

SIP-DECT 8.1SP1

Release Notes

Version 8.1SP1-FA27

January 2020



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 8.1

January 2020

MSD-depl-8.1-197 / 2.0 / Valid

®,™ Trademark of Mitel Networks Corporation
© Copyrights 2020, Mitel Networks Corporation
All rights reserved

Table of Contents

| | |
|--|----|
| Release Notes for SIP-DECT 8.1SP1 | 1 |
| SW identification | 2 |
| Current delivery | 2 |
| Previous deliveries | 3 |
| Product enhancements and functional changes | 4 |
| New features | 4 |
| MSD-743 Mitel DECT Phone charger in/out event | 4 |
| MSD-745 New built-in XML hook Hotkey | 6 |
| MSD-769 Support of 5 VLSTs each with up to 15 entries | 6 |
| Additional changes | 7 |
| PSEC-442 SIP-DECT MITM OMM RFP encryption vulnerability | 7 |
| MSD-801 DFR18040 Menu enhancement for text message with only 2 confirmation requests | 11 |
| OVA CentOS update..... | 12 |
| MSD-1193: Update to AdoptOpenJDK 8u242 | 12 |
| MSD-1192 Update to AdoptOpenJDK 11.0.6 | 12 |
| MSD-823 wpa_supplicant (802.1x supplicant) updated to version 2.9 | 12 |
| MSD-834 Hostapd updated to version 2.9..... | 12 |
| Installation and upgrade information for SIP-DECT 8.1..... | 13 |
| Update from previous releases | 13 |
| Recommended MOM Web frontend configuration | 14 |
| Linux server OMM | 14 |
| Further installation and upgrade information..... | 14 |
| Product compatibility with Mitel Call Server | 15 |
| Where to find the latest information | 15 |
| Product areas improved in this release..... | 15 |
| Known issues and Limitations..... | 16 |

Release Notes for SIP-DECT 8.1SP1

This document describes the following components related to SIP-DECT 8.1SP1-FA27:

- 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.

SW identification

Current delivery

The following software is part of **SIP-DECT 8.1SP1-FA27**:

- **iprpf3G.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 7.3.2
 - Mitel 602d V2 DECT Phone firmware 7.3.2
- **iprpf4G.dnld**: software for RFP 44 IP, RFP 45 IP, RFP 47 IP, and RFP 48 WLAN. including the Mitel 600d DECT Phone family firmware and the iprpf3G.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 |
|--|----------------------------------|
| FindMySIP-DECTbasestation.zip | 9b2fdd683f61f79263e6272cb5d3a901 |
| iprpf3G.dnld | c44a81f0960e36143368a4e4d6a01f1d |
| iprpf4G.dnld | fc3f1360b6cfa6606f2dc3f94e9dad81 |
| SIP-DECT.bin | 687d1b5fd221a39952cd24ac31b1daba |
| OM_Configurator_Installer_SIP-DECT_8.1.exe | 3f5543686a25921091d9d7ea8edc9797 |
| OMP_Installer_SIP-DECT_8.1.exe | e6a59f207eb0abcf394689409570341 |
| OMP_Runtime_Image_Linux.tar.gz | 1b87716ad76dcaed65825caaacb1c4a5 |
| OMP_Runtime_Image_Win.zip | cafb999d31e5e90c6bad6d97ecaa89d3 |
| OMCFG_Runtime_Image_Linux.tar.gz | 0dc0d9752434970b88a555fce11a01d8 |
| OMCFG_Runtime_Image_Win.zip | 548931ab4c77d0654633ef252b7d4fba |
| SIP-DECT-MOM-8.1SP1_FA27-0.i686.rpm | 095fd74ad026768843722738385cbde7 |
| OML.war | d5a284280a64961c5e6a366f3029003f |
| SIP-DECT_CentOS7-B190716_200101.tar.gz | 1c17e57eada6ab7d5a70438d2e98542a |
| SIP-DECT_8.1SP1-FA27.zip | f1207684554cb75d9d92dccb8180bff3 |
| SIP-DECT_8.1SP1-FA27.ova | 291eea4bc190c8bad0e5b1748d9a9d7b |

The SIP-DECT OM XML Application Interface of this delivery uses the protocol version **50**.

Mitel Software Download Center download links:

[SIP-DECT 8.1SP1-FA27.zip](#)
[SIP-DECT 8.1SP1-FA27.ova](#)
[FindMySIP-DECTbasestation.zip](#)

The OMM's and MOM's default certificate chain is available via the following links:

[OMMDefaultCertChain.pem](#)
[MOMDefaultCertChain.pem](#)

Previous deliveries

- SIP-DECT 8.1-EJ02 October 2019
 - Mitel 6x2d/650c DECT Phone firmware 7.2.6.SP3
 - Mitel 602d V2 DECT Phone firmware 7.2.6.SP3
- SIP-DECT 8.0SP2-FA16 January 2020
 - Mitel 6x2d/650c DECT Phone firmware 7.2.6.SP3
 - Mitel 602d V2 DECT Phone firmware 7.2.6.SP3
- SIP-DECT 8.0SP1-HF02EL21 December 2019
 - Mitel 6x2d/650c DECT Phone firmware 7.2.6.SP3
 - Mitel 602d V2 DECT Phone firmware 7.2.6.SP3
- SIP-DECT Software Version 8.0SP1-EF04 June 2019
 - Mitel 6x2d/650c DECT Phone firmware 7.2.6
 - Mitel 602d V2 DECT Phone firmware 7.2.5
- SIP-DECT Software Version 8.0-HF01DI16 November 2018
- SIP-DECT Software Version 8.0-DI16 October 2018
- SIP-DECT Software Version 7.1SP1-DI02 September 2018
- SIP-DECT Software Version 7.1-CK14 December 2017

Product enhancements and functional changes

New features

MSD-743 Mitel DECT Phone charger in/out event

As of SIP-DECT 8.1SP1 and Mitel DECT Phone firmware 7.3.2, a charger events are signaled via AXI and XML Action URI application hook.

In the AXI EventPPState, there are the following 2 related state information provided.

| Parameter | Description |
|----------------|--|
| isUsbConnected | „1” or “true”, if this DECT phone is connected to USB else “0” or “false”. |
| isInCharger | „1” or “true”, if this DECT phone is in charger else “0” or “false”. |

| Example AXI Event | Description |
|---|-----------------------------------|
| <EventPPState ppn="1" ppnHex="0x1" isInCharger="0" isUsbConnected="0"/> | not in charger, not USB connected |
| <EventPPState ppn="1" ppnHex="0x1" isInCharger="1" isUsbConnected="0"/> | In charger, not USB connected |
| <EventPPState ppn="1" ppnHex="0x1" isInCharger="0" isUsbConnected="1"/> | not in charger, USB connected |

Further information can be found in the SIP-DECT OM Application XML interface, which is available via MSA.

The XML Action URI provides the same status information if the following parameter are specified in the parameter set.

| Parameter | Description |
|-----------|------------------------------|
| {usb_y} | USB Connected |
| {usb_n} | USB Disconnected |
| {chg_y} | DECT phone is in charger |
| {chg_n} | DECT phone is not in charger |

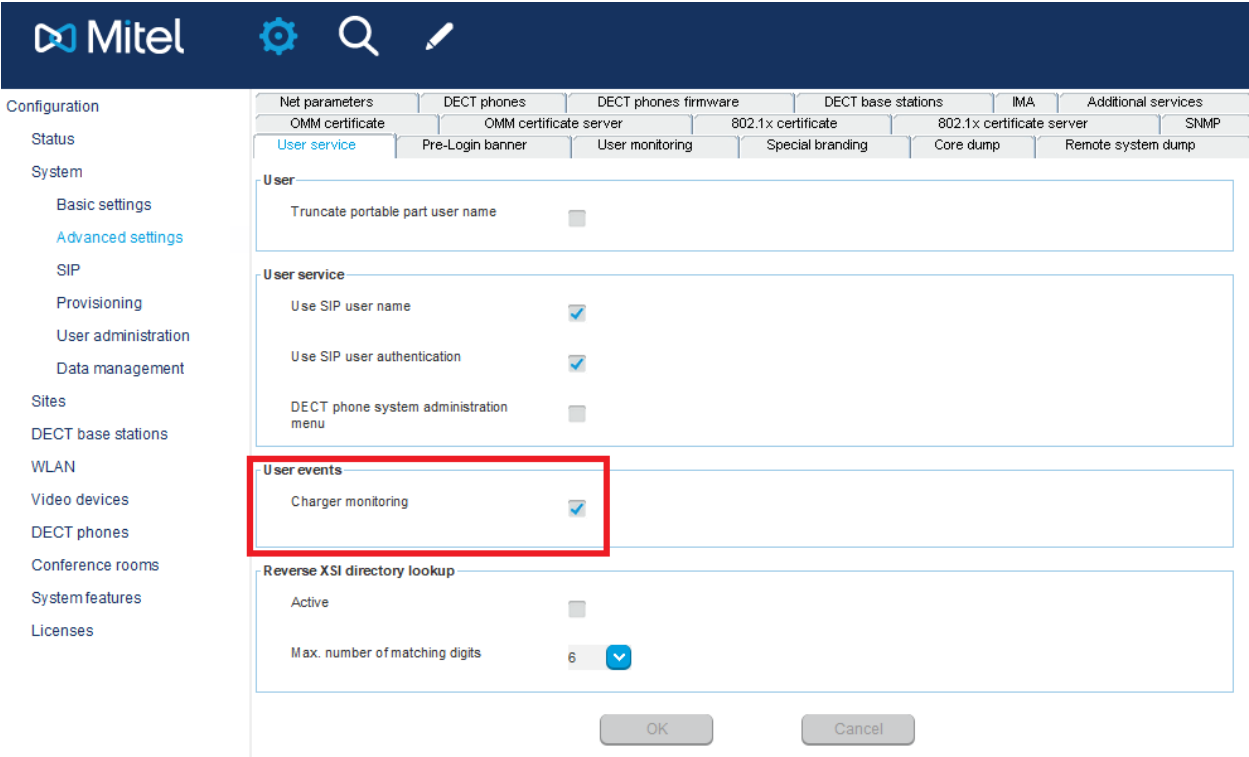
Example:

```
path=sipDectTerm.xml?...&inCharger={chg_y}&notInCharger={chg_n}&usbconn={usb_y}&usbdisconn={usb_n}
```

For more information please see the SIP-DECT XML Terminal Interface for Mitel 600 DECT Phone Family.

The charger event signaling can be activated via OMP in the extended system settings in the user service area.

Note: If multiple state changes occur in a short period of time then only the final state will be reported after ~ 10 seconds to avoid message bursts.



| | |
|-----------------------------|--|
| Parameter / Parameter group | Charger monitoring |
| Description | Activates or deactivates sending a charger event via AXI or XML terminal IF. To receive an event, a proper configuration of the XML action URI or an event subscription via AXI is required too. |
| Format | Boolean |
| Range | 0, false; 1, true |
| Default value | 0 |
| Web | N/A |
| OMP | System > Advanced Settings > User service > User events > Charger monitoring |
| OMM configuration files | <SetChargeStateMonitoring enable="1" /> |
| DECT Phone | n.a |
| User configuration files | n.a. |

MSD-745 New built-in XML hook Hotkey

As of SIP-DECT 8.1SP1 and Mitel DECT Phone firmware 7.3.2, the new predefined XML application hook “Hotkey” is supported. This is a new application access function that is used by external application servers to provide additional functions for DECT telephone users via the SIP-DECT XML terminal interface. The “Hotkey” can be programmed on a selected key of a Mitel 602d DECT phone. This can be done either manually or via CoA.

The XML hook can be configured via OMP or via OMP and OMM Web UI as existing XML hooks.

MSD-769 Support of 5 VLSTs each with up to 15 entries

As of SIP-DECT 8.1SP1 and Mitel DECT Phone Firmware 7.3.2, Configuration over Air (CoA) supports 5 VLSTs, each with up to 15 entries. Please note the maximum file size of 4000 bytes for a CoA file. 5 times 15 entries already exceed the maximum size.

Example extract:

```
UD_ConfigurationName=VLIST TEST

UD_KeyAssignmentIdleMaster = long.d1 vlst1
...
UD_KeyAssignmentIdleMaster = long.d5 vlst5

UD_VListName = 1 "VL1" #Titel
UD_VListShortName = 1 "VL1" #Softkey
UD_VListSubItems = 1 0

...

UD_VListName = 5 "VL5" #Titel
UD_VListShortName = 5 "VL5" #Softkey
UD_VListSubItems = 5 0

UD_VListEntry = 1 1 "<inf=VL1 E_1><r=2000>" "VL1 E_1" "" "" ""
...

UD_VListEntry = 5 15 "<inf=VL5 E_15><r=2000>" "VL5 E_15" "" "" ""
```

Additional changes

PSEC-442 SIP-DECT MITM OMM RFP encryption vulnerability

During RFP enrolment, an RFP specific random authentication key is exchanged between OMM and RFP used for authentication and encryption.

The enrolment of RFPs comprises of the following 2 steps:

- Add RFP to OMM database (create a DB entry for the RFP)
- First connection between RFP and OMM





It is a precondition that the enrolment of the RFP takes place in a safe environment i.e. the installer ensures that an authentication key exchange between RFP and OMM during enrolment cannot be compromised: no man-in-the-middle attack possible, no tampered RFP etc.

Note: The key exchange takes place automatically during the upgrade / update to 8.1SP1 if the previous software did not yet support this function.

To successfully enroll an RFP, the RFP must not have an authentication key from previous enrolments. The authentication key can be removed from an RFP with a reset to factory defaults. To remove an existing key for an RFP from the OMM, the RFP must be removed from the OMM DB.

If an RFP is removed from the OMM DB and the RFP is connected to the OMM then the authentication key is automatically removed from the RFP as well. The RFP can be enrolled on this or another OMM without a reset to factory defaults.

RFP connection status in OMM: encryption activated

The administration interfaces of the OMM show the RFP connection status. The intermediate state between disconnected and successful connection (encrypted) is called “encryption activated”. This intermediate state is indicated by a key icon  in the connection state column. This status is usually very short and therefore not noticeable. However, if there is an encryption issue, then the successful connection state, indicated by a green checkmark , cannot be reached and “encryption activated” will last for ~20 seconds and returns to disconnected (Web: , OMP: ) periodically.

| | ID | Name | MAC address | IP address | HW type | RPN | Connected | Active |
|---|------|------------|-------------------|---------------|---------|-----|---|---|
|  | 0000 | OMM RFP | 08:00:0F:C3:DF:0A | 10.103.35.162 | RFP 47 | 00 |  |  |
|  | 0001 | RFP 4x 2nd | 08:00:0F:C3:DE:FD | 10.103.35.123 | RFP 47 | 01 |  | - |
|  | 0002 | RFP32 | 00:30:42:12:33:16 | 10.103.35.239 | RFP 32 | 02 |  |  |
|  | 0003 | RFP43 / 3X | 00:30:42:17:8E:3E | 10.103.35.172 | RFP 43 | 03 |  |  |

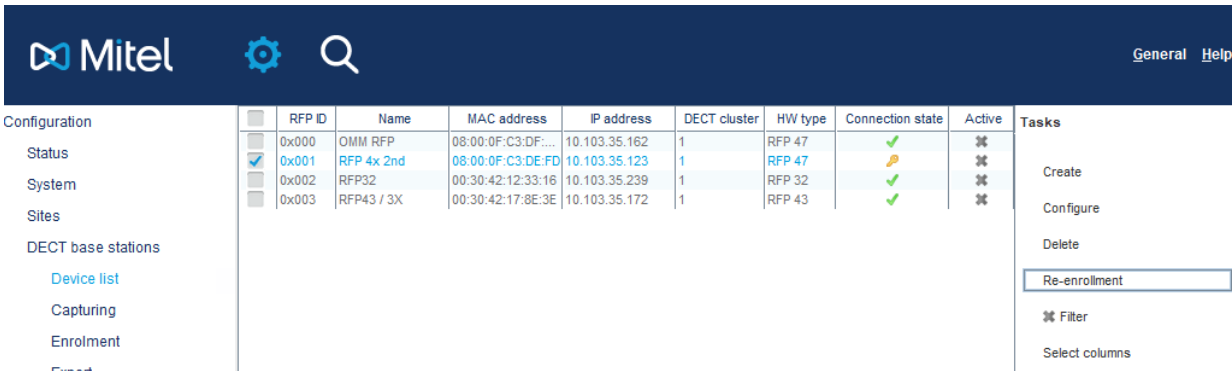
Encryption activated state displayed by Web UI

Re-enrolment function

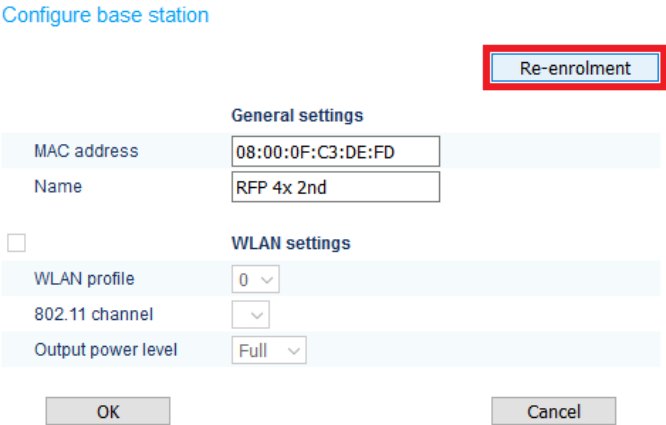
The re-enrolment function can be used to address authentication key issues between OMM and RFP if the RFP was already enrolled in the OMM and encrypted communication was already in place before. Please, see the table below. Please be aware that this function can help to solve only specific scenarios.

If re-enrolment is activated for an RFP, then the OMM sends an encrypted message (AES-256) to the RFP with the next connection attempt of the RFP. This message is validated by the RFP to ensure that the OMM is the sender (SHA-2, SHA256). The RFP can only decrypt and validate the message if the RFP has the same root credentials as the OMM (exchanged during earlier encrypted communication). The message provides a new authentication key to the RFP. The RFP uses the new authentication key for encryption of following traffic.

The re-enrolment function is available via OMP and OMM Web UI.



Re-enrolment via OMP



Re-enrolment feature in the Configure Base Station dialog box of the Web admin user interface

To initiate the re-enrolment, select the RFP and press Re-enrolment. This action is ignored for successful connected RFP.

Switch between software versions that support and do not support authentication keys

Switch between software versions that support and do not support authentication keys causes a loss of keys in OMM. When update/upgrade again to SW with authentication key support, apply the OMM DB backup with the latest RFP authentication keys. RFPs cannot connect to the OMM if the RFPs have a key and the OMM does not, as shown in the following screen shot.

| ID | Name | MAC address | IP address | HW type | RPN | Connected | Active |
|------|------------|-------------------|---------------|---------|-----|-----------|--------|
| 0000 | OMM RFP | 08:00:0F:C3:DF:0A | 10.103.35.162 | RFP 47 | 00 | ✓ | ✓ |
| 0001 | RFP 4x 2nd | 08:00:0F:C3:DE:FD | 10.103.35.123 | RFP 47 | 01 | ✗ | – |
| 0002 | RFP32 | 00:30:42:12:33:16 | 10.103.35.239 | RFP 32 | 02 | ✗ | – |
| 0003 | RFP43 / 3X | 00:30:42:17:8E:3E | 10.103.35.172 | RFP 43 | 03 | ✗ | – |

RFPs cannot connect because keys do not match

The event log messages provide a further indication why the connections fail.

| Severity | Count | Time (UTC) | Event |
|----------|-------|-------------------------|--|
| 3 | 1 | 2019/12/20 13:14:59.183 | IPL : RFP(0001) disconnected, might have different encryption keys => try re-enrolment |
| 3 | 1 | 2019/12/20 13:14:51.427 | IPL : RFP(0003) reconnected |
| 3 | 1 | 2019/12/20 13:14:49.402 | IPL : RFP(0003) disconnected, might have different encryption keys => try re-enrolment |
| 3 | 1 | 2019/12/20 13:14:40.437 | IPL : RFP(0002) reconnected |
| 3 | 1 | 2019/12/20 13:14:38.406 | IPL : RFP(0002) disconnected, might have different encryption keys => try re-enrolment |
| 3 | 1 | 2019/12/20 13:14:36.674 | IPL : RFP(0001) reconnected |
| 3 | 1 | 2019/12/20 13:14:34.662 | IPL : RFP(0001) disconnected, might have different encryption keys => try re-enrolment |
| 3 | 1 | 2019/12/20 13:14:26.895 | IPL : RFP(0003) reconnected |
| 3 | 1 | 2019/12/20 13:14:24.870 | IPL : RFP(0003) disconnected, might have different encryption keys => try re-enrolment |
| 3 | 1 | 2019/12/20 13:14:15.881 | IPL : RFP(0002) reconnected |

Event log messages if RFPs and OMM keys do not match

After applying the correct OMM DB with latest keys, the problem will disappear. Re-enrolment can be an alternative if the root credentials do not differ between RFPs and OMM.

| ID | Name | MAC address | IP address | HW type | RPN | Connected | Active |
|------|------------|-------------------|---------------|---------|-----|-----------|--------|
| 0000 | OMM RFP | 08:00:0F:C3:DF:0A | 10.103.35.162 | RFP 47 | 00 | ✓ | ✓ |
| 0001 | RFP 4x 2nd | 08:00:0F:C3:DE:FD | 10.103.35.123 | RFP 47 | 01 | ✓ | ✓ |
| 0002 | RFP32 | 00:30:42:12:33:16 | 10.103.35.239 | RFP 32 | 02 | ✓ | ✓ |
| 0003 | RFP43 / 3X | 00:30:42:17:8E:3E | 10.103.35.172 | RFP 43 | 03 | ✓ | ✓ |

RFPs are connected again after applying an OMM DB with matching key

Authentication key mismatch scenarios

There are various scenarios which can cause a key mismatch between RFP and OMM. In general, this requires a factory reset of the RFP and to delete and re-create the RFP in the OMM DB. This is applicable for many scenarios and for a lower number of RFPs. Some scenarios can cause a mismatch for many or all RFPs in one installation. To address these scenarios a specific re-enrolment mechanism is available.

Note: The re-enrolment function will only work if root credentials match between OMM and RFP. It does not work e.g. if RFP moved to different SIP-DECT installation, assuming credentials differ.

The following table shows the scenarios, how they can occur and how they must be addressed.

| Scenario | How to be caused (always based on a previous successful enrolment) | Comments | Default procedure | Alternative |
|--|---|--|--|---|
| OMM uses authentication key, but there is no in RFP | <ul style="list-style-type: none"> Factory reset of RFP | There can be no conflict for RFPs on which the OMM is running (both in one device) | Delete and recreate RFP in OMM DB (license RFPs cannot be deleted in OMM) | Delete authentication key in OMM using the OMM cnf console command "akd". |
| RFP uses an authentication key, but RFP is not enrolled in OMM | <ul style="list-style-type: none"> SW down/upgrade (partially Loss OMM DB data); Delete and recreate RFP in OMM DB (if RFP is not connected with OMM) Apply DB backup to OMM with outdated RFP data OMM failover during key exchange Discard OM DB RFP moved to another OMM/SIP-DECT installation | <p>Keys are automatically removed from RFP if RFP is connected (encrypted connection in place) with OMM when deleted in OMM</p> <p>There can be no conflict for RFP on which the OMM is running (both in one device)</p> | Factory reset of all affected RFPs and enroll RFPs; if necessary delete RFPs in OMM and enroll again | Re-enrolment function (if RFP was already connected with OMM and has the same root credentials (locally stored) |
| RFP and OMM are using different keys | <ul style="list-style-type: none"> Apply DB backup to OMM with outdated RFP data* | | Factory reset of all affected RFP, delete RFPs in OMM and enroll again | Re-enrolment function (if RFP was already connected with OMM and has the same root credentials (locally stored) |

*** Example scenario:**

RFP OMM Standby configuration; OMM DB reset on OMM1; failover to OMM 2; automatic enrolment of RFP part of active OMM 2 (new authentication key); apply OMM DB backup; failover to OMM 1; mismatch of authentication keys in OMM 1 (old key) and RFP of OMM 2 (new key); Solution: automatically corrected with the next failover to OMM 2 or use re-enrolment

Support and maintenance

To delete an authentication key in OMM the OMM cnf console command "akd" can be used.

```
cnf rfp akd <dez RFP ID>
```

Note: Please be aware that an operational RFP will be put out of operation if the authentication key is deleted from the OMM.

To trigger the re-enrolment the OMM cnf console command “ren” can be used.

```
cnf rfp ren <dez RFP ID>
```

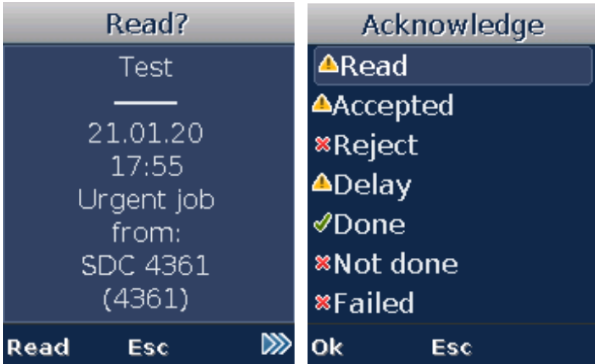
MSD-801 DFR18040 Menu enhancement for text message with only 2 confirmation requests

As of SIP-DECT 8.1SP1 and Mitel DECT Phone Firmware 7.3.2, the text messaging and altering usability is improved for message which request only 2 confirmations of the same type or only two confirmations remain after e.g. read confirmation has been sent. If there are only 2 confirmations, then both are accessible via softkey and there is no need to access the menu via the left soft key.



Read Yes /No Order OK / NOK Complete Done/ Not Done
Only 2 confirmations requested

There is no change if there are more than 2 confirmations or confirmations of different types requested. The menu to select from the confirmation list is presented on the left soft key



More than 2 confirmations requested

MessageConfirmType is an enumeration value defined as follows*:

| Value | Description |
|-----------------|--|
| ReadYes | Message was opened for reading |
| ReadNo | Message was deleted without reading it. |
| OrderOk | Order accepted |
| OrderNok | Order not accepted |
| OrderDontKnow | Not sure whether the order could be accomplished |
| CompleteDone | Accomplished |
| CompleteNotDone | Not accomplished |
| CompleteFailed | Failed to accomplish order |

* Further information can be found in the SIP-DECT OM Application XML interface, which is available via MSA.

OVA CentOS update

The MOM/OMM OVA comes with updated CentOS 7 kernel and packages CentOS7-B180518 01.01.2020.

MSD-1193: Update to AdoptOpenJDK 8u242

As of SIP-DECT 8.1SP1, the AdoptOpenJDK used to build OM Locating has been updated to 8u242.

MSD-1192 Update to AdoptOpenJDK 11.0.6

As of SIP-DECT 8.1SP1, the AdoptOpenJDK runtime of the OMP and OMC has been updated to 11.0.6.

MSD-823 wpa_supplicant (802.1x supplicant) updated to version 2.9

As of SIP-DECT 8.1SP1, the wpa_supplicant has been updated to version 2.9.

MSD-834 Hostapd updated to version 2.9

As of SIP-DECT 8.1SP1, the hostapd has been updated to version 2.9.

Installation and upgrade information for SIP-DECT 8.1

Update from previous releases

- Mitel DECT Phone SW 7.2.5 and 7.2.6 do not allow downgrading to previous SW builds.
- The SIP-DECT 8.1 upgrade installation is validated on top of the SIP-DECT 8.0, 7.1 and 7.0 releases. The upgrade to the SIP-DECT 8.1 release stream 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.

The screenshot shows the Mitel OMM configuration interface for SIP-DECT with Cloud-ID 8.0. The 'Advanced' tab is active. In the 'System Settings' section, the option 'Preserve user device relation at DB restore' is checked and highlighted with a red box. Other settings include Enhanced DECT security (unchecked), Authenticate before ciphering (unchecked), DECT authentication code (35157), DECT phone user login type (Number), Regulatory domain (None), Dynamic Frequency Selection (unchecked), ToS for voice packets (00), ToS for signalling packets (B8), and TTL (Time to live) (32). The footer indicates copyright 2006-2018 Mitel Networks Corporation.

Note: Ensure that with every major and minor release of SIP-DECT, you use the corresponding latest OVA instead of upgrading the existing OVA.

Note: Each delivered SIP-DECT release contained in the OVA file is based on a certain CentOS® 7 repository base marked by a certain date. Mitel provides the latest CentOS patches for SIP-DECT OVAs with service packs.

For security reasons, it is recommended that in the interim period between SIP-DECT releases, users access official CentOS repositories and run 'yum updates' to install CentOS patches released as fixes for critical issues.

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 8.1 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 8.1 release requires a restart of the entire SIP-DECT system.
- An upgrade 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.
- As of SIP-DECT 8.1, the 2nd generation RFPs (RFP 32, RFP 34, RFP 42) are not any longer supported. After an upgrade, configured RFP 42 WLAN profiles remain in the configuration but have no effect. Please, transform/remove such profiles.

Product compatibility with Mitel Call Server

Please see the Mitel call server release notes and the information provided with the Mitel Product Compatibility Matrix.

Where to find the latest information

Please Note: During EFT the update documentation will be made available by your Mitel trials contact.

You can access the most up-to-date versions of the following documents from the Mitel Document Center ([Link](#)).

SIP-DECT 8.1 Documentation Set:

- 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
 - MiVoice MX-ONE: SIP-DECT Migration from Legacy DECT Technologies

 - 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 8.1SP1-FA27 and 8.1-EJ02.

- MSD-930 GS-280326 No name displayed on DT phones if language changed
- MSD-1044 AXI clients can request data that exceeds size limit of data that can be transmitted within one AXI request
- MSD-962 MOM: Creation of a PP device with an invalid AC results in a wrong error message
- MSD-961 Creation of a PP device with an invalid AC results in a wrong error message
- MSD-1179 In special rare DNS SRV scenario could cause OMM restart
- MSD-1120 GS-287602 COA behavior for system_x is not as described/expected
- MSD-1123 OMP: changing the parameter "DECT phone system administration menu" has no effect
- MSD-1105 GS-286855 RFP 45 in SDC mode can connect only once in VLAN environment
- MSD-1086 PP does not return to idle state after FAC procedure
- MSD-1088 After successful 802.1x certificate configuration the stop button remains active
- MSD-1090 OMP: Standby-RFP-OMM can be selected for deletion

- MSD-1080 OMP provides RFP hardware type selection RFP32/34 and RFP42 for new DECT base station
- MSD-1163 CNF: loading of configured SIP trusted certificate not correct handled when the BEGIN line ends with \r\n
- MSD-1202 RFP does not activate new SW image
- MSD-1187 OMP crash when RFP enrolment file is not OK

Known issues and Limitations

- None

