versucht der Server alle Sätze mit der vorgegebenen Priorität.
- Der Timeout bei der Abfrage von Systemdaten beim Export von Logs wurde erhöht, damit dies auch bei ausgelasteten System funktioniert. Dies beseitigt ein Problem mit fehlenden Daten in Exportlogs.
- Die bisherige Größenbegrenzung auf vier Kilobyte bei importierten Zertifikatsdateien wurde entfernt.
- Wenn der Anwender keinen Displaynamen gesetzt hat, wird nicht länger ein leeres Displaynamenfeld im SIP-Header hinzugefügt.

**Geänderte Konfigurationsparameter**

| Datei | Aktion | Parameter | Beschreibung |
|---|---|---|---|
| config.xml | Hinzugefügt | dect.handset_sharing | Bedienung, wenn gemeinsame Nutzung des Handteils aktiviert ist (Lizenz erforderlich)<br>Werte: true / false<br>Defaultwert: false |
| config.xml | Hinzugefügt | dect.handset_login | Bedienung, wenn gemeinsame Nutzung des Handteils aktiviert ist (Lizenz erforderlich)<br>Werte: true / false<br>Defaultwert: false |
| config.xml | Hinzugefügt | security.strict_password | Bedienung, wenn strikte Regeln für die Passwordqualität aktiviert sind<br>Werte: true / false<br>Defaultwert: false<br>Anmerkung: Kann nur mit Auslieferzustand deaktiviert werden. |
| config,xml | Hinzugefügt | security.password_lifetime | Setzt wie viele Tage das Passwort der Weboberfläche gültig ist.<br>Werte: 0 (forever), 30, 90<br>Defaultwert: 0<br>Anmerkung: Kann nur mit Auslieferzustand deaktiviert werden. |
| Config.xml | Hinzugefügt | security.allow_http | Kontrolliert, ob unverschlüsselte HTTP Requests an das Web-UI zulässig sind.<br>Werte: true / false<br>Defaultwert: false |

## Version: 17A (Q1 2017)

**Änderungen** :

- Der Linux-Kernel bekam ein Update auf Version 4.4.32
- Update der Standard-Zertifikate. Die Liste der Certificate Authorities, die dem IP-DECT-Server bekannt sind, erhielt ein Update. Dies soll sicherstellen, dass neue genutzt werden können und unsichere entfernt wurden.
- Die Produkt-IDs aller angeschlossenen Basisstationen werden nun in den exportierten Logdateien mit aufgenommen.
- Der interne Gesprächskontrollstatus ist nun textlich in den Einträgen für unnormale Gesprächsabbrüche repräsentiert.
- Die IP-DECT-Server unterstützen jetzt Handteilanmeldung mit Platzhaltern. Dies erlaubt die Anmeldung von Handteilen direkt „out oft he box“ ohne vorher den Server konfigurieren oder User anlegen zu müssen, obwohl die Handteile dann noch nicht in der Lage sind, Gespräche zu führen. Dies kann hilfreich sein in manchen Ausrollszenarien oder bei der Fehlersuche.
- Die Paketfehler- oder –verluststatistik zeigt nun auch die Gesamtzahl der Pakete zusätzlich zu dem Prozentwert der verlorenen/fehlerhaften Pakete.

**Entfernte Leistungsmerkmale**

- Keine

**Korrekturen**

- Es wurde ein Problem behoben, das PKCS12-formatierte Zertifikatketten am Import hinderte, die ein Zwischenzertifikat enthalten.

- Handhabung von Wettlaufsituationen in bestimmten Vermittlungsszenarien, die zu einem Absturz in der Hauptserverkomponente führen konnten, was eine Beendung aller aktiven Gespräche bewirkte (Fehler: DECTESC-739).
- Ignorieren von DECT CC-Infonachrichten nur wenn sie nicht beachtete proprietäre Elemente enthielten, was zum Abbruch von Gesprächen kurz nach dem Setup führte (Fehler: DECTESC-744).
- Bei der Bandbreitenzuteilung für Lync/Skype for Business misslang die Zuteilung, wenn entweder die RTP- oder die RTCP-Zuteilung misslang. Vorher war ein Anruf möglich auch wenn nur RTCP-Bandbreite verfügbar war.
- Bei der Bandbreitenzuteilung für Lync/Skype for Business für TCP Media Verbindungen benutzt der Server den reflexive candidate des entfernten Endpunktes wenn kein host candidate verfügbar ist.

**Änderungen von Konfigurationsdateiparametern**

- Keine

## Version: 16F_ (Q4 2016)

**Änderungen** :

- Der Linux-Kernel bekam ein Update auf Version 4.4.18
- Update der Standard-Zertifikate. Die Liste der Certificate Authorities, die dem IP-DECT-Server bekannt sind, erhielt ein Update. Dies soll sicherstellen, dass neue genutzt werden können und unsichere entfernt wurden.
- Der UDP-Port-Bereich, der für den RTP-Verkehr zwischen den Basisstationen und den Media Ressources genutzt wird, kann nun konfiguriert werden.
- Die TOS/DiffServ-Werte können für PTP-Pakete konfiguriert werden, die für LAN-Sync genutzt werden.
- Die rfps.xml-Datei enthält nun die volle Nachbarschaftstabelle mit RSSI und Versatzwerten für jede Basisstation innerhalb der Reichweite.
- Etliche LAN-Sync Diagnostikwerte sind in der rfps.xml hinzugefügt worden:
  - delay_min: Die minimale Verzögerung in ns zwischen dem Master und dem Slave über das letzte 1-Minuten-Intervall.
  - delay_max: Die maximale Verzögerung in ns zwischen dem Master und dem Slave über das letzte 1-Minuten-Intervall.
  - delay_avg: Die durchschnittliche Verzögerung in ns zwischen dem Master und dem Slave über das letzte 1-Minuten-Intervall.
  - delay_dev: Die Standardabweichung in ns der Verzögerung zwischen Master und Slave über das letzte 1-Minuten-Intervall.
  - longterm_delay_dev_max: Die maximale Standardabweichung in ns der Verzögerung zwischen Master und Slave seit Start.
  - lucky_rate: Das Verhältnis der Pakete nutzbar für den Sync-Algorithmus während des letzten 1-Minuten-Intervalls.
  - longterm_delay_min: Die minimale Verzögerung in ns zwischen Master und Slave seit Start.
  - longterm_delay_max: Die maximale Verzögerung in ns zwischen Master und Slave seit Start.
  - longterm_delay_avg: Die durchschnittliche Verzögerung in ns zwischen Master und Slave seit Start.
  - longterm_delay_dev: Die Standardverzögerung in ns zwischen Master und Slave seit Start.
  - longterm_lucky_rate: Das Verhältnis der Pakete nutzbar für den Sync-Algorithmus seit Start.
  - rate_correction: Die angewandte Frequenzkorrektur in Teile pro Million.
  - rate_dev: Die Standardabweichung der Frequenzkorrektur in Teile pro Million.
  - offset_dev: The Standardabweichung des geschätzten Versatzes zum LAN Sync Master in ns.
- Der LAN-Sync-Regulierungsalgorithmus wurde eingestellt um in Netzwerkumgebungen mit Jitter besser zu funktionieren.

- Wenn der LAN-Sync sein Synchronisierung mit dem Master verloren hat, erfolgt kein Reset mehr, solange die Basisstation aktive Sessions hat, sondern verzögt dies bis zum Leerlaufbetrieb. Während die Basisstation keine Synchronisierung hat, werden neue Verbindungen abgewiesen bis der LAN-Sync wieder steht oder die Basisstation zurückgesetzt ist.

**Entfernte Leistungsmerkmale**

- Keine

**Korrekturen**

- Es wurde ein Problem in der Lync/Skype for Business-Umgebung beseitigt, bei dem RTP und RTCP unterschiedliche Netzwerkpfade gewählt haben zum entfernten Endpunkt.
- Das Zeichen für den ersten ulaw-Codepoint war falsch.
- Es wurde ein Problem beseitigt, bei dem ein hängende Systemkomponente verhinderte, dass ein SysLog fertig exportiert wurde.
- Vermeidung einer Wettlaufsituation zwischen dem Beenden einer Media-Einrichtung und dem Erhalt einer Re-invite-Nachricht mit einem Replace-Header, was zu einem Gesprächsabbruch führte.
- Es wurde ein Problem beseitigt, das dazu führte, dass das User Interface abstürzte, wenn eine Paketerfassung gestartet wurde, bei der nur entschlüsseltes SIPS gewählt war.
- Lync/Skype for Business Anwendernamen können nun das Zeichen „&“ enthalten.
- Die Schleifenerkennung der Basisstationen geht nun davon aus, dass Basisstationen in unterschiedlichen Clustern keine Schleifen bilden können.

**Änderungen von Konfigurationsdateiparametern**

- Keine

## Version: 16E_

Dies war eine nicht veröffentlichte Version, die keine für Anwender relevante Änderungen enthielt.

## Version: 16D_ (Q3 2016)

**Änderungen** :

- Der Linux-Kernel erhielt ein Update auf Version 4.4.11
- Update der Standard-Zertifikate. Die Liste der Certificate Authorities, die dem IP-DECT-Server bekannt sind, erhielt ein Update. Dies soll sicherstellen, dass neue genutzt werden können und unsichere entfernt wurden.

**Entfernte Leistungsmerkmale**

- Keine

**Korrekturen**

- Es wurde ein Problem beseitigt bei Lync/Skype for Business-Umgebungen mit dem installierten, letzten kumulativen Update und Bandbreitenkontrolle aktiviert, bei dem abgehende Gespräche in einigen Situationen einseitiges Audio hatten.
- Es wurde ein Problem beseitigt, das dazu führen konnte, dass Early Media ignoriert wurde, wenn es in vermittelten Gesprächen enthalten war.

**Änderungen von Konfigurationsdateiparametern**

- Keine

## Version: 16C_ (Mai 2016)

**Änderungen** :

- Keine

**Entfernte Leistungsmerkmale**

- Keine

**Korrekturen**

- Verbesserte Auswahl der Kanäle für den Dummy Bearer in DECT 6.0-Systemen.

## Version: 16B_ (Q2 2016)

**Änderungen** :

- Keine

**Entfernte Leistungsmerkmale**

- Keine

**Korrekturen**

- Verbesserte Erkennung von anderen Systemen und eigenen Basen; dadurch Verbesserung der Fähigkeit der Handteile bei Handover-Situationen die Basisstation zu finden.

## Version: 16A (Q2 2016)

**Änderungen** :

- Lync Quality of Experience (QoE) reporting. Dieses Leistungsmerkmal ermöglicht erweiterte Überwachung und Auswertung einer großen Anzahl an Merkmalen und Informationen über die Medienqualität, Gerätetypen, Teilnehmer usw., die an den Gesprächen beteiligt sind.
- Die Funktion endpoint_partial_clear wurde beim XML-RPC-Schnittstelle hinzugefügt. Diese Funktion wird genutzt, um Nachrichten und Anruflisten in den Handteilen zu löschen.
- Die Artikelnummern der Handteile aus der PP7-Generation werden jetzt im User Interface erkannt.
- Lync DNS basierende selbsttätige Auffinden des Frontend-Servers/-Pools. Dies änderte die DNS-Prozeduren um mehr wie Microsoft-Client zu erscheinen und eine einfachere Integration in eine Lynx-Umgebung zu erlauben.
- Streaming von Packet Capture und Log-Download. Dies erlaubt die Erfassung von Paketen und Systemlogs über längere Perioden indem dies nicht mehr auf dem Server gespeichert wird sondern direkt in den Browser geladen wird.
- Die normale Maximallänge von MSF-Nachrichten wurde erhöht von 72 auf 180 Zeichen und die normale maximale Länge der Rückrufnummer wurde erhöht von 24 auf 64 Zeichen. Die alten Maximallängen werden benutzt, wenn die Einstellung allow_long_messages auf Falsch gesetzt wird.
- Das alte KWS600v3 MSF-Protokoll ist nun per Default deaktiviert. Es kann auf der Konfigurationsseite des Wireless Servers aktiviert werden.
- Wenn Lync aktiviert ist, wird ein Accept Language Header hinzugefügt bei abgehenden INVITE-Nachrichten.
- Die Zeitintervalle für die SIP-Registrierung- und -Reregistrierung enthalten nun einen zufälligen Anteil, der helfen soll, die Last auf den Server beim Neustart zu verringern.

**Entfernte Leistungsmerkmale**

- Keine

**Korrekturen**

- Es wurde ein Problem mit einseitigem Audio bei bestimmten PSTN-Gateways beseitigt in Lync/Skype for Business-Umgebungen.
- Es wurde ein Problem bei LAN-Sync beseitigt, wenn UDP zum Transport benutzt wurde.
- Der Einstellparameter des LAN-Sync-Algorithmus wurden angepasst, um eine größere Auswahl an Switches zu unterstützen.
- Es wurde Blockaden beim Aufbau einer TLS-Verbindung beseitigt.
- Es wurde der Buffer-Overflow beim Erhalt von großen DNS-Resultaten beseitigt.

- Es wurde ein Memoryleak beseitigt, wenn ein SIP redirect loop entdeckt wird.
- Es wurde ein Memoryleak beseitigt, wenn der Zähler für SNMP ipDectAbnormalReleaseTotal abgefragt wird.
- Es wurde keine neue Cisco CallManager SEP Nummer erzeugt, wenn der Anwendername geändert wurde.

**Änderungen von Konfigurationsdateiparametern**

- Keine

**Bekannte Punkte**

- Nach dem Upgrade auf Version PCS16A_ ist es nicht mehr möglich auf PCS15__ oder früher zurückzugehen. Als provisorische Lösung kann man zunächst auf Version PCS16__ gehen und dann auf die gewünschte Version.

## Version: 16 (Q1 2016)

**Änderungen** :

- Der IP-DECT-Server ist nun in der Lage, Gespräche in eine überbrückte Ad-hoc-Konferenz am Cisco Unified Communications Manager zu verbinden.
  Das Leistungsmerkmal ist vorhanden, wenn zwei Gespräche am Handteil aktiv sind und mit „Konferenz beitreten“ aus dem Menü Gesprächsoptionen aufgerufen wurden. Wenn die Konferenz dann besteht, können zusätzliche Teilnehmer hinzugefügt werden durch das Hinzufügen und Einbinden weiterer Gespräche in die Konferenz.
  Ad-hoc-Konferenzen benötigen die neueste Handteilplattform und werden derzeit nur vom M-210 unterstützt. Das M-100 und M-200 werden nicht unterstützt. Zusätzlich wird die Lizenz “Cisco Unified CM Enhanced features” benötigt.
- Automatisches Lync Presence Bootstrapping wird nun unterstützt.
  Lync erfordert Bootstrapping der Anwesenheit eines Benutzers, damit ein Gerät in der Lage ist, die Anwesenheit zu veröffentlichen. In früheren Versionen der Firmware wurde automatisches Bootstrapping nicht unterstützt und der Administrator musste Power Shell-Befehle erstellen oder sich bei einem Lync-Client anmelden, um Präsenzstatus zu ermöglichen. Ab dieser Version der IP-DECT-Server wird automatisch Bootstrapping ausführen und es sind keine manuellen Schritte notwendig, um Präsenz zu aktivieren.
- Das Firmentelefonbuch unterstützt nun LDAPS für sichere Kommunikation mit einem Firmenverzeichnis. Dies kann genutzt werden indem eine ldaps:// URL in der Konfiguration des Telefonbuchs angelegt wird.
- Der IP-DECT-Server unterstützt jetzt die internen/externen Klingelmelodien auf Cisco Unified Communications Manager. CUCM unterstützt mit speziellen Alarm-Info-Header, um anzuzeigen, ob ein Anruf intern oder extern ist. Diese Header werden jetzt analysiert und von dem IP-DECT-Server erkannt. Die Handteile haben zwei Varianten der einzelnen Klingelmelodien, die es ermöglichen zu hören, ob ein Anruf intern oder extern ist. Das Symbol für einen eingehenden Anruf zeigt, ob der Anruf intern oder extern ist.
- Die DECT Dummy Bearer –Handhabung in den Basisstationen ist verbessert worden.
  Die Übertragung ist jetzt schneller, um den günstigsten DECT-Kanal für die Dummy Bearer zu finden, wenn der Dummyträger bewegt wird. Dies verringert die Chance, dass das Handteil oder die Basisstationen das Signal zu verlieren, das die Dummy-Bearer für die Synchronisation verwenden.

- Für LAN-basierte Synchronisation ist es erforderlich, dass die Verzögerung in beide Richtungen niedrig ist, bevor die Pakete für die Synchronisation genutzt werden. Anderenfalls könnte das System am Ende in einer Schleife mit zunehmendem Bitversatz, die nicht korrigiert werden kann. Damit befasst sich DECTEC-639 und verbessert die Stabilität der LAN-basierte Synchronisation.
- Startet den NTP-Sync-Algorithmus, wenn nicht synchron nach 2000 Sync-Zyklen. Damit befasst sich DECTEC-639 und verbessert die Stabilität der LAN-basierte Synchronisation.
- Lässt die Übertragung von frühen RTP durch den Peer ICE-Status kontrollieren und nicht durch den Session-ICE-Status.
  Dies sorgt dafür, dass die Medienressource frühe RTP für abgehende Anrufe auf nicht-ICE peers übertragen werden, auch wenn die globale ICE-Einstellung aktiviert ist. Dies ist erforderlich, um einen Durchlass zu öffnen, damit frühe Nachrichten durch eine NAT / Firewall empfangen werden können.
- Hält die Übertragung der Basisstation aktiv für etwa drei Minuten, wenn die Verbindung zum IP-DECT-Server(n) verloren geht.
  Dies erhöht die Verfügbarkeit der Anlage, weil kleinere Verbindungsunterbrechungen und Server-Neustarts nicht die Synchronisation abreißen lassen und die Mobilteile ihr DECT-Signal nicht verlieren.
- Der Umgang mit der SUBSCRIBE NOTIFY-Signalisierung bei der Verbindung mit einem Microsoft Lync Server wurde verbessert.
  Die IP-DECT-Server erlauben nun, dass Lync das erste NOTIFY mit dem 200 OK für SUBSCRIBE mitschickt.
  Darüber hinaus wird nun die BENOTIFY-Anforderung unterstützt. BENOTIFY ist best-effort NOTIFY – also ein NOTIFY, das ohne eine Transaktion gesendet wird und keine Antwort erforderlich macht.
  Beides verbessert die Skalierbarkeit, weil es Menge der notwendigen Signalisierungen reduziert.
- Die Handhabung von SIP-Registrierungen wurde verbessert, wenn mit Microsoft Lync verbunden. Der IP-DECT-Server unterstützt jetzt Lync keep alive-Signalisierung. Wenn SIP-Registrierungen vom IP-DECT-Server gesendet werden, signalisiert er, dass er Lync keep alive unterstützt und extrahiert das Keep alive-Timout aus dem Register und sendet Keep alive-Signale in der Abfolge, die Lync spezifiziert hat.
- Änderung der SIP-Signalisierung im Zusammenwirken mit dem Cisco Unified Communications Manager (um ähnlicher wie die Cisco SIP-Telefone zu agieren).
- Das DECT-Produktportfolio benutzt nun eine neue Bibliothek für sichere Kommunikation über TLS. Neben anderen Dingen bedeutet dies, dass nun Zertifikate mit sha384 und ecdsa Signaturen unterstützt werden.
- Update der CA-Pakete. Dieses Update der Liste der Certificate Authorities stellt sicher, dass das System die neuen Zertifikate kennt und alte entfernt werden.
- Etliche Open Source-Pakete, die in der Firmware verwendet werden, sind upgedated worden, um durch die Fortentwicklung Verbesserungen und Sicherheitsfixes zu erhalten.
- Der Linux-Kernel wurde upgedated von Version 3.16.2 auf Version 4.2.3
- Das RTP- und STUN/TURN/ICE-Handling wurde restrukturiert, um es zu korrigieren und leichter zu pflegen.
  Das Handling hatte ein paar Probleme, die zu Abstürzen in speziellen Situationen führen konnten. Diese Probleme sind mit der Restrukturierung beseitigt.
- Die Benutzung des SIP Warning Header in Protokolleinträgen bei Übertragungsfehlern schlug fehl. Der Cisco Unified Communications Manager kopiert zusätzliche Informationen in den Warning Header. Diese Informationen warden nun den Protokolleinträgen beigefügt, um Debugging einfacher zu machen.
- Die Freischaltung von Kanälen bei Media Resources wurde verbessert.
  Dieses eliminiert den kritischen Fehlereintrag „Received session new for unused ResourceId=1” der auftreten kann, wen nein Gespräch beendet wird, während es aufgebaut wird. Daneben

wurden die Fehlereinträge herabgestuft von „Kritisch“ zu „Fehler“, weil sie das allgemeine System nicht beeinträchtigen.

- Es wurde die Art verbessert, in der Base Stations Einstellungen in redundanten Setups vom IP-DECT-Server erhalten.
  Vorher wurden zum Beispiel geänderte Funksynchronisations-Einstellungen von den Base Stations empfangen, aber in einigen Situationen nicht korrekt aktiviert und ein Neustart der Base Station war notwendig, um das zu beheben.
- Es wurde eine SRTP SDP Verschlüsselung ohne MKI hinzugefügt, wenn MKI aktiviert und das lokale MKI aus der Ferne upgedated worden ist.
  Dies soll die Fähigkeit verbessern, die SRTP-Verschlüsselung mit verschiedenen SIP Endgeräten zu verbessern.
  Es gibt zwei Formate: Ein Binärformat wird zum Download im Spectralink Support Portal zur Verfügung stehen und ein anderes Format wird während des Fertigungsprozesses benutzt.

**Korrekturen**

- Provisioning wird nur von den IP-DECT-Servern unterstützt; es gibt keinen Support durch die Media Resources und die Base Stations. Vorher wurde dies nicht korrekt umgesetzt und eine Base Station konnte in einigen Fällen versuchen, eine Provisionierung zu starten, was zu Problemen führen konnte. Dieses Problem wurde berichtet in DECTESC-633 und ist nun korrigiert.
- Setzen des aktuellen Teilnehmers beim Komplettieren des ICE. Dies beseitigt einseitige Audioprobleme in einigen Call Forking-Szenarien.
- Fehler beseitigt bei Vermitteln mit Ankündigung zu nicht erreichbaren oder besetzten Nicht-NG-Handteilen.
  Wenn ein Vermitteln mit Ankündigung versucht wurde mit einem Nicht-NG-Handteil und das Vermittlungsziel war nicht erreichbar oder besetzt, war es nicht möglich, zum Ursprungsgespräch zurückzukehren oder einen neuen Vermittlungsversuch zu starten. Dies wurde berichtet in DECTESC-643
- Es wurden keine TURN Refresh Anforderungen geschickt bei gekapselten Anzeigewerten
  Die TURN-Verbindung wurde nicht korrekt unterstützt, wenn TURN in nicht-Lync-Umgebungen genutzt wurde.
- Es konnte kein IPv4 TURN relay benutzt werden bei IPv6.
- Es wurde ein Absturz beseitigt wenn MWI oder Präsenzdaten gelöscht wurden, während Auslieferung an das Handteil anstand.
- Es wird nun ein Absturz vermieden, wenn ein außenliegender Teilnehmer eine erwartete ICE-Komponente vermisst.

**Änderungen von Konfigurationsdateiparametern**

Keine