SIP-DECT 8.0

Release Notes
Version 8.0-DI16
October 15th, 2018

Mitel

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

Trademarks

SIP-DECT - Release 8.0
October 2018
depl-2594 /1.0

Table of Contents

Availability of SIP-DECT 8.0-DI16 for EFT

This document describes the following components related to SIP-DECT 8.0-DI16:

- SW identification.
- Product enhancements and functional changes.
- Essential installation and upgrade information.
- Product compatibility with Mitel Call Server.
- How to locate the latest version of our guides.
- Product areas improved in this release.
- Known issues and Limitations.
- Q&A

SW identification

Current delivery

The following software is part of **SIP-DECT 8.0-DI16**:

- **iprfp2G.tftp**: software for RFP 32 IP, RFP 34 IP, and RFP 42 WLAN.
- **iprfp3G.dnld**: software for RFP 35 IP, RFP 36 IP, RFP 37 IP, and RFP 43 WLAN. including the Mitel 600d DECT Phone family firmware package:
  - Mitel 6x2d/650c DECT Phone firmware 7.2.
  - Mitel 602d V2 DECT Phone firmware 7.2.
- **iprfp4G.dnld**: software for RFP 44 IP, RFP 45 IP, RFP 47 IP, and RFP 48 WLAN. including the Mitel 600d DECT Phone family firmware package and the iprfp3G.dnld SW package.
- **SIP-DECT.bin**: software for Linux Server based OMM including Mitel 600 DECT Phone firmware.
- OM Configurator (OMC).
- OM Management Portal (OMP).
- SIP-DECT Multi-OMM Manager (MOM).
- OM Locating (OML).
- OVA file to deploy the SIP-DECT MOM or OMM under VMware ESXi™
- Find my SIP-DECT base station: java script to be executed in a Web browser which helps to find SIP-DECT base stations in the network, to identify their IP address and to access the OMM Web service

File	MD5 checksum
iprfp3G.dnld	9ddce86c072228e746baa6d834f9dc5b
iprfp4G.dnld	4b6791673626959f58626c0bdbaaf06b
iprfp2G.tftp	c0395a05c7e76aeb41708232b2a8d319
SIP-DECT.bin	74e4c6137b5538877c8bd334c34addc1
OMP.jar	6ca917f5c6d1bd9e5e908e3d92cb4970
OM_Configurator.jar	b59fd46fe6650ff337c7be3f67e3b23c
SIP-DECT-MOM-8.0_DI16-0.i686.rpm	bcb8dd7a8c3641738a653d6fbe2e25b5
OML.war	093e40604d3daa3396f7756b6f0c96a6
SIP-DECT_8.0-DI16.zip	9df486274f2e887d2b130dc05cc8c571
SIP-DECT_8.0-DI16.ova	21a97531b2606ce233267d4f8c6f8dbd
FindMySIP-DECTbasestation.zip	9b2fdd683f61f79263e6272cb5d3a901

The SIP-DECT OM XML Application Interface of this delivery uses the protocol version 46.

Download links:

File	URL
SIP-DECT_8.0-DI16.zip	http://gsd.aastra.com/SIP-DECT/SW/8.0-DI16/SIP-DECT_8.0-DI16.zip?encoded=048fbeaf6e536b3f4d91b
SIP-DECT_8.0-DI16.ova	http://gsd.aastra.com/SIP-DECT/SW/8.0-DI16/OVA/SIP-DECT_8.0-DI16.ova?encoded=0aec8da001462df13e13f
FindMySIP-DECTbasestation.zip	http://gsd.aastra.com/SIP-DECT/SW/8.0-DI16/FindMySIP-DECTbasestation.zip?encoded=058f47356e8d68297cb94

Previous deliveries

- SIP–DECT Software Version 7.1-CK14
  SIP-DECT 7.1 GA version

- SIP–DECT Software Version 7.1SP1-DI02
  Fist SIP-DECT 7.1 service pack including
  - Mitel 6x2d/650c DECT Phone firmware 7.2
  - Mitel 602d V2 DECT Phone firmware 7.2

Product enhancements and functional changes

New features since SIP-DECT 7.1-CK14

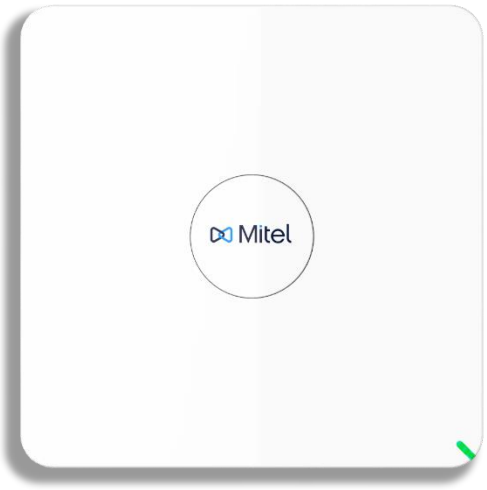
MSD-24: 4th Generation DECT Base Station family

About 4th Generation DECT Base Stations

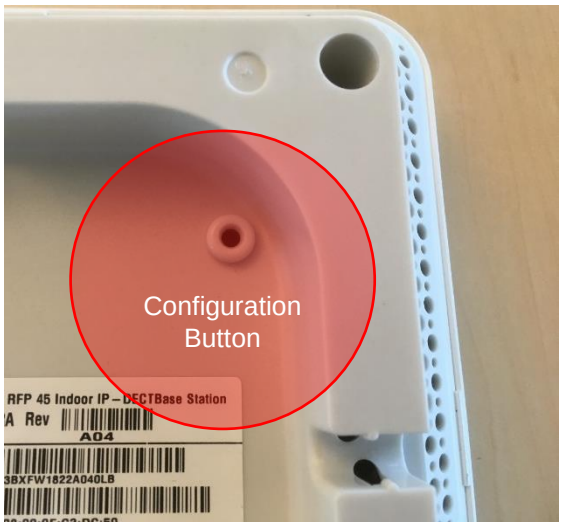
As of SIP-DECT 8.0, SIP-DECT supports the 4th base station generation (RFP4G). This 4th RFP generation comprises of:

- RFP 44 IP
  DECT RFP as indoor model with 4 narrow band voice channels and internal antennas
- RFP 45 IP
  DECT RFP as indoor model with 8 narrow band voice channels and internal antennas
- RFP 47 IP
  DECT RFP as indoor model with 8 narrow band voice channels and 2 SMA connectors for external directional antennas
- RFP 47 DRC
  RFP 47 preinstalled with directional antennas in an outdoor enclosure
- RFP 48 WLAN
  DECT RFP with 8 narrow band voice channels + WLAN Access Point as indoor model with internal antennas for DECT and WLAN

The hardware of all the RFPs complies with the different regulatory domains. There are no specific hardware variants required to use specific frequency bands and field strengths. Transmit Power, frequency band and carrier frequencies are controlled by software.

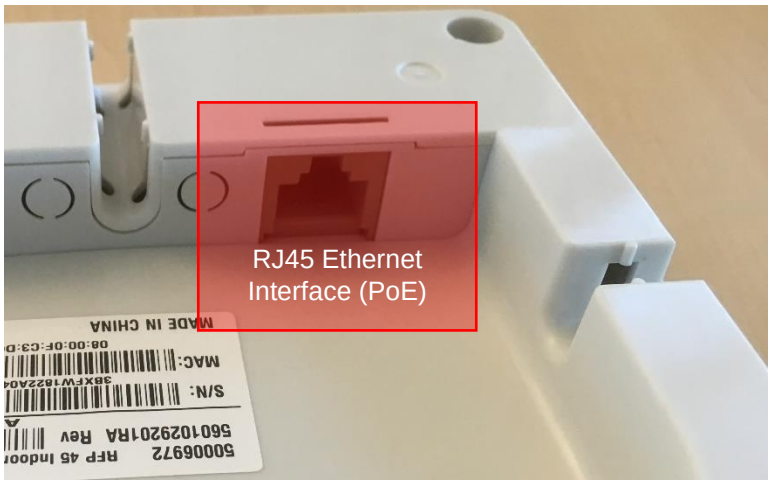


RFP 44/45/47/48
1 LED



Configuration Button used to:

- Switch to SIP-DECT with Cloud-ID mode
- reset RFP to factory defaults



RFP 44,45,47: 100Mbit/s Ethernet interface, PoE
RFP 48: 1Gbit/s Ethernet interface, PoE

Differences compared to the 3rd RFP generation family (RFP 35,36,37 IP and RFP 43 WLAN) are:

- RFP 48 WLAN supports 5GHz WLAN according to 802.11ac and 3x3 MIMO
- Configuration button
- Separate outdoor enclosure available for outdoor usage
- No external power supply (PoE only)
- No USB interface

There are no differences regarding the SW update process compared with the 3rd RFP generation, except a SW update via USB is not possible because the RFP4G does not come with a USB interface.

One SW for SIP-DECT and SIP-DECT with Cloud-ID

As of SIP-DECT 8.0 the SIP-DECT can operate in the standard SIP-DECT mode or in the SIP-DECT with Cloud-ID (SDC) mode. There is no specific SIP-DECT with Cloud-ID SW anymore.

The standard SIP-DECT mode is the default mode. After reset to factory defaults, a base station operates in the SIP-DECT mode.

The RFP configuration button is used to switch to the SDC mode and to appoint the RFP to be the SDC OMM.

3rd generation RFP houses the OMM

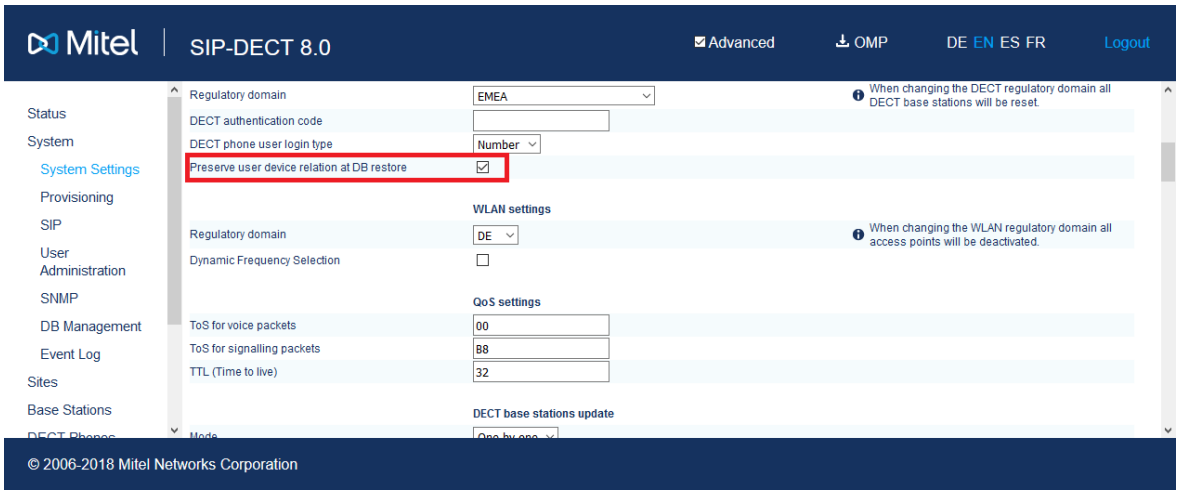
The 3rd generation RFPs can house the SIP-DECT 8.0 OMM as in previous releases. The OMM supports the 2nd, 3rd and 4th generation RFPs.

4th generation RFP houses the OMM

As the 4th generation RFPs come with more HW resources in terms of CPU speed and memory, it is strongly recommended to operate the OMM on a 4G RFP.

Note: If you move the OMM and you want to keep the existing dynamic user phone relation which is stored in the OMM DB backup file then activate the option "Preserve user device relation at DB restore" in the new OMM. The new OMM will restore the relation between the user and the DECT phone during DB import.

If this option is not set, then all dynamic user will be logged out from their DECT phones when importing the OMM DB into the new OMM.



If the OMM is operated on 4G RFP, then 1024 DECT users and phones are supported. (512 DECT users and phones if the OMM is operated on a 3G RFP).

The 4G RFP comes with the configuration button, which allows to switch to the SIP-DECT with Cloud-ID (SDC) mode. As of SIP-DECT 8.0, a 4G RFP is required to run an SDC OMM.

DECT Base station configuration files

As the previous RFP generation, the 4G RFP supports configuration files known as RFP or base station configurations files.

Such files can contain the URL for the RFP SW update.

As of SIP-DECT 8.0, the new parameter OM_SwImageUrl4G is introduced to configure the SW update URL for 4G RFPs.

The SW update URL for 3G RFPs can be configured with the existing parameter OM_SwImageUrl or the new parameter OM_SwImageUrl3G.

Example:

path to the software image

OM_SwImageUrl=ftp://login:password@server/iprfp3G.dnld

OM_SwImageUrl3G= ftp://login:password@server/iprfp3G.dnld

OM_SwImageUrl4G= ftp://login:password@server/iprfp4G.dnld

OMM Capacities and RFP support

The following table summarizes OMM capabilities:

	As of SIP-DECT 6.0		**As of SIP-DECT 8.0**	
	RFP OMM	**Linux server OMM**	**RFP OMM**	**Linux server OMM**
RFP 32/34 IP and RFP 42 WLAN	256	2048	256	4096
RFP 35/36/37 IP and RFP 43 WLAN	256	2048	256	4096
RFP 44/45/47 IP and RFP 48 WLAN	Not applicable	Not applicable	256	4096
DECT phones / users	512	4500	1024 (RFP4G OMM) 512 (RFP3G OMM)	10000

File naming conventions

The following table lists the file names for SIP-DECT software deliverables.

Software package	**As of SIP-DECT 7.1**	**As of SIP-DECT 8.0**
Software image for RFP 32/34 IP / RFP 42 WLAN	iprfp2G.tftp	iprfp2G.tftp
Software image for RFP 35/36/37 IP / RFP 43 WLAN	iprfp3G.dnld	iprfp3G.dnld

Software package	As of SIP-DECT 7.1	As of SIP-DECT 8.0
Software image for RFP 44/45/47 IP / RFP 48 WLAN	Not applicable	iprfp4G.dnld
OMM software for Linux Red Hat server (self-extracting executable)	SIP-DECT_<version>.bin	SIP-DECT_<version>.bin
OMM software rpm	SIP-DECT-OMM-<version>.i686.rpm	SIP-DECT-OMM-<version>.i686.rpm
DECT phone firmware rpm	SIP-DECT-HANDSET-<version>.i686.rpm	SIP-DECT-HANDSET-<version>.i686.rpm
SIP-DECT OMM/MOM OVA	SIP-DECT_<version>.ova	SIP-DECT_<version>.ova

Login and passwords

The following table summarizes the default login and passwords for SIP-DECT system components.

Interface/Tool	SIP-DECT OMM SDC OMM	RFP 32/34 IP / RFP 42 WLAN	RFP 44/45/47 IP / RFP 48 WLAN RFP 35/36/37 IP / RFP 43 WLAN
Initial configuration via OM Configurator login / password (no previous connection with the OMM)	n/a	No login required	“omm” / “omm”
Initial OMM configuration via Web or OMP standard full-access account login / password	“omm” / “omm” “Omm”/ “Omm”	n/a	n/a
OMM access via Web or OMP (after initial OMM configuration)	Read-only or full-access accounts as configured	n/a	n/a
Configuration via OM Configurator after connection with OMM login / password (system-wide set by OMM)	n/a	OMM standard full-access account login / password	OMM standard full-access account login / password
ssh (no previous connection with the OMM)	n/a	User shell: “omm” / “omm” Root shell: “root” / “22222”	User shell: “omm” / “omm” Root shell: “root” / “22222”

Interface/Tool	SIP-DECT OMM SDC OMM	RFP 32/34 IP / RFP 42 WLAN	RFP 44/45/47 IP / RFP 48 WLAN RFP 35/36/37 IP / RFP 43 WLAN
ssh (with previous connection with the OMM) (system-wide set by OMM)	n/a	User shell: OMM standard full-access account login / password Root shell: as configured	User shell: OMM standard full-access account login / password Root shell: as configured

OMM Standby configuration

OMM standby configuration must be built of the same RFP generations. Valid configurations are:

- RFP4G <- Standby -> RFP4G
- RFP3G <- Standby -> RFP3G
- Linux Server/OVA <- Standby -> Linux Server/OVA

As in previous releases, an OMM standby configuration is not available for SIP-DECT with Cloud-ID i.e. in SDC mode.

DECT base station SW image from OMM RFP

As of SIP-DECT 6.0, RFP3G base stations can load their software image directly from the connected OMM RFP3G to simplify the upgrade process for installations in provider environments. If an RFP has no valid URL from where to load the software, they attempt to load the software from the connected OMM. If the OMM is running on an RFP, the OMM RFP delivers its software to the connected RFPs.

As of SIP-DECT 8.0, an OMM RFP4G provides SW images for RFP3G and RFP4G base stations. Because the RFP3G is not able to hold the RFP4G SW image, an OMM RFP3G cannot provide the iprfp4G.dnld to an RFP4G.

RFP4G reset to factory defaults

The configuration button can be used to reset the RFP to factory defaults. After the reset to factory defaults, the RFP operates in the standard SIP-DECT mode.

Press configuration button to starts the configuration process. The LED starts flashing green to indicate that the button is pressed. Keep the button pressed until it starts flashing red (10 sec < t < 15 sec).

Release the button while the LED is flashing red to reset the RFP to factory defaults.

The RFP performs a reset to factory defaults and reboots. After reboot the RFP is started in the standard SIP-DECT mode.

Note: If the button is pressed until it is flashing green again then the button has no effect.

Support of 802.11ac-WLAN for RFP48 WLAN

The RFP48 WLAN has a new WLAN module which supports the WLAN ac mode wave 1. Within the 5 GHz spectrum the ac mode is 2,5x faster as the n mode of WLAN. Compared with the RFP43 with its only two antennas, the RFP48 is 4x faster. This is achieved by more efficient coding (256-QAM), more bandwidth (HT80) per channel and one more antenna (3x3 MIMO compared to the RFP 43: 2x2 MIMO).

For more information about data rates please see: http://mcsindex.com/

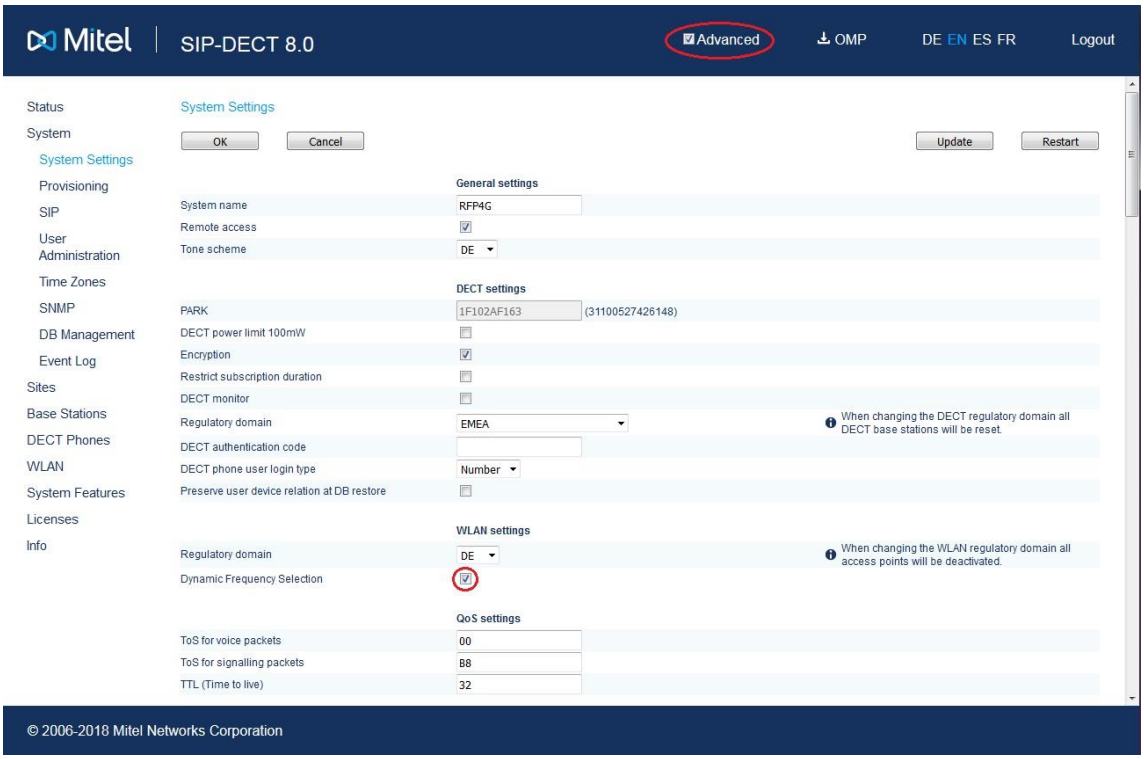
802.11ac is backwards compatible with 802.11a and n. Like the RFP43, the RFP48 can only work in one WLAN spectrum at the same time (2.4 GHz or 5 GHz). Within the 2.4 GHz spectrum the WLAN module supports the 802.11b/g/n modes in the same way as the RFP43.

The WLAN module of RFP48 supports Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC). These features are required for the radar detection (flight and weather) and are necessary to use the WLAN channels 52 – 140 in Europe and USA. If radar pattern detected, the RFP48 changes its WLAN channel by itself to another channel without radar for a half hour.

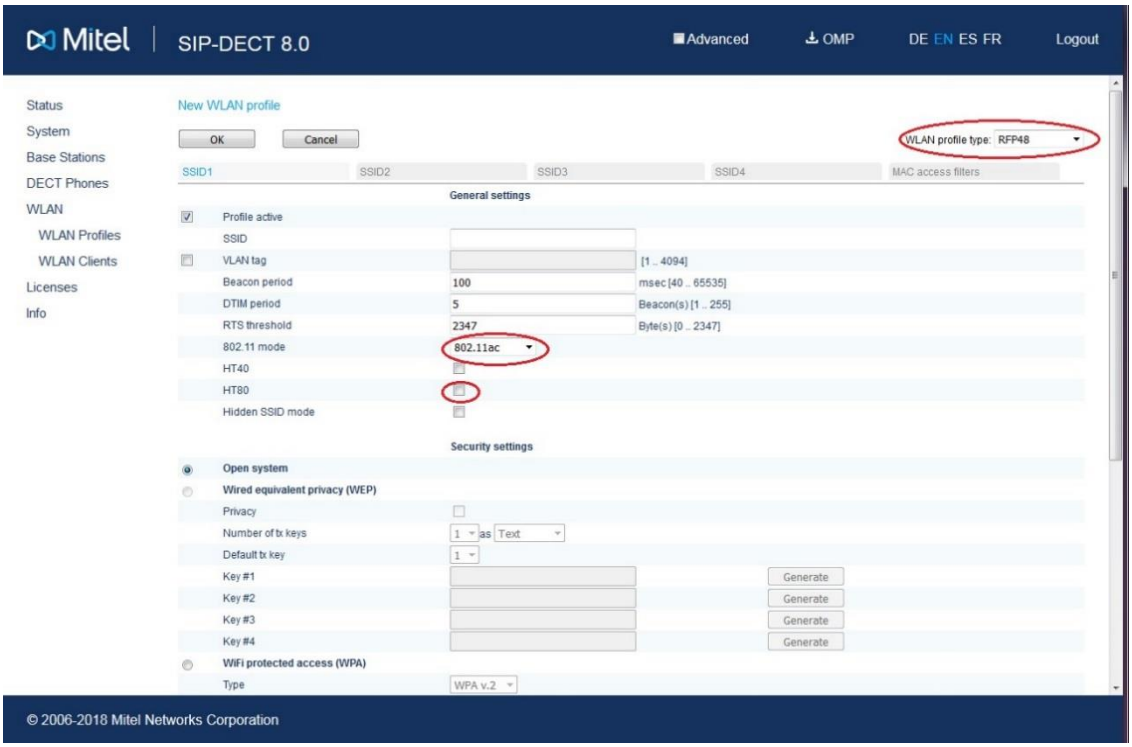
The 5 GHz high band with its channels 149 – 165 is supported too.

Configuration items:

- to enable the DFS channels: System/System Settings (Advanced)

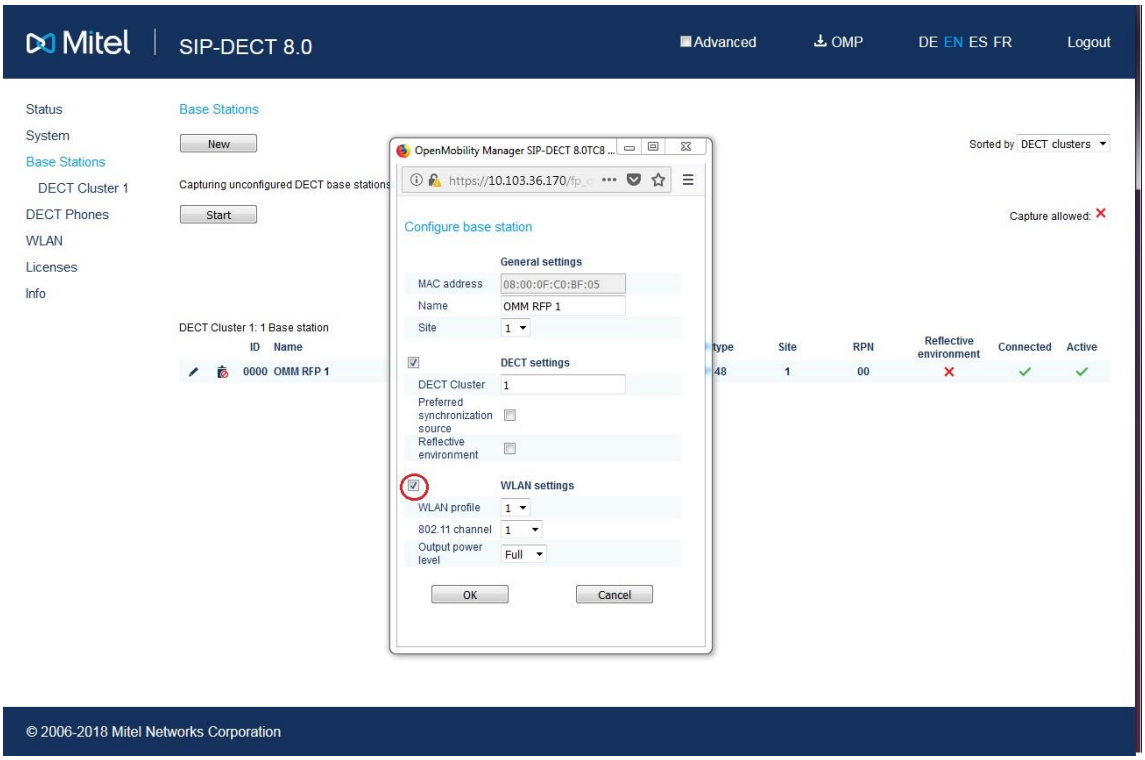


- to enable the ac mode and HT80: WLAN\WLAN Profiles (new/edit)



HT80 includes the HT40/HT20 bandwidth setting. A channel with a bandwidth of 80 MHz occupies 4 WLAN channels with a bandwidth of 20 MHz.

- to activate WLAN and to set the WLAN profile / channel / power level for a base station (edit):



The selectable WLAN channels have a default bandwidth of 20 MHz. If the WLAN profile options HT80/ HT40 MHz have been activated, the necessary center channel will be automatically selected in the corresponding areas by configuration itself.

In the 2.4 GHz band, a channel with 40 MHz bandwidth is only established if no other 20 MHz channel is disturbed. Otherwise, a fallback to 20 MHz bandwidth will be made.

WLAN is a shared media. It is depending on the application, if it may to be useful to have 4 RFPs with a bandwidth of 20 MHz – example: canteen – or to have one RFP with a bandwidth with 80 MHz – example: video conference room.

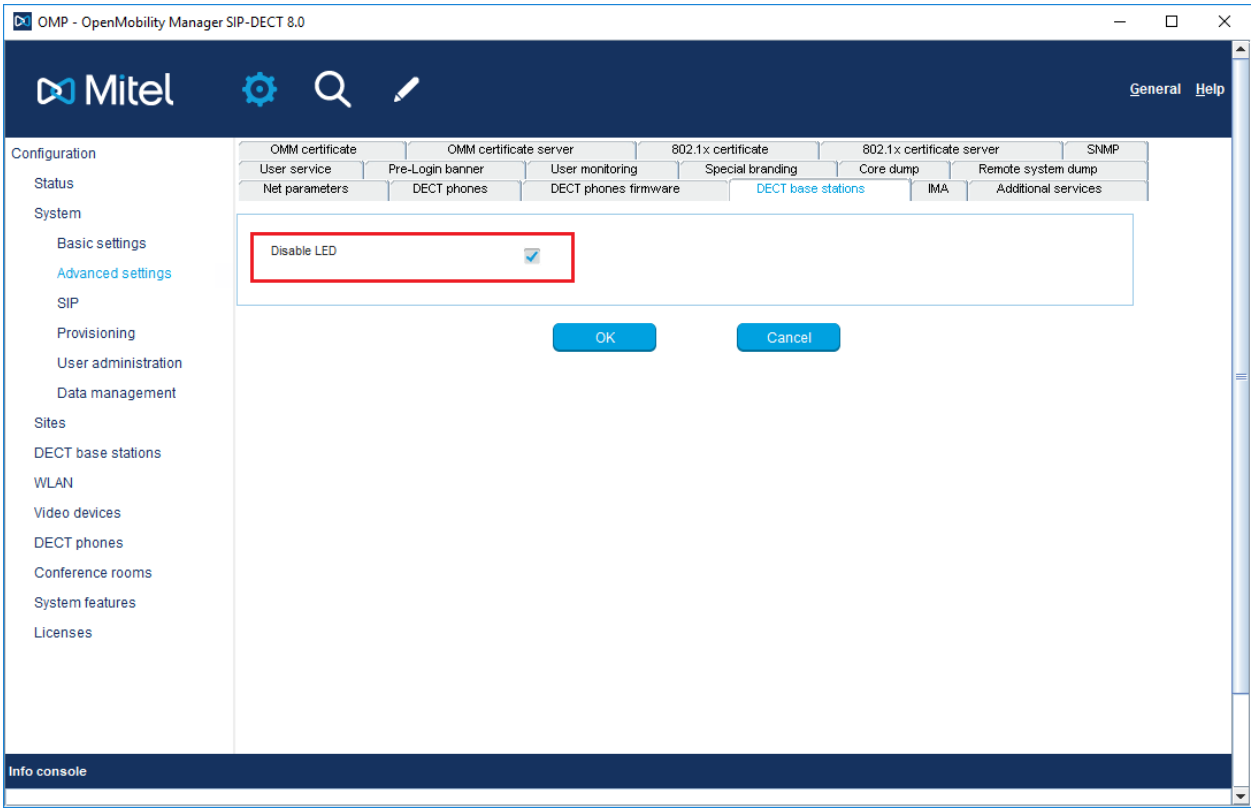
RFP4G LED states

The new RFP family is equipped with one colored LED, which shows the individual states of the 4th generation RFP.

LED color/rhythm		Description
continuous		Booter phase
continuous		Kernel boot phase
1s	1s	Configuration phase
1,9s	0,1s	DHCP failure (idle loop)
continuous		System up and Running (with or without OMM)
1s	1s	OMM connection phase
continuous		OMM connected
1s	1s	DECT inactive (not synced yet)

continuous		DECT “on air”
continuous		WLAN “on air”
1s	1s	DECT inactive (not synced yet) + WLAN “on air”
continuous		DECT + WLAN “on air”
0,1 sec	0,1 sec	Button pressed : 0 sec < t < 3 sec = no action
0,1 sec	0,1 sec	Button pressed : 3 sec < t < 8 sec = Activate Cloud-Id
0,1 sec	0,1 sec	Button pressed : 8 sec < t < 10 sec = no action
0,1 sec	0,1 sec	Button pressed : 10 sec < t < 15 sec = Factory Reset
0,1 sec	0,1 sec	Button pressed : 15 sec < t < oo = no action

Option to turn off the RFP4G LED

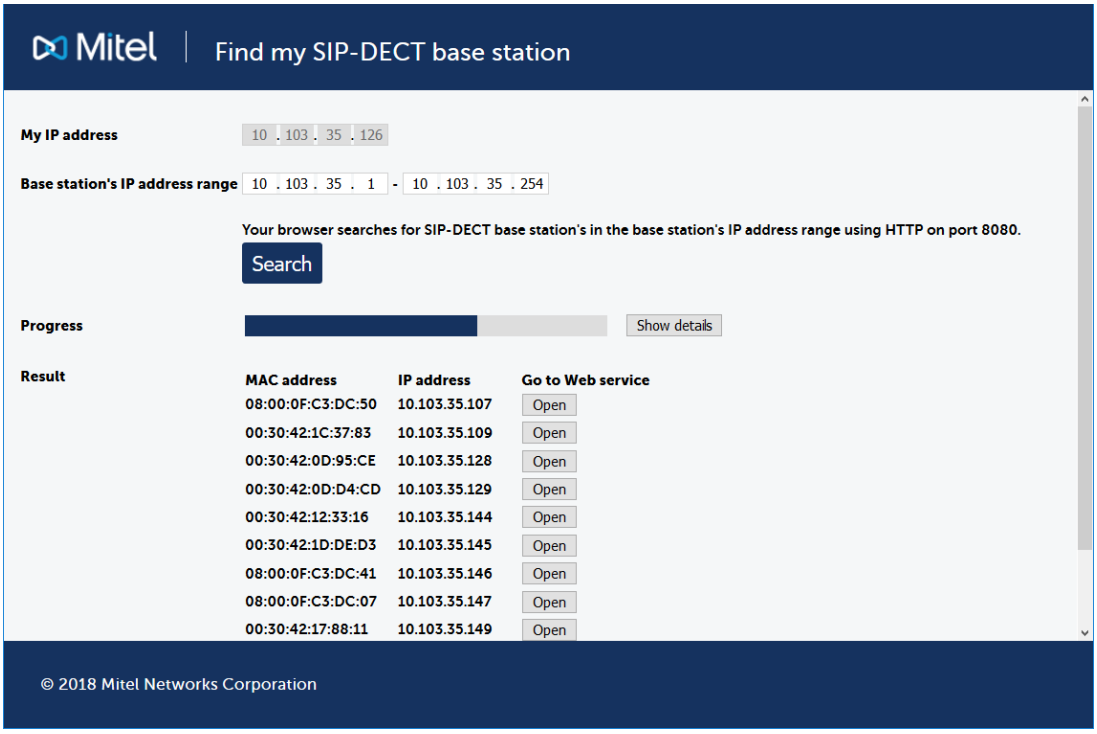


It is possible to disable the LED for the active DECT and WLAN states.

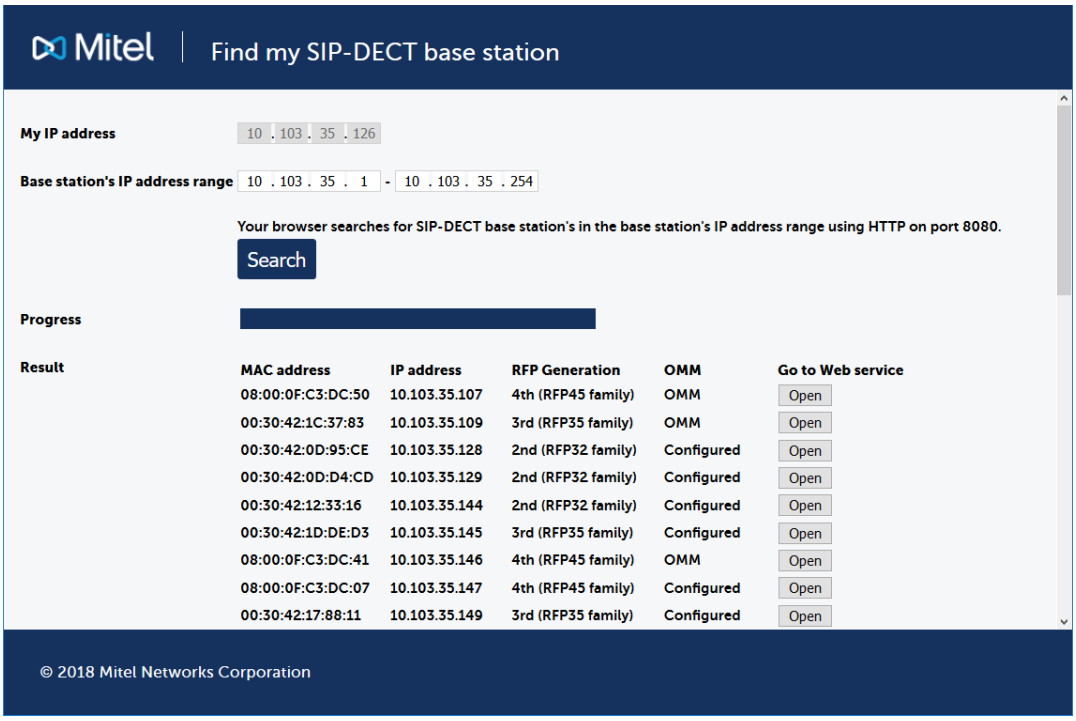
Find my SIP-DECT base station

“Find my SIP-DECT base station” is a java script application which will scan the local customer network for RFPs running a SIP-DECT 8.0 SW or higher. This helps to determine the IP addresses of the base stations assigned by DHCP. The java script of “Find my SIP-DECT base station” is executed in a Web browser from a local drive. Download and extract the FindMySIP-DECTbasestation.zip and open the index.html.

If supported by the browser, the IP address of the client PC will be determined automatically, and the search IP range will be initialized automatically. Otherwise the customer needs to enter the IP range.

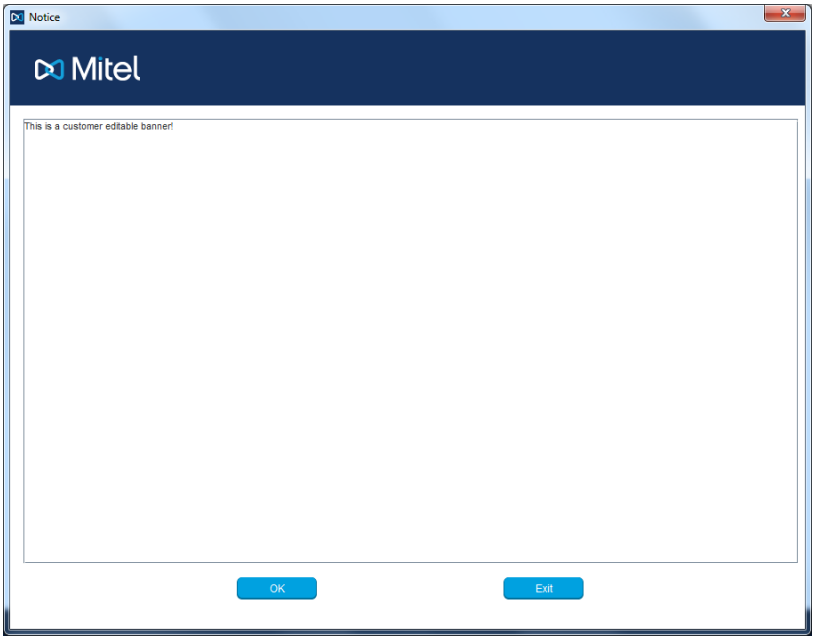


The results will be listed with the base station MAC address, IP address and optionally the RFP generation and configuration state. The configuration web GUI of the OMM running on the base station or the base station is assigned to, can be opened by pressing the ‘Open’ button of the listed data record.

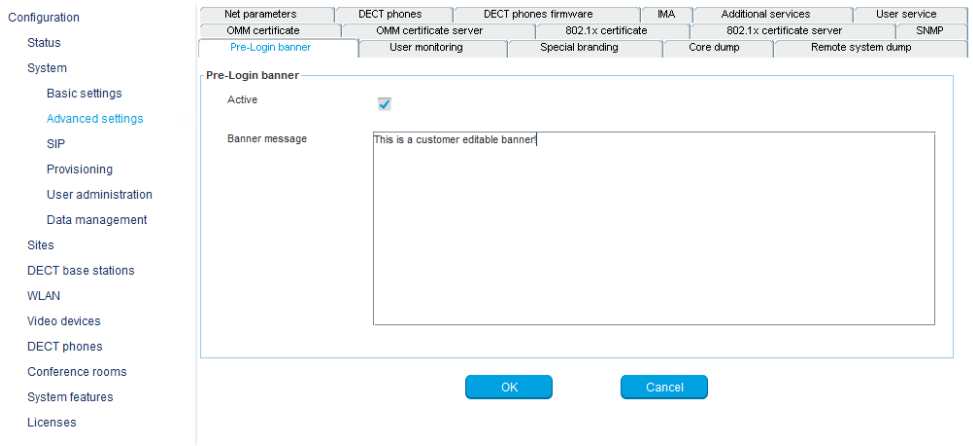


MSD-127 Customer editable banner to be displayed prior to login on every management UI

There is an optional customer editable banner available which allows to display security notes or similar on OMP and OMM's Web interface prior to login.



The banner can be modified and activated via OMP.



MSD-143 Reset DECT phone key lock PIN to default "0000" and delete call filter on user logout

As of SIP-DECT 7.1SP1 and 8.0, the DECT phone key lock PIN to protect the Mitel 600d DECT phone is reset to default "0000" on user logout to improve usability in shift worker scenarios. Additionally, call filter which were set from the user are removed.

MDP-26 Lock Mitel DECT Phone USB interface when key lock with PIN is active

The Mitel 600d DECT Phone USB interface is automatically locked when the phone is locked with a PIN.

If the phone was already connected via USB before the lock, then the connection remains active.

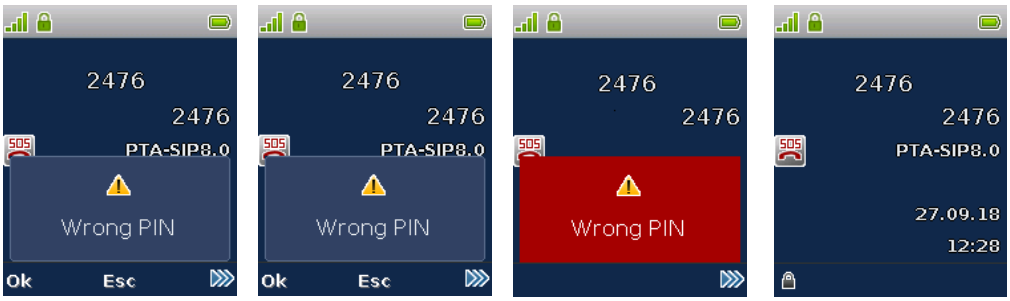
MDP-25 Timeout if wrong PIN entered more than 3 times.

There is a timeout of 60 seconds after the third failed attempts to unlock the device to prevent a security attack by entering all possible PINs.

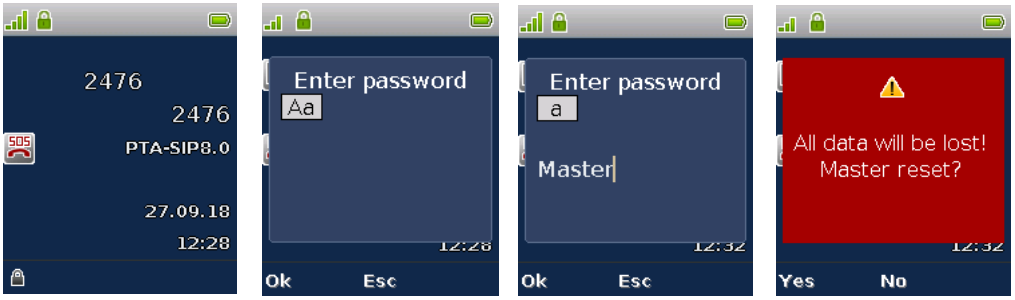
MDP-7 Manual reset of a locked Mitel 600d DECT phone

As of SIP-DECT 7.1SP1 and 8.0 together with DECT phone SW 7.2, the DECT phone can be reset to factory defaults if the DECT phone is protected with a PIN and no other option can be used to unlock the phone e.g. set the PIN via the OMM to a defined value.

If a wrong PIN were successively entered 3 times, then a reset procedure can be activated by entering the code “***778#”.



1. Wait until the red window disappears and the DECT phone returns to the idle state



2. Enter the code “***778#” to start the reset procedure

3. Enter the password “Master”

4. Confirm the reset of the DECT phone data.

The reset procedure resets all data on the phone, which also removes the subscription and the PIN lock.

The DECT phone needs to be subscribed with a DECT system after the reset.

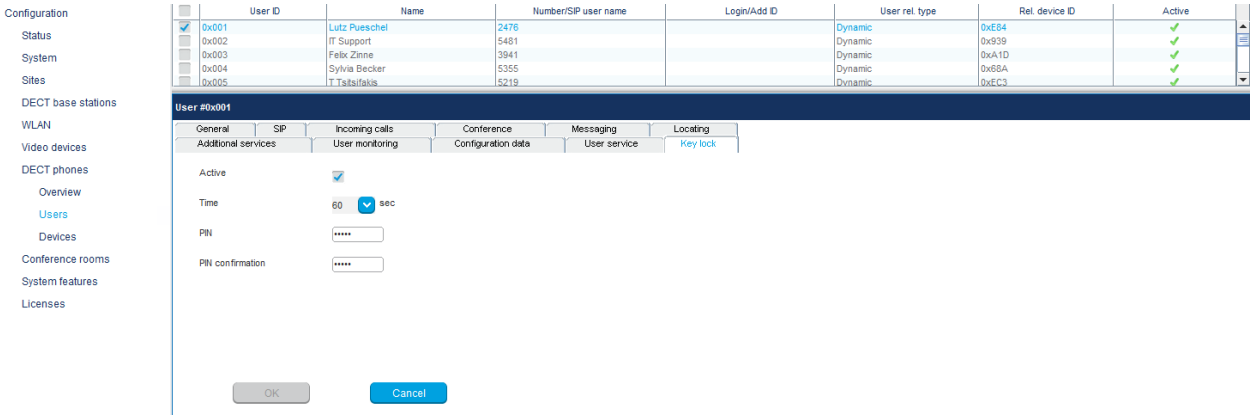
MSD-144 Local DECT phone key lock handling with PIN replaced by OMM key lock management

The Mitel 600d DECT phone family offers an optional PIN to protect the DECT Phone. As of SIP-DECT 8.0 and the DECT phone SW 7.2, the key lock PIN is managed by the OMM to improve the shift worker support and the roaming between OMMs in a MOM setup.

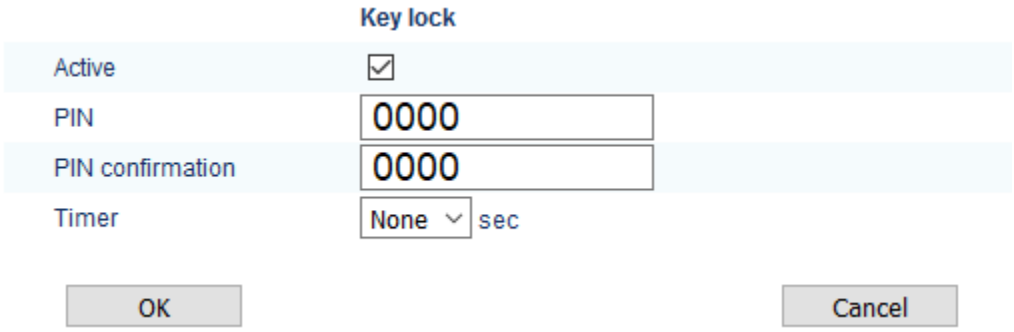
The local DECT phone key lock PIN settings are suppressed if the DECT phone is subscribed with a SIP-DECT system.

The key lock with PIN can be managed via Web, OMP, OMM configuration files and by the user via the DECT phone UI in System menu/ Administration/ Key lock.

Please be aware, that this is not possible for external users, i.e. users who are provisioned via user.cfg file. If user data are provisioned via user.cfg files, then the provisioning platform is the data master and there is no option to update data towards the provisioning platform when changed in the SIP-DECT system. Therefore, data changes in the SIP-DECT system are prevented.



The following default values are applied when creating a new user or when upgrading from the previous release 7.1-CK14 or older.



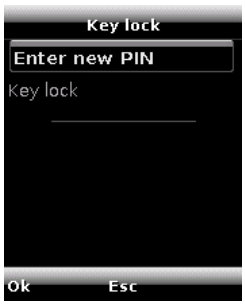
These default values result in the following system behavior:

- The Active flag set enables the Key lock menu under System menu/Administration on the Mitel 600d DECT phone
- The DECT phone default PIN “0000” is set. It is the same default PIN as for the local DECT phone feature

- The timer is set to “None” (“Off” on the DECT phone). The key lock is not automatically activated if the DECT phone is not used and the long press of the # key ()does not activate the key lock with PIN

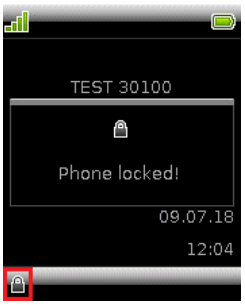
From the user perspective, the DECT phone key lock with PIN is not active by default but can be activated via the DECT phone UI.

If the active flag is not set, then the whole feature is disabled, and the possibility to set keylock is removed from the DECT phone UI. But the submenu “Enter new PIN” remains. That is necessary, because the PIN may be mandatory to open some DECT phone menus like “Security”, or others if configured by COA. The user shall have the opportunity to change the PIN by himself, even if keylock feature is disabled.



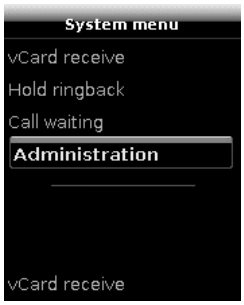
The submenu Key lock is hidden if the feature is disabled.

The following pictures show an example how to turn off the DECT phone key lock with PIN via the Mitel 600d DECT Phone UI.

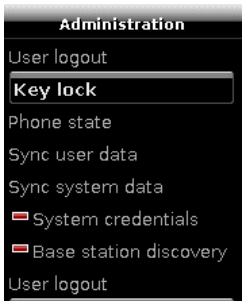


Select the lock key and enter the PIN to unlock the phone

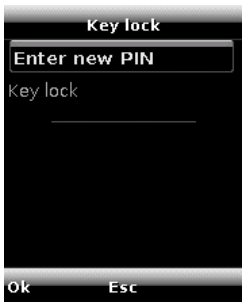
Long press of the option soft key opens the system menu



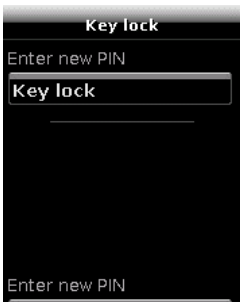
Select Administration



Select Key lock

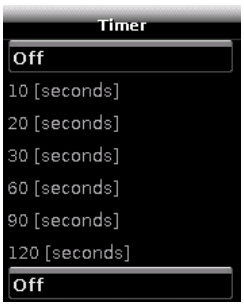


Option to change the PIN



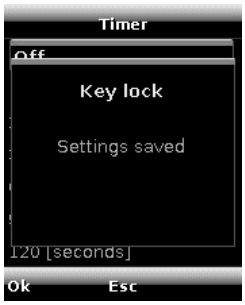
Option to change the key lock parameter

Time for the automatic key lock is set to 120 seconds



Off and various timer values are available

Choose the desired value e.g. Off and confirm with OK



Confirmation that the chosen values is stored

Key lock with PIN is turned off

The update to SIP-DECT 7.1SP1 causes a reset of the DECT phone key lock PIN to default “0000”.

Parameter / Parameter group	**Key lock: Active**
Description	Enable keylock management: Set "1" or "true", if the keylock management of the DECT phone user shall be enabled. The user can activate the automatic keylock, if the keyLockTime is unequal to 0. The manual key lock () is activated then too. Set "0" or "false", if the keylock management of the DECT phone user is disabled. Any keylock is disabled on the users DECT phone. Default value is "true".
Format	Bool
Range	True/False
Default value	True
Web	Advanced: Dect Phones
OMP/AXI	DECT Phones -> Users -> Keylock

OMM Configuration files	AXI commands:
	`<SetPPUser> <user uid="8" keyLockEnable="1"/> </SetPPUser>`
	`# keyLockEnable="1","true" # keylock management enabled`
	`# keyLockEnable="0","false"# keylock management disabled`
	<user>.cfg files:
	`UD_KeyLockEnable=1`

DECT Phone	n.a.

Parameter / Parameter group	**Key lock: Time**
Description	Set keylock time: If keyLockEnable is “true”, the keylock can be activated by setting the keylock time for the DECT phone user. The valid activation values are 10, 20, 30, 60, 90 or 120 seconds. The deactivation value is 0. Default setting is 0 seconds.
Format	Enumerated
Range	0 (None, Off), 10, 20, 30, 60, 90 or 120 seconds.
Default value	0 (None, Off)
Web	Advanced: Dect Phones
OMP/AXI	DECT Phones -> Users -> Keylock

OMM Configuration files	AXI commands:
	`<SetPPUser> <user uid="8" keyLockTime="60"/> </SetPPUser>`
	`# keyLockTime={"0","10","20","30","60","90","120"}`
	<user>.cfg files:
	`UD_KeyLockTime=60`

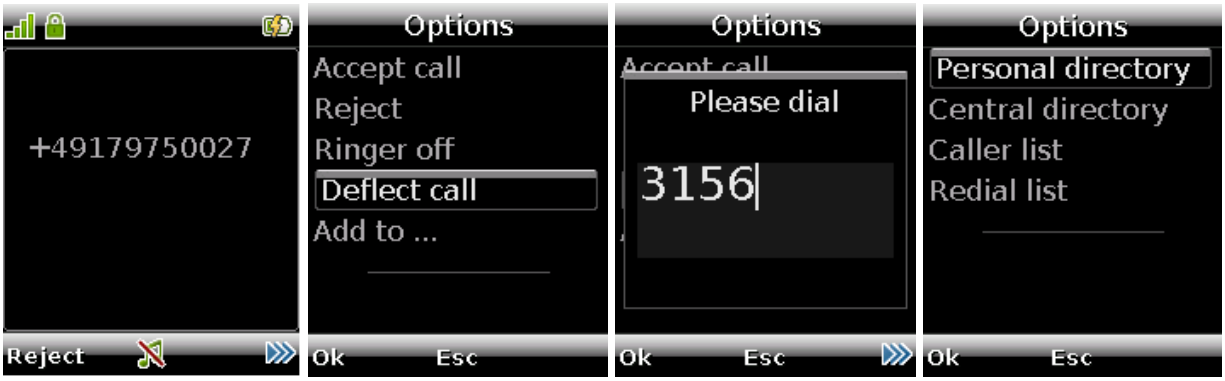
DECT Phone	Only applicable if “keylock active=true”: (long pressed “>>>” key) -> Administration->keylock->keylock

Parameter / Parameter group	**Key lock: PIN**
Description	Set keylock PIN: Key-Lock-PIN number to unlock the DECT phone. This is encrypted with the public key. Default value is “0000”.
Format	Exactly 4 digits
Range	Exactly 4 digits
Default value	“0000”
Web	Advanced: Dect Phones
OMP/AXI	DECT Phones -> Users -> Keylock
OMM Configuration files	AXI commands: <SetPPUser plainText="1"> <user uid="8" keyLockPin="4711" /> </SetPPUser > # Please note: the tag plainText="1" is mandatory for PIN # settings by AXI configuration files <user>.cfg files: UD_KeyLockPin=4711
DECT Phone	(long pressed “>>>” key) -> Administration->keylock->Enter new PIN

MSD-82 Call Deflection for incoming call in ringing state (DFR016023)

As of SIP-DECT 8.0, an incoming call can be deflected to another extension.

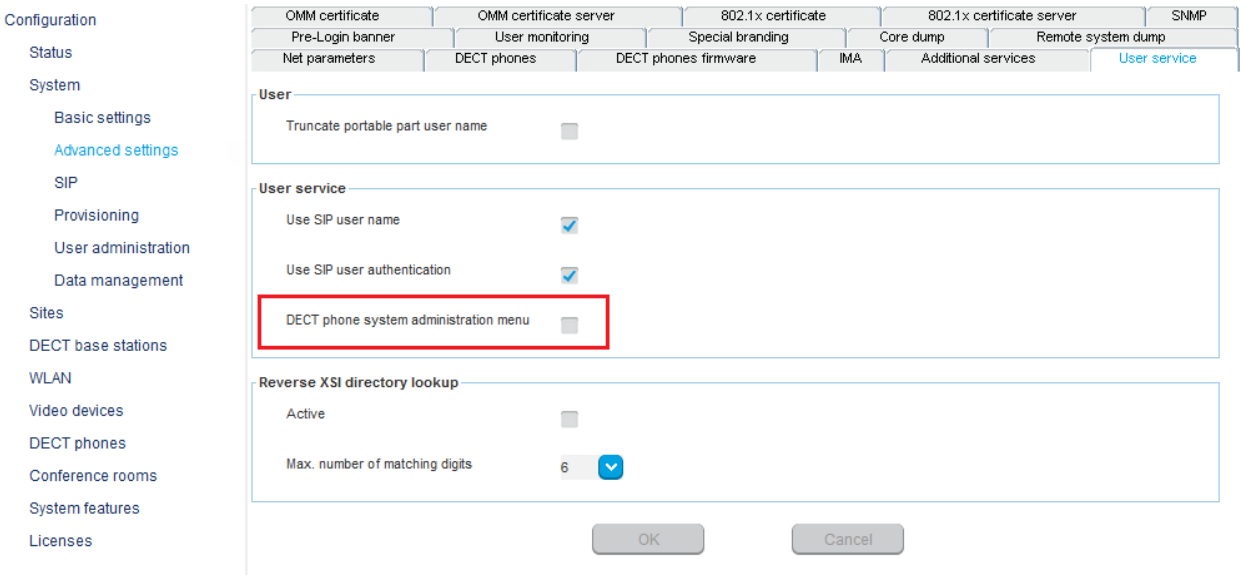
In ringing state, “Deflect call” is offered in the option menu. This option allows to enter the target extension to which the call shall be deflected. The target can also be chosen from one of the directories or call logs.



The DECT phone returns to the idle state after confirming the target extension. Depending on the actual call log management of the call server platform, the deflected call is shown as an answered or missed call.

MSD-155 Disable DECT phone UI System menu/ Administration/System and User/Devices in SIP-DECT by default

As of SIP-DECT 8.0, the access to the system configuration via the DECT phone UI is disabled by default to improve system security. It is possible to enable the menus via OMP.



MSD-92: SIP-DECT with Cloud-ID without Cloud-ID stick

Overview

SIP-DECT with Cloud-ID (SDC) is special variant of SIP-DECT for small auto-provisioned cloud deployments.

The 4th generation RFPs are not equipped with an USB interface. Therefore SIP-DECT 8.0 does not support the Cloud-ID stick anymore and a 4th generation HW is required, to run the OMM in the SDC mode.

As of SIP-DECT 8.0, there are the following necessary steps to startup SIP-DECT with Cloud-ID on a RFP4G

- Unpack RFP
- Remove back cover
- Plug Ethernet and power up RFP
- Press configuration button to appoint RFP to the OMM RFP and switch to SDC mode
- Release the button while the LED is flashing blue to switch to SDC mode
- Determine the RFP's/OMM's IP address and connect to the OMM's Web service
- Login at the OMM's Web service
- Confirm EULA
- Enter Cloud-ID key to set Cloud-ID, PARK and regulatory domain

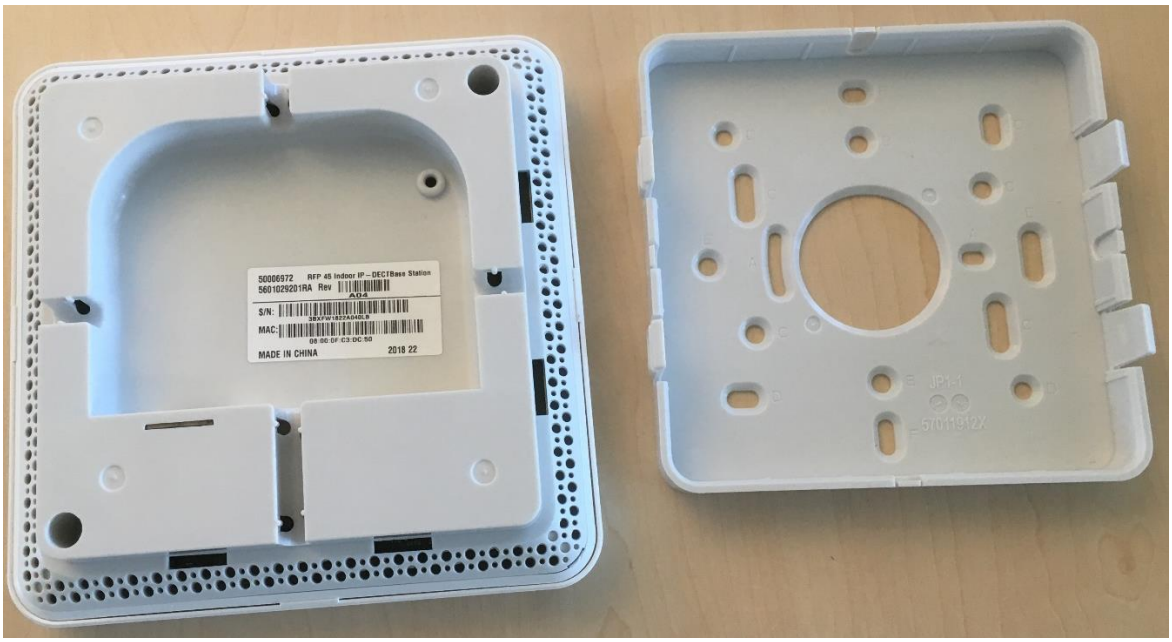
SDC 8.0 startup process

Prerequisite

I. DHCP for basic IP configuration (e.g. IP address, netmask, default GW)
II. PoE to power the RFP

Unpack RFP

Remove back cover



Plug the Ethernet cable and power up RFP

Boot Phase (LED: red)

Startup Phase (LED: yellow)

System up and running (LED: magenta)

Press configuration button to appoint RFP to the OMM RFP and switch to SDC mode

Press the configuration button to appoint RFP to the OMM RFP and switch to SDC mode (SIP-DECT with Cloud-ID mode). The LED starts flashing green to indicate that the button is pressed

Keep the button pressed until it starts flashing blue (approx. 5 sec)

Release the button while the LED is flashing blue to switch to SDC mode

The RFP performs a reset to factory defaults and reboots. After reboot the OMM is started and the SDC mode is set.

Note: If the button is pressed until it is flashing green again then the button has no effect.

Determine the RFP's/OMM's IP address and connect to the OMM's Web service

Determine the RFP's/OMM's IP address and connect to the OMM's Web service after the startup phase (LED: yellow)

If the IP address cannot be determined, then the java script “Find my SIP-DECT base station” can be used.

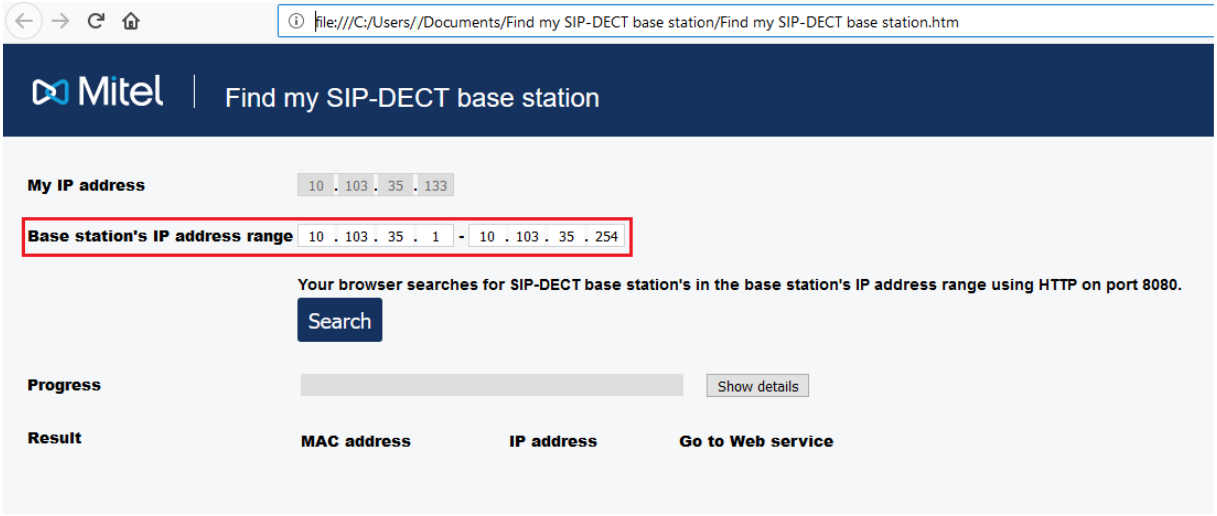
The java script of “Find my SIP-DECT base station” is executed in a Web browser from a local drive. Download and extract the FindMySIP-DECTbasestation.zip and open the index.html.

Find my SIP-DECT base station

Start “Find my SIP-DECT base station” in your Web browser

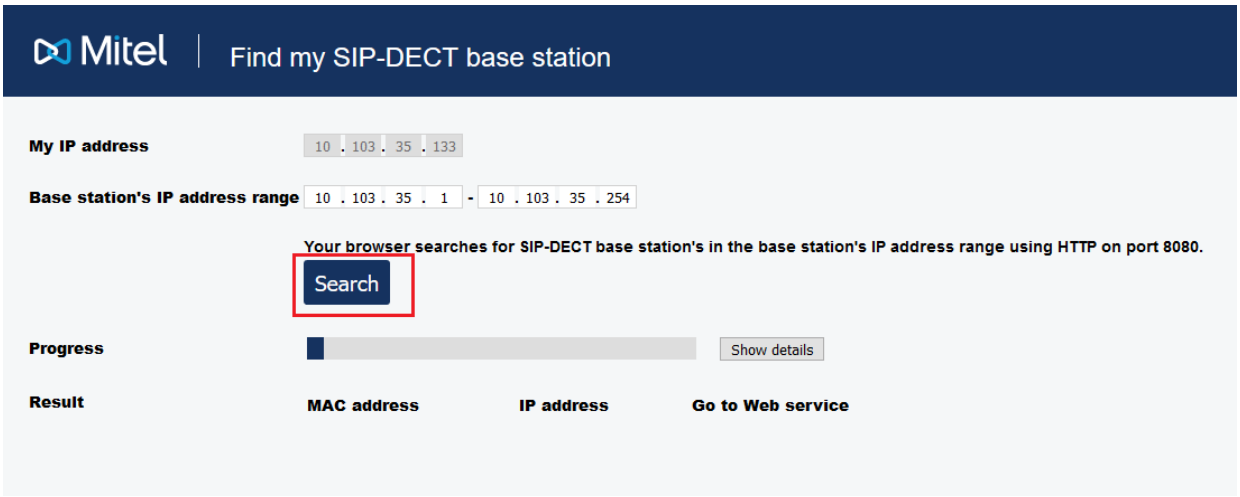
Start “Find my SIP-DECT base station” in your Web browser from the URL or from the extracted zip archive.

Check and adjust the IP address range if necessary

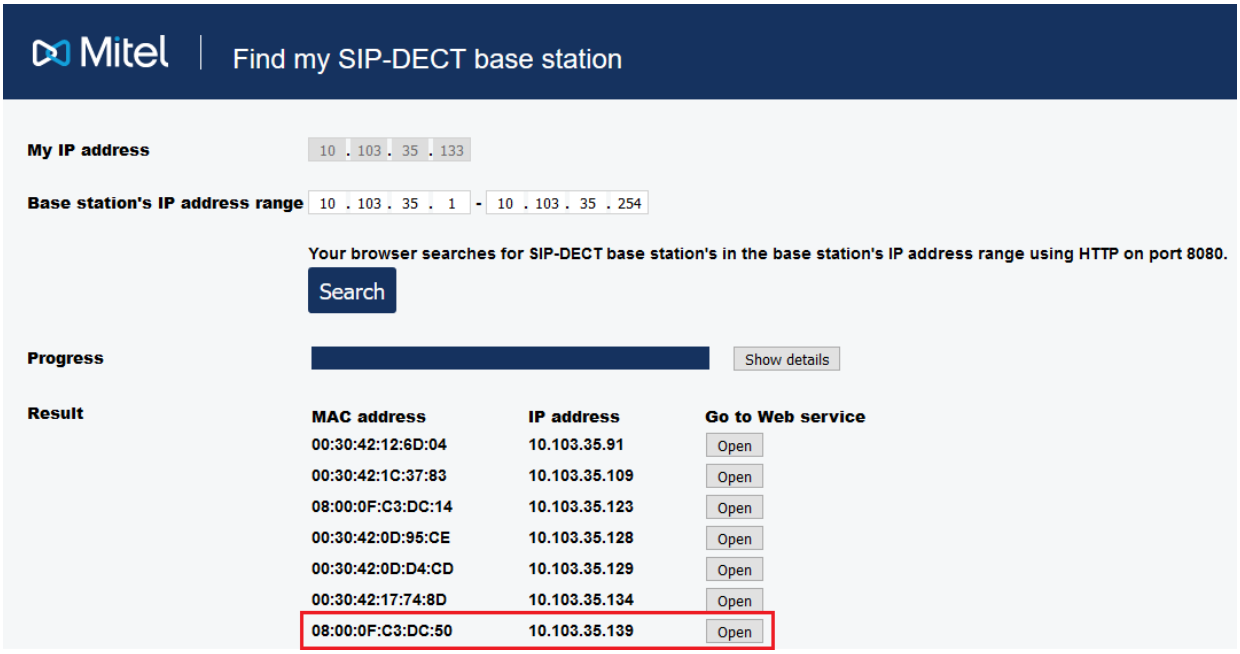


Start the search

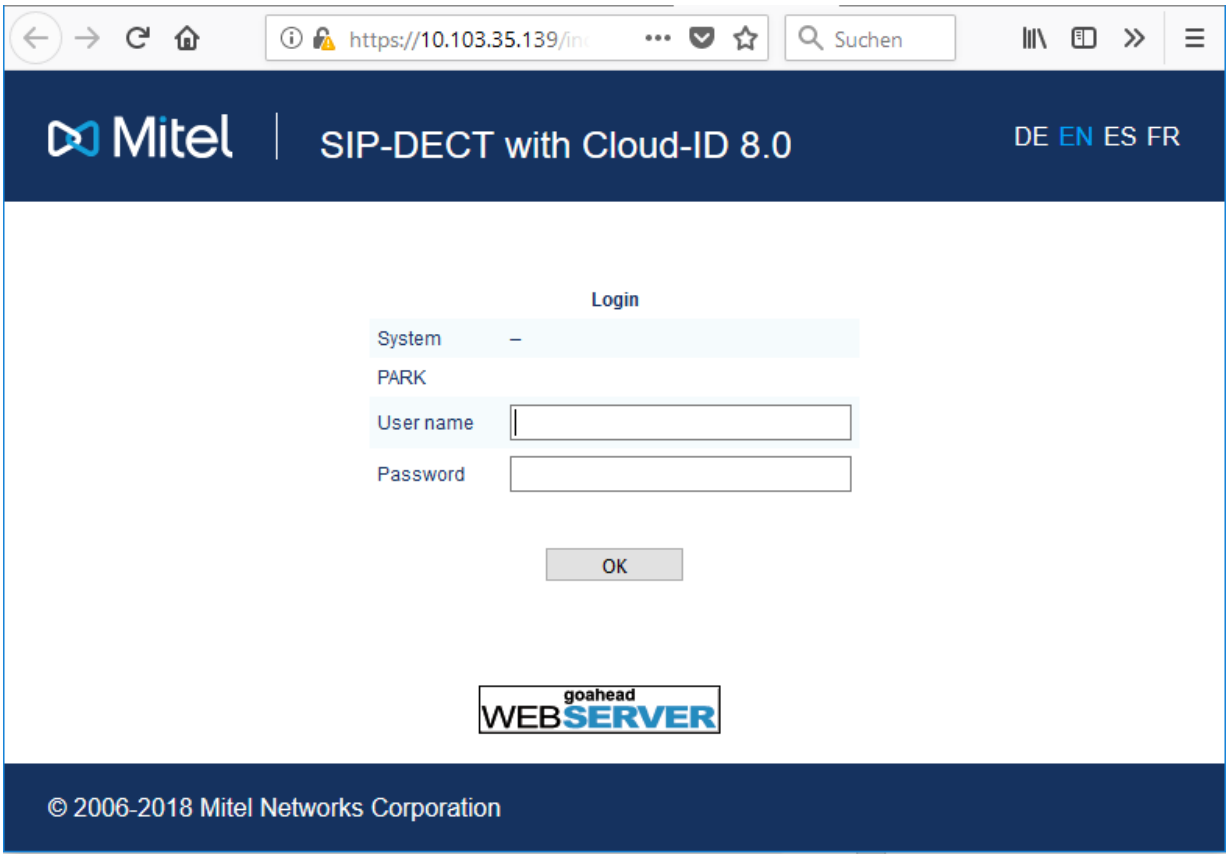
Press the search button and wait for results.



Wait for the RFP's MAC address and click on open to connect to the OMM's Web service



Login at the OMM's Web service

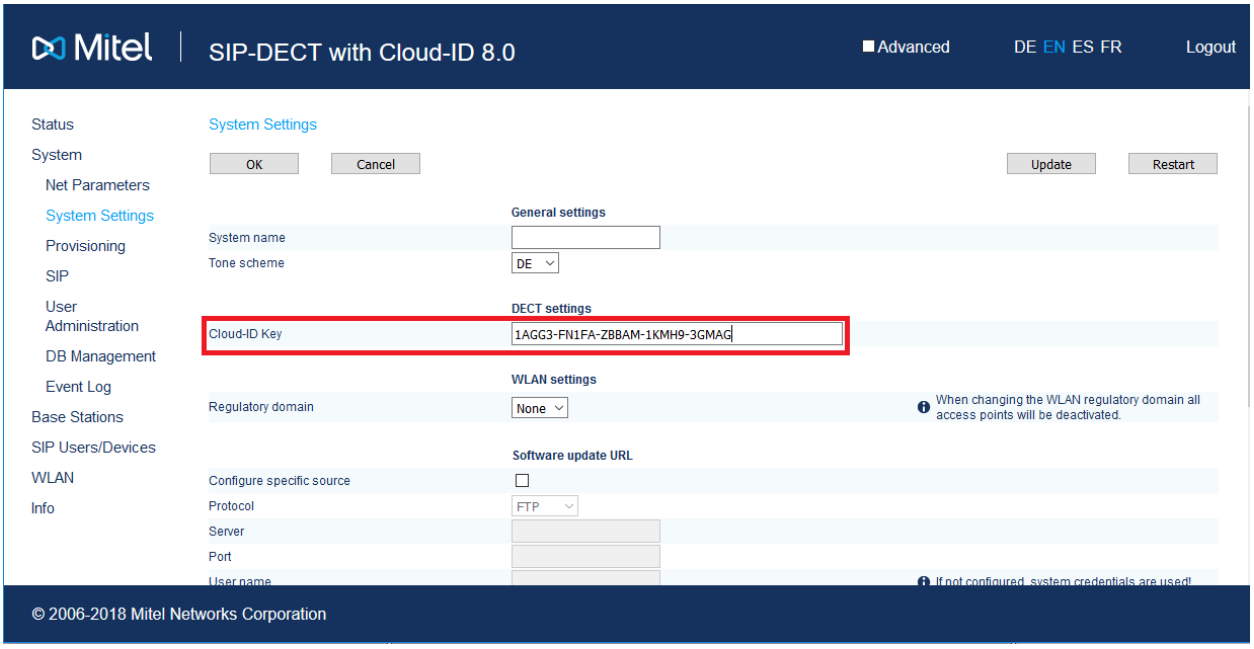


The default login and password were not changed compared with previous SIP-DECT with Cloud-ID releases. Login and password are both "Omm".

Bookmark the link to the OMM's Web service.

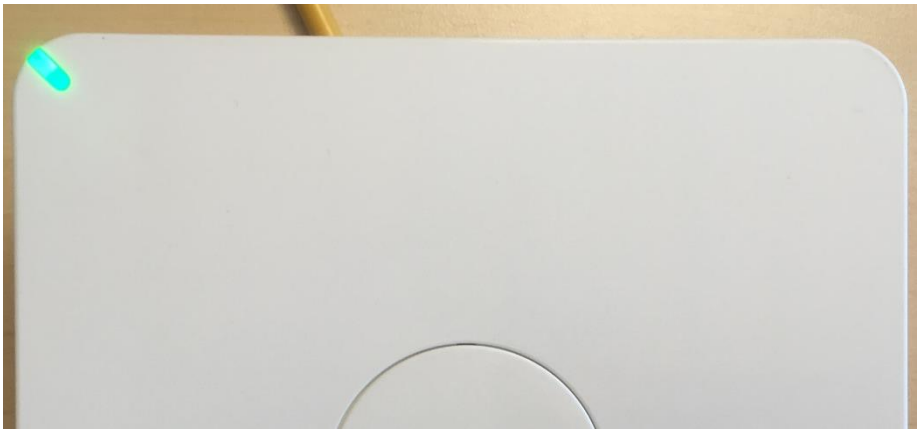
Confirm EULA

Enter Cloud-ID key to set Cloud-ID, PARK and regulatory domain



The RFP automatically restarts after applying a valid Cloud-ID Key.

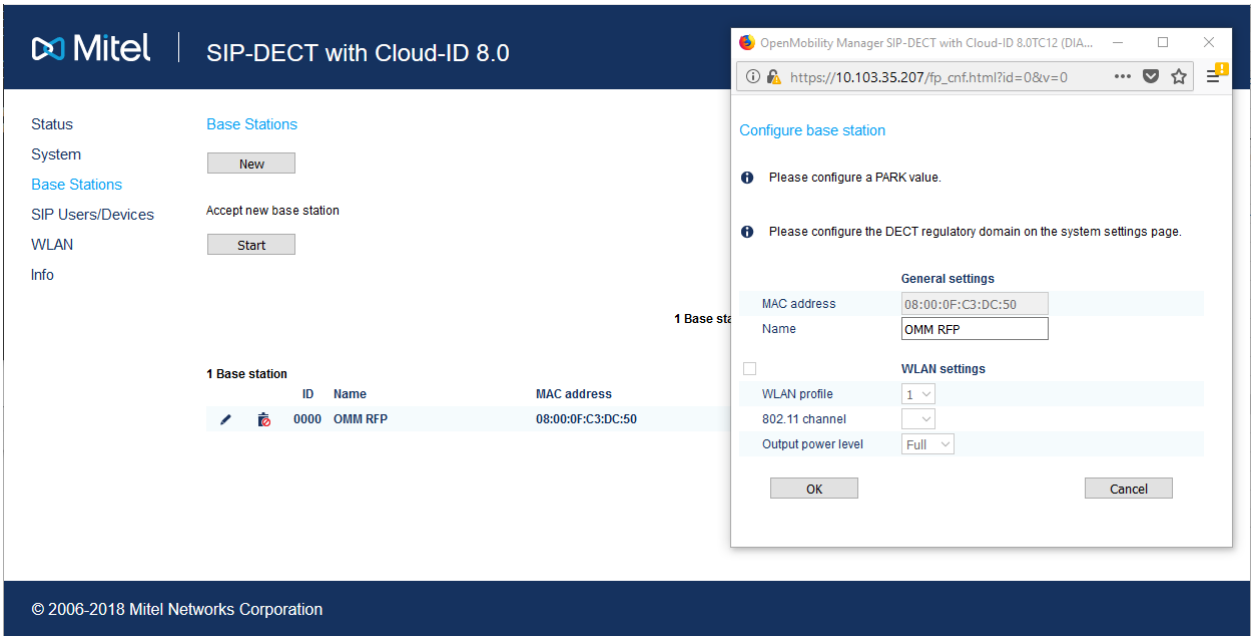
After restart the PARK is display at the Web server and the DECT air interface is active. The active DECT interface is indicated by a green LED.



At this stage, the RFP and OMM have the same operational status as the previous RFP generation after the USB stick has been plugged which causes a SW update to the SDC SW, appoints the RFP to be the OMM RFP and the Cloud-ID and applies the PARK and regulatory domain from the Cloud-ID.xml file

There is no difference regarding further configuration steps compared to previous releases.

Please be aware that the following notices regarding PARK and DECT regulatory domain will be displayed as long as no Cloud-ID key has been applied.



Operational mode of additional RFPs

The operational mode “SIP-DECT” or “SDC” of additional RFPs within an installation is managed by the OMM.

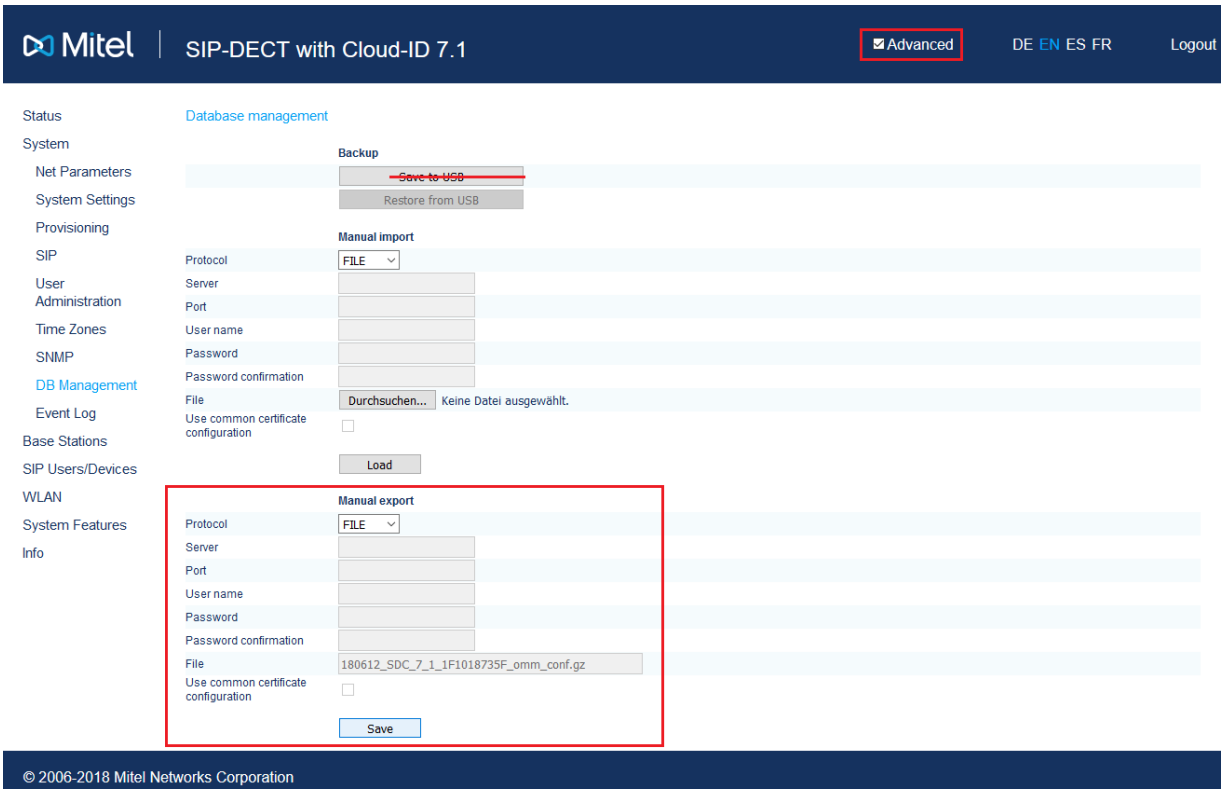
If the mode is unknown and if there is no OMM to connect to then the RFP can be reset to factory defaults via the configuration button.

Migration from RFP3G SIP-DECT with Cloud-ID 7.1

This section describes the migration from RFP3G SIP-DECT with Cloud-ID 7.1 to RFP4G SIP-DECT with Cloud-ID 8.0

There is no Cloud-ID key required to migrate from a RFP3G SIP-DECT with Cloud-ID system to RFP4G SIP-DECT with Cloud-ID as the relevant data Cloud-ID, PARK and DECT regulatory domain are stored in the OMM database.

Create OMM DB backup from RFP3G SIP-DECT with Cloud-ID 7.1



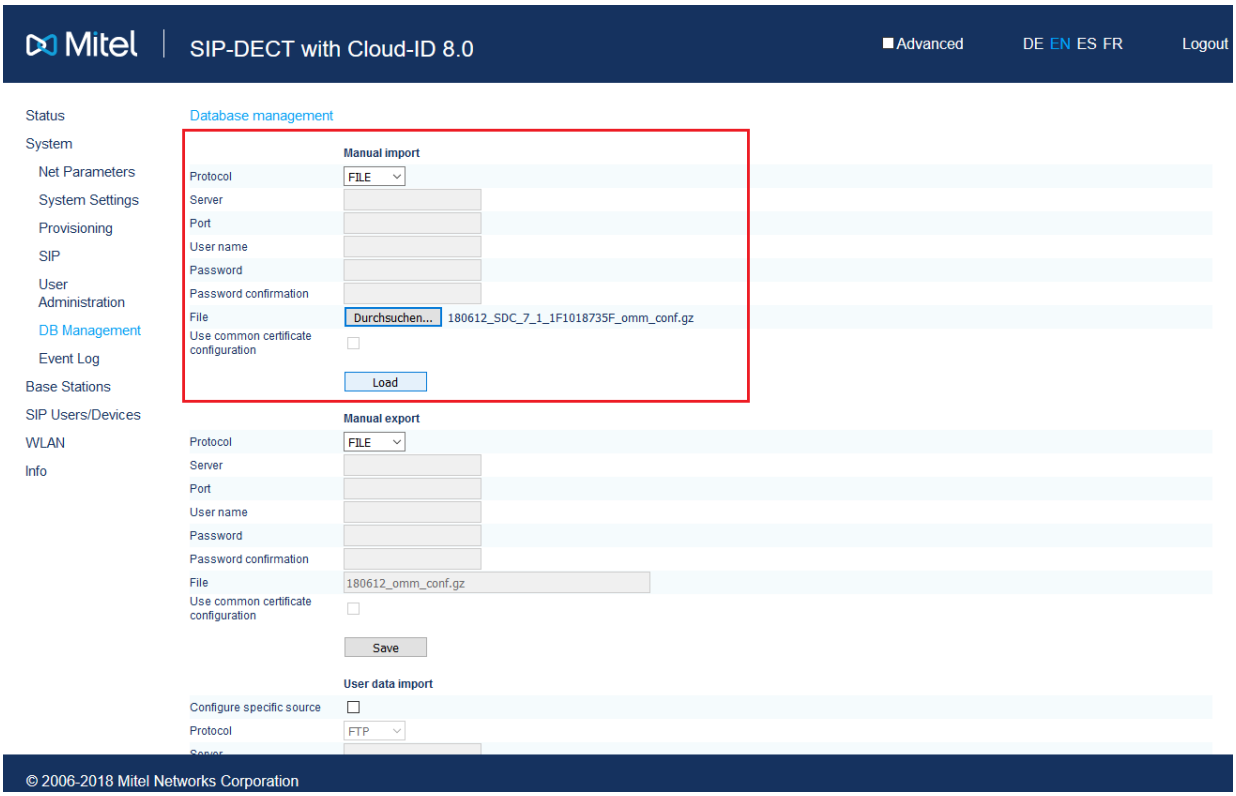
Save the RFP3G SIP-DECT with Cloud-ID 7.1 data backup on your PC. Please, use the manual export feature for this. “Save to USB” cannot be used as the RFP4G cannot restore the backup from USB.

Startup your RFP4G as a SIP-DECT with Cloud-ID OMM

Execute all steps as described in section “SDC 8.0 startup process” including to confirm the EULA.

Stop the process before “Enter Cloud-ID key to set Cloud-ID, PARK and regulatory domain”

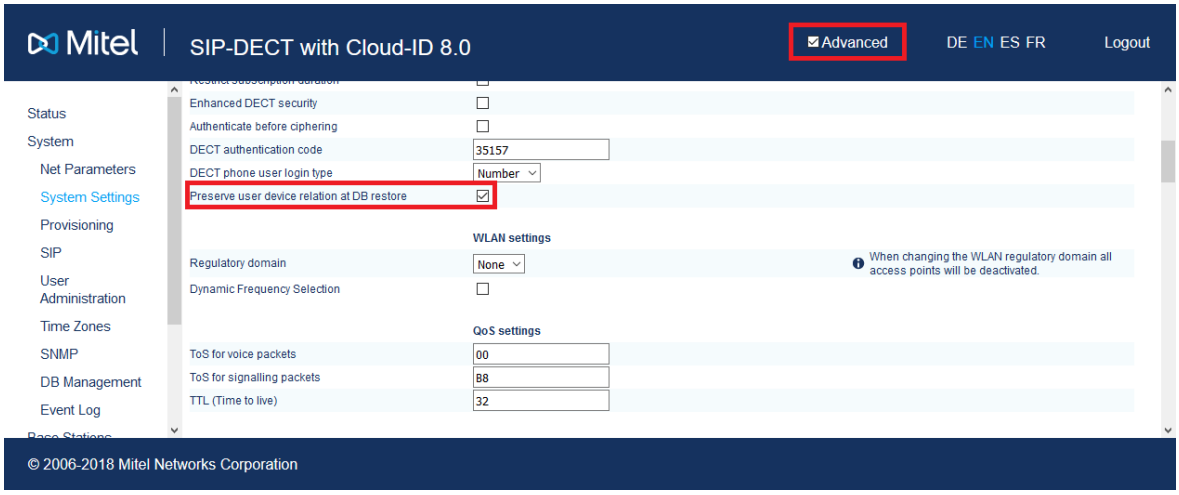
Apply the OMM DB backup from RFP3G SIP-DECT with Cloud-ID 7.1 to the RFP4G SDC OMM



Please use the manual import feature to apply the OMM database backup. The system will restart during the import process and use the Cloud-ID, PARK and DECT regulatory domain provided with the OMM database.

Note: Please activate the option "Preserve user device relation at DB restore" in the new OMM. The new OMM will restore the relation between the user and the DECT phone during DB import.

If this option is not set, then all dynamic user will be logged out from their DECT phones when importing the OMM DB into the new OMM.

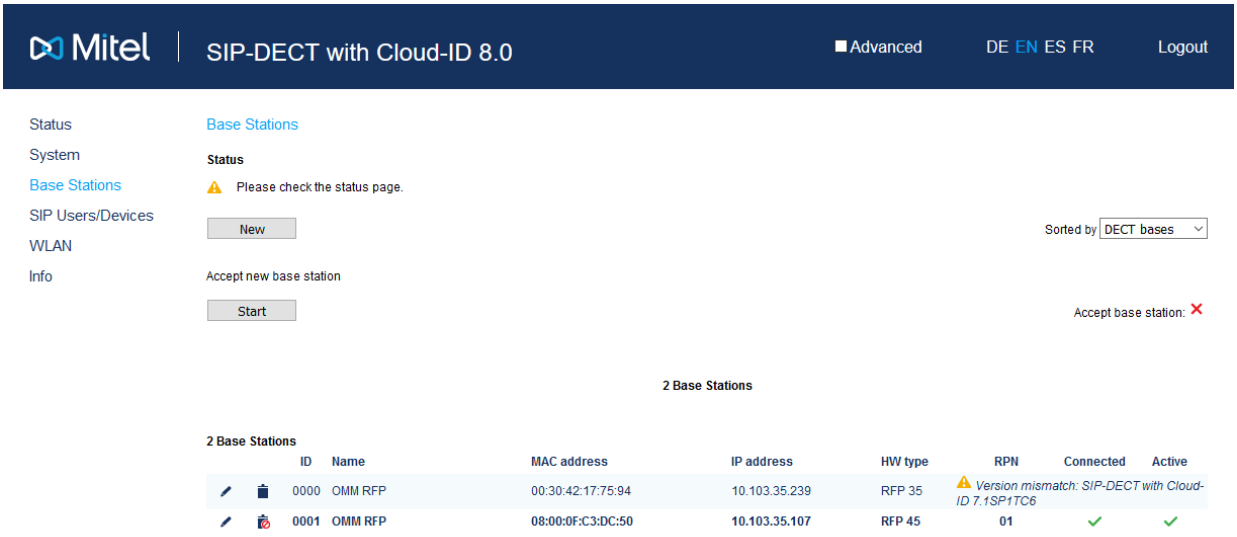


As it is not possible two SDC systems with the same identification at the same time, please put the SIP-DECT with Cloud-ID 7.1 OMM out of operation.

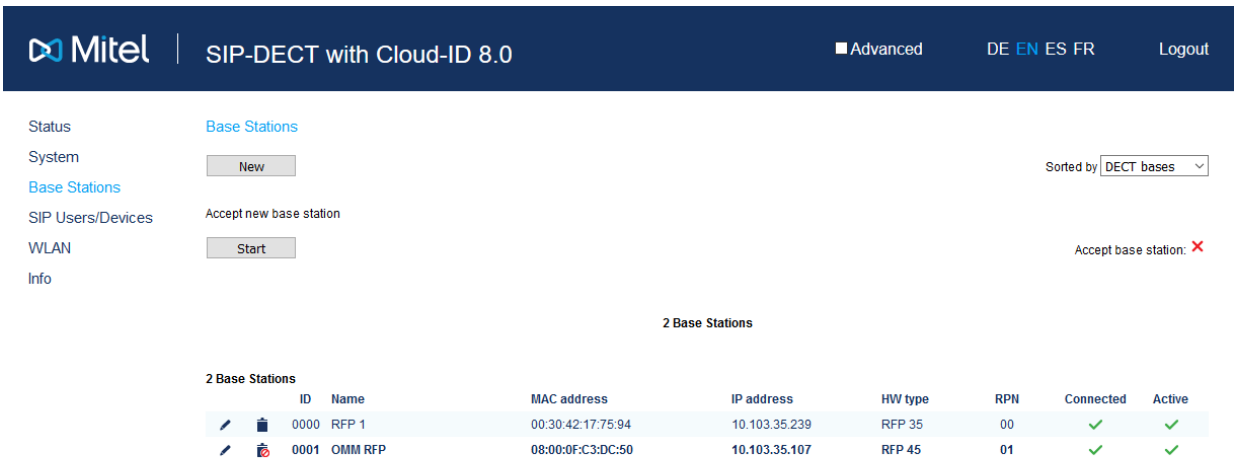
Operate the former RFP3G OMM RFP in RFP-only mode

The RFP3G, which were housing the SIP-DECT with Cloud-ID 7.1 OMM, can be operated in an RFP-only mode with the new RFP4G SDC OMM. This requires resetting the RFP3G to factory defaults, so that the RFP does not house its own OMM anymore. After reset, the RFP can be operated as any other RFP with the RFP4G SDC OMM.

The RFP automatically finds the new OMM, performs a SW update to SIP-DECT 8.0 and is put into operation.



Before the SW update, the OMM reports a SW version mismatch.

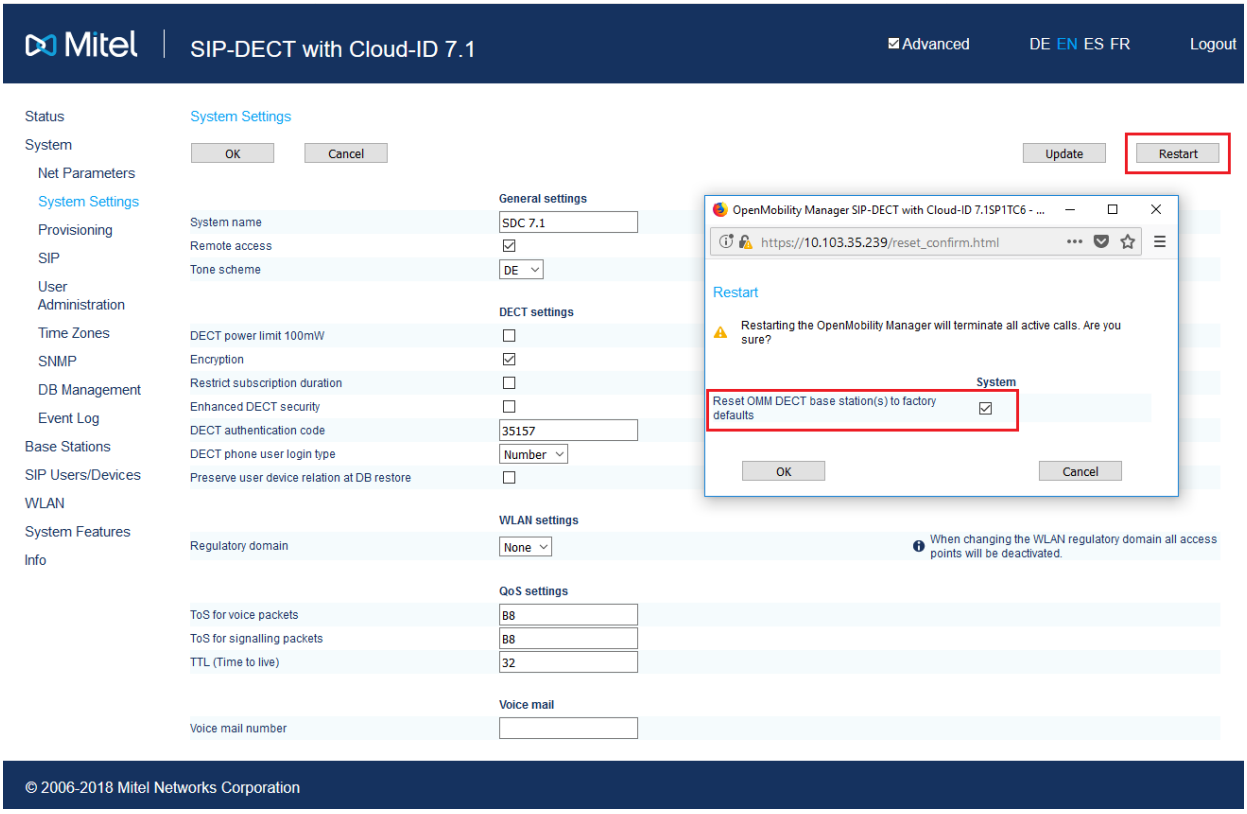


After the automatic SW update, the SW version mismatch disappears, and the RFP is automatically put into operation. The name of the previous OMM RFP can be changed to avoid confusion.

There are two options available to reset the RFP3G to factory defaults:

1. Reset to factory defaults via the OMM's Web service
2. Reset using the USB stick

Reset to factory defaults via the OMM's Web service



Execute the reset to factory defaults via the Web service of the SIP-DECT with Cloud-ID 7.1 OMM. Make sure that you remove the USB Cloud-ID stick from the RFP right after the reset is initiated to avoid that the RFP reads again the information from the stick during startup.

Reset using the USB stick

Create a file "factoryReset" on the USB Cloud-ID stick. This file must not have a file extension. Plug the stick in the RFP which houses the SIP-DECT with Cloud-ID 7.1 OMM. Remove the USB stick right when the RFP restarts to avoid that the RFP reads again the information from the stick during startup.

Operate RFP4G and RFP3G in one SDC installation

As of SIP-DECT 8.0, the OMM in the SDC mode can only be operated on a 4th generation RFP (RFP4G) e.g. RFP45.

3rd generation RFPs e.g. RFP 35 can be used in an RFP-only mode.

As in previous releases, the OMM RFP will provide SW updates to the other RFPs of the installation. SW updates are supported for both RFP generations, RFP4G and RF3G. This is possible since the RFP4G SW image (iprfp4G.dnld) includes the RFP3G SW image.

RFP3G with SIP-DECT 7.x vs. RFP4G with SIP-DECT 8.0

RFP3G with SIP-DECT 7.x	RFP4G with SIP-DECT 8.0
Cloud-ID Stick to appoint OMM RFP	Configuration button to appoint OMM RFP
Cloud-ID Stick to provide SDC SW	One SW for SIP-DECT and SDC; Configuration button to switch to SDC mode
Cloud-ID Stick to provide Cloud-ID, PARK, DECT regulatory domain	Cloud-ID key to be entered via OMM's Web service
Cloud-ID Stick to store backups beside other backup alternatives	Not applicable; other backup alternatives still available
Cloud-ID Stick to reset the RFP to factory defaults	Configuration button to initiate a reset to factory defaults
OMM provides SDC or SIP-DECT SW to connected RFPs to switch operational modes	Just one SW for both, SIP-DECT and SDC; OMM provides operational mode (**SDC or SIP-DECT)** to connected RFPs; (SW update provided from OMM RFP still maintained)
SW update via USB stick beside other SW update options	Not applicable; other SW update options still available
Subscribing a DECT phone after applying the Cloud-ID SW and Cloud-ID from stick even w/o IP configuration	Subscribing a DECT phone after switching to SDC mode via configuration button and applying the Cloud-ID key via the OMM's Web service; an IP configuration via DHCP is required to apply the Cloud-ID key
Static IP configuration via DECT phone after applying the Cloud-ID SW and Cloud-ID from stick	Static IP configuration via DECT phone after switching to SDC mode via configuration button and applying the Cloud-ID key via the OMM's Web service
Subscribed DECT phone to determine the IP address assigned to the RFP/OMM	"Find my SIP-DECT base station" Web browser script

Additional changes since SIP-DECT 7.1-CK14

MSD-473 SIP-DECT OM AXI changed behavior using Boolean true/false instead of 1 and 0

As of SIP-DECT 8.0 the AXI interface provides “true” and “false” instead of “1” and “0” for boolean parameter.

MSD-104, 105, 106 NTP client, pcap tools and editor nano added to OVA

The following packaged were added to the OMM/MOM OVA to improve usability:

- NTP client
- pcap tools
- nano editor

OVA CentOS update

The MOM/OMM OVA comes with the current CentOS 7 kernel and packages
CentOS kernel version: kernel-3.10.0-862.14.4.el7.x86_64.
CentOS patches date: 08/31/2018

MSD-277 System menu or global phone book not closed automatically

The system menu or global phone book will be closed automatically at

- 2 minutes timeout, when an application cannot be started (e.g. corporate Directory is called but not configured)
- 10 minutes timeout, if System menu or call deflection is started

MSD-208 OMM provisioning URL also to be used for RFP configuration files

A new DHCP option 236 is introduced to control which instance shall use the given Provisioning URL (Option 43-2, 66 or 234).

Valid values of the new Provisioning URL mode are:

1: The RFP shall use the given Provisioning URL

2: The OMM and RFP shall use the given Provisioning URL

else: the OMM shall use the given Provisioning URL

```
dhcp.conf example for option 236

option provurl_mode          code 236 = unsigned integer 8;

option provurl_mode 2;          # option 236
```

MSD-272 CoA: Change of "UD_SosNumber" --> "UD_SosNum" caused on double definition

Due to the double definition of the parameter for the features "configuration over air" and "external user provisioning" the name must be changed for the features "configuration over air" to avoid unexpected system behavior at the DECT phones.

MSD-204 OMM provisioning file support strings within strings

As of SIP-DECT 8.0, OMM configuration files e.g. Cloud-ID/PARK.cfg can contain commands with strings e.g. DECT phone profiles which itself contain strings (quotation marks). These quotation marks must be escaped with backslashes. Example:

```
<SetPpProfile ><ppProfile id="1" name="test 1" ppData="

…

UD_VListEntry = 1 5 \"*6<close>\" \"Pickup\" \"\" \"\" \"\"

…

" />

</SetPpProfile>
```

MSD-187 Implement BroadWorksSIP basic authorization for XSI directory

The Broadsoft specific authorization method “BroadWorksSIP basic” is supported for the XSI directory service with SIP user authentication.

MSD-329 Update to current Mozilla CA Certificate Store

The SIP-DECT trusted certificate store were updated to the current Mozilla CA Certificate Store (June 25th, 2018).

MSD-123 SIP-DECT EULA update

The SIP-DECT EULA was updated.

MSD-194 RFP configuration files (ipdect/<mac>.cfg) be overwritten by invalid content

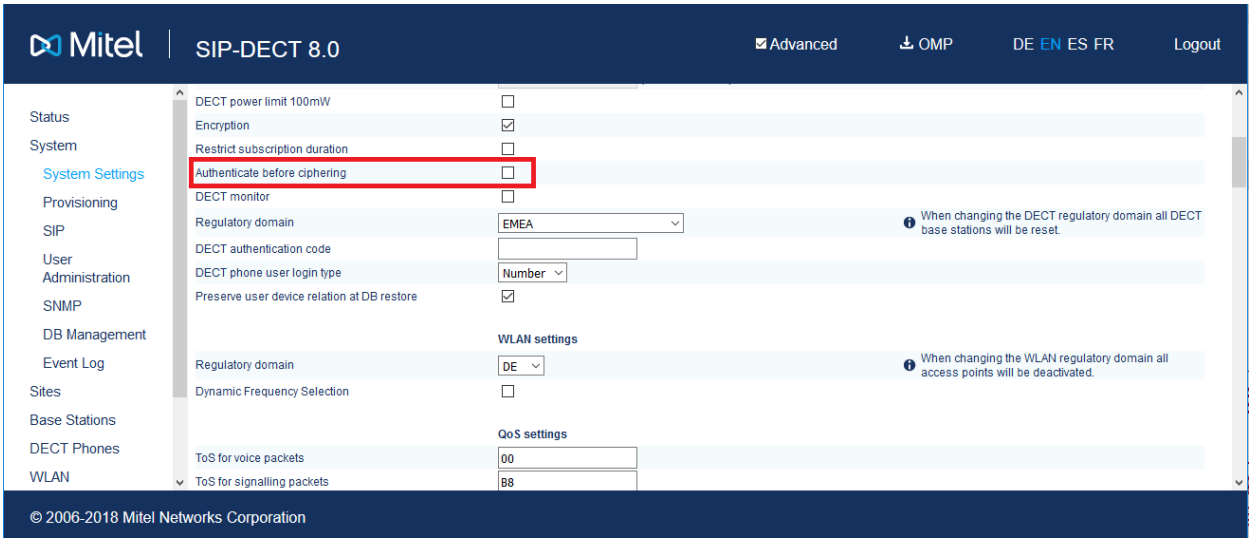
If a http(s) get request was answered e.g. with 404 File not found, then the RFP configuration files were overwritten by the error message content. That caused a SIP-DECT system restart without successful startup until RFP configuration files were available again.

The RFP configuration files are still mandatory at startup but the SIP-DECT system will not go out of operation if the files are not available during operation.

MSD-358 Support option to enable “Authenticate before Ciphering”

By default, Mitel SIP-DECT and DECT phones perform the DECT authentication procedure in a ciphered connection. For compatibility reasons, with the option “Authenticate before Ciphering” it is possible to force the system to authenticate before the connection is ciphered (Authenticate before Ciphering active).

This option should only be enabled if there is a strong indication that this solves compatibility problems in a specific SIP-DECT installation. This option is deactivated by default.



Update to OpenSSL 1.0.2n (DEV-19972/ VUL-244)

Critical vulnerabilities, (CVSS = 10) are reported on OpenSSL libraries, 1.0.1 thru 1.0.1r and 1.0.2 thru 1.0.2f. The OpenSSL was updated to 1.0.2n

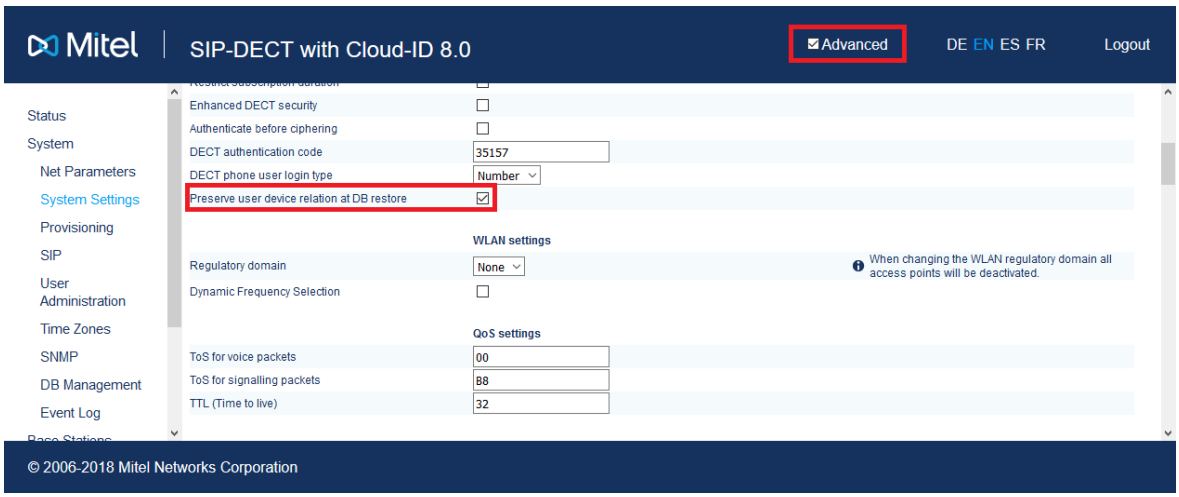
Installation and upgrade information for SIP-DECT 8.0

Update from previous releases

- The SIP-DECT 8.0 upgrade installation is validated on top of the SIP-DECT 7.0 and 7.1 releases. The upgrade to SIP-DECT 8.0 requires a restart of the whole system and cannot be executed in a one-by-one mode.
- As of SIP-DECT 7.1, RedHat 7 and CentOS 7 are supported and are required for a Linux server installation.
- The update to SIP-DECT 8.0 causes a reset of the DECT phone key lock PIN to default “0000”.
- Please be aware that the AXI interface provides “true” and “false” instead of “1” and “0” for Boolean parameter.

Note: Please activate the option “Preserve user device relation at DB restore” in the new OMM. The new OMM will restore the relation between the user and the DECT phone during DB import.

If this option is not set, then all dynamic user will be logged out from their DECT phones when importing the OMM DB into the new OMM.



Recommended MOM Web frontend configuration

The following configuration is recommended to run the MOM Web frontend:

- Display resolution 1920 x 1200.
- Up-to-date PC example, Intel® Core™ i5 processor and 8 GB RAM.
- Google Chrome™ browser (because of experienced performance and resource (RAM and CPU) consumptions for large configurations).

Mozilla Firefox® and Microsoft Internet Explorer® were also used to validate the MOM Web frontend.

Linux server OMM

SIP-DECT 8.0 is tested with the current CentOS™ 7 - as well as VMware vSphere ESXi™ 6.5. and VMware vSphere ESXi™ 6.7.

As of SIP-DECT 6.2, the OMM requires 4 GB RAM for the maximum configuration size of 10000 DECT Phone / users and 4096 base station.

Further installation and upgrade information

- The database built with this release is not backward compatible with older releases. A downgrade to an older release or version requires a database matching the older version.
  A database backup is strongly recommended before and after upgrading the SIP-DECT software.
- An upgrade to 8.0 release requires a restart of the entire SIP-DECT system.
- An update from SIP-DECT 3.0 release requires an intermediate upgrade to SIP-DECT 5.0 release. The upgrade from releases before 3.0 version requires an upgrade to 3.0.
  * For a detailed update description including upgrades from previous releases, please look up the related Mitel Knowledge Management System articles e.g. “SIP-DECT Knowledge Base: SIP-DECT System Update”.
- As of SIP-DECT 5.0, only a new license file format and mechanism is supported. This requires an update to 5.0 or later before importing a 5.0 license file. A license for SIP-DECT 5.0 or later cannot be imported into SIP-DECT 4.0 or previous releases.
- The browser used for service access must have frame support, JavaScript, and cookies enabled.
- When upgrading or downgrading the SIP-DECT software, delete the cookies and the cache in your browser after the upgrade / downgrade and before connecting with the new OpenMobility Manager (OMM). Otherwise the OMM Web service may be locked.

Product compatibility with Mitel Call Server

SIP-DECT 8.0 interoperability is provided with the following Mitel PBX/Call Servers:

MiVoice 5000

- MiVoice 5000 6.5 SP1

MiVoice MX-ONE

- MiVoice MX-ONE 7.0
- MiVoice MX-ONE 6.3SP3

MiVoice Business

- MiVoice Business 8.0 SP3
- MiVoice Business 9.0
- MiVoice Business 9.0 SP1
-

MiVoice Office 400

- MiVoice Office 400 6.0
- MiVoice Office 400 6.0 SP1

MiVoice Office 250

- MiVoice Office 250 6.3 SP2

For other Mitel call server or for more information, please see the Mitel call server release notes.

Where to find the latest information

You can access the most up-to-date versions of the following documents from http://edocs.mitel.com.

- SIP-DECT 8.0 Documentation Set including
  - SIP-DECT Multi-OMM Manager ADMINISTRATION GUIDE
  - SIP-DECT OM System Manual ADMINISTRATION GUIDE
  - SIP-DECT Integrated Messaging and Alerting Application ADMINISTRATION GUIDE
  - SIP-DECT OM Locating Application ADMINISTRATION GUIDE
  - SIP-DECT User Monitoring ADMINISTRATION GUIDE
  - SIP-DECT Phone Sharing and Provisioning ADMINISTRATION GUIDE
  - SIP-DECT Phone Synchronization ENGINEERING GUIDELINES
  - SIP-DECT with Cloud-ID System Manual ADMINISTRATION GUIDE

- SIP-DECT OM Application XML Interface*
- SIP-DECT XML Terminal Interface for Mitel 600 DECT Phone Family*

* available via MSA

Product areas improved in this release

Improvements between 8.0-DI16 and 7.1SP1-DI02.

- None

Improvements between 8.0-DI16 and 7.1-CK14.

- MSD-371 GS-261053 IMA config file download active and failed and switched off afterwards -> Still warning
- MSD-195 GS-253671 DSCP - tagging issues
- MSD-166 XSI reverse lookup fails: bug in parsing of the results
- MSD-131/GS-251030 XSI directory requests send by HTTP instead of HTTPS
- MSD-116 XML: Too long XML content freezes the handset SIP-DECT directory / GS-249848: SIP DECT display "Not OK, timeout" at corporate directory search, LAN trace says search OK)
- MSD-130/GS-250960 The OMM system is restarting
- CUS-19980 CLIP Display on Call Transfer (GS-249193: No COLP info op SIP DECT handsets after transferring from a - SIP-DECT on MiVO 400)
- DEV-19957 a SIP TCP disconnect can cause OMM restart in special rare conditions
- MSD-115/GS-245892 call reject on silent charging does not work when fully charged (silent charging state info lost after a while)
- MSD-183/GS-252084 Specific DECT GAP phone in idle mode blocks all air channels on RFP35 after some hours
- MDP-33 6x2dV2 In a noisy environment: audio level is too quiet. Also, the ringing is not loud enough
- MDP-37 Coverage warning do not follow settings
- MDP-38 End of editor beep even if End of menu tone disabled
- MDP-39 6x2dV2 with BT: Hang up with headset button (Voyager5200) during first outgoing call does not work
- MDP-40 Key programming of BT state
- MDP-42 6x2dV2/Mitel100/BT: Hang up with headset button does not work in some cases
- MDP-44 GS-259173;Mitel 600 DECT phone shows wrong Park/SARI/PARI
- MDP-45 ENH-18674: 6x2dV2 adjust Bluetooth volume in DECT phone
- MDP-46 6x2dV2 mute Bluetooth microphone from DECT phone
- MDP-54: BT Jabra headsets 9400BS, Evolve 75e and Speak 710 do not work (6x2dv2 only)
- MSD-379 Web-EULA contains three times identical information for busybox

- MSD-433 OMP does not show WLAN reg domain None
- *Various smaller fixes and improvements*

Known issues and Limitations

- None.

Q&A

Does the RFP3G OMM support mixed RFP3G and RFP4G installations?	Yes, as of SIP-DECT 8.0, the RFP3G OMM supports RFP2/3/4G base stations.
What is the OMM's user and device capacity?	Server OMM: 10000 user/devices 4096 RFPs SIP-DECT 8.0 RFP4G OMM: **1024** user/devices, 256 RFPs SIP-DECT 7.x/8.0 RFP3G OMM: **512** user/devices, 256 RFPs
Can the OMM standby configuration be built of different RFP generations?	No, this is not possible. **RFP3G <- Standby -> RFP4G NOK** RFP <- Standby -> Linux server **NOK** RFP4G <- Standby -> RFP4G OK RFP3G <- Standby -> RFP3G OK Linux Server <- Standby -> Linux Server OK
Can OMM DB backups be transferred between OMM's independent of RFP generation.	Yes, if limits are not exceeded. Similar question if a Linux server OMM backup shall be applied to an RFP OMM. OMM rejects the DB if the number of users, devices or RFPs excites the limits. (up path only are reasonable scenarios i.e. 3G -> 4G; RFP -> Linux server).
Does the RFP3G OMM provide the RFP4G SW for RFPs?	No, the RFP3G OMM can only provide its own SW image because of HW capacity limitations. The RFP4G OMM provides SW for 3G and 4G RFPs.
Which migration options are supported?	1. Migration from SIP-DECT <=7.1 to SIP-DECT 8.0 2. From RFP 3G OMM (Standby) to RFP3G OMM (Standby) 3. From RFP3G OMM (Standby) to RFP4G OMM (Standby) 4. From Linux Server (Standby) to Linux Server (Standby) 5. RFP OMM (Standby) to Linux Server (Standby)