Configuration Notes

for Cisco CallManager in Ascom IP-DECT System

14 May 2012 / Ver. F

Contents

1 Introduction

This document is intended as a guide when using a Cisco CallManager (CCM) in the Ascom IP-DECT System. The document will describe some of the settings necessary to gain good performance when the Ascom IP Base Stations is used with CCM.

The document has been updated to cover Cisco Unified CallManager and Cisco Unified Communication Manager (CUCM).

The different Cisco product names will be referred to in this document as Cisco CallManager or simply CallManager.

Note: It is not within the scope of this document to describe the configuration process of the IP Base Station, please refer to the appropriate IP Base Station manual.

1.1 Abbreviations and Glossary

CCM	Cisco CallManager, Cisco Unified CallManager
CUCM	Cisco Unified Communications Manager
DECT	Digital Enhanced Cordless Telecommunications: global standard for cordless telephony.
SAN	Subject Alternative Name
SIP	Session Initiation Protocol
VoIP	Voice over Internet Protocol

2 IP-DECT Configuration

2.1 DECT

System

Select DECT -> System

Parameter	Value	Information
Local R-Key Handling	Enable	Keypad information is handled locally

Suppl. serv.

Select DECT -> Suppl. serv.

Parameter	Value	Information
Enable Supplementary Services	Enable	The supplementary services are activated.

Master

Select DECT -> Master

Parameter	Value	Information
Proxy	For example, 10.0.0.7	Enter the Cisco CallManager IP address or host name
Alt. Proxy		If applicable, enter the alt. Cisco CallManager IP address or host name
Domain	For example, enter ascom.se from the domain name 123456@ascom.se	Enter the domain part of the SIP address or leave this field blank if not used.
Enbloc Dialing	Enable	The keystrokes on the handsets are buffered in the IP-DECT device for a short period of time before sent to the IP-PBX
Allow DTMF through RTP	Enable	DTMF digits are sent as RTP payload directly to the other endpoint.
Register with number	Enable	The number is used for registrations towards the IP-PBX instead of name. Name will be used for authentication.

2.2 Users

Users

Select Users -> Users -> New.

Parameter	Information
Long Name	Mandatory, unique string
Name	Same as "User ID" of the Digest User in Cisco CallManager
Number	Same as "Directory Number" in Cisco CallManager
Password	Same as "Digest Credentials" in Cisco CallManager if digest authentication is used

3 Cisco CallManager

This section describes the necessary configuration of the Cisco CallManager for the IP-DECT system. For more information on how to configure the Cisco CallManager, see applicable documentation from Cisco.

3.1 User Management

Add a new End User and enter User ID. Make sure it corresponds with the settings in the IP-DECT system, see 2.2 Users on page 2. The User ID must be the *Name* configured for the IP-DECT user. If digest authentication is used, the *Digest Credentials* must be the same as the password for the IP-DECT user.

3.2 Device

Phone

Add a new phone and select type "Third-party SIP device (Basic)". In the *Device Security Profile* drop-down list, select "Third-party SIP Device Basic - Standard SIP Non-secure Profile".

For Digest User, point to the previously created End User. This is used for identification and authentication.

3.3 Call Routing

Directory Number

Add a new Directory Number (same as the "Number" for IP-DECT users) and tie it to the previously created phone.

3.4 System (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 *The SIP Station UDP Port Throttle Threshold* value if needed.

4 Click "Save".

4 No Digest Authentication

Note: No Digest Authentication for Third-party SIP Device types works only with CallManager version 5 and 6.

If digest authentication is not used for the IP-DECT system, there is no need to create an End User in the CCM and the configuration becomes simpler.

1 In the IP-DECT menu select VoIP > SIP.

2 Select the *Add instance id to the user registration with the IP-PBX* check box.

3 In the CCM set the MAC address to the Directory Number prefixed with Es.

For example, if the Directory Number is "1234", the MAC address should be set to "EEEEEEEE1234".

4 Skip chapter 3.1 User Management and no digest user is needed in chapter 3.2 Device.

5 Leave the Name and Password fields blank when configuring users in chapter 2.2 Users.

5 KPML

Note: This option requires that KPML has been enabled in the IP-DECT system.

If this option is enabled in the CCM, 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.

5.1 Enable KPML in the CCM

To enable KPML, perform step 1 to 4 below for each phone in the IP-DECT system:

1 In the CCM select Device > Phone.

2 Scroll down to the *Protocol Specific Information* section.

3 Select the *Require DTMF reception* check box.

4 Click "Save".

5.2 Enable KPML in IP-DECT

To enable IP-DECT for KPML, 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".

6 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 CCM 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.

6.1 Configure CCM for Call Back

To configure CCM 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".

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

3 If multiple CUCM clusters exist, there must be a SIP Inter Cluster Trunk (ICT) that accepts SIP Presence Subsriptions. 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".

6.2 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". For information about Call Completion, see 7.11.3 Call Completion on page 12.

6.3 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.

7 Cisco Licensed Functions

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

- SIP Secure (SIPS) and Secure RTP (SRTP), see 7.1 SIP Secure (SIPS) and Secure RTP (SRTP) on page 6.
- Music on Hold, see 7.2 Music on Hold on page 7.
- Ad Hoc Conference, see 7.3 Ad Hoc Conference on page 8.
- Meet-Me Conference, see 7.4 Meet-Me Conference on page 8.
- Call Pickup, see 7.5 Call Pickup on page 8.
- Call Park, see 7.9 Call Park on page 10.
- Abbreviated Dialing, see 7.10 Abbreviated Dialing on page 11.

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).

7.1 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 7 Cisco Licensed Functions on page 6.

This section describes briefly how to setup CCM 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 CCM 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 CCM) in the Ascom IP-DECT system. To be able to use SRTP with Ascom IP-DECT system, SIPS must also be used.

7.1.1 Enable SIPS and SRTP in the CCM

To enable SIPS and SRTP in the CCM, 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. See also step 2 in 7.1.2 Enable SIPS and SRTP in IP-DECT on page 7.

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.

7.1.2 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 CCM. See also step 3 in 7.1.1 Enable SIPS and SRTP in the CCM on page 7.

3 Import the CCM 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 CCM server certificate.

7.2 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 CCM. See 7 Cisco Licensed Functions on page 6.

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.

7.3 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 CCM. See 7 Cisco Licensed Functions on page 6.

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.

7.3.1 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

7.4 Meet-Me Conference

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

7.4.1 Configure CCM for Meet-Me Conference

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

7.4.2 Configure IP-DECT for Meet-Me Conference

1. Select DECT > Suppl. Serv. Enable "Call Service URI". For information about Call Service URI, see 7.11.1 Call Service URI on page 11.

7.4.3 Initiate Meet-Me Conference

1. Dial the feature code including the Meet-Me Number to initiate and be connected to the conference. For information about feature code, see 7.11.1 Call Service URI on page 11.
2. Other users may participate by calling the Meet-Me Number and automatically be connected to the conference.

7.5 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 CCM. See 7 Cisco Licensed Functions on page 6.

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.

7.5.1 Configure CCM 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".

7.5.2 Configure IP-DECT for Call Pickup

1 Select DECT > Suppl. Serv. Enable "Call Service URI". For information about Call Service URI, see 7.11.1 Call Service URI on page 11.

7.5.3 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 7.11.1 Call Service URI on page 11.

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.

7.6 Call Pickup Other Group

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

7.6.1 Configure CCM for Call Pickup Other Group

1 See step 1 and 2 in 7.5.1 Configure CCM for Call Pickup.

2 Configure associations between groups in Call Routing->Call Pickup Group.

3 See step 3 in 7.5.1 Configure CCM for Call Pickup on page 9.

7.6.2 Configure IP-DECT for Call Pickup Other Group

1 See 7.5.2 Configure IP-DECT for Call Pickup on page 9.

7.6.3 Initiate Call Pickup Other Group

1 See 7.5.3 Initiate Call Pickup. Note: No notification is given.

7.7 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 CCM. See 7 Cisco Licensed Functions on page 6.

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.

7.7.1 Configure CCM for Group Call Pickup

1 See 7.5.1 Configure CCM for Call Pickup.

7.7.2 Configure IP-DECT for Group Call Pickup

1 See 7.5.2 Configure IP-DECT for Call Pickup on page 9.

7.7.3 Initiate Group Call Pickup

1 Dial the feature code including the Group Number of the Pickup Group.
For information about feature code, see 7.11.1 Call Service URI on page 11.

2 See step 3 in 7.5.3 Initiate Call Pickup.

7.8 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 CCM. See 7 Cisco Licensed Functions on page 6.

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.

7.8.1 Configure CCM for Directed Call Pickup

1 See 7.5.1 Configure CCM for Call Pickup.

7.8.2 Configure IP-DECT for Directed Call Pickup

1 See 7.5.2 Configure IP-DECT for Call Pickup on page 9.

7.8.3 Initiate Directed Call Pickup

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

7.9 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 CCM. See 7 Cisco Licensed Functions on page 6.

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 CCM.

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 CCM.

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

7.9.1 Configure CCM for Call Park

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

7.9.2 Configure IP-DECT for Call Park

1 Select DECT > Suppl. Serv. Enable "Call Park". For information about Call Park, see 7.11.2 Call Park on page 12.

7.9.3 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 7.11.1 Call Service URI on page 11.

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

7.10 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 CCM. See 7 Cisco Licensed Functions on page 6.

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

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

7.10.1 Configure CCM for Abbreviated Dialing

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

7.10.2 Configure IP-DECT for Abbreviated Dialing

1 See 7.5.2 Configure IP-DECT for Call Pickup on page 9.

7.10.3 Initiate Abbreviated Dialing

1 Dial the feature code including the abbreviated number. For information about feature code, see 7.11.1 Call Service URI on page 11.

7.11 Supplementary Services

7.11.1 Call Service URI

Call Service URI is used to initiate some of the features in the CCM. The local feature code is translated to a CCM default "Service URI" according to the table below. The CCM 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 CCM (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
Call Pickup Other Group	x-cisco-serviceuri-opickup	2	NA	*52
Group Call Pickup	x-cisco-serviceuri-gpickup	3	Group Number	*73<number>#
Meet-Me Conference	x-cisco-serviceuri-meetme	4	Conference Number	*74<number>#

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)#

7.11.2 Call Park

This feature code takes one feature argument consisting of one digit. In a CCM 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 CCM system.

Default value: #16$(1)

7.11.3 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#

8 Related Documents

System Description, Ascom IP-DECT System	TD 92375GB
System Planning, Ascom IP-DECT	TD 92422GB
Installation and Operation Manual, IP-DECT Base Station & IP-DECT Gateway	TD 92579EN

Document History

Version	Date	Description
A	2007-01-15	First version
B	2008-09-03	Second version. • 3.4 System (VoIP security): Denial-of-Service updates • Other minor changes
C	2009-02-02	Third version. Several updates, see change bars.
D	2010-10-04	Fourth version. Added chapter about KPML.
E	2011-04-05	Fifth version. Added chapter about SIP Secure (SIPS) and Secure RTP (SRTP). For other changes, see change bars.
F	2012-05-14	Sixth version. Added chapter 6 and 7 about Call Back and Cisco Licensed functions.