



RELEASE NOTES

Ascom IP-DECT v13.1.10



GENERAL

Software name: IP-DECT (IPBL, IPBS1, IPBS2, IPBS3, IPVM)
Software version: 13.1.10
Release date: 2026-03-13

Downgrade/Upgrade concerns

From version 9.1.X and later the IPBS1 only has radio functionality

Background:

Due to lack of available flash space for new firmware/boot on IPBS1, we need to remove reserved space for persistent data in order to make more space available.

Solution:

This means that the central software components are no longer supported on IPBS1. The IPBS1 is now only able to host the DECT Radio component. All IPBS1 in a system using any other functionality than DECT Radio component (i.e. Master, Mobility Master, Crypto Master, Kerberos server, Central Phonebook, Gateway) need to be replaced/swapped by IPBS2/IPBS3/IPVM/IPBL1 before upgrade.

If central software components are enabled for an IPBS1 there is a risk that there already are too little space in the flash to be able to upload the firmware. In that case a factory reset is needed to resolve the issue.

G.723 and G.729 are phased out

G.723 and G.729 codecs is no longer supported by the IP-DECT system.

SNMP is disabled by default

The SNMP service is disabled by default. To enable use the enable option on Services->SNMP page. Note that after upgrade of an existing system, the SNMP functionality will be disabled and needs to be enabled again for each device. For large systems, support can assist with tools to do this as a bulk change.

Upgrading from version 8.X.X

ICE enabled

Background:

After upgrade to 10.0.X, ICE functionality is enabled.

Solution:

The option to disable ICE has moved from the VoIP page to the DECT->System page. If ICE was disabled, then it must be manually disabled again on DECT->System page after an upgrade.

Upgrading from version 7.X.X

SMS encryption enabled by default

Background:

After the upgrade, SMS Encryption will be enabled by default.

Solution:

If SMS encryption is not wanted, it needs to be disabled both in Unite (see Unite documentation) and in the IPBS (see Installation and Operation manual).

Downgrading to 10.0.X (or earlier)

Device Not Reachable

Background:

If IPv6 has been used in the configuration the device becomes unreachable (or stuck in boot loop) after downgrade to a version that does not support IPv6.

Solution:

Restore old configuration before downgrade.

Limitations

- IPDECT-3111: Incorrect IP address with the ASCOM-IPDECT-MIB when listing events or alarms reported from a device using IPv6. The MIB currently uses the IpAddress syntax from SNMPv2-SMI which only supports IPv4. As a result, only the least significant 4 bytes of the IPv6 address will be displayed as an IPv4 address.

Recommended browsers

- Firefox
- Chrome
- Edge

Supported VMware ESXi versions for IPVM

- 8.0
- 7.0
- 6.7
- 6.5

Release Notes IPDECT - Version 13.1.4 to 13.1.10

NCR

Teams: Handset parameter sync fails

JIRA: IPDECT-6571

NCR/CR: CIT-54882

Affects system/s: Teams

Background:

When connected to Teams SIP Device Gateway the handset parameters are set depending on signed-in/out state. This sync of the parameters is failing. I.e. the menus/soft-keys in the handset is not updated with the sign-in and sign-out options.

Solution:

Corrected a problem when handling the IP-DECT config that caused this behavior.

PCAP to WebDAV logging will eventually get wrong timestamp

JIRA: IPDECT-6534

NCR/CR: CSE-37777

Background:

When tracing to pcap file using webdav, the pcap file will eventually get faulty timestamps.

Solution:

The timestamp was based on a counter that wraps around after about 6.2 days after power-on. Because of this the pcap timestamp could suddenly jump back the same amount of time. When this happened was depending on when the trace was started relative to the power-on time. The behavior repeats with the 6.2 days interval. The wraparound of the counter used for the packet timestamps is now handled.

RFP base station disconnect (Error event 0x000e0001)

JIRA: IPDECT-6479

NCR/CR: CSE-37581

Components: IPBL

Background:

Sometimes RFPs are disconnected from the IPBL for a short while

Solution:

Improved handling of segmented messages for data link layer between IPBL and RFP.

RFPI Collision alarm (0x00140068) after a move operation

JIRA: IPDECT-6474

NCR/CR: CSE-37673

Background:

RFPI Collision 0x00140068 alarms from both the pari-master and standby pari-master when a base station is replaced and a move operation is done to get the old base's RFPI assigned to the new.

Solution:

RFPI Collision events are no longer triggered for move operations.

Trap in SIP_TRANSPORT on SOCKET_RECVFROM_RESULT(0x716)

JIRA: IPDECT-6620

NCR/CR: CIT-54147

Affects system/s: SIP

Background:

When the PBX is trying to initiate an outgoing call from a handset using CTI functionality and this outgoing call fails in some way, e.g. is rejected this could cause a restart on the IPBL platform and potentially cause other problems on other platforms.

Solution:

The restart is fixed and handling of a failed call in this scenario has been improved.

Routing table not properly executed

JIRA: IPDECT-6641

NCR/CR: CFR-18394

Background:

After upgrading from version 11.x to 12.x or later the Gateway routing configuration (Gateway->Routing page) is no longer executed as expected.

Solution:

Routing functionality has been restored.

Handsets not reachable / No Access

JIRA: IPDECT-6597

Background:

Handsets are not reachable in an area where there are lockers with hundreds of handsets stored.

Solution:

Some traffic scenarios (CISS related, e.g. idle display, MWI, multicast group assignment, ...) in combination with roaming, there could be a resource leak in the DECT stack. Eventually all resources will be consumed and no DECT traffic will be possible on the affected device resulting in "No Access" of the handsets. This resource leak has been identified and corrected.

Bug

Login fails using Firefox

JIRA: IPDECT-6532

Background:

When using Firefox (version 142) to login to IP-DECT you are often kicked back to the first login screen again after clicking ok on the welcome screen.

Solution:

The method to advertise the login session cookie lifetime has been changed to a relative value that is also shorter than before, so it shouldn't be rejected by the web browser

Enforced update of PP parameters after a switch off is broken

JIRA: IPDECT-6435

Affects system/s: Teams

Background:

The procedure to enforce a handset parameter update by switch off/on a handset does not work anymore. The checksum is cleared as expected in the database, but a cached value in another module is not, causing the checksum compare to anyway prevent an update. A new Teams onboarding of the device in Teams makes the checksum to change due to unique URLs so this is a workaround if the PP has for some reason got out of parameter sync.

Solution:

The handset parameter reset procedure has been restored. Normally, there should be no need to do this.