



## RELEASE NOTES

Ascom IP-DECT v11.9.11



# GENERAL

Software name: IP-DECT (IPBL, IPBS1, IPBS2, IPBS3, IPVM)  
Software version: 11.9.11  
Release date: 2023-03-31

## 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 is phased out

G.723 codec 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.
- IPDECT-5757: User Administrator role is not possible to create in a Microsoft Teams system. When migrating from an existing system with User Administrator accounts they will not be able to add handsets to the Anonymous list. Additionally these accounts will consume IPDECT-LU licenses.

## Recommended browsers

- Firefox
- Chrome
- Edge

## Supported VMware ESXi versions for IPVM

- 8.0
- 7.0
- 6.7
- 6.5

# Release Notes IPDECT - Version 11.8.10 to 11.9.11

## New Feature

### Microsoft Teams personal sign in

**JIRA:** IPDECT-5610

Background:

Allow for personal sign in / sign out initiated from the DECT handset.

Solution:

Handsets that are onboarded will display a login softkey button which is used to initiate the personal sign in. For more details see "Ascom IP-DECT and Microsoft Teams, Integration Guide".

## NCR

### Master gets into an unrecoverable overload situation

**JIRA:** IPDECT-5654

Background:

The IP-DECT master seems to get into an unrecoverable overload situation when switching active mirror master.

Solution:

The SIP implementation has been updated to better handle high concurrent load that occurs e.g., during a mirror master switch. However even with this improvement the maximum number of supported users on an IPBS2/IPBL1 master has been reduced, see NCR IPDECT-5655.

## **Master memory usage above 85%**

**JIRA:** IPDECT-5655

### Background:

An alarm for high memory usage is triggered even if the number of users is less than the maximum supported limit of 500 users for SIP/TLS.

### Solution:

Due to feature growth and support for more advanced TLS ciphers etc. the maximum number of users on an IP-DECT master have been reduced. This applies to IPBS2 and IPBL1 (IPBS3 and IPVM remain unchanged). New maximum values are:

#### IPBS2:

- SIP/TLS 250 users
- SIP/UDP 500 users
- SIP/TCP 500 users

#### IPBL1:

- SIP/TLS 250 users
- SIP/UDP 1000 users
- SIP/TCP 1000 users

Note: This NCR is dependent on NCR IPDECT-5654

## **Certificate error when using Chrome browser version 107**

**JIRA:** IPDECT-5668

**NCR/CR:** CDACH-35464

### Background:

With version 107 of the Chrome browser it is no longer possible to bypass the privacy error that shown when browsing to a IP-DECT device that is using a self-signed certificate, as chrome reports the certificate as invalid (NET::ERR\_CERT\_INVALID). It is possible to work around this by typing "thisisunsafe" while the privacy error screen is shown.

### Solution:

Chrome has switched from relying on the operating system to validate the certificates to using "Chrome Certificate Verifier" and this is treating IP-DECT certificates as invalid. The root cause of the problem is the use of non-critical flag in the "Authority Key Identifier" and "Subject Key Identifier" extensions. These flags have now been removed from our certificates. Note that new certificates must be generated for each device for this problem to be resolved.

## **Assert in MATP (object deleted)**

**JIRA:** IPDECT-5633

**NCR/CR:** CSE-30053

### Background:

Unexpected master restart

### Solution:

If an interrupt occurred within a very short time window, when tearing down Unite communication instances (e.g., after handset parameter sync), it could lead to an unexpected restart. The tear-down sequence has now been refactored to resolve this problem.

## **Entering wrong IP address for device management makes system go down**

**JIRA:** IPDECT-5625

### Background:

After entering wrong IP address for Unite device management, several other configurations are overwritten.

### Solution:

If Unite device management IP address was configured to another IP-DECT device, this caused that device to push settings to the master. The reason for this is that IP-DECT has its own lightweight device management module used for running in DMS mode (e.g. BroadWorks) which then pushed settings when the master registered. Now internal device management module is only active when there is a DMS URL configured to prevent these consequences of a misconfiguration.

## **Assert in REG\_PRI on timeout/IRQL on SERIAL\_CLOSE (MEM-DELETE inconsistent)**

**JIRA:** IPDECT-5618

**NCR/CR:** CDACH-34757

### Background:

The DNS cache handling in the SIP stack is sometimes affected by a memory inconsistency problem leading to a watchdog restart. This has been seen in large systems with thousands of users when using DNS name for the proxies.

### Solution:

A weakness in the memory management has been solved.

## **Assert in KRB\_LOGIN\_CLIENT on SOCKET\_RECVFROM\_RESULT(0x716) and SOCKET\_BIND\_RESULT(0x703)**

**JIRA:** IPDECT-5724

**NCR/CR:** CSE-30899

### Background:

Unexpected restart when logging in to IP-DECT using Kerberos

### Solution:

Added protection against multiple intersecting login requests

# Improvement

## **Teams: Select language based on handset during onboarding**

**JIRA:** IPDECT-5650

**Affects system/s:** Microsoft Teams

Background:

Control language for texts sent by Teams to handsets, e.g. call forward status.

Solution:

IP-DECT will do the Teams onboarding using the language selected in the handset, as long as it is a language that Teams support, i.e. English, French, German, Spanish or Portuguese. If the selected language in the handset is not supported by Teams it will be onboarded using the default language. Default language is English but can be changed by adding "/lang\_xx" at the end of the DMS URL where xx is the language code. For more details see "Ascom IP-DECT and Microsoft Teams, Integration Guide".

## **Change default value of TLS profile**

**JIRA:** IPDECT-5628

Background:

Change default TLS profile to disable unsecure TLS versions.

Solution:

Default TLS profile is set to "secure" which means that only TLS 1.2 is supported (TLS 1.0 and TLS 1.1 are disabled).

## **IPBL shall only consume as many Teams licenses as there are RFPs connected**

**JIRA:** IPDECT-5556

Background:

Instead of having an IPBL always acquire 16 Teams licenses it shall only acquire as many as there are RFPs connected.

Solution:

Each connected RFP now consumes one IPDECT-LC or IPDECT-LM license

## **Port connectivity test**

**JIRA:** IPDECT-5707

Background:

Add functionality to check if a certain IP address and port is reachable from IP-DECT, e.g., to test if network firewall allows IP-DECT master to establish SIP/TLS connection towards Microsoft Teams.

Solution:

TCP port check utility has been added to Diagnostics->Port Check page.

## **Support CFW status retrieval**

**JIRA:** IPDECT-5581

**Affects system/s:** Teams

### Background:

As Microsoft Teams does not push call forward information to the idle display of the handset there needs to be a way for the user to check the current status.

### Solution:

Teams SIP gateway supports to poll for call forward and do not disturb status. Two menu options in the handset is added to the call services menu to utilize this functionality. By default IP-DECT will configure the right softkey of the handsets to be a shortcut to the call services menu. This shortcut can be overridden from the Unite device manager.

## **Bug**

### **A-party handover before answer + codec change => no audio**

**JIRA:** IPDECT-5727

### Background:

Problem precondition 1. An outgoing call has been initiated from the handset and ring-back signal is played. 2. The handset makes a handover to new Radio 3. The call is answered by the remote party In this state there is a problem if a media-renegotiation is made that changes the codec. The new codec will not be used by the new Radio where the handset is located. There will be no audio in the call.

### Solution:

The problem with a media renegotiation in this state has been solved.

### **SIP/TCP/TLS: Idle persistent transport connections are reconnected repeatedly**

**JIRA:** IPDECT-5689

**Affects system/s:** SIP/TCP/TLS

### Background:

There is a SIP transport maintenance functionality that tries to reestablish persistent TCP and TLS connections to the proxy if the connection goes down. This is done quite rapidly. During some scenarios with failover and fallback the connections are not closed correctly internally, causing the maintenance function to still try to reestablish unused connections. This can cause TCP and TLS connections to be attempted more often than expected to a primary proxy that is down. Also, unused connections to alternative proxies can be reestablished and kept alive while connected to the primary proxy without sending anything over them. This problem is normally invisible to users, and everything still looks to be working fine, but causes additional CPU and network load and can cause performance problems in larger systems.

### Solution:

Unused SIP transport connections are now closed correctly.



## **SIP/DNS: SRV priority and load balancing not working as expected**

**JIRA:** IPDECT-5547

**Affects system/s:** SIP

### Background:

Via DNS SRV records for a domain you can point out several hosts for a specific service like SIP. For each host you can specify its priority and weight to control failover behavior and load balancing between hosts for each priority level. This mechanism has not been working as expected. You could get fail-over between hosts with the same priority level and load balancing was not working.

### Solution:

The load balancing within a priority level and failover between priority levels should now work as expected.

## **Active standby master does not respond to SMSC heartbeat**

**JIRA:** IPDECT-5699

### Background:

When standby master goes active it does not respond to SMSC heartbeat messages which leads to messaging working intermittently.

### Solution:

This breakage was introduced in 11.8.X and has now been corrected.

## **SIP: DNS-SRV certificate validation can fail**

**JIRA:** IPDECT-5693

**Affects system/s:** SIP/TLS w/ DNS SRV

### Background:

When the system is configured using DNS SRV lookup and several hosts serves the domain, the TLS certificate validation might fail if the server certificate only contains the host name.

### Solution:

The SIP server certificate subject/name check should now work as expected also when using DNS-SRV lookup of the server.

## **Messaging over WebSocket does not work for Standby Master**

**JIRA:** IPDECT-5695

### Background:

In an IP-DECT system with master/standby configuration, using WebSocket to connect to Unite, the messaging stops working when the standby master takes over.

### Solution:

The messaging module (SMSRL) now connects to the WebSocket interface once the standby master goes into active state. This problem was introduced in 11.8.X.

## **Not possible to configure alternative Kerberos server**

**JIRA:** IPDECT-5764

### Background:

Not possible to configure alternative Kerberos server. The settings page configuration is cleared after enabling LDAP replication from another Kerberos server.

### Solution:

This problem was introduced in 11.7.X when increasing the supported password max length for the Kerberos server to meet new security requirements. This has been resolved so that it is now possible to configure an alternative Kerberos server.