SIP-DECT
DECT Phone Sharing and Provisioning

RELEASE 6.1
ADMINISTRATION GUIDE
# DECT PHONE SHARING AND PROVISIONING

- OpenMobility Provisioning ............................................. 3
- Features and Benefits ................................................. 3
- Basic Concepts .......................................................... 4
  - Data Model .............................................................. 4
  - Feature Access Codes ............................................... 5
- Other Documentation .................................................... 6

- OMM Administration Infrastructure ................................. 7
- OM Management Portal (OMP) ........................................ 7
- DECT Phone ............................................................... 8
- Provisioning server ...................................................... 8

- Subscription Handling .................................................. 10
  - Standard Subscription with IPEI .................................. 11
  - Wildcard Subscription ............................................... 11
  - Auto-create on Subscription ....................................... 12

- Feature Access Codes .................................................. 13
  - Configuring via OMM Web Service ................................. 13
  - Configuring via OMP .................................................. 16
  - Using FACs on the DECT Phone ................................... 18
  - Available FACs ....................................................... 19
    - Subscription FAC .................................................. 19
    - Login / Logout FACs .............................................. 20

- Data Set Associations .................................................. 22
  - Creating DECT Phone Data Sets ................................... 22
    - Enabling Subscription ............................................ 24
    - Initiating Subscription ......................................... 25
Creating User Data Sets .............................................. 27
Viewing User and Device Data ................................. 31
  OM Management Portal (OMP) .............................. 31
  OMM Web service ............................................. 32
Troubleshooting Dynamic Subscriptions .................... 32
  Check the DECT Phone’s IPEI ............................... 32
  Wildcard Subscription Enabled ............................. 33

External User Data Provisioning ................................. 34
  Using External User Data ..................................... 34
  Activating External User Data ............................. 36
  External User Data during Runtime ....................... 37
  OMM Database Provisioning Dependencies ............... 38
  Dependencies For Dynamically Linked Devices .......... 39
  External User Data Server File Specifications .......... 40
    Example: “user_common.cfg” .............................. 40
    Example: “<user>.cfg” or “<LoginID>.cfg” .............. 43
DECT PHONE SHARING
AND PROVISIONING
This document describes the DECT Phone sharing and provisioning feature, which has been enhanced for the OpenMobility SIP-DECT solution as of release 2.1 or higher.

The enhanced DECT Phone sharing and provisioning concept enables you to comfortably manage a large number of DECT phones and provides a more flexible subscription model. The SIP-DECT system supports features such as logging in and out with a personalized user account on different DECT phones, automatically subscribing new DECT phones or controlling subscription to specific system functions from DECT phones.

FEATURES AND BENEFITS

• “Auto-create on subscription” feature: Reduces administration effort by automatically creating DECT phone data in large systems during subscription (the SIP-DECT solution supports up to 2,048 DECT stations with up to 4,500 DECT phones).

• Moving a DECT phone from one user to another no longer requires administration (as with SIP-DECT releases < 2.1).

• Provisioning/Import of user data from an external source (“external provisioning server”), no redundant OMM administration required.

• Splitting of user data and DECT phone data is supported which allows the creation of a dynamic association between a DECT phone and a registered user.

These features support the following use cases:

• One DECT phone can be shared by different users at different points in time (“free seating”). The DECT phone is linked/unlinked by the user’s login/logout.
• Login with credentials of an user account that is administered externally is also possible.

BASIC CONCEPTS

Usually the Portable Part (PP) object in the OMM database represents a real DECT phone which contains specific DECT handset data (IPEI, AC, etc), as well as the data of the DECT phone user (number, name, etc). Both data sets have a fixed relation and the user cannot switch to another DECT phone without any administrative action.

Alternatively, is possible to split the PP data into DECT phone data and user data in the OMM database. This enhanced DECT Phone Sharing and Provisioning concept introduces a new data model that adds flexibility.

DATA MODEL

Data sets
While the OpenMobility SIP-DECT solution release 2.1 and earlier managed user data and DECT phone data in a single and fixed data set, newer SIP-DECT releases (release 2.1 and later) support two different data sets:

• A handset data set that stores data for the known DECT phones, such as the IPEI, access code and encryption information.

• A user data set, that stores the user specific settings, such as the phone number and the SIP account data.

Data set relations
Both data sets provide a relation to each other:

• A fixed relation between a user data set and the corresponding DECT phone data set is used to convert existing subscriptions from previous versions of the OpenMobility SIP-DECT solution or when you create subscription data with the OMM Web service.
• A **dynamic relation** which supports, for example, login and logout, is created if you use the OM Management Portal (OMP) Java tool to create new subscriptions.

**Note:** A database upgrade/migration (SIP-DECT release 1.5 to release 2.1 or higher) also results in fixed relations of user and device data sets. If you want to switch an imported subscription from a fixed to a dynamic relation, you can do so via the OM Management Portal (OMP).

**FEATURE ACCESS CODES**

You can use feature access codes (FACs) to control subscription specific features from a DECT phone. You can call a special phone number which accepts additional code digits to trigger a feature. This includes:

- Feature access code settings.
- Block-dialing of the feature access codes to trigger the feature or function.

Using a FAC, you may activate the subscription of new DECT phones, deactivate subscription, or login / logout a user.
OTHER DOCUMENTATION

This user guide describes installation, administration and usage of the Handset Sharing and Provisioning features. Please refer also to the information in the documentation related to other parts of your SIP-DECT installation:

- **SIP-DECT OM System Manual**
  Describes installation, administration, and maintenance of a SIP-DECT system.

- **SIP-DECT OM Locating Application**
  Describes how to install and use the DECT phone locating application.

- **SIP-DECT OM Integrated Messaging and Alerting Application**
  Describes messaging features and the integrated messaging solution.

- **SIP-DECT OM User Monitoring**
  Describes how to use the OM monitoring capabilities on DECT phones.

- **SIP-DECT Mitel 600 Messaging & Alerting Applications**
  Describes the messaging features specific to the Mitel 600 DECT phones.

- **Mitel 600 series DECT Phone User Guide**
  Describes using the Mitel 600 DECT phones on the SIP-DECT system.
OMM ADMINISTRATION INFRASTRUCTURE

Different instances that take effect for the user and device data set administration in the OMM database release 2.1 or higher. The following figure provides an overview:

OM MANAGEMENT PORTAL (OMP)

You can use the OM Management Portal (OMP) to

- create or delete fixed data sets
- create or delete unbound user data sets
- create or delete unbound device data sets
DECT PHONE

During the subscription process the DECT phone can

- create an unbound subscribed device data set
- change an unbound device data set to a subscribed one (where the IPEI fits)
- change a fixed device data set to a subscribed one (where the IPEI fits)
- change an unbound device data set to a fixed subscribed one (wildcard subscription)

A dynamically configured DECT phone can

- change unbound device and user data sets to dynamic linked ones (by performing a user login procedure),
- change dynamic linked device and user data sets to unbound ones (by performing a user logout procedure).

PROVISIONING SERVER

A provisioning server is any computer system that is able to provide the necessary files by tftp, ftp(s), http(s). The provisioning server provides a common user data file that specifies common user data settings (“user_common.cfg”). This file is queried and retrieved by the OMM when:

- the OMM starts up
- new server configuration settings are done
- a specified update interval elapsed

The provisioning server also provides a user file per user for the OMM (“<user>.cfg” or “<LoginID>.cfg”, or “user.cfg”). These files are queried and retrieved by the OMM when:

- a user logs in to a DECT phone
- a specified update interval elapsed during a login session
• a user data set in the OMM database is built
• a user data set is updated from data settings in the user and common user data file

**Note:** The OMM queries the provisioning server to retrieve the user data files. It is not a push operation by the server.

The provisioning server implicitly deletes user data sets in the OMM database when the user file disappears on the server – this is apparent at login time or when an update interval elapses.

For more information on the provisioning server please see “Using External User Data” on page 34.

For the user data file format description please refer to “External User Data Server File Specifications” on page 40.
SUBSCRIPTION HANDLING

The SIP-DECT solution supports the following subscription methods:

- standard subscription with IPEI
- wildcard subscription
- auto-create on subscription

After startup of the system, if no device has successfully completed the subscription process, manual subscription (including auto-create on subscription) are enabled permanently. When the first subscription is successfully completed, additional subscriptions are allowed for 24 hours or until the subscription mode is disabled by Feature Access Code (FAC), via the OMM Web service or the OM Management Portal (OMP) tool.

Manual and wildcard subscription can also be enabled and disabled by FAC, OMM Web service, or OMP.

**Note:** Mitel 600 DECT phones need the current DECT phone software version installed to support all features described in this document. You must initially subscribe Mitel 600 DECT phones with outdated software to update the software via download-over-air. See the “Download Over Air” section in the *SIP DECT OM System Manual* for details.
STANDARD SUBSCRIPTION WITH IPEI

The manual subscription method is characterized by management of user and device data with a fixed relation in the OMM database. Both user and device data are configured in one step.

From SIP-DECT release 2.1 and later, the system supports a fixed or dynamic association between a user and a device data set, depending on the administration mechanism:

- **OMM Web service**: supports only fixed associations between user and device data sets.
- **OM Management Portal (OMP)**: supports fixed and dynamic associations between user and device data sets.
- **External user data server** (see also “External User Data Provisioning” on page 34): only dynamic associations between user and device data sets are supported.

If manual subscription mode is enabled, the IPEI of the DECT phone performing the subscription procedure must be found in a device data set in the OMM database. Otherwise, subscription fails.

WILDCARD SUBSCRIPTION

The wildcard subscription method is a convenient method for assigning DECT phones to users without any device administration. Wildcard subscription only works for fixed associations between user and device data sets.

If wildcard subscription is enabled, the IPEI of the DECT phone performing subscription must not be stored in the OMM database. The additional ID entered at the DECT phone identifies the desired user data set. Because only fixed associations between user and device data sets are supported with wildcard subscription, the new DECT phone’s device data overwrites previously stored device data.
AUTO-CREATE ON SUBSCRIPTION

Auto-create on subscription allows the subscription of DECT phones automatically, without any device administration. This subscription method creates an unbound device data set. The mapping to a specific user data set is done in a second step with a user login procedure.

The Auto-create on subscription option is only available on the System settings page of the OMP (see “Creating DECT Phone Data Sets” on page 22). To activate this feature, you must enable the Auto-create on subscription option and also enable the subscription mode, either by FAC, OMM Web service, or OMP.

If the IPEI of a DECT phone that performs the subscription procedure is not found in the OMM database, a new (unbound) device data set is created. During the subscription procedure, the DECT authentication code configured in the OMM system settings must be entered on the DECT phone.

The duration for this functionality is identical to manual subscription period. The feature is inactive if “wildcard subscription” is activated.
FEASURE ACCESS CODES

The Feature Access Codes (FACs) allow you to control certain functions from a DECT phone. The functions available are related to the management of DECT phone subscriptions.

CONFIGURING VIA OMM WEB SERVICE

You activate and configure the desired set of Feature Access Codes through the OMM Web service.

1. Open a web browser and enter the DNS name or IP address of the OMM in the browser’s address input field.

   The OMM Web server switches to the secured HTTPS protocol and typically displays a certificate warning.

2. To bypass the browser warning automatically, a regularly re-paid validation certificate for the OMM network address must be issued by a third party. For connection to the OMM Web user interface in your LAN, you can safely ignore this message and store a permanent exception in your browser.

   When the certificate warning has been acknowledged, the browser displays the OMM login page.

3. Enter the **User name** that is configured at the OMM for the “Full access” account type (default is “omm”) and the password for the user account. Confirm with OK.

   The OMM Web service main page is displayed.

4. In the menu tree on the left, navigate to the System features -> Feature Access Codes page. Note that the
**Advanced** option in the title bar must be enabled to view this menu.

5. In the **FAC number** field, enter a phone number not currently in use by any other DECT phone. Use any combination of digits 0-9, the asterisk (*), or hash (#).

6. Enable the desired actions associated with the feature access code by enabling the appropriate check box, as well as the desired FAC action number code (0-9, *, or #).

 Protect critical functions with a longer sequence. To trigger a feature on the DECT phone, the DECT phone user must dial the FAC number, followed by the desired FAC action number code. See below for an example configuration.
7. Click **OK** to confirm your settings.

The feature access code configuration is applied immediately and can be used without restarting the OMM.

**Note:** While you are free to choose any valid sequence as a Feature Access Code, you should ensure that the FAC is compatible with the connected PABX system and that there are no conflicts. In the above example, an OpenCom 100 system is connected as SIP back-end. The OpenCom 100 PABX offers dialing codes for SIP phones that never start with a hash. To prevent conflicts, the above example uses the hash sign as the FAC number.
CONFIGURING VIA OMP

You can also configure Feature Access Codes through the OM Management Portal (OMP) tool. SIP-DECT supports Java web start to launch the OMP. You must have Java 1.7 or later runtime environment installed on your PC to run the OMP. The OMP.jar file is available in the OMM software installation directory, or you can download the jar file from the OM Web service interface.

1. Double-click on the OMP.jar file to launch the OMP.

   The OMP tool starts and displays a login window. Note that the System name drop-down list is empty if you started the tool for the first time.

2. Enter the IP address of the DECT base station or Linux server hosting the OMM, and the User name and Password required to access the OMM (i.e., “Full access” account, default is “omm”).
3. In the left navigation pane, click on **System features** to expand the list of sub menus, then click **General settings** to display the **General** tab.

4. In the **FAC number and prefix for alarm triggers** field, enter a phone number not currently used by any other DECT phone. Use any combination of digits 0-9, the asterisk (*), or hash (#).

5. Click **OK** to confirm.

6. In the left navigation pane, navigate to the **System features** -> **Feature access code** menu.

7. Enable the desired feature access codes by activating the appropriate check box, as well as the desired FAC action.
number code (0-9, *, or #). Protect critical functions with a longer sequence.

8. Click **OK** to confirm your settings.

**USING FACS ON THE DECT PHONE**

You can use FACs from any DECT phone subscribed to the OMM.

1. In the idle state of the (subscribed) DECT phone, enter the FAC number on the phone’s dial pad, including the digits for the desired FAC action.

   Note that you cannot activate a feature access code by dialing digit-by-digit. You must use block-dialing.

2. Press the call key to activate the feature access code.
   - If you dialed the correct code, you hear an acknowledgment sequence that consists of a deep tone followed by a high-pitched tone.
   - If you dialed the correct FAC number but an unknown FAC action code, you hear a negative acknowledgment.
• Otherwise, you hear a busy tone.

**Note:** The dialed feature access codes are not added to the DECT phone’s re-dial list.

### AVAILABLE FACS

The following feature access codes are available. The listed dialing sequences (shown in parenthesis) are examples which are valid with the example configuration provided in “Configuring via OMM Web Service” on page 13.

### SUBSCRIPTION FAC

**Activate subscription (**134567**)

Enables or extends the standard subscription period for 24 hours. Completing the subscription is possible only for DECT phones for which a subscription entry exists that includes the IMSI number in the OMM’s DECT phone database. Note that you should configure a longer and secret FAC action code for this function to maintain system security.

The standard subscription mode automatically ends after one hour.

**Activate wildcard subscription (**134568**)

Enables or extends the wildcard subscription period for 1 hour. Completing the subscription is possible from any DECT phone by using the correct access code (refer to the DECT authentication code field on the System -> System settings page of the OMM Web service). You should configure a longer and secret FAC action code for this function to maintain system security.

The wildcard subscription mode automatically ends after two minutes. After two minutes, the standard subscription mode is active for one hour.
Note that the **Auto-create on subscription** option available on the **System -> Basic settings** page (**DECT** tab) of the OM Management Portal (OMP) tool is inactive when wildcard subscription is enabled (see “Creating DECT Phone Data Sets” on page 22).

**Deactivate subscription (**19)**
Disables the subscription mode immediately. DECT phones cannot subscribe to the OMM in this operating mode.

**LOGIN / LOGOUT FACS**

Dynamic devices require a user login operation and a logout operation to disassociate the device from a user and prepare it for a new login (e.g., for a different user). To login/logout on an unbound device, a feature access code followed by the user’s telephone number must be dialed en-bloc.

The login/logout operation is implemented by using the DECT user authentication mechanism (defined in the DECT standard), to ensure security. Optional encrypted data transfer can be used over the air interface. For more information on data encryption, refer to the *SIP-DECT OM System Manual*.

**User login (**11[user phone number / login ID])**
Enter this feature access code to log in. Extend the FAC with the phone number of the user who wants to log in. Press the call key and enter the user’s PIN to complete.

This feature access code can be executed only on DECT phones that have a dynamically linked DECT phone data set. User login is initiated when this FAC is received. After the DECT user authenticates successfully, the DECT phone data set is linked to the desired user data set. Phone calls to the user’s phone number are signalled on the DECT phone.
Feature Access Codes

FAC Login Procedure

Display shows phone is unbound.  Dial the FAC plus user number (1012).  Enter the PIN to gain access.  You are now logged in.

User logout (*12)
Enter this feature access code to log out. Press the call key and enter the user's PIN to complete. This FAC can only be executed on DECT phones with a dynamically linked handset data set. If this FAC is received, the OMM marks the corresponding DECT phone data set as unused, which unlinks it from the user data set. Phone calls to the user's phone number are no longer signalled on the DECT phone, and another user may log in to the DECT phone.

FAC Logout Procedure

Dial FAC to initiate logout. Enter PIN to proceed. System confirms the process. Display shows phone is unbound.
DATA SET ASSOCIATIONS

The standard association between a DECT phone and a user is static. This means that the association between the DECT phone data set (IPEI, encryption data) and the corresponding user data set (phone number, name) is fixed. If another user wants to use the DECT phone, the DECT phone must be unsubscribed and resubscribed for the new user.

The SIP-DECT solution also supports a dynamic association between the DECT phone data set and a user data set. You must subscribe a DECT phone in a specific way. A DECT phone with a dynamic subscription can be linked to a user data set by means of a login procedure. Likewise, you can free the DECT phone data set with a logout procedure.

CREATING DECT PHONE DATA SETS

While you can manage fixed subscriptions with the OMM Web service, you must use the Java-based OMP tool to create and manage dynamic subscriptions.

When the Auto-create on subscription feature is enabled, a dynamic data set is automatically created when a new and unknown DECT phone subscribes to the OMM. Because you do not add a data set manually, you cannot assign individual authentication codes for each DECT phone. Instead, the authentication code configured in the DECT authentication code field can be used to subscribe DECT phones.

1. Launch the OMP by double-clicking on the “OMP.jar” file (located in the SIP-DECT installation directory, or downloaded from the OMM Web service).

   The OMP starts and displays a login window.

2. Enter the IP address of the DECT base station or Linux server hosting the OMM, and the User name and Password required to access the OMM (i.e., “Full access” account, default is “omm”). Click OK to login.
3. Navigate to the **System -> Basic settings** page and select the **DECT** tab.

4. Enable the **Auto-create on subscription** parameter.

5. Select the login method for all DECT phone users in the **Portable part user login type** field. The user can be identified during login by the telephone number or SIP user name (**Number/SIP user name**) or by the unique user login ID (**Login ID**). Both elements are part of each user data set. This setting is system-wide.

   **Note:** Changing this setting forces an automatic logout on all logged in DECT phones.

6. Click **OK** to confirm your settings. Note that the activated Auto-create on subscription status is displayed at the bottom of the OMP window.
ENABLING SUBSCRIPTION

For security reasons, the subscription feature is initially turned off. To subscribe a new DECT phone (and thereby create a dynamic subscription), you must enable the Subscription allowed status. You can enable this feature via the following methods:

• OMM Web service: In the OMM Web interface, navigate to the DECT Phones page. Click the Start button below the Subscription with configured IPEIs caption.

• OMP: In the OMP, navigate to the DECT Phones -> Devices page. Click on the Subscription command in the Tasks pane to enable subscription allowed mode.
• **Feature Access Code:** Use a Feature Access Code to enable the subscription from a DECT phone. Dial the desired FAC code and trigger it by pressing the call key. You should hear the positive acknowledgment sequence.

**INITIATING SUBSCRIPTION**

Initiate the subscription on the desired DECT phones.

1. Open the DECT phone’s **System** menu and select the **Subscriptions** entry.

2. When prompted for the system PARK, you may optionally type in the 14 digit decimal PARK number of the appropriate SIP-DECT system. This number is displayed in the OMM Web service on the **System** -> **System settings** page.

3. When prompted for the access code, enter the SIP-DECT system’s DECT authentication code. This number is displayed in the OMM Web service on the **System** ->
**System settings** page (and can be modified). The OMP also displays this number on the **System -> Basic Settings** page (DECT tab).

4. Complete the subscription process as usual. The DECT phone should indicate a successful subscription with the appropriate message. The following images illustrate an example performed with a Mitel 600 DECT phone.

**Dynamic Subscription**

<table>
<thead>
<tr>
<th>Open the <strong>System</strong> menu on the DECT phone.</th>
<th>Select the <strong>Subscriptions</strong> -&gt; <strong>New system</strong> command.</th>
<th>Enter the DECT authentication code.</th>
<th>Wait for subscription to complete.</th>
</tr>
</thead>
</table>

If the subscription completes successfully, the DECT phone shows a “Please Login” home screen. Repeat these steps for any number of DECT phones. When complete, you must create at least one user data set to perform a successful login (“Creating User Data Sets” on page 27).

**Note:** The above example shows the subscription without entering the PARK on the DECT phone. However, if more than one DECT system is active in the area, you should also enter the PARK code during the subscription process.
CREATING USER DATA SETS

With a standard fixed subscription you can use the DECT phones after a successful subscription. With dynamic subscriptions, you must add at least one user account in order to log in.

1. Launch the OMP and navigate to the DECT Phones -> Users page.

2. Click the Create command in the Tasks menu on the right. The New user window opens below the Users table.

3. Select the General tab and enter the following information:
   - **Name**: The name displayed on the DECT phone home screen after the user successfully logs in.
   - **Number/SIP user name**: The phone number or SIP user name for the user. After a successful login, this number can be called by other DECT phones to reach the user.
   - **Description 1 / Description 2**: Text to describe the user data set.
• **Login/Additional ID**: A unique ID to distinguish different user data sets. The login ID can be used instead of the phone number when the Login ID login variant is set in the **Portable part user login type** parameter of the OMP System -> Basic settings page, DECT tab.

• **PIN, PIN confirmation**: To log in and out, the user must provide a PIN code when entering the appropriate feature access code. Enter this PIN in these fields.

4. Select the **SIP** tab and enter the SIP account data for the user. If you do not configure a valid SIP account, the logged in user cannot make phone calls.

   • **User name**: Enter the authenticating user name for the SIP account.

   • **Password**: Enter the SIP password.

   • **Password confirmation**: Re-enter the SIP password for confirmation.

   • **VIP**: Enable this option if the registration of this user should be prioritized. VIP users are registered first. For more information on prioritized registration see the **SIP-DECT OM System Manual**.

   • **Used for visibility checks**: Enable or disable the use of this user account to check availability of the iPBS (e.g., in failover situations). For more information on this feature, see the **SIP-DECT OM System Manual**.

   • **Fixed port**: Specify the port to use for SIP signaling. If set to 0, an automatically calculated port is used. For more information on SIP multi-port, see the **SIP-DECT OM System Manual**.

Note that all SIP-DECT users use the same SIP server. The SIP server settings are available on the OMP System -> **SIP** page.

5. Select the **Incoming calls** tab to specify settings for auto-answering of incoming calls.
• **Auto answer**: Enable or disable auto-answer on incoming calls.

• **Microphone mute**: Enable or disable microphone muting when incoming calls are automatically answered.

• **Warning tone**: Enable or disable the playing of a warning tone on an incoming call. A short ring tone is played if there are no active calls. If there is an active call (in a “barge in” situation) the ringing is in-band.

• **Allow barge in**: Allow or disallow “barge-in” on existing calls.

6. Select the Conference tab to configure three-way conferencing settings.

   • **Server type**: Specify the conference service to be used for three-way conferencing (“None”, “Global”, “Integrated”, or “External”).

   • **URL**: If the conference server type is “External”, specify the URL to reach an external conference server.

7. Select the **Messaging** tab to configure the OM Integrated Messaging and Alerting service for the user data set. For more information, see the *SIP-DECT OM System Manual*.

   • **Sending messages permission**: If enabled, the DECT phone can send messages (if supported by the device).

   • **Sending vCards permission**: Allows the user to send personal directory entries as vCard messages from the DECT phone to other users (if supported by the device).

   • **Receiving vCards permission**: If enabled, all received vCard messages are automatically processed and written into the personal directory of the DECT phone (if supported by the device).
8. Select the **Locating** tab to change the settings for the OM Locating application. These settings determine whether the DECT phone is locatable from the Locating application when the user is logged in. See the *SIP-DECT OM Locating Application* guide for details.

9. Select the **Additional services** tab to configure additional settings for the user data set. See the *SIP-DECT OM System Manual* for more information.

   - **SOS number**: Specify the number called if the logged in user presses the SOS key on the phone (e.g., on a Mitel 600).
   - **ManDown number**: Specify the number called if the DECT phone (e.g., a Mitel 600) detects a ManDown condition.
   - **Voice mail number**: Specify the number called for voice mail on the DECT phone. If no number is specified, the system-wide number is used.
   - **Keep personal directory**: Enable or disable preservation of the personal directory data in the DECT phone when the user logs out.
   - **External**: Specify whether the user data set is provisioned on an external user data server or locally in the OMM database. See the *SIP-DECT OM System Manual* for information on this feature.
   - **Video stream permission**: Enable or disable video stream permission. When enabled, the DECT phone user can choose a camera from a list in the system menu. See the *SIP-DECT OM System Manual* for information on the Terminal Video feature.

10. Select the **User Monitoring** tab to enable user monitoring.

    - **Monitoring mode**: Specify the monitoring mode for the user (Active, Passive, or Off). “Off” disables user monitoring. “Passive” and “Active” enable user monitoring and control the mode of the DECT phone activity.
Data Set Associations

status supervision. Default setting is Off.

Note that if user monitoring is activated, the VIP option on the SIP tab is automatically enabled. The VIP option is not reset if the user monitoring mode is set to “Off”. See SIP-DECT OM System Manual for more information on the User Monitoring feature.

11. Select the Configuration data tab to assign a Configuration over Air (CoA) profile.

   • **Profile id**: Select the CoA profile to use from the drop-down list. For more information on this feature, see the SIP-DECT OM System Manual.

12. Click OK to create the new DECT phone user data set.

You can repeat these steps for any number of user data sets. Alternatively, you can import user data sets from an external server (e.g., for a large number of data sets, see “External User Data Provisioning” on page 34).

**VIEWING USER AND DEVICE DATA**

You can view user and DECT phone data through the OMP or the OMM Web service.

**OM MANAGEMENT PORTAL (OMP)**

Associated users and devices are listed on the OMP DECT Phones -> Overview page. Data sets with imported user data are marked with a checkmark in the External column.

Imported user data sets are also listed in the on the DECT Phones -> Users page and marked with a checkmark in the External column. For information on importing user data see “External User Data Provisioning” on page 34.

If the login is successful, the user and DECT phone are associated. The association is displayed on the DECT Phones
-> Devices page, where the Device rel. type column shows the Dynamic as the relation type.

OMM WEB SERVICE

User and device data are combined into DECT phone data in the OMM Web service.

External or unbound user data sets (configured with OMP) do not have a dedicated DECT phone. Users must login to a DECT phone first.

All DECT phone data that are configured as unbound (split into device and user data) are listed in the OMM Web service when users are logged in to the device. They cannot be deleted or changed.

TROUBLESHOOTING DYNAMIC SUBSCRIPTIONS

If you cannot dynamically subscribe a new DECT phone to the SIP-DECT system, you should check the following.

CHECK THE DECT PHONE’S IPEI

You cannot re-subscribe a known DECT phone to the SIP-DECT system. If you have a DECT phone that you cannot subscribe, it is likely that a previous subscription is still active.

The IPEI should not be known to the SIP-DECT system. To verify, do the following:

1. On the DECT phone, open the System -> Show IPEI menu to display the unique IPEI number (for example “03586 0017017 7”).

2. Start the OMP and navigate to the DECT Phones -> Devices page. Click on the IPEI table heading to sort the display by number.
3. If the IPEI in question is displayed in the list, you must remove the subscription to proceed. Highlight the desired device item and click the **Delete** command from the Tasks menu in the right pane.

4. Click **OK** in the confirmation dialogue to confirm that you want to remove the device.

To create a dynamic subscription for the DECT phone, follow the steps described in “Creating DECT Phone Data Sets” on page 22.

**WILDCARD SUBSCRIPTION ENABLED**

With the wildcard subscription feature, you can subscribe a DECT phone without entering the IPEI number. Note, however, that this “first come – first served” approach conflicts with the dynamic subscription feature.

1. Log into the OMM Web service and navigate to the **DECT Phones** page. Verify that the **Wildcard subscription** option is disabled. If the feature is enabled, click the **Stop** button below the **Wildcard subscription** caption.

2. Launch the OMP and navigate to the **System -> Basic settings -> DECT** tab. Enable the Auto-create on subscription option and click **OK** to confirm.

After completing the above steps, you can subscribe new DECT phones while creating a dynamic subscription.
EXTERNAL USER DATA PROVISIONING

Although you must subscribe a DECT phone to the SIP-DECT system manually, the process of creating new user accounts can be automated. This feature allows you to manage a large number of users who can log in to the subscribed DECT phones.

Scenario:
You operate an external provisioning system that can provide user account data. Also, you have registered a larger number of DECT phones while creating a dynamic subscription. The solution to integrate these two systems is to use external configuration files that are loaded when the SIP-DECT solution starts or when a new and currently unknown user performs the first login operation.

USING EXTERNAL USER DATA

You can import user data from an external server. On the external TFTP, HTTP or FTP server a specific file must be provided for each user. The file has a similar format as the other OMM configuration files. Secure protocols can optionally be used for security reasons (FTPS or HTTPS). LDAP user data import is *.ffs.

In addition, a common configuration file (e.g. for default user data) is requested from the server for all external users. Some data sets in a user data file overwrite the data of the common configuration file.

All additional user data values that can be changed at the DECT phone (call forwarding, etc) are saved locally in the OMM database and are used as long as the user is available on the external server. A user that disappears on the server is also deleted in the OMM database, and the DECT phone is unlinked from the user (automatically logged out).
Common file name conventions must be used on the server. The server can distinguish different OMM systems in different directories. The following conventions are used:

- **common user configuration file** “user_common.cfg”
  
  This file contains user configuration settings common to all users. See “Example: “user_common.cfg”” on page 40 for a detailed description of the file format.

- **user data files:** “<user>.cfg” or “<LoginID>.cfg” or user.cfg
  
  Each user’s configuration settings are stored in a user-specific file where the file name contains the phone number of the user. See “Example: “<user>.cfg” or “<LoginID>.cfg”” on page 43 for a detailed description of the file format.

With SIP-DECT 6.0 or later, <user>.cfg can also refer to user.cfg, a common file name for all users. If the “UDS_CommonUserFileName” configuration attribute is enabled in the user_common.cfg file, the OMM tries to fetch the same user.cfg file for each user executing the login procedure (i.e., the login credentials of each user are used to access the provisioning server). This means that the provisioning server executes user authentication and provides a user-specific user.cfg when the user is authorized. This concept allows the provisioning server to provide user-specific settings on demand, using one file name based on the specific user credentials.

To remain in sync with the server’s data, the common configuration and the user data file can contain parameters for an update interval (default are 24 hours for both if not explicitly set):

- **Common configuration file:** the timer starts when the file is imported.

- **User data files:** the timer starts at login. The user data file is also re-imported at any login.
ACTIVATING EXTERNAL USER DATA

You need an external TFTP, HTTP or FTP server to deploy external user data configuration files to the SIP-DECT system. You can also use secure protocols (e.g., FTPS or HTTPS) for security reasons. You enable the external user data server through the OMP.

1. Launch the OMP and navigate to the System -> Data management page. Select the User data import tab.

2. Enter the following information:
   - Enable the Configure specific source option. This ensures that the OMM retrieves the user data file from the specified server, instead of the centralized external provisioning server. (See the SIP-DECT OM System Manual for more information on the provisioning server feature.)
   - Select the Protocol to use (i.e., FTP, TFTP, FTPS, HTTP, HTTPS, or SFTP).
   - Enter the server IP address or DNS name.
   - If you selected the FTP(S) or HTTP(S) protocol, enter a User name and a Password for downloading the files. A TFTP server does not require this data.
• Specify the Path to the sub-directory where the configuration files are stored (relative to the server root directory).

3. Click OK to confirm the settings and activate the configuration.

EXTERNAL USER DATA DURING RUNTIME

With the above example configuration, the following occurs during the SIP-DECT startup and runtime:

• When the OMM starts, it reads in the defaults file named “user_common.cfg”. In the above example, the “tftp://192.168.112.109/user_config/user_common.cfg” is loaded.

• When a new user logs in, a specific user configuration file is loaded. For example, if the Feature Access Code for the 4711 user is used, the “tftp://192.168.112.109/user_config/4711.cfg” file is loaded.

Both files determine the user configuration of the newly logged in user. You can set, for example, a common log in PIN code that is valid for all users (user_common.cfg). You can then provide more specific settings, for example by specifying an arbitrary display name for the 4711 user in the <4711.cfg> file.

See “External User Data Server File Specifications” on page 40 for two example files.
OMM DATABASE PROVISIONING DEPENDENCIES

The following dependencies exist when the database is loaded after OMM startup:

- Dynamic links between user and DECT phone data sets are restored.
- User data including personal settings (e.g. call forwarding) are stored permanently in the OMM database as long as the user is known on the server. This allows the system to keep data changed by the user between logout and the next login.
- All external user data is re-imported at startup. When they no longer exist on the server, the respective user data sets are also removed from the OMM database. Removing a user data set also forces a logout on all affected DECT phones.
- The login status is not restored by an OMM database restore operation. Users must login again in this case.

The OMP interface can also affect user and device data:

- When a dynamically linked DECT phone data set is deleted, the bound/linked user data set is set to logged out.
- When a dynamic linked user data set is deleted, the corresponding DECT phone is logged out and a login mask is displayed.
- Dynamic user/device data sets can not be administered through the OMM Web service. They are displayed as read-only.
DEPENDENCIES FOR DYNAMICALLY LINKED DEVICES

Dynamically linked DECT phones must perform certain procedures to operate (e.g., login, logout). For security reasons, authorization is required when a user executes such a procedure, so that each procedure is secured through user identification and a PIN code. This authentication is accomplished with the DECT user authentication mechanism specified in the DECT standard. This mechanism ensures that the PIN is not exchanged on the air interface. All DECT phones support this mechanism.

DECT phones that are dynamically linked to users have the following dependencies:

• DECT user authentication is not supported with the Mitel 600 feature pack 1. You must upgrade the DECT phone firmware to the latest version.

• The login and logout procedures are available on all GAP phones by initiating a call. Specific FAC numbers are used to distinguish those procedures from other call activities.

• You cannot manipulate the display on a GAP DECT phone when the device is not in call state. The login mask cannot be displayed when the GAP phone is logged out. The OMM sends the “Please login” display to a GAP phone when the device is placed off-hook.

• The following information is stored locally on a DECT phone:
  - Message list
  - Message icon
  - Received call list
  - Caller list
  - Local phone book
  - Call forwarding icon
For privacy protection, these are deleted when the user logs out. This is only possible for Mitel 600 DECT phones, and is not supported on GAP devices.

- The DECT phone maintains a local configuration. That local configuration data is not cleared if a new user logs in.

- User name and number:
  - **GAP devices and Mitel 142d DECT phones**: User name and number must be manually set on the DECT phone after login. Local lists (e.g. redial list) must be manually cleared after logout.
  - **Mitel 600 DECT phones**: User name and number are automatically set on the DECT phone after user login. Local lists on the handset (e.g. redial list) are automatically cleared after logout.

**EXTERNAL USER DATA SERVER FILE SPECIFICATIONS**

This section contains the file format description of the configuration files which can be retrieved from an external user data provisioning server.

**EXAMPLE: “USER_COMMON.CFG”**

The common user data configuration file “user_common.cfg” is an ASCII file. The file is processed line by line, and any content that follows a hash sign (#) is treated as a comment and is ignored. You should use the UNIX style line end convention (UTF-8 encoded).

Usage of the “user_common.cfg” configuration file is optional.

```
# user_common.cfg sample configuration file for Automatic User Import
# retrieved via the net using file transfer protocols like tftp, ftp(s) or http(s)
# comments are starting with the hash sign: "#"
```
# BOOL variables support YES Y 1 TRUE or NO N 0 FALSE
# (case does not matter), other values are interpreted as false

# Common User data configuration possibilities:

# OM_<variable>  # Identifier for an OMM variable setting
# UDS_<variable>  # Identifier for a user data server variable # setting
# UD_<variable>   # Identifier for a user data variable setting

UDS_CommonUpdateInterval=6  # Interval to re import this file in hours /
                            # default=24 hours when not set
UDS_CommonUserFileName=NO  # Enables / disables use of same
                            # user.cfg file for each user logging in.
UD_SosNumber=112  # Common SOS number when needed
UD_ManDownNumber=112  # Common ManDown number when
                      # needed
UD_Pin=1234  # User PIN, all user data sets will be set
             # to this value initially when not set in the
             # "<user>.cfg" file / default=0000 / can
             # also be given in a public key encrypted
             # form
UD_UpdateInterval=4  # Interval to re import user data files in
                    # hours / default=24 hours when not set
UD_Locatable=FALSE  # BOOL, if TRUE the user is locatable
                   # per default (licensed)
UD_LocatingPermission=FALSE  # BOOL, if TRUE locating for the user is
                             # allowed per default (licensed)
UD_Tracking=FALSE  # BOOL, if TRUE live tracking for the
                   # user is activated per default
UD_AllowMsgSend=FALSE  # BOOL, if TRUE permission to send
                      # messages for the user is activated per
                      # default (licensed)
UD_AllowVCardSend=FALSE  # BOOL, if TRUE permission to send
                     # vcard from DECT phone user is activated
UD_AllowVCardRecv=FALSE  # BOOL, if TRUE permission to receive vcard on DECT phone is activated

UD_KeepLocalDir=FALSE  # BOOL, if TRUE permission to keep local directory after DECT phone log off is activated

UD_VoiceMailNumber=22222  # User voice mail number when needed

UD_UserMonitoring=Active  # One of "Off", "Active" or "Passive" to set the user monitoring mode

UD_ConferenceServerURI=  # Conference server URI

UD_ConferenceServerType=  # Conference server type “Global”, “Off”, “External”, “Integrated”

#UD_Vip=FALSE  #BOOL, if TRUE SIP prioritization is enabled / Supported >= OMM release 4.0

#UD_AllowVideoStream=FALSE  # BOOL, if TRUE video streaming is enabled / Supported >= OMM release 5.0

#UD_PpProfileId=0  # Id of the CoA profile data (setting to 0 means no profile to use) / Supported >= OMM release 6.0

#UD_AutoAnswer=Global  # One of "On", "Off" or "Global" / Allows auto answering for n call / Supported >= OMM release 6.0

#UD_MicrophoneMute=Global  # One of "On", "Off" or "Global" / Microphone controlling for calls made by the originating caller / Supported >= OMM release 6.0

#UD_WarningTone=Global  # One of "On", "Off" or "Global" / Controls warning tone to play when the PP receives an incoming call on an active line / Supported >= OMM release 6.0

#UD_AllowBargeIn=Global  # One of "On", "Off" or "Global" / Controls the behavior how the PP handles incoming calls while the phone is on an active call / Supported >= OMM # release 6.0
Note: In addition to the parameters listed above, there are additional parameters for the Configuration over Air feature (SIP-DECT 6.0 and later). See the SIP-DECT OM System Manual for a complete list of supported parameters.

EXAMPLE: “<USER>.CFG” OR “<LOGINID>.CFG”

The user data configuration file “<user>.cfg” (e.g., “4711.cfg” for the 4711 user) or “<LoginID>.cfg” (e.g. “1001.cfg” for the 1001 login ID) is an ASCII file. The file is processed line by line, and any content that follows a hash sign is treated as a comment and is ignored. You should use the UNIX style line end convention (UTF-8 encoded).

The specific user data settings in the “user.cfg” file will overwrite settings that are specified in the common user configuration file (“user_common.cfg”). The following example shows a user configuration file sample for the user “4711”.

# 4711.cfg sample user configuration file
# Possible user data configuration settings:

UD_PinDel=FALSE # BOOL, if TRUE the user PIN is deleted in
# OMM private data to default "0000"; must
# be set to FALSE after the file is processed
# to allow setting of a new user PIN at the
# linked DECT phone.
# PIN updates are not applied as long the
# user is active

UD_Pin=4711 # User PIN to login and logout. Can only be
# used until PIN is changed at the DECT
# phone. Can also be given in a public key
# encrypted format

UD_UpdateInterval=1 # Interval to re-import user data files in hours
# / default=24 hours when not set
SIP-DECT DECT Phone Sharing and Provisioning Guide

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UD_Number=4711</td>
<td># Subscriber number or SIP call name, ignored when DECT phone user login type is set to “Number”. # (See System settings in Web or OMP.)</td>
</tr>
<tr>
<td>UD_Name=Julian</td>
<td># Displayed name</td>
</tr>
<tr>
<td>UD_SosNumber=112</td>
<td># Common SOS number when needed</td>
</tr>
<tr>
<td>UD_ManDownNumber=112</td>
<td># Common ManDown number when needed</td>
</tr>
<tr>
<td># UD_VoiceMailNumber=22222</td>
<td># User voice mail number when needed</td>
</tr>
<tr>
<td>UD_SipAccount=4711</td>
<td># SIP account</td>
</tr>
<tr>
<td>UD_SipPassword=0815</td>
<td># SIP password</td>
</tr>
<tr>
<td># UD_Vip=TRUE</td>
<td># BOOL, if TRUE SIP prioritization is enabled</td>
</tr>
<tr>
<td>UD_Locatable=FALSE</td>
<td># BOOL, if TRUE the user is locatable, default is FALSE (licensed)</td>
</tr>
<tr>
<td>UD_LocatingPermission=FALSE</td>
<td># BOOL, if TRUE locating for the user is allowed per default (licensed)</td>
</tr>
<tr>
<td>UD_Tracking=FALSE</td>
<td># BOOL, if TRUE live tracking for the user is activated per default</td>
</tr>
<tr>
<td>UD_AllowMsgSend=FALSE</td>
<td># BOOL, if TRUE permission to send messages for the user is activated per default (licensed)</td>
</tr>
<tr>
<td>UD_AllowVCardSend=FALSE</td>
<td># BOOL, if TRUE permission to send vcard from DECT phone user is activated</td>
</tr>
<tr>
<td>UD_AllowVCardRecv=FALSE</td>
<td># BOOL, if TRUE permission to receive vcard on DECT phone is activated</td>
</tr>
<tr>
<td>UD_KeepLocalDir=FALSE</td>
<td># BOOL, if TRUE permission to keep local directory after DECT phone log off is activated</td>
</tr>
<tr>
<td># UD_UserMonitoring=Active</td>
<td># One of &quot;Off&quot;, &quot;Active&quot; or &quot;Passive&quot; to set the user monitoring mode</td>
</tr>
<tr>
<td>UD_HierarchyName1=first aider</td>
<td># Optional 1. hierarchy name of a user, to make groups of users up to 16 bytes</td>
</tr>
</tbody>
</table>
# UD_HierarchyName2=f  # Optional 2. hierarchy name of a user, to  
# make groups of users up to 16 bytes

# Conference server URI

# UD_ConferenceServerURI=

# Conference server type “Global”, “Off”,  
# “External”, “Integrated”

#UD_AllowVideoStream=  # BOOL, if TRUE video streaming is enabled  
FALSE  # / Supported >= OMM release 5.0

#UD_SipRegisterCheck=  # BOOL, if TRUE this user is enabled for SIP  
FALSE  # register checking / Supported >= OMM  
# release 5.0

#UD_PpProfileId=0  # Id of the CoA profile data (setting to 0  
# means no profile to use) / Supported >=  
# OMM release 6.0

#UD_AutoAnswer=Global  # One of "On", "Off" or "Global" / Allows auto  
# answering for n call / Supported >= OMM  
# release 6.0

#UD_MicrophoneMute=Global  # One of "On", "Off" or "Global" / Microphone  
# controlling for calls made by the originating  
# caller / Supported >= OMM release 6.0

#UD_WarningTone=Global  # One of "On", "Off" or "Global" / Controls  
# warning tone to play when the PP receives  
# an incoming call on an active line /  
# Supported >= OMM release 6.0

#UD_AllowBargeIn=Global  # One of "On", "Off" or "Global" / Controls the  
# behavior how the PP handles incoming  
# calls while the phone is on an active call /  
# Supported >= OMM release 6.0