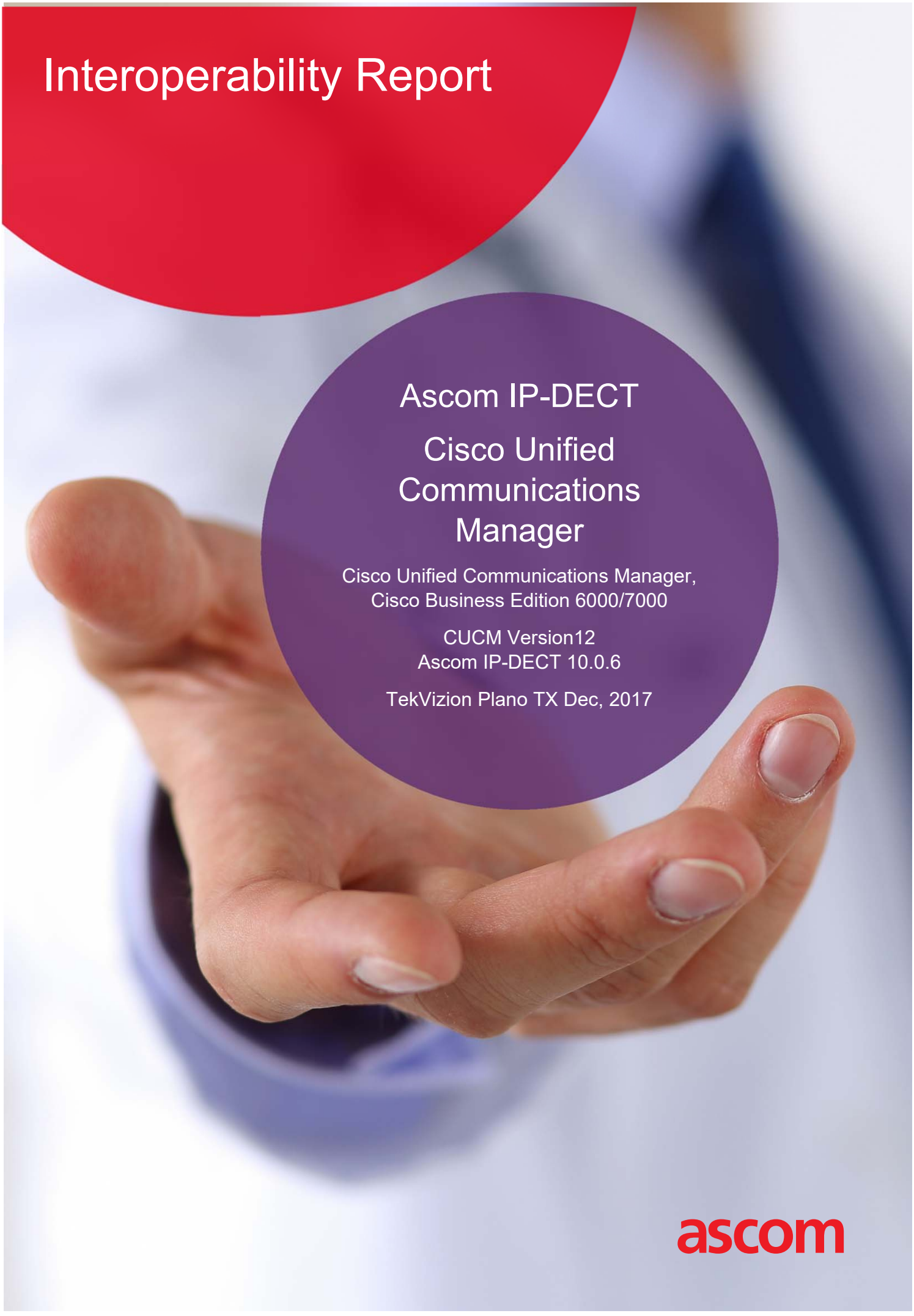
Interoperability Report



Ascom IP-DECT

Cisco Unified Communications Manager

Cisco Unified Communications Manager,
Cisco Business Edition 6000/7000

CUCM Version12
Ascom IP-DECT 10.0.6

TekVizion Plano TX Dec, 2017

ascom

Contents

Introduction **4**

About Ascom 4

About Cisco 4

Site Information **5**

Verification site 5

Participants 5

Verification topology 5

Summary **6**

General conclusions 6

Compatibility information 6

Verification overview 7

Known limitations 8

Appendix A: Verification Configurations **9**

Cisco Unified Communications Manager (CUCM), version 12 configuration 10

Additional Configuration - (VoIP security) 15

Denial-of-Service Protection Flag 15

SIP Station UDP Port Throttle Threshold 15

Call Back 16

International number plan E.164 18

Cisco Licensed Functions 21

SIP Secure (SIPS) and Secure RTP (SRTP) 22

Enable SIPS and SRTP in the CUCM 22

Enable SIPS and SRTP in IP-DECT 23

Music on Hold 23

Ad Hoc Conference 23

Initiate Ad Hoc Conference 23

Meet-Me Conference 24

Call Pickup 25

Call Pickup Other Group 26

Group Call Pickup 26

Directed Call Pickup 28
Call Park 29
Call Forward All 31
Hunt group login/logout 32
Cisco shared line - remote resume 33
Supplementary Services 34
Ascom IP-DECT version 8.0.9 configuration 36
Document History 40

Introduction

This document describes a summary of the interoperability verification results of the Ascom's and Cisco's platforms, necessary steps and guidelines to optimally configure the platforms and support contact details. The report should be used in conjunction with both Cisco's and Ascom's platform configuration guides.

About Ascom

Ascom is a global solutions provider focused on healthcare ICT and mobile workflow solutions. The vision of Ascom is to close digital information gaps allowing for the best possible decisions – anytime and anywhere. Ascom's mission is to provide mission-critical, real-time solutions for highly mobile, ad hoc, and time-sensitive environments. Ascom uses its unique product and solutions portfolio and software architecture capabilities to devise integration and mobilization solutions that provide truly smooth, complete and efficient workflows for healthcare as well as for industry, security and retail sectors.

Ascom is headquartered in Baar (Switzerland), has subsidiaries in 15 countries and employs around 1,300 people worldwide. Ascom registered shares (ASCN) are listed on the SIX Swiss Exchange in Zurich.

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide technology leader that has been making the Internet work since 1984. Our people, products and partners help society securely connect and seize tomorrow's digital opportunity today. Discover more at thenetwork.cisco.com and follow us on Twitter at @Cisco.

.

Site Information

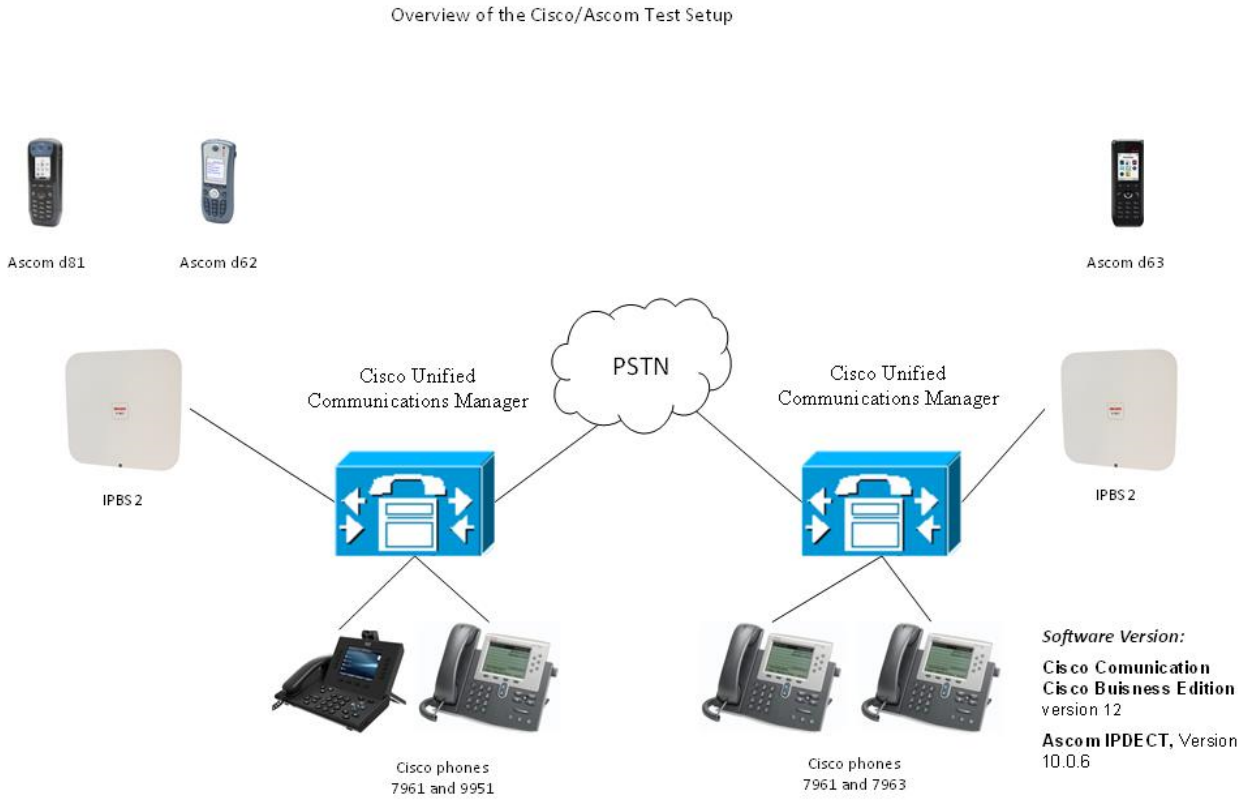
Verification site

TekVizion Labs
Plano, TX
US

Participants

Johan Andrén , Ascom , Gothenburg, Sweden
'Richard Moreno , TekVizion, Plano TX,US

Verification topology



Product	Type	Comment	Number
CUCM	WM on UCS	Publisher and 2 Subscriber nodes	2
Cisco 3845 (PSTN GW)		PSTN gateway	1
Cisco SIP Phones	9971,9951,7975,	Endpoint	1 (each)
Cisco SCCP Phones	7960, 7961, 7961	Endpoint	1 (each)
Ascom IP-DECT base station	IPBS2*	Version 10.0.6	2
Ascom d81 handset	d81	Version 4.5.2	1
Ascom d62 handset	d62	Version 4.5.2	1
Ascom d63 handset	d63	Version 2.1.4	1

*) IPBS2 is fully compatible with IPBS1 and IPBL.

Summary

General conclusions

This test was performed as a CDN IVT (Interoperability Verification Test) at TekVizions lab. Cisco's test plan was used.

Ascom interoperability verification produced in general very good results towards Cisco Unified Communications Manager (CUCM), version 12.0

IP-DECT handsets were configured to register at the CUCM with their endpoint numbers and to provide DTMF signalling through RTP (RFC2833). The codec of choice for these tests was G.711u, with a packet interval of 20ms, while the "Hold Type" was left at its default setting, namely "inactive". Parameter settings are elaborated upon in the "Appendix" section for respective platform later on.

Basic Call, brokering/enquiry, (un)attended transfers, Call Diversion (CDIV) and Message WaitingIndication (MWI) passed. It should be emphasised that Call Waiting (CW), Do-not-Disturb (DND),CDIV and MWI were tested locally with Supplementary Services enabled on the IP-DECT base station (IPBS2).

Compatibility information

Through the certification of Cisco Unified Communications Manager, Cisco and Ascom also grant compatibility with Cisco Business Edition 6000/7000. Features and configurations are identical.

Verification overview

Cisco Unified Communications Manager (CUCM), version 12.0 test result. Queries about Cisco UCM licensing should be directed to Cisco.

Please also see “Appendix A: Test Configurations” for further details.

Unified Communication Services

High Level Functionality	Result	Comments
Basic Call	OK	
DTMF	OK	
Hold, Retrieve, Enquiry and Brokering	OK	
Attended Transfer	OK	
Unattended -transfer	OK	
Call Forward Unconditional	OK*/**	
Call Forward No Reply	OK*/**	
Call Forward Busy	OK*/**	
Call Waiting	OK*	
Message Waiting Indication	OK*	
Do Not Disturb	OK*/**	
Calling Line/Name Identification	OK	
Connected Line/Name Identification	OK	
Call Back Busy Subscriber	OK*	
Call Back No Reply	OK*	
Registration as “Ascom IP-DECT device”	OK***	
Music On Hold	OK***	
Ad Hoc Conference	OK***	
Initialize Meet Me Conference	OK***	
Call Park	OK*/***	
Call Pickup	OK*/***	
Shared Line	OK***	
Native Call Queuing	OK	
SIP-TLS and SRTP	OK***	

*) Supplementary Services enabled in IP-DECT
**) Call Forward and DND configured locally in IP-DECT through supplementary services.
***) Requires additional license in IP-DECT system “License for Additional Cisco functionality”

Known limitations

Description and Consequences	Workaround	Ticket(s) raised
COP file version 10.5v1 is incompatible with CUCM version 12.0.	Make sure that COP file version 11.0v1 is used together with CUCM v12.0	n:a
Support for registration without digest authentication (instance-id) was removed by Cisco from version 7 and above when it comes to third-party SIP devices.	Registration without digest authentication is however possible if the Ascom system is registered as an “Ascom IP-DECT Device” in the CUCM. This option requires an identification file for the CUCM and the additional license “License for Additional Cisco functionality” installed in the IP-DECT system	n:a

For additional information regarding the known limitations please contact **interop@ascom.com** or **support@ascom.com**.

For detailed verification results, refer to document CUCM 12 0 SIPEndPoint Certification-Ascom Dect Test Plan_V1.

Appendix A: Verification Configurations

There are now two ways of adding devices into the Cisco Unified Communications Manager.

1. Device added as “Third-party SIP Device”.

    - This method requires both a “Device” and an “End User” to be created in the CUCM.
    - Digest user has to be enabled. (Support for registration without digest authentication was removed by Cisco from version 7 and above when it comes to third-party SIP devices)

2. Device added as “Ascom IP-DECT Device”

    - Requires only that a “Device” is created in the CUCM.
    - An identification file (.cop)* to be uploaded to all servers in the CUCM cluster to enable the functionality of “Ascom IP-DECT device”
    - Requires a license** key to be entered in the base station

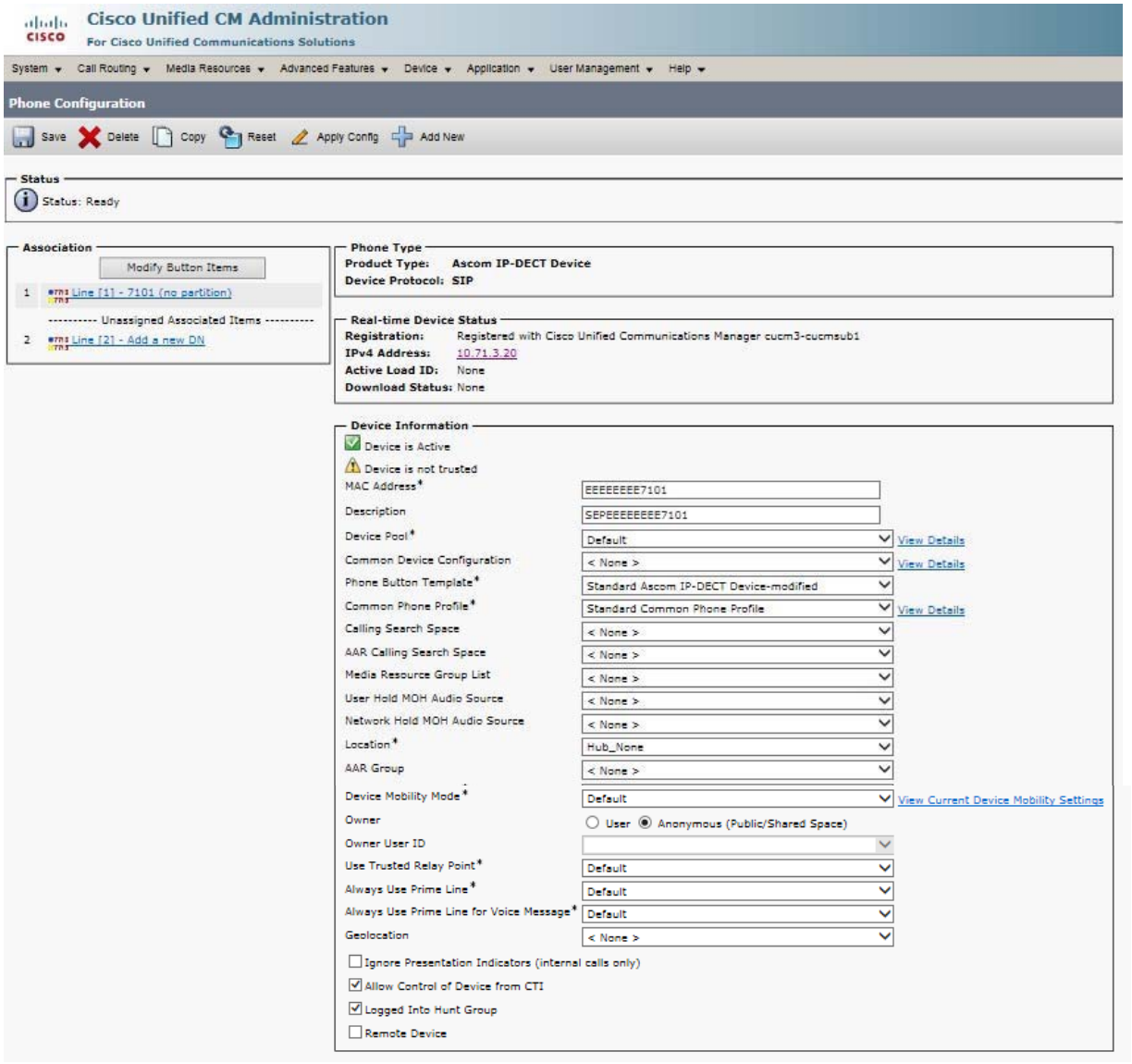
    *) The identification (.cop) file is provided by Ascom.
    **) License is provided through the license web.

    Part numbers:
    IPBS1-L01 (License for Additional Cisco functionality for IPBS1)
    IPBS2-L01 (License for Additional Cisco functionality for IPBS2)
    IPBL1-L01 (License for Additional Cisco functionality for IPBL1)

CUCM endpoint licensing require one ”Enhanced UCL” for every IP-DECT device.

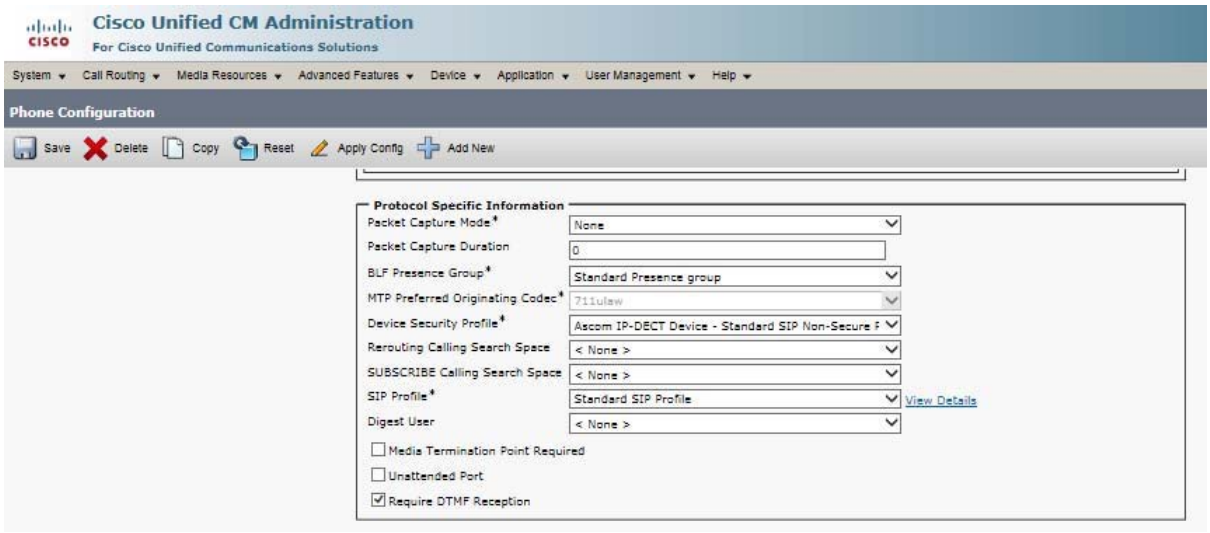
Please refer to Cisco’s documentation for further details about CUCM configuration and licensing.

- Handsets require fictitious MAC addresses
- Caller Line Identities (CLI) require additional configuration
- CUCM license for “Third-party SIP device” implies some limitations, e.g. no Music-on-Hold (MoH) and lack of telephony features configurable from the handset etc.



1. Device->Phone: Adding a device (phone). Part 1.

Note that IP-DECT endpoints require fictitious MAC addresses. For example, if the Directory Number is "7100", the MAC address should be set to "EEEEEEEE7100".

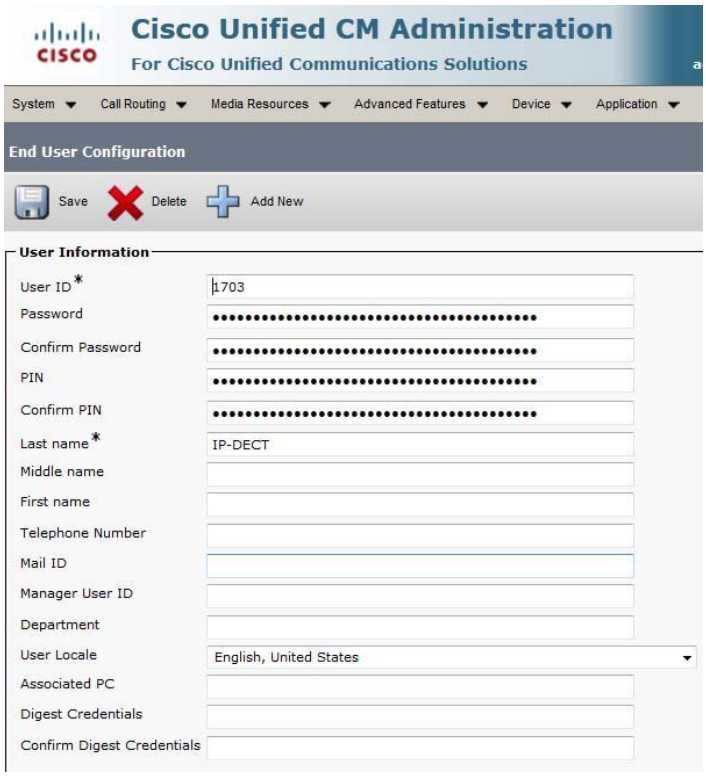


2. Device->Phone: Adding a device (phone). Part 2

Note. In the above mentioned example “Digest User” is set to <None>. If the handsets are added as “Third party SIP devices” instead of “Ascom IP-DECT Device”, the Digest User has to be pointed to an End User.

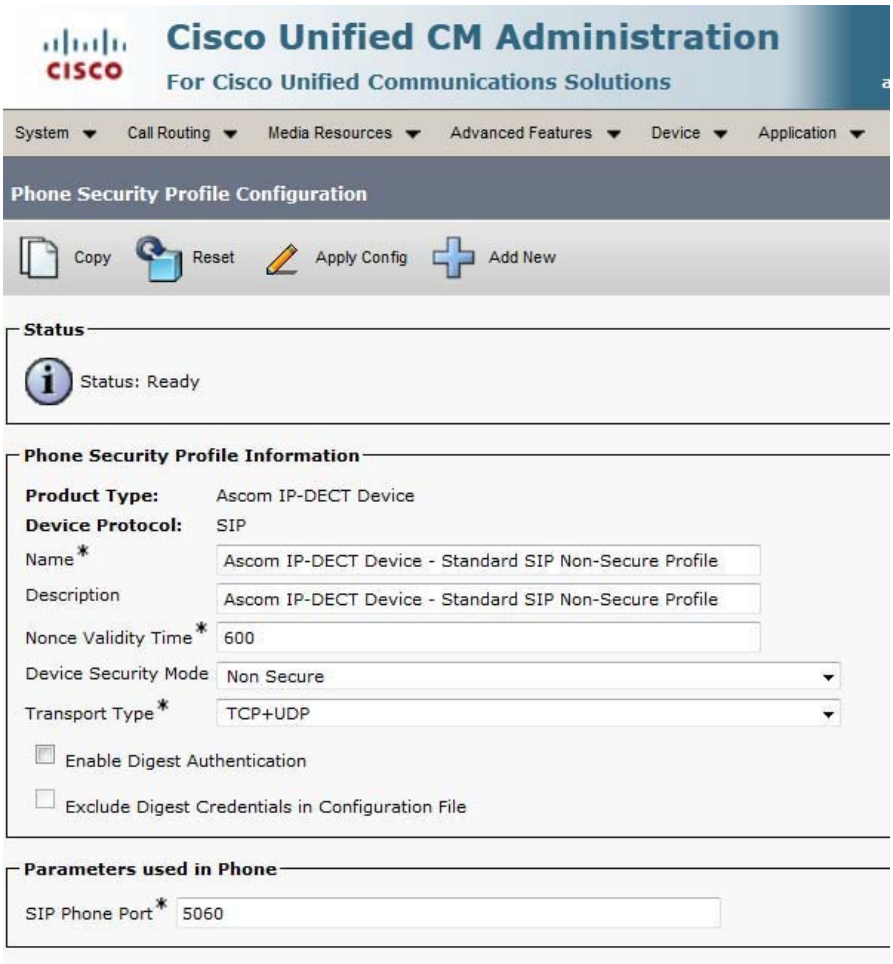
Note. “Require DTMF Reception” is required to utilize KPML.

If this option is enabled in the CUCM, the DTMF digits are sent with the SIP signalling using the Keypad Markup Language (KPML) method. With this method single DTMF digits can also be sent during call setup to add digits to the called number (overlap sending). Enbloc dialing can then be unchecked. KPML is optional.



3. User Management -> End User: Adding an user ID

Note that adding a user is only necessary if the handsets are added as "Third-party SIP devices" or if digest authentication is used.



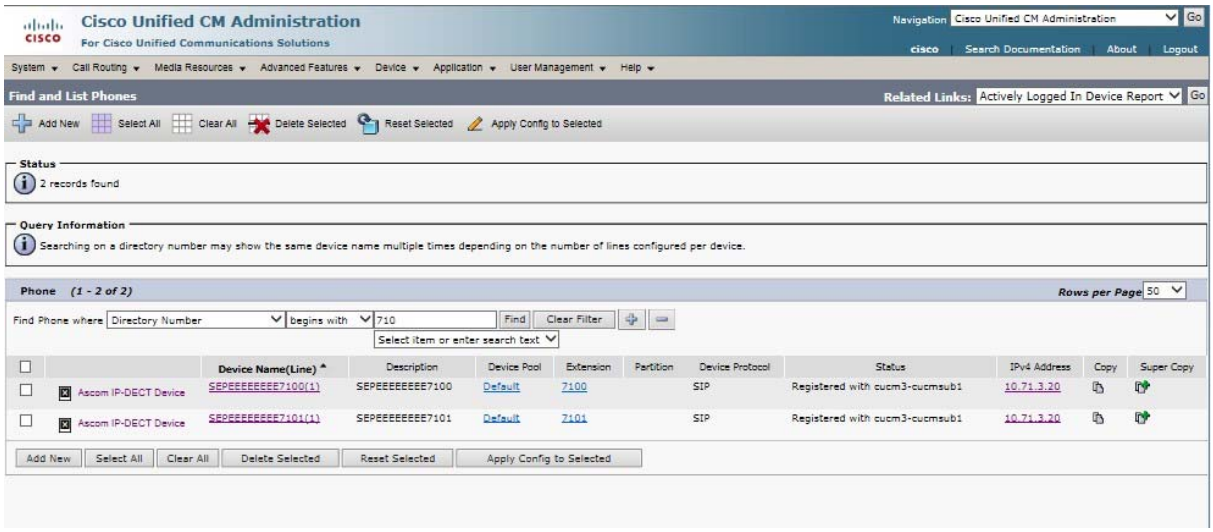
4. System->Security->Security Profiles.

   - ”Ascom IP-DECT Device” default security profile.

5. System->Security->Security Profiles.

Security profile to utilize SIP over TLS.

- Device Security Mode: Encrypted
- Transport Type: TLS



6. Device Overview. (Device->Phone)

Additional Configuration - (VoIP security)

The following two parameters - Denial-of-Service Protection Flag and SIP Station UDP Port Throttle Threshold - can be used in CallManager to configure VoIP security.

The concerns for VoIP security (primarily Denial-of-Service attacks) needs to be addressed when the number of users, calls and master registrations increases.

When used with CallManager the IP-DECT Master acts as a VoIP component and therefore is network addressed. From a network point of view all users (handsets) belonging to a specific IP-DECT Master share the same common IP address. Without proper handling, this could during periods of high system loads be detected as UDP Flooding or network attacks which could slow down the system.

Denial-of-Service Protection Flag

This parameter enables protection used to thwart certain Denial-of-Service attacks. Default value: True. This is an optional but recommended parameter.

1. Select System > Enterprise Parameters.
2. Scroll down to the Denial-of-Service Protection section
3. Select "True" in the Denial-of-Service Protection Flag drop-down list
4. Click "Save".

SIP Station UDP Port Throttle Threshold

If the Denial-of-Service Protection Flag is enabled, the SIP Station UDP Port Throttle Threshold parameter defines the maximum incoming packets per second that Cisco CallManager can receive from a single (unique) IP address that is directed at the SIP station UDP port.

When the threshold is exceeded, Cisco CallManager throttles (drops) the packets that exceed the threshold.

Range: 10-500. Default value: 50.

1. Select System > Service Parameters.
2. Scroll down to the Clusterwide Parameters (Device - SIP) section.
3. Modify the SIP Station UDP Port Throttle Threshold value if needed.
4. Click "Save".

Call Back

The Call Back feature allows users to receive call-back notification on their DECT handset when a called party line becomes available.

Both the CUCM and the IP-DECT device(s) have to be configured to support Call Back.

This feature is based on Presence, so the configuration in the CUCM is about Presence. The Cisco Call Back functionality is not used.

Configure CUCM for Call Back

To configure CUCM for Call Back, do as follows:

1. Make sure the phones that should be able to invoke call back with each other are part of the same Presence Group, or that Presence Subscriptions are allowed between the groups in question. Configuration of Presence Groups are made in System -> Presence Group and for the Phone Device specify "Presence Group". (Screen shot 2)

2. If using Calling Search Spaces (CSS), for the Phone Device specify "SUBSCRIBE CallingSearch Space".

3. If multiple CUCM clusters exist, there must be a SIP Inter Cluster Trunk (ICT) that accepts SIP Presence Subscriptions. The trunk must also be part of a Presence Group that allow Presence Subscriptions from the originating group. If using CSS, specify the "SUBSCRIBE Calling Search Space".

Configure IP-DECT for Call Back

To configure IP-DECT for Call Back, do as follows:

1. Select DECT > Master. Enable or disable the following options:

   - Enable "KPML support".
   - Disable "Enbloc Dialing".
   - Disable "Allow DTMF Through RTP".
   - Disable "Send Inband DTMF".

2. Select DECT > Suppl. Serv. Enable "Call Completion".

   The suffix digit used to initiate Call Completion can be configured. This must be a single digit.

   Default value: 5

   The feature code to cancel an initiated Call Completion can be configured.

   Default value: #37#

Initiate Call Back

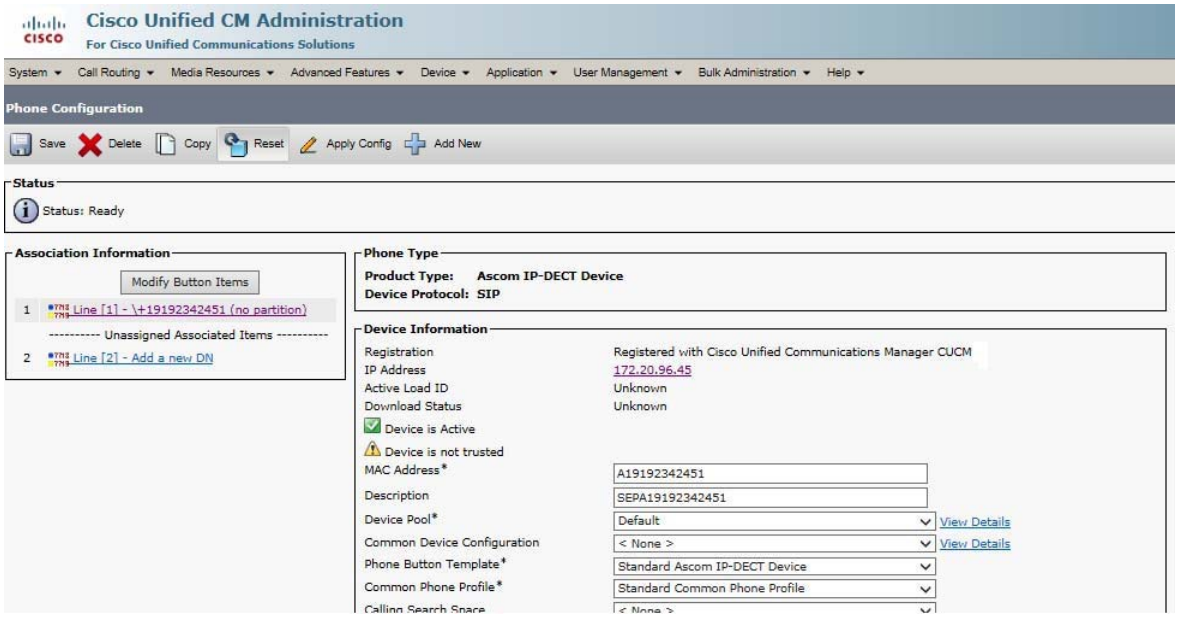
1. When called party is busy or not answering and progress tones are heard, press suffix digit '5' to initiate Call Back.

2. When Call Back is possible the original caller will get a recall. When answering the Call Back will start.

3. To cancel the Call Back dial #37# from idle.

International number plan E.164

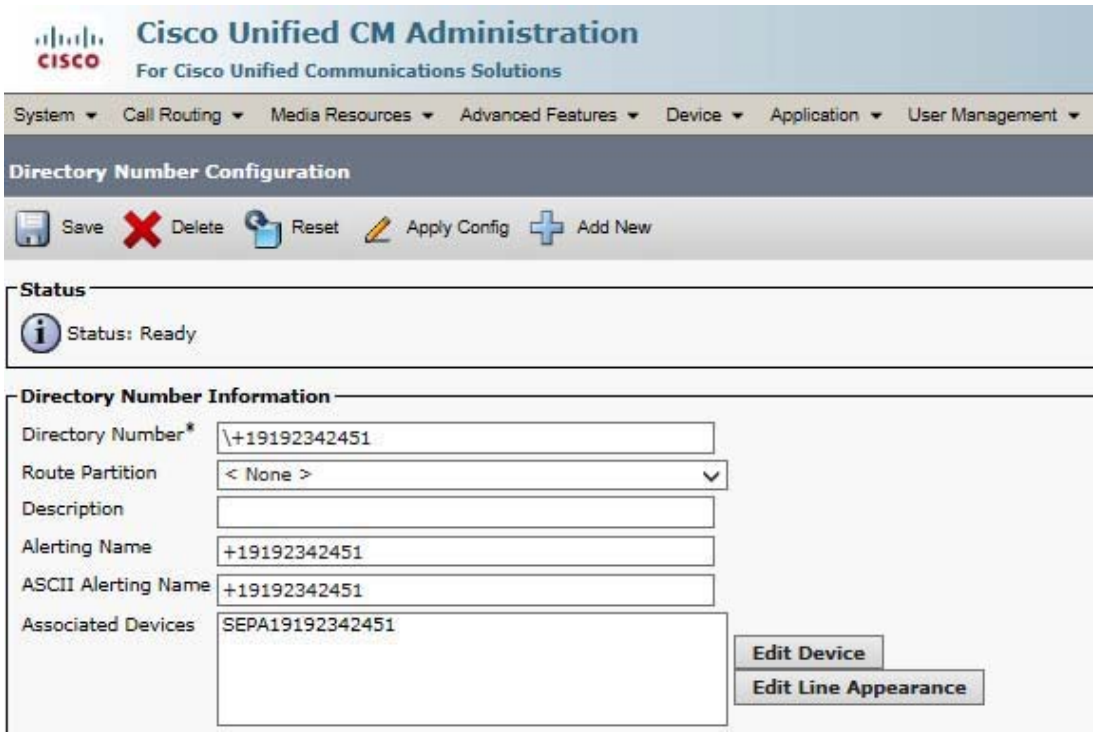
Configure Cisco CUCM for international number plan



Devices -> Phone

The conversion of the '+' sign in the E.164 directory number to an 'A' in the mac-address field is an addition to the normal procedure when adding a phone device of type "Ascom IP-DECT Device". If the number of digits (including '+') is shorter than a mac-address you add a prefix of 'E' characters. If it is longer you instead leave out the most significant digits (including '+'). E.g.

DN	Mac-address (12 hex-digits)
+123456	EEEEEA123456
+12345678901234	345678901234

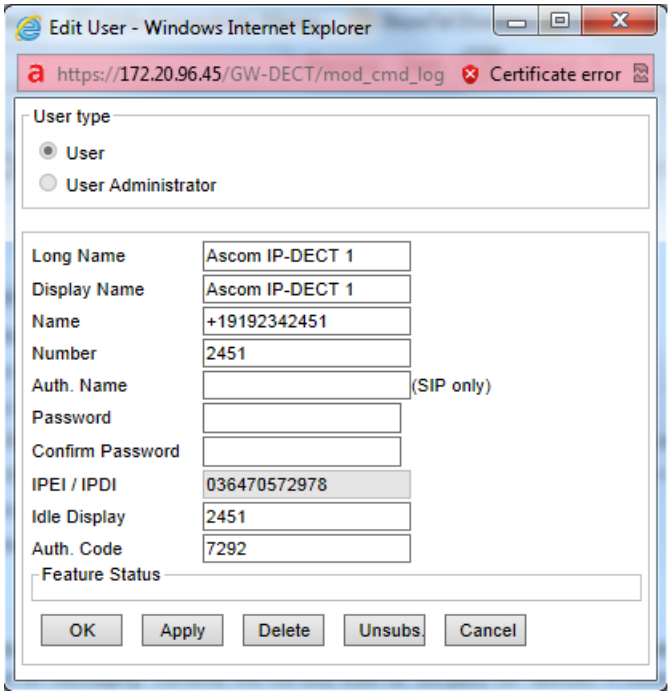


Device -> Phone -> Directory Number

The “+” sign in the Ddirectory number must follow a backslash.

Configure Ascom IP-DECT for international number plan

In the IP-DECT GUI select DECT > Master. Uncheck the “Register with number” setting. This implies that the name field in the User configuration will be used instead of the number field.



Make sure the input in the Name field matched the Directory Number in the CUCM

Cisco Licensed Functions

Following functions require the installation of a Cisco license in the IP-DECT device and a COP-file in the CUCM, see further down below.

- SIP Secure (SIPS) and Secure RTP (SRTP)
- Music on Hold
- Ad Hoc Conference
- Meet-Me Conference
- Call Pickup
- Call Park
- Abbreviated Dialing
- Call Forward All
- Hunt group login/logout
- Shared line - remote resume

To enable Cisco licensed functionality in IP-DECT, do as follows:

1. In the IP-DECT GUI menu select VoIP > SIP. Depending on what kind of protocol that is used, select the SIP or SIPS check box for the following two options:
   - Add instance id to the user registration with the IP-PBX
   - Use local contact port as source port for TCP/TLS connections (if using SIPS)

   Click "OK".

2. Select Configuration > General > License.
   In the License Key field, enter a Cisco license code. Click "OK".
   Note: If there are several IP-DECT devices to be configured, a Device Manager can be used instead. See the User Manual for Device Manager in IMS3, TD 92956EN, or the User Manual for the Device Manager in Unite Connectivity Manager, TD 92855EN.

3. In the "Cisco Unified OS Administration" GUI: Select Software Upgrades > Install/ Upgrade. Install COP-file for device type “Ascom IP-DECT Device” (supplied by Ascom). Install on the Publisher first, then on all Subscribers and then restart all nodes.

4. Select Device > Phone. Add new phone devices of type “Ascom IP-DECT device” and set the MAC address to the corresponding phone number prefixed with ‘E’s. E.g. “EEEEEEEE1001”. If Digest Authentication is not used, then there is no need to create a Digest User.

5. Select Require DTMF Reception (to enable out of band DTMF and overlap dialing).

SIP Secure (SIPS) and Secure RTP (SRTP)

Note: This feature requires that a Cisco license has been installed in the IP-DECT device and that a COP-file has been installed in the Cisco CallManager. See Cisco licensed functions

This section describes briefly how to setup CUCM and IP-DECT to enable SIP Secure (SIPS) and Secure RTP (SRTP). More detailed information can be found in the "Cisco Unified CM Security Guide" online document. These are steps needed in addition to how you setup Ascom IP- DECT as a “Third party SIP device”.

How to setup the Ascom IP-DECT system to enable SIP Secure (SIPS) and Secure RTP (SRTP) is described in the document Installation and Operation Manual, IP-DECT Base Station & IP- DECT Gateway, TD 92579EN.

SIP Secure (SIPS) is used to encrypt the signalling communication between the CUCM and the Ascom Base Stations. SIPS uses the TLS protocol for encryption.

Secure RTP (SRTP) is used to encrypt media streams. The encryption is activated if the SRTP is also enabled with AES128/32 (the only SRTP option supported by CUCM) in the Ascom IP-DECT system. To be able to use SRTP with Ascom IP-DECT system, SIPS must also be used.

Enable SIPS and SRTP in the CUCM

To enable SIPS and SRTP in the CUCM, do as follows:

1. Set “Cluster Security Mode” to “Mixed” (both secure and unsecure devices supported). How to do this is explained in the "Cisco Unified CM Security Guide" online document. You will need available USB Security Tokens.

2. In the "Cisco Unified CM Administration" GUI: Select System > Security Profile > Phone Security Profile. Click on "Add New". In the list of devices, select "Ascom IP-DECT Device". Click "Next".
3. In the Name field: Enter a name in FQDN format (Fully Qualified Domain Name), e.g. secure-profile.ascom-ws.com. This name must match the SubjectAltName (SAN) of the X.509 Certificate of the IP-DECT Master.

4. Select "Encrypted" in the Device Security Mode drop-down list.

5. Select "TLS" in the Transport Type drop-down list.

6. For each device, select the Device Security Profile created above in step 3.

7. In the "Cisco Unified OS Administration" GUI: Select Security > Certificate Management. Click "Upload Certificate". Import the X.509 Certificate of the IP-DECT Master to the certificate trust list by selecting "CallManager-trust" in the Certificate Name drop-down list.

Enable SIPS and SRTP in IP-DECT

To enable SIPS and SRTP in IP-DECT, do as follows:

1. Select General > Certificates.
2. Create a new device certificate (as described in the document Installation and Operation Manual, IP-DECT Base Station & IP-DECT Gateway, TD 92579EN) and specify a DNS name in FQDN format. This name must be identical to the name of the Security Profile in the CUCM. See also step 3 in Enable SIPS and SRTP in the CUCM
3. Import the CUCM server certificate to the Trust List either by file import or by trust action in the Web GUI for the IP-DECT device.
4. Select DECT > Master.
5. Check that the content in the Proxy field or the Domain field match the Subject of the CUCM server certificate.

Music on Hold

Note: This feature requires that a Cisco license has been installed in the IP-DECT device and that a COP-file has been installed in the CUCM. See “Cisco Licensed Functions”.

Music on Hold allows users to place calls on hold with music that a streaming source provides. The system invokes Music on Hold when a user selects to put the call on hold.

For more information about Music on Hold, see the "Cisco Unified Communications Manager Features and Services Guide" online document.

Music on hold is now supported both as Unicast and Multicast. (Prior version 8.0.x only Unicast support)

Ad Hoc Conference

Note: This feature requires that a Cisco license has been installed in the IP-DECT device and that a COP-file has been installed in the CUCM. See “Cisco Licensed Functions”.

The Ad Hoc Conference feature allow users to add multiple participants to a call.

For more information about Ad Hoc Conference, see the "Cisco Unified Communications Manager Features and Services Guide" online document.

Initiate Ad Hoc Conference

1. User A and user B are in a call. User A wishes to add user C to the call.
2. User A places user B on hold by pressing R and calls user C.
3. User C answers.
4. User A adds user C to the call with user B by pressing R3. The call is now a conference call.
5. To add additional users, repeat step 2-4

Meet-Me Conference

Allows a user to initiate a Meet-Me (dial-in) Conference

Configure CUCM for Meet-Me Conference

1. Configure Meet-Me Conference Numbers in Call Routing->Meet-Me Number/Pattern.

Configure IP-DECT for Meet-Me Conference

1. Select DECT > Suppl. Serv. Enable "Call Service URI". For information about Call Service URI, see “Call Service URI”.

Initiate Meet-Me Conference

2. Dial the feature code including the Meet-Me Number to initiate and be connected to the conference. For information about feature code, see “Call Service URI” on page 12.

3. Other users may participate by calling the Meet-Me Number and automatically be connected to the conference.

Call Pickup

Note: This feature requires that a Cisco license has been installed in the IP-DECT device and that a COP-file has been installed in the CUCM. See “Cisco Licensed Functions”.

The Call Pickup feature allows users to pick up incoming calls within their own group. Cisco Unified Communications Manager automatically dials the appropriate call pickup group number when the user activates this feature from a DECT handset.

For more information about Call Pickup, see the "Cisco Unified Communications Manager Features and Services Guide" online document.

Configure CUCM for Call Pickup

1. Configure Call Pickup Groups in Call Routing->Call Pickup Group. To get a notification when a call can be picked up, specify visual alert. IP-DECT does not support audible alert only. The notification is only supported on the latest handset models.

2. For the Directory Number (DN), specify the "Call Pickup Group" to be part of.

3. Configure for auto-mode. Auto-mode is a service parameter for Call Pickup features. Select System > Service Parameters > Cisco CallManager Service. Set the parameter "Auto Call Pickup Enabled" to "True" or False".

Configure IP-DECT for Call Pickup

1. Select DECT > Suppl. Serv. Enable "Call Service URI". For information about Call Service URI, see “Call Service URI”.

Initiate Call Pickup

1. When there is a call possible to pickup, a notification is received by the phone.

2. Dial the feature code. For information about feature code, see “Call Service URI”.

3. Depending on the setting on the auto-mode (This step applies to all types of Call Pickup), following happens:
    a. The feature call is cleared and the call to pickup is redirected to the phone as an incoming call.
    b. The call to pickup is connected immediately.

Call Pickup Other Group

Allows a user belonging to a Call Pickup Group to pickup calls for members of associated group.

Configure CUCM for Call Pickup Other Group

1. See step 1 and 2 in “Configure CUCM for Call Pickup”.
2. Configure associations between groups in Call Routing->Call Pickup Group.
3. See step 3 in “Configure CUCM for Call Pickup”.

Configure IP-DECT for Call Pickup Other Group

See “Configure IP-DECT for Call Pickup”

Initiate Call Pickup Other Group

1. See “Initiate Call Pickup”. Note: No notification is given.

Group Call Pickup

Note: This feature requires that a Cisco license has been installed in the IP-DECT device and that a COP-file has been installed in the CUCM. See “Cisco Licensed Functions”.

Allows a user belonging to a Call Pickup Group to pickup calls to members of any group by specifying the Group Number.

For more information about Call Pickup, see the "Cisco Unified Communications Manager Features and Services Guide" online document.

Configure CUCM for Group Call Pickup

1. See “Configure CUCM for Call Pickup”.

Configure IP-DECT for Group Call Pickup

1. See “Configure IP-DECT for Call Pickup” on page 9.

Initiate Group Call Pickup

1. Dial the feature code including the Group Number of the Pickup Group.
   For information about feature code, see “Call Service URI”.

2. See step 3 in “Initiate Call Pickup”.

Directed Call Pickup

Note: This feature requires that a Cisco license has been installed in the IP-DECT device and that a COP-file has been installed in the CUCM. See “Cisco Licensed Functions“.

Allows a user belonging to a Call Pickup Group to pickup calls to a specific member of the own or an associated group by specifying the Directory Number. This feature uses the same feature code as Group Pickup.

For more information about Call Pickup, see the "Cisco Unified Communications Manager Features and Services Guide" online document.

Configure CUCM for Directed Call Pickup

1. See “Configure CUCM for Call Pickup”.

Configure IP-DECT for Directed Call Pickup

1. See “Configure IP-DECT for Call Pickup“.

Initiate Directed Call Pickup

1. Same as Group Pickup, except specify the Directory Number instead of the Group Number

Call Park

Note: This feature requires that a Cisco license has been installed in the IP-DECT device and that a COP-file has been installed in the CUCM. See “Cisco Licensed Functions”.

The Call Park feature allow users to place a call on hold, so it can be retrieved from another phone. The parking lot number is selected by CUCM.

Directed Call Park is possible with a third-party SIP device. Directed Call Park allows a user to transfer a call to an available user-selected directed call park number configured in the CUCM.

For more information about Call Park, see the "Cisco Unified Communications Manager Features and Services Guide" online document.

Configure CUCM for Call Park

1. Specify Call Park Numbers/Ranges where call can be parked in Call Routing->Call Park.

Configure IP-DECT for Call Park

1. Select DECT > Suppl. Serv. Enable "Call Park". For information about Call Park, see “Call Park”.

Initiate Call Park

1. While in an ongoing call with party to be parked Press R+<local feature code>. The parking lot number is shown on the display. For information about feature code, see “Call Service URI“.

2. Hangup and retrieve the call on another phone by dialing the parking lot number.

Abbreviated Dialing

Note: This feature requires that a Cisco license has been installed in the IP-DECT device and that a COP-file has been installed in the CUCM. See “Cisco Licensed Functions “.

The Abbreviated Dialing feature allow users to make a call by enter an available abbreviated number configured in the CUCM for a call number.

For more information about Abbreviated Dialing, see the "Cisco Unified Communications Manager Features and Services Guide" online document.

Configure CUCM for Abbreviated Dialing

1. For the Phone Device select Related Links: "Add/Update Speed Dials" to open and manage the list with abbreviated numbers.

Configure IP-DECT for Abbreviated Dialing

1. See “Configure IP-DECT for Call Pickup”.

Initiate Abbreviated Dialing

1. Dial the feature code including the abbreviated number. For information about feature code, see ”Call Service URI”.

Call Forward All

Note: This feature requires that a Cisco license has been installed in the IP-DECT device and that a COP-file has been installed in the CUCM. See “Cisco Licensed Functions.

The Call Forward All feature can be initiated from the CUCM or a handset and allow users to forward numbers to voice mail (can only be initiated from the CUCM) or another number.

For more information about Call Forward All, see the "Cisco Unified Communications Manager Features and Services Guide" online document.

Initiate Call Forward All from the CUCM

1. Select Call Routing > Directory Number.
2. Select the number that is to be forwarded.
3. Under section "Call Forward and Call Pickup Settings", go to "Forward All" and select the "Voice Mail" check box or enter the destination number in the "Destination" text box.

Initiate Call Forward All from a Handset

1. Enter in the handset *75<number># where "number" is the destination number.

Clear Call Forward All in CUCM

1. To clear Call Forward All in the CUCM: Depending on what has been chosen, deselect the
   "Voice Mail" check box or delete the destination number in the "Destination" text box.

Clear Call Forward All from a Handset

1. To clear Call Forward All from a handset can be done in two ways:
   A. Enter in the handset *55.
   B. Enter in the handset *75#.

Hunt group login/logout

Note: This feature requires that a Cisco license has been installed in the IP-DECT device and that a COP-file has been installed in the CUCM. See “Cisco Licensed Functions“.

Login/Logout from the handset of a CUCM hunt group. It is indicated in the idle display when logging out of a hunt group.

Note. A forceful login/logout performed through the Cisco UCM administrative interface will not be reflected on the handset until the handset has logged in/out.

Configure CUCM for Hunt group login/logout

1. Hunt groups needs to be configured in the Cisco UCM.

Configure IP-DECT for Hunt group login/logout

1. Select DECT > Suppl. Serv. Enable the supplementary service "Soft key".

Initiate Hunt group login/logout

1. The user dials the configured feature access code and supplies "0" as the argument to toggle the login/logout status of the device in the hunt group.

Cisco shared line - remote resume

Note: This feature requires that a Cisco license has been installed in the IP-DECT device and that a COP-file has been installed in the CUCM. See “Cisco Licensed Functions“.

Allows the user to "move" a call between two devices that share the same line by putting it on hold on one device and resuming it on another.

Note. An Ascom IP-DECT handset cannot share line with another Ascom IP-DECT handset

Note. Handset d62,d63 and d81 has all functionallety, limited functionality with d41 and d43

Configure CUCM for Shared line- remote resume

1. No configuration needed except that Ascom IP-DECT handset needs to share line with other device (Note that second device cannot be an IP-DECT device)

Configure IP-DECT for Shared line- remote resume

1. Select DECT > Suppl. Serv. Enable the supplementary service "Call Park".

Initiate Shared line- remote resume

1. When there is a call on hold on the shared line used by a DECT handset, information about this call will be shown in a dialog including a position number (N) on the handset. The user can resume this call by pressing the "OK" button (only d62,d63 and d81), or remove the notification by using the "Cancel" button. This will work both if the handset is idle or already in a call. In case the call is resumed from another phone the dialog will be automatically closed. If there are several calls that can be resumed, they will be shown one at a time. A specific call can also be resumed by manually dialing the feature access code for Un-park and supplying the position number (N), e.g. If using d41 or d43 the dialog was closed.

Supplementary Services

Call Service URI

Call Service URI is used to initiate some of the features in the CUCM. The local feature code is translated to a CUCM default "Service URI" according to the table below. The CUCM service URIs can be found in the SIP profile used by a SIP phone. Select Device > Device Settings > SIP Profile.

The table below shows the default settings that must be used for IP-DECT.

Feature	Service URI in CUCM (Default values)	Feature Number, $(1)	Feature Argument, S#	Default Value
Abbreviated Dialing	x-cisco-serviceuri-abbrdial	0	Abbreviated Number	*70<number>#
Call Pickup	x-cisco-serviceuri-pickup	1	NA	*51
Group Call Pickup	x-cisco-serviceuri-gpickup	3	Group Number	*73<number>#
Meet-Me Conference	x-cisco-serviceuri-meetme	4	Conference Number	*74<number>#
Call Forward All	x-cisco-serviceuri-cfwdall	5	Forward Number	*75<number>#
Call Pickup Other Group	x-cisco-serviceuri-opickup	2	NA	*52

All Call Service URI feature codes takes a Feature Number as the first user provided digit. This number corresponds to which feature to use and is not configurable.

Without Argument

This feature code takes only the Feature Number as the user provided digit, which specifies which Call Service URI feature to use, see table above.

Default value: *5$(1)

With Argument

This feature code takes in addition to the feature code above, also one feature argument with an unspecified length

Default value: *7(1)#

Call Park

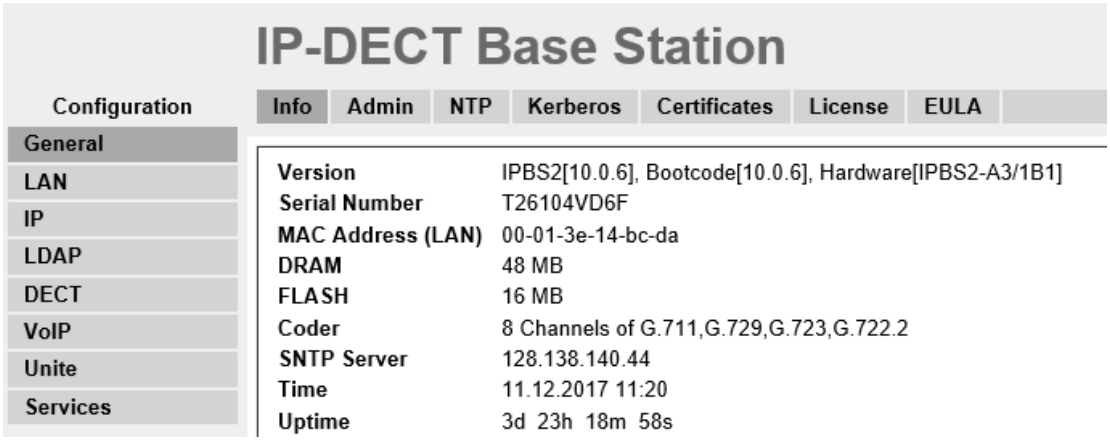
This feature code takes one feature argument consisting of one digit. In a CUCM system this argument is not used for anything and can be any digit.

Default value: *16$(1)

The second feature code for Call Park is not used in a CUCM

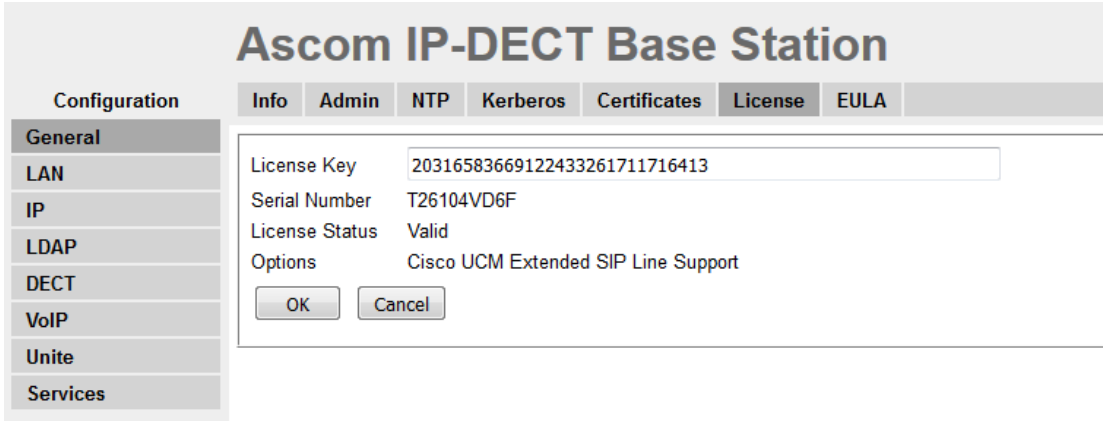
system. Default value: #16$(1)

Ascom IP-DECT version 10.0.6 configuration



General->Info

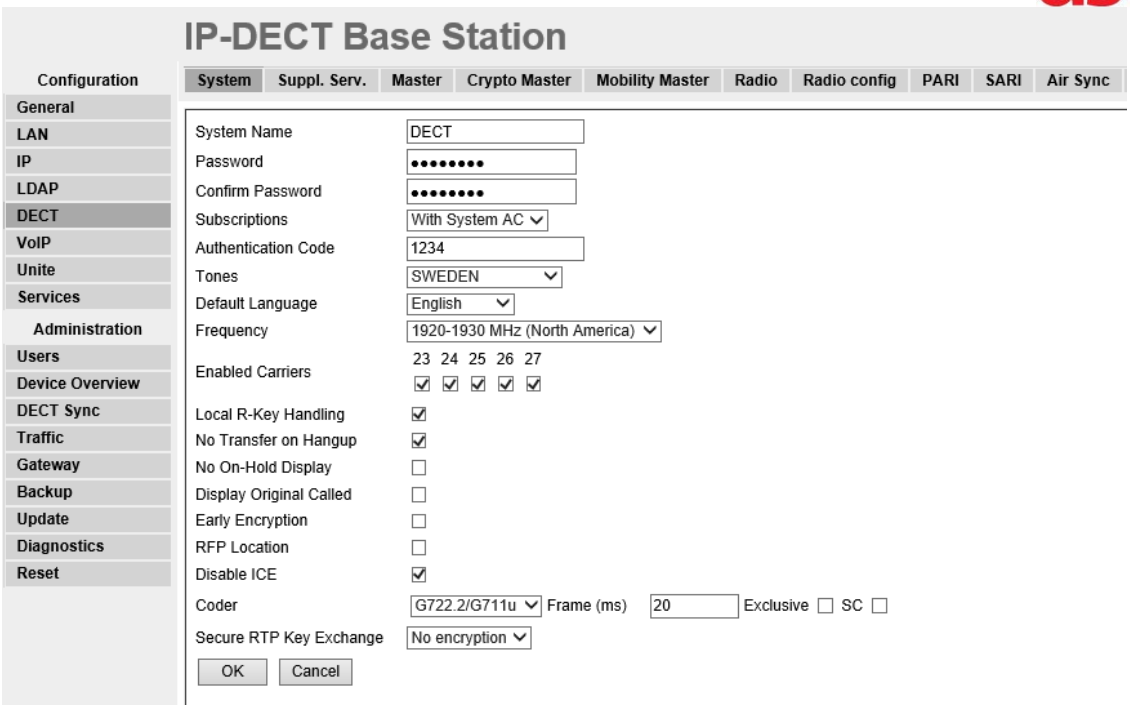
- General information. Software version etc.



General->License.

- A license key is required in order to register as “Ascom IP-DECT device”.

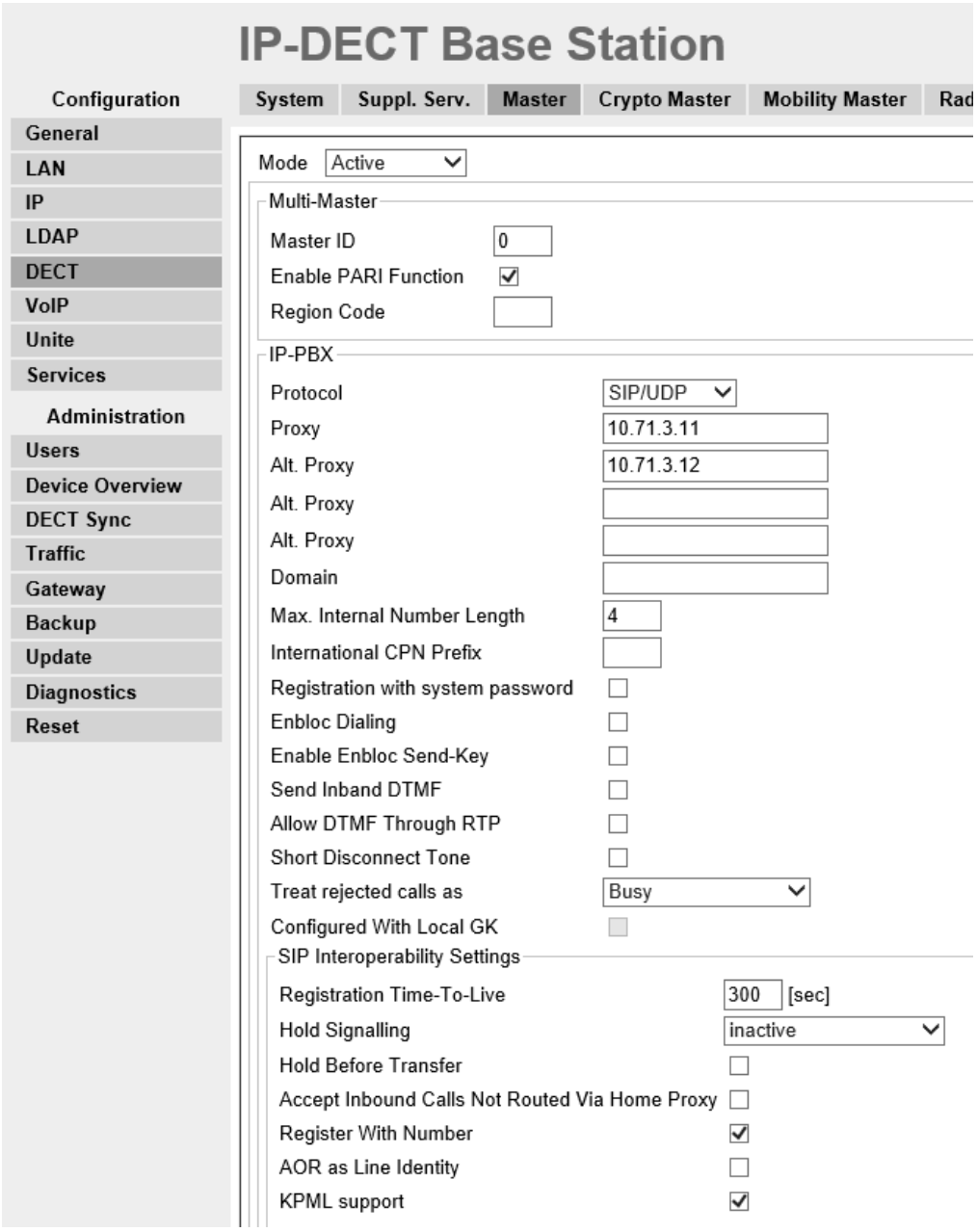
Note. A license key is not needed if handsets are registered as a “Third-party SIP device”.



DECT->System

- Disable ICE

Note that the settings shown above apply for a system located in North America.

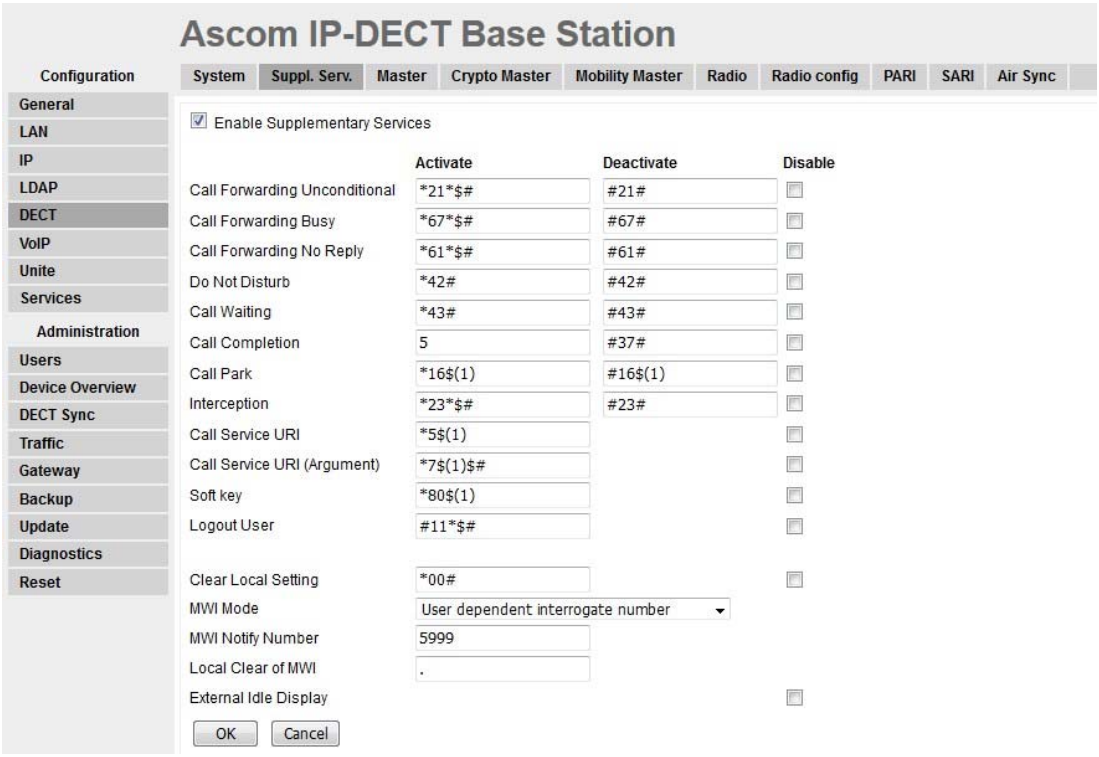


DECT ->Master.

- Disable “Enbloc Dialing”
- Disable “Allow DTMF Through RTP”
- Registration Time-To-Live is kept as default (120s)
- Hold signaling: inactive
- Enable “Register With Number”
- Enable “KPLM support”

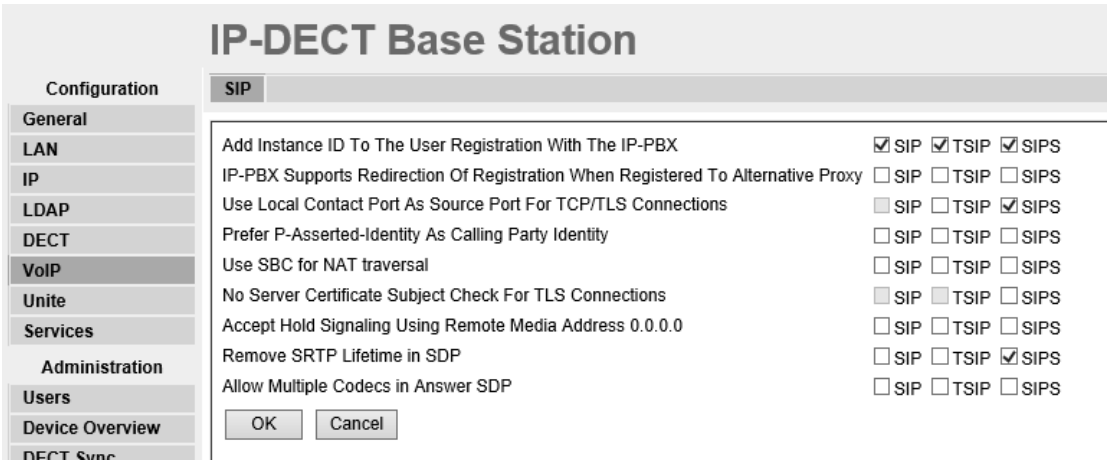
Note. The setting “Allow DTMF-through-RTP” should be enabled in VoIP environments where non-KPML-endpoints cannot rely on CUCM to translate between KPML and RFC2833/4733 DTMF signaling.

Note. Alt Proxy was entered for test purpose in order to verify redundancy. Domain was entered in order to test SIP-TLS.



DECT -> Supplementary Services

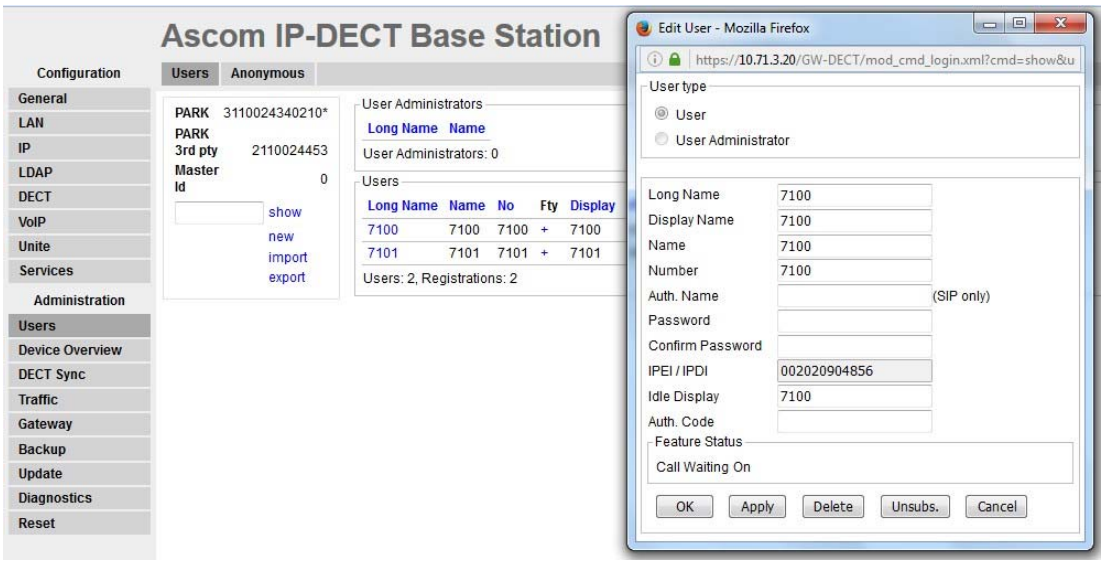
- Make sure Supplementary Services are enabled.
- MWI Mode: User dependent interrogate number. This means that the user's own call number is used as MWI Interrogate number.
- MWI Notify Number: Enter the number to the Voice Mail.



VoIP->SIP

- "Use Local Port As Source For TCP/TLS Connections" is required when using TLS

Important. Instance ID can only be used if the Ascom endpoints are added as "Ascom IP-DECT Device" in the CUCM. If the Ascom device are added as a "3rd Party SIP device", Instance ID cannot be used.



Users - > Users

Note. Password is needed only if the CUCM security profile is set as to use digest authentication.

Document History

Rev	Date	Author	Description
PA1	2013-07-09	SEKMO	Initial draft CUCM v9.1.1.
R1	2013-07-18	SEKMO	Minor corrections. Revision 1
R2	2013-11-18	SEKMO	Clarified licensing info on page 7. Revision 2
P3	2014-03-12	SEKMO	Merged info from Ascom Configuration Note for CUCM
R3	2014-03-25	SEKMO	Minor corrections after review. Revision 3
P4	2014-08-26	SEKMO	Updated to UCM 10.x. Added E.164 info.
R1	2015-02-26	SEKMO	Updates to known issues and Ascom version (7.2.7)
R2	2015-05-29	SEKMO	Updates regarding IP-DECT version 8. MOH, shared line - remote resume, hunt group login/logout
R3	2016-04-25	SEJAn	Updated to CUCM v11.0
R4	2018-03-09	SEJAn	Updated to CUCM v12.0 and new layout