SIP-DECT

Release Notes
Version 7.1-CK14
December 2017

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.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

SIP-DECT - Release 7.1
depl-2552/1.0

Table of Contents

Release Notes for SIP-DECT 7.1-CK14

This document describes the following components related to SIP-DECT and SIP-DECT with Cloud-ID 7.1-CK14:

- SW identification
- Product enhancements and functional changes
- Essential installation and upgrade information
- Product compatibility with Mitel Call Server
- Where to find the latest information
- Product areas improved in this release

SW identification

Current delivery

The following software is part of **SIP-DECT 7.1-CK14**:

- **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 7.0.SP11
  - Mitel 602d V2 DECT Phone firmware 7.0.SP11
- **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™

File	MD5 checksum
iprfp2G.tftp	1649492b79e24168d28735f4760f4507
iprfp3G.dnld	1666ef134551229839942daa48ed2636
SIP-DECT.bin	fc2670c47936610fc02d9011bedffdab
OMP.jar	83268fe61711d60c25579e2ee182a2cc
OM_Configurator.jar	bf74fbb2f2a10765ad9b51ea032fc995
SIP-DECT-MOM-7.1_CK14-0.i686.rpm	530afbc9c102a3c4b0608253f80445bd
OML.war	767a62fc76ed921a891ee86cb4200948
SIP-DECT_7.1-CK14.zip	5add7e206bc5a791a2609f2e80349eaf
SIP-DECT_7.1-CK14.ova	b604b664df95375d360ed0040b6dda06

The SIP-DECT OM XML Application Interface of this delivery uses the protocol version 45.

Download link: SIP-DECT_7.1-CK14.zip

SIP-DECT_7.1-CK14.ova

The following software is part of SIP-DECT with Cloud-ID* 7.1-CK14:

- **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 7.0.SP11
    - Mitel 602d V2 DECT Phone firmware 7.0.SP11

File	MD5 checksum
SIP-DECT_with_Cloud-ID_7.1-CK14.zip	b8df75e9aa7c25fd44850db45d76c819
iprfp3G.dnld	fc207d67b03facbad5639b38c1768925

Download link: SIP-DECT_with_Cloud-ID_7.1-CK14.zip

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

Last delivery

- SIP–DECT Software Version 7.0SP3-CI25.
- Mitel 600 DECT Phone family firmware package including:
    - Mitel 6x0d DECT Phone firmware:
        - Mitel 6x2d/650c DECT Phone firmware: 7.0.SP11
        - Mitel 602d V2 DECT Phone firmware: 7.0.SP11

Product enhancements and functional changes

New features

NFR-13819 (EPIC SIP-DECT MSD-1) 802.1x certificate based authentication of RFPs

As of SIP-DECT 7.1, SIP-DECT supports 802.1x certificate based authentication for SIP-DECT base stations.

802.1x certificate data is stored centrally in OMM database and can be set by OMP, via an OMM provisioning file or from a certificate server. The centrally stored 802.1x certificate data remains valid until it is changed or removed by one of the configuration sources. For the group certificate, one 802.1x identity for all RFPs is supported.

Base stations receive the encrypted 802.1x certificate data from OMM via a HTTP file request e.g. after reboot or after notification of new certificate data from the OMM. The 802.1x certificate data will be stored locally on Base stations. Only Base stations can decrypt and use the certificate data.

EPIC SIP-DECT MSD-2 CentOS 7 Support

As of SIP-DECT 7.1, CentOS 7 is supported by the Linux server OMM.

CentOS 6.x cannot be used with SIP-DECT 7.1 OMM.

For more information please see: SIP-DECT Linux Server Installation ADMINISTRATION GUIDE.

EPIC SIP-DECT MSD-3 OVA Support / OMM/MOM as VMware OVA image

As of SIP-DECT 7.1, a OVA file is part of the SIP-DECT deliverables to deploy the SIP-DECT MOM or OMM under VMware ESXi™. The OVA file comes with CentOS 7.

For more information please see: SIP-DECT Linux Server Installation ADMINISTRATION GUIDE.

Enhanced DNS-SRV behavior

As of SIP-DECT 7.1, SIP-DECT supports a failover to the next server (listed in the DNS-SRV query results) when a 5xx response is received for an initial request.

The failover mechanism is triggered with each 5xx response except the both configurable “Call reject state code” (user reject / state unreachable).

NFR-14045/ ENH-19471 VLAN management for SDC

As of SIP-DECT 7.1, SIP-DECT supports VLAN tagging referring to IEEE 802.1Q.
The VLAN-ID can be set via provisioning file, Web GUI or DHCP.

VLAN priority settings referring to IEEE 802.1p is also supported (call control / audio).

NFR-14172/ ENH-19425 N-way conference support with third party conference servers

As of SIP-DECT 7.1, SIP-DECT supports n-way conferencing with third party conference servers, which are compliant with RFC4579 e.g. BroadSoft ™ BroadWorks.

This functionality allows to easily extend an already established 3-way conference by adding further participants.

NFR-14397/ ENH-19456 Cloud-ID on User Agent field for SW requests

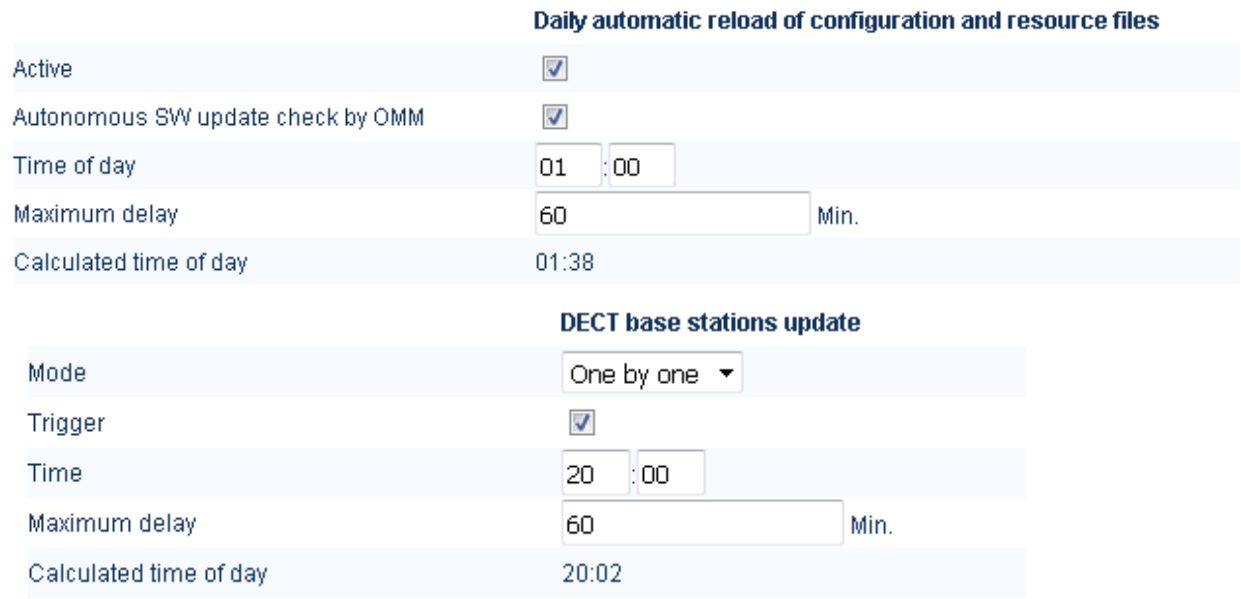
As of SIP-DECT 7.1, SIP-DECT adds the Cloud-ID on the User Agent field when the OMM-RFP requesting a new SW image from an external server using HTTP or HTTPS.

NFR-14308/ ENH-19424 Configuration and resource file reload and update time spread

SIP-DECT supports 2 features to control and manage the update process in SIP-DECT system:

- Time-controlled Daily automatic reload of configuration and firmware files
- Time-controlled RFP software update

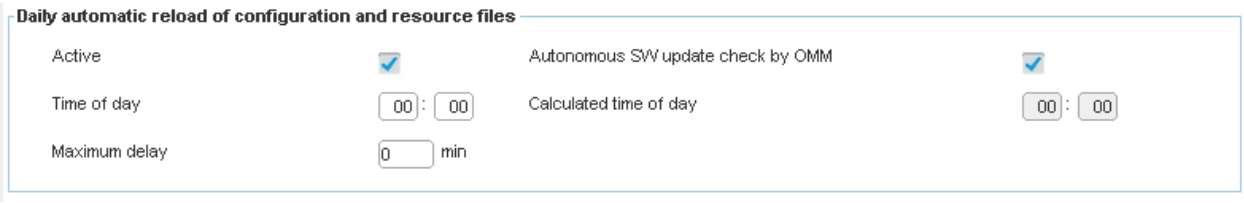
A new configuration parameter “Maximum delay” allows a given delay, when a reload or an update starts.



This allows automatically spreading the download and updating processes of multiple SIP-DECT installations, which are provisioned with the same configuration settings.

If the features are activated or re-configured then the OMM calculates a random start time between 0 and “Maximum delay” past the given “Time of day” and save it as “Calculated time of day”. This means that the “Calculated time of day” is the actual daily start time and is equal to “Time of day” when “Maximum delay” is zero.

Additionally, the new configuration parameter “Autonomous SW update check by OMM” allows to disable the default behavior of the RFP-OMMs to check a new software image, whenever a RFP re-configuration (DHCP renew, OM Configurator, ipdect.cfg, <MAC>.cfg) happens.



By default, the autonomous SW update check by OMM is enabled and no change of the behavior compared to previous SW releases.

NFR-14496 (EPIC SIP-DECT MSD-73) Device Management improvement

An improper manipulation of user data in a OMM configuration file caused various database inconsistencies between a device management system and the SIP-DECT OMM. This includes the issue that the device and user assignment was modified for all user and devices when the first user entry has been removed and the device management system re-assigned a new UID to all remaining users.

Only the user management via CFG files (ipdect.cfg, <MAC>.cfg, <Cloud-ID>/00<PARK>.cfg) was affected.

Because of the improvement to handle such scenarios by SIP-DECT, all users must be specified in one of the CFG files independent of which file has been chosen to provide the user data (ipdect.cfg, <MAC>.cfg, <Cloud-ID>/00<PARK>.cfg).

Please also see: GS-237178: Rebuild users file change users in handsets - SIP-DECT on SIP Call Manager.

There is no specific configuration required to enable the improvement.

NFR-14468 (EPIC SIP-DECT MSD-74) Support Caller ID when receiving a call from a XSI directory contact (Caller-ID from XSI directory)

As of SIP-DECT 7.1, SIP-DECT supports the XSI lookup for the caller number to display the caller’s name if no caller’s name is provided by other means for an incoming call.

The following parameters must be configured

Parameter / Parameter group	**Enable reverse XSI directory lookup**
Description	Reverse lookup must be explicitly activated
Format	Bool
Range	on/off
Default value	off
Web	Advanced: System > User service > Reverse XSI directory lookup
OMP/AXI	System > Advanced settings > User service > Active
OMM Configuration files	<SetAdditionalSettings revXsiDirLookup="1" />
DECT Phone	n.a.
User configuration files	n.a.

Parameter / Parameter group	Max. matching digits for reverse XSI directory lookup
Description	Number of last digits, which will be used for a partly qualified search. This shall avoid conflicts which can be occur due to different kind of representation of area codes or numbering plans
Format	enumerated
Range	1..9, all digits=0
Default value	6
Web	Advanced: System > User service > Max. number of matching digits"
OMP/AXI	System > Advanced settings > User service > Max. number of matching digits
OMM Configuration files	<SetAdditionalSettings revXsiDirLookupMatchingDigits="5" />
DECT Phone	n.a.
User configuration files	n.a.

A search will be executed in all active XSI directories in the following order:

- For "Number" in "XSI personal"
- For "Number" in "XSI group"
- For "Number" in "XSI enterprise"
- For "Number" in "XSI group common"
- For "Number" in "XSI common"
- For "mobileNo" in "XSI group", if number of digits >= revXsiDirLookupMatchingDigits
- For "mobileNo" in "XSI enterprise", if number of digits >= revXsiDirLookupMatchingDigits

To avoid multiple XSI lookups the information fetched from the XSI directory are hold in a cache.

NFR-14123/ ENH-19754 Netherlands - Specific behavior when Alarm Button is pressed / Config over Air DECT Phone key programming for SOS Call State

To enable certain DECT phone keys to be active in the SOS call state (SOS call has been setup via this DECT phone) the key behavior can be programmed via Configuration over Air (CoA).

By default, the majority of DECT phone keys are disabled in SOS call state.

Example to enable 0 to 9 and '' and '#' via CoA profile:

UD_KeyAssignmentActiveSosMaster = star dial_star

UD_KeyAssignmentActiveSosMaster = hash dial_hash

UD_KeyAssignmentActiveSosMaster=red nop

UD_KeyAssignmentActiveSosMaster=d0 dial_0

UD_KeyAssignmentActiveSosMaster=d1 dial_1

UD_KeyAssignmentActiveSosMaster=d2 dial_2

UD_KeyAssignmentActiveSosMaster=d3 dial_3

UD_KeyAssignmentActiveSosMaster=d4 dial_4

UD_KeyAssignmentActiveSosMaster=d5 dial_5

UD_KeyAssignmentActiveSosMaster=d6 dial_6

UD_KeyAssignmentActiveSosMaster=d7 dial_7

UD_KeyAssignmentActiveSosMaster=d8 dial_8

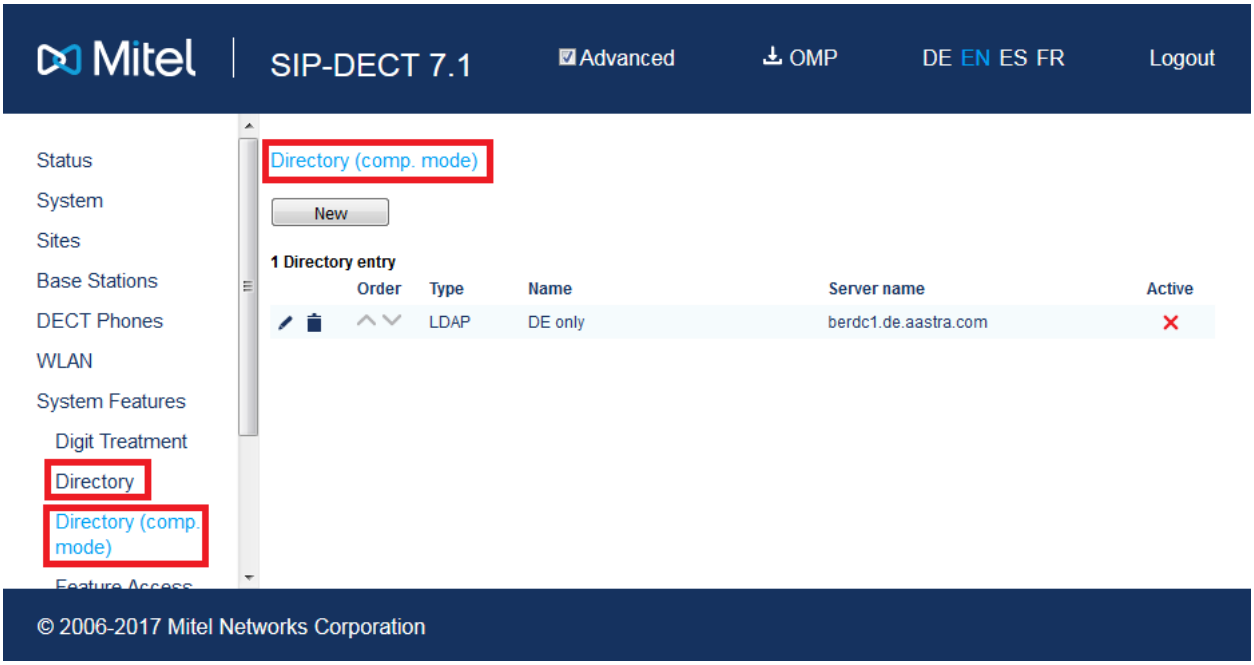
UD_KeyAssignmentActiveSosMaster=d9 dial_9

Additional changes

ENH-19495 Easy migration from corporate directory (comp. mode) to new directory structure via provisioning

As of SIP-DECT 6.2, a new directory configuration has been introduced which supports 3 types of directories: LDAP, XML and XSI (Enterprise, Group, Personal). Additionally, the configuration via provisioning (OMM configuration files) is supported for the new directory configuration.

To provide backwards compatibility, the old directory configuration “Directory (comp. mode))” for LDAP or XML directories is still supported.



As of SIP-DECT 7.1, SIP-DECT automatically removes entries from the “Directory (comp. mode)” if there is a matching entry in the new directory configuration to simplify the migration from the old to the new directory structure especially when provisioning via OMM configuration files is used.

This allows to create directory entries in the new directory, e.g. via provisioning files, without the risk to create duplicated entries in the DECT phone menu. There is no need to manually check and modify the “Directory (comp. mode)”.

The following parameters are considered for comparison:

- Directory type (LDAP, XML)

- Name
- Server
- Path

ENH-19889 Random Source Port Option for SIP Persistent TLS

To improve the integration with the MiCloud Office/Telepo platform, SIP-DECT supports a random source port selection mode for the SIP transport protocol “Persistent TLS”.

If “Persistent TLS" is selected and the special local TLS port range 0-0 is configured then the OMM determines at startup a random source port in the range 17000 - 32767 and use that port number as source port until next OMM restart. The special port range 0-0 can be set for "PP user TLS" and "Conference room TLS".

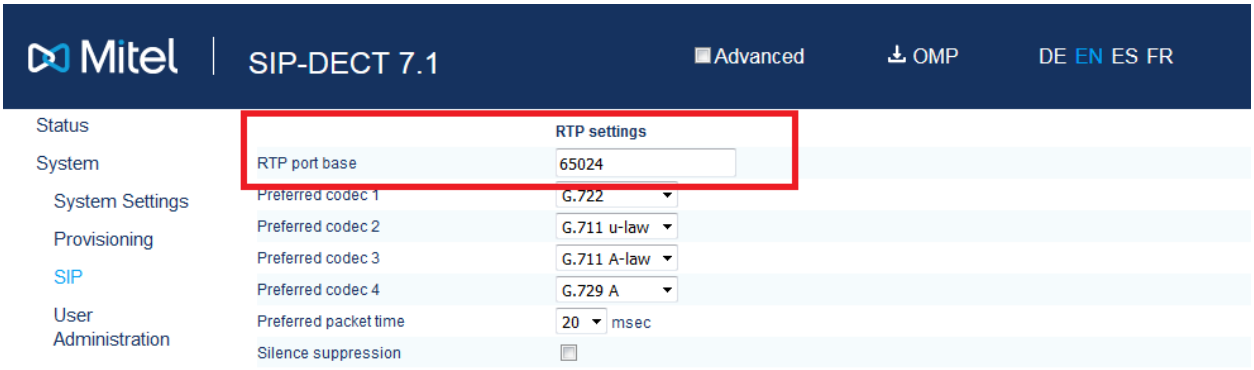
NFR-14579: Voba Breisgau RTP Port usage 65024 and above

The supported RTP port range includes the range of 65024 to 65535.

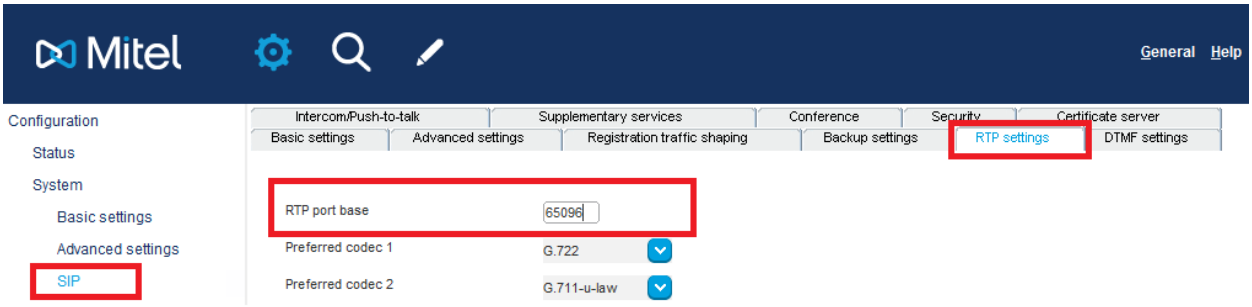
Because SIP-DECT allows to configure a RTP port base the range for the RTP port base is extended by 65024 to 65462 (65535 minus Number of RTP ports used by base station).

The RTP port base can be set via OMM Web GUI, OMP or OMM configuration files.

OMM Web GUI



OMP



OMM Configuration file:

```
<SetRTP
   portBase="65024"
   >
</SetRTP>
```

SIP-DECT MSD-23 Enhancement for update MiVB hot-desking PIN by user

As of SIP-DECT 7.1, the following limitation does not longer exist: *“Hot Desk users should NOT change their PIN if hot desking on SIP-DECT handsets (612, 622, 632, 650). If the PIN is changed while the user is logged in to these devices, the system will force a log out. Subsequent log in attempts will fail because the device base station will NOT have the new PIN.”*

There is no need any more to (re-)configure the SIP-DECT user login PIN which is also used for the MiVB Hot Desk user authentication e.g. if the MiVB hot desk PIN has been modified.

SIP-DECT determines automatically a valid PIN when the user enters the PIN during the DECT phone login process at the DECT phone and the PIN is validated by the MiVB Hot Desk user authentication.

This applies only to the Mitel DECT Phone 600d family and NOT to 3rd party GAP phones or the 142d.

Installation and upgrade information for SIP-DECT/SDC 7.1-CK14

Update from previous releases

The SIP-DECT Version 7.1 upgrade installation is validated on top of the following SIP-DECT releases: 4.0SP3, 6.0SP2, 6.1SP1, 6.2 and 7.0SP2. 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”.

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 7.1 is tested with CentOS™ 7.1611 - Based on Source Code for Red Hat Enterprise Linux 7.3 - as well as VMware vSphere ESXi™ 6.0.0 (Build 3562874) and VMware vSphere ESXi™ 6.5.0 Update 1 (Build 5969303).

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 7.1 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

Please examine the Mitel call server release notes and the Mitel Product Compatibility Matrix to check if SIP-DECT 7.1 is available for a specific Mitel platform and version.

Where to find the latest information

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

- SIP-DECT 7.1 updated documentation set includes:
  - SIP-DECT OM System Manual ADMINISTRATION GUIDE
  - SIP-DECT with Cloud-ID System Manual ADMINISTRATION GUIDE
  - SIP-DECT LINUX System Installation ADMINISTRATION GUIDE
  - SIP-DECT OM Application XML Interface*
  - SIP-DECT XML Terminal Interface for Mitel 600 DECT Phone Family*
  - *Available through MSA.

- Other documents: The SIP-DECT 7.0 version applies.

Product areas improved in this release

The following fixes were included in this release:

- GS-238824: Wrong XSI request for Enterprise_Common
- DEV-19809: invalid <cr> characters in PEM files cause that openssl doesn't read all certs
- DEV-19850: St-Etienne: DECT device unreachable semi attended transfer fails
- CUS-19835: DECT-To-DECT Blind transfer fails due to INVITE without SDP
- CUS-19761: SIP-DECT OMM restart with core dump
- DEV-19854: memory leak during failover to secondary proxy
- DEV-19927 missing decoding of LATIN 1 character set in XsiCommon... and ...Personal
- DEV-19930: 602d caller list and redial list not available after handset power off/on
- *Various smaller fixes and improvements*