SIP-DECT Phone Sharing and Provisioning

ADMINISTRATION GUIDE

RELEASE 8.0

Mitel®

NOTICE

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

Trademarks

SIP-DECT Phone Sharing and Provisioning
Administration Guide
Release 8.0 - September 2018

DECT PHONE SHARING AND PROVISIONING

DECT PHONE SHARING AND PROVISIONING

OPENMOBILITY PROVISIONING

The DECT phone sharing and provisioning feature makes it easier to 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 reduces administrative effort by automatically creating DECT phone data in large systems during subscription (the SIP-DECT solution supports up to 4096 DECT stations with up to 10,000 DECT phones).
- Moving a DECT phone from one user to another does not require any administrator action (SIP-DECT 2.1 and later).
- Provisioning/Importing user data from an external source (“external provisioning server”) does not require any additional OMM administration.
- 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 to a user when the user logs in or logs out.
- Login with credentials of an user account that is administered externally is also possible.

BASIC CONCEPTS

Typically, the Portable Part (PP) object in the OMM database represents a real DECT phone that contains specific DECT phone data (IPEI, AC, etc), as well as data for the DECT phone user (number, name, etc). There is a fixed association between the two data sets and the user cannot switch to another DECT phone without an administrative action.

SIP-DECT also supports splitting the device data into DECT phone data and user data in the OMM database. This enhanced DECT phone sharing and provisioning feature concept introduces a new data model that adds flexibility.

DATA MODEL

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

- A DECT phone 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 associations
There are two types of association between a DECT phone data set and a user data set:

- A **fixed association** indicates that the user can only use the specified DECT phone, and vice versa. The DECT phone is not shared with other users. When you add a new device record via the OMM Web service, you must specify a user (and thereby create a fixed user/device data set).
- A **dynamic association** indicates that the DECT phone can be used by more than one user. The association between the DECT phone and a user is established when

the user logs in and logs out. You can create unbound user and device data sets through the OM Management Portal (OMP) tool.

Note: A database upgrade/migration (SIP-DECT 1.5 to 2.1 or higher) results in fixed associations between user and device data sets. If you want to switch an imported subscription from a fixed to a dynamic association, 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 that accepts additional digits to trigger a feature, including:

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

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

ADMINISTRATION MENU

With SIP-DECT 6.0 and later, the Mitel 600 DECT phones include an **Administration** menu that offers administrative functions to the user, such as login, logout, and configuration and status summary display.

The menu is available as an option under the **System** menu on the DECT phone (available from the main menu, or by pressing and holding the softkey)

See the *Mitel 600 Series DECT Phone User Guide* for more information.

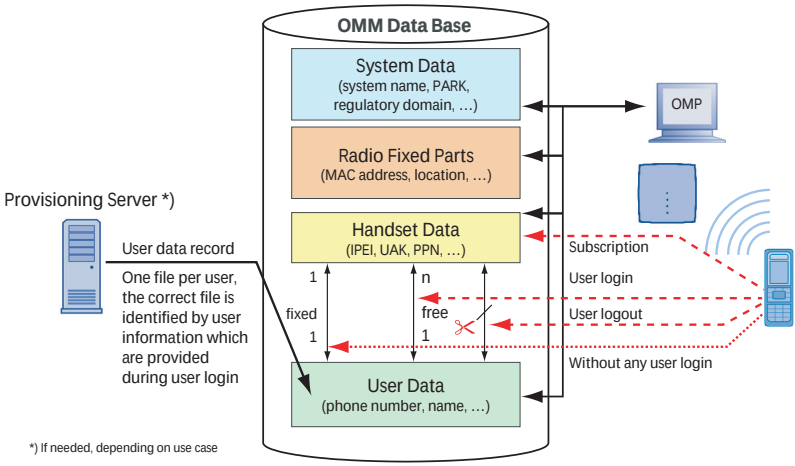
OTHER DOCUMENTATION

This user guide describes the administration and usage of the DECT phone sharing and provisioning features. Please refer also to the information in the documentation related to other parts of your SIP-DECT installation:

- *SIP-DECT 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

The following figure provides an overview of the OMM database infrastructure:



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
- change user-device assignments from fixed to dynamic
- change a user data set from an external user data server to an internally provisioned data set

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 applied
- a specified update interval elapses

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 elapses during a login session
- a user data set in the OMM database is created
- 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, see “Using External User Data” on page 35.

For the user data file format description, see “External User Data Server File Specifications” on page 41.

SUBSCRIPTION HANDLING

The SIP-DECT solution supports the following subscription methods:

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

After system startup, if no device has successfully completed the subscription process, manual subscription (including auto-create on subscription) is 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), through the OMM Web service or the OM Management Portal (OMP) tool. The time is further limited if the feature 'Restrict subscription duration' is active (refer to the *SIP-DECT OM System Manual*).

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 older 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 user and device data with a fixed association 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 35): 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

Wildcard subscription allows the assignment of 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 automatic subscription of DECT phones, without any device administration. This subscription method creates an unbound device data set. The

device is mapped to a specific user data set when the user logs into the phone.

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 21). 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 user must enter the DECT authentication code configured in the OMM system settings.

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

FEATURE ACCESS CODES

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 FACS 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 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**.

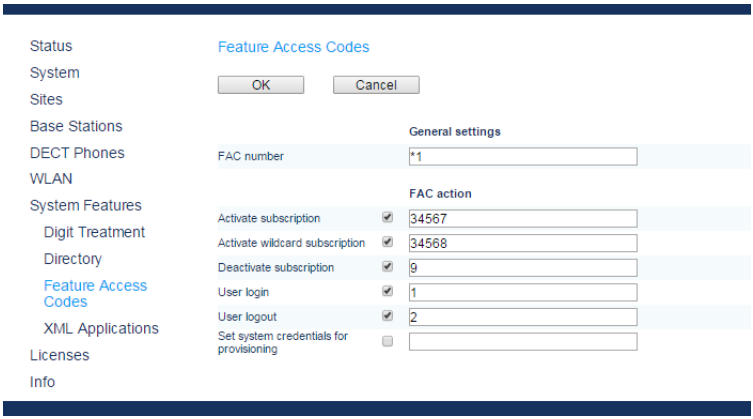
   The OMM Web service main page is displayed.

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.



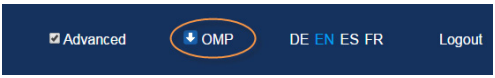
7. Click **OK** to confirm your settings.

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

Note: While you can choose any valid sequence as a Feature Access Code, you should ensure that the FAC is compatible with the connected PBX 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 FACS 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.

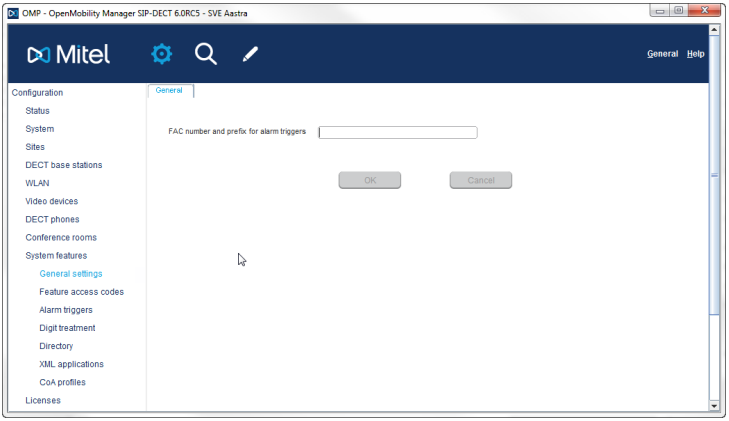


1. Double-click on the OMP.jar file to launch the OMP.

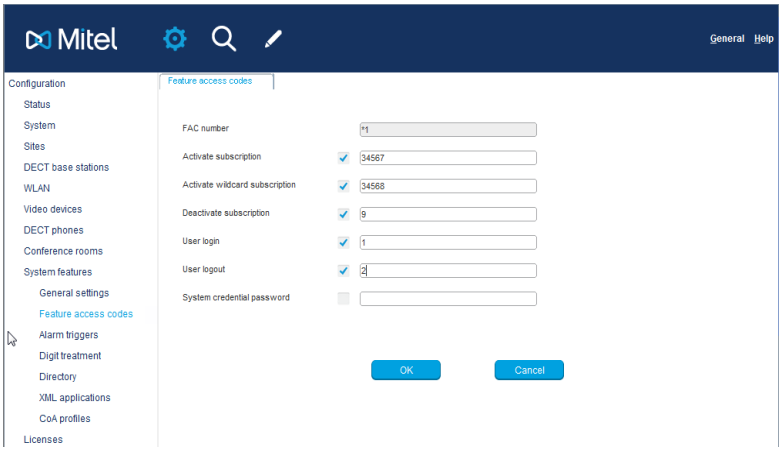
   The OMP tool starts and displays a login window. Note that the **System name** drop-down list is empty if you started the tool for the first time.

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 FACs 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 21).

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.

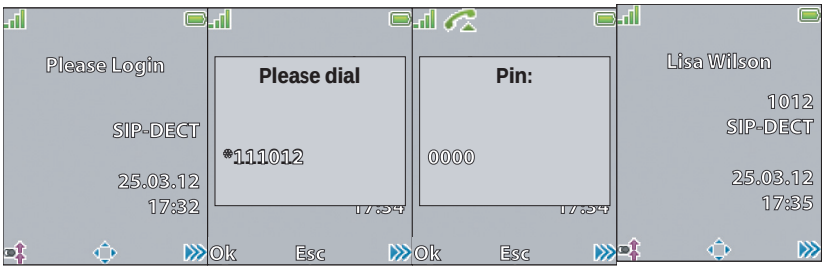
The login/logout operation is implemented by using the DECT user authentication mechanism (defined in the DECT

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 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.

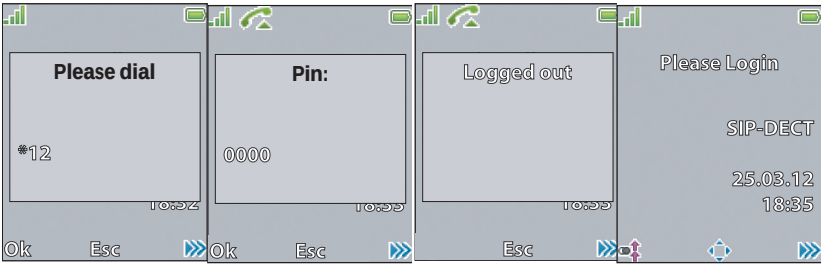
FAC Login Procedure



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 MANAGEMENT

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).

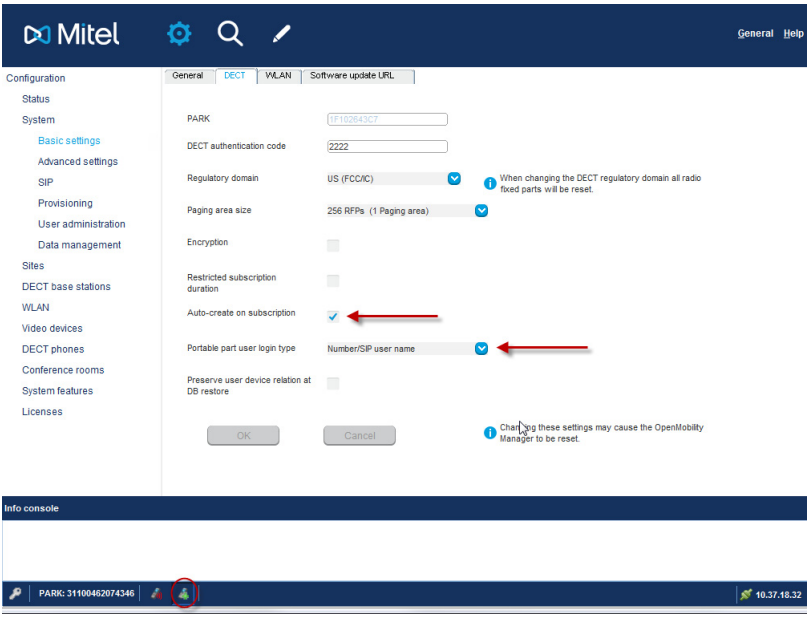
   The OMP starts and displays a login window.

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.

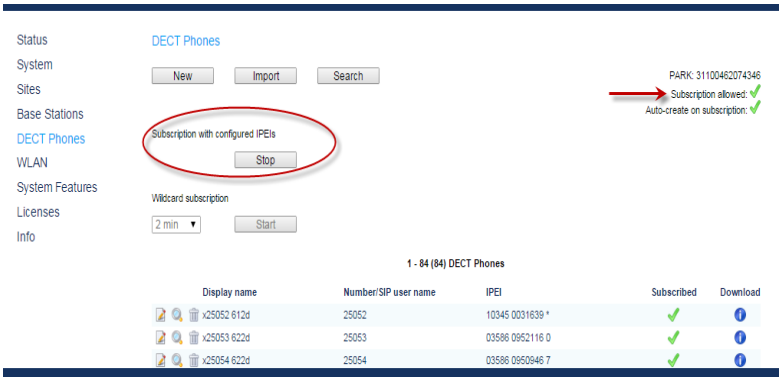
6. Click **OK** to confirm your settings. Note that the activated Auto-create on subscription status is displayed at the bottom of the OMP window.



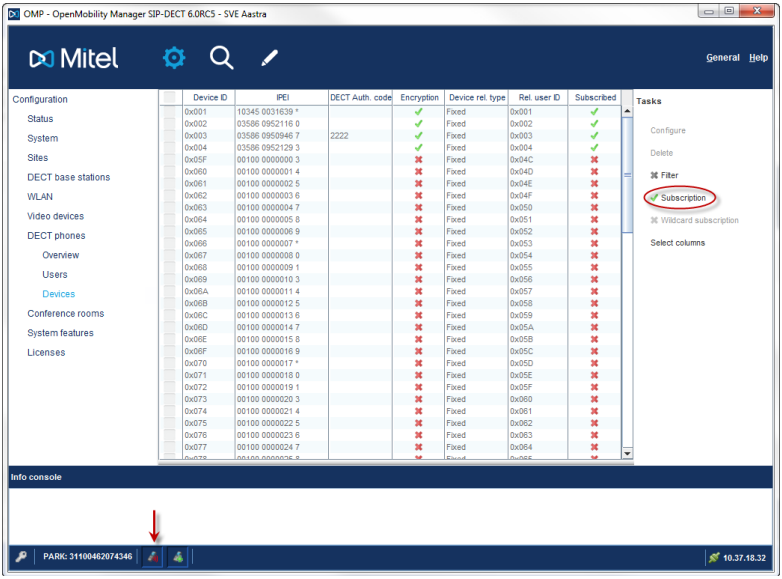
ENABLING SUBSCRIPTION

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

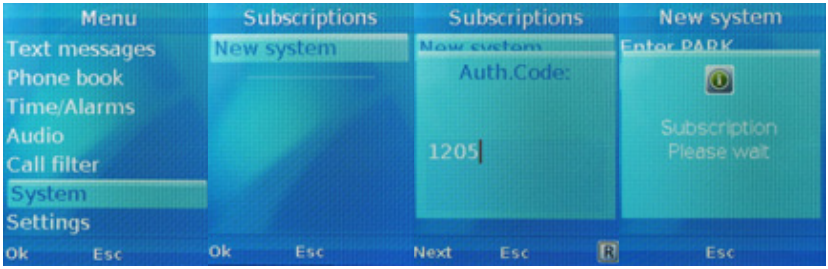
Initiate the subscription on the desired DECT phones.

1. Open the DECT phone's **System** menu and select the **Subscriptions** command.
2. When prompted for the system PARK, you may optionally type in the14 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



Open the **System** menu on the DECT phone.	Select the **Subscriptions** -> **New system** command.	Enter the DECT authentication code.	Wait for subscription to complete.

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 26).

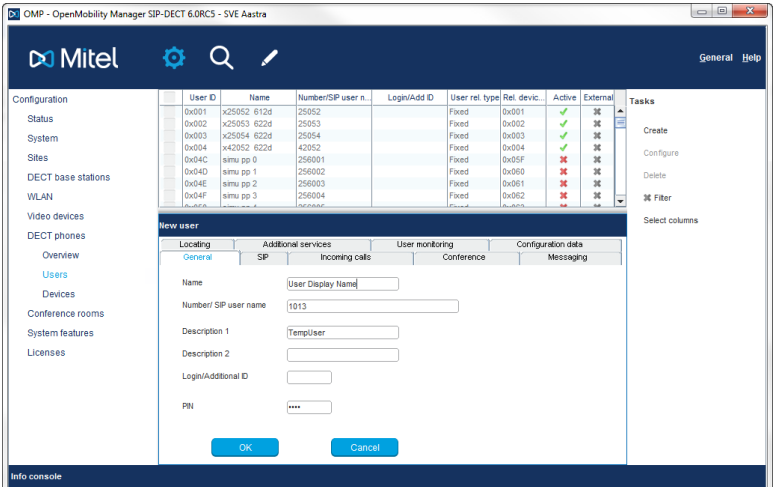
Note: The above example shows the subscription without entering the PARK on the DECT phone. However, if more than one DECT system is active in the area, you should also enter the PARK code during the subscription process.

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 iPBX (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.

   - **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 specifies, 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 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 System Manual* for information on the Terminal Video feature.
   - **Hot desking supported**: enables or disables Hot desking functionality (for SIP-DECT systems using the MiVoice Business platform). Only available for users with a dynamic association with a DECT phone. See

the *SIP-DECT System Manual* for information on the Hot Desking feature.

- **Auto logout on charging**: enables or disables automatic user log out on the DECT phone when the device is placed in the charger cradle. Only available for users with a dynamic association with a DECT phone. Note that the **Silent charging** option must be enabled on the DECT phone.

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 status supervision. Default setting is Off.

      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 the *SIP-DECT User Monitoring Administration Guide* 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 System Manual*.
12. Click **OK** to create the new user data set.

You can repeat these steps for additional user data sets. Alternatively, you can import user data sets from an external server. See “External User Data Provisioning” on page 35 for more information.

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 35.

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, doe 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 21.

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.

CENTRALIZED USER AND DEVICE DATA MANAGEMENT

With SIP-DECT 7.0 and later, the SIP-DECT solution supports centralized user and device management through the Multi-OMM Manager (MOM).

The MOM is a server application that provides centralized provisioning and user/device data synchronization across multiple SIP-DECT sites within a SIP-DECT system. You can deploy OMMs and DECT base stations as a standalone system at each site, but manage the entire SIP-DECT system through the MOM interface.

ROAMING BETWEEN SITES

The MOM allows users/devices to roam seamlessly between different SIP-DECT sites and ensures that each OMM has the necessary user/device data records to initiate SIP registration when a user changes location.

When a user roams to another site, the DECT phone connects to a base station at the new site, which triggers a location registration with the local OMM. The new OMM notifies the

MOM of the device's new location, and the MOM transfers the user/device record from the old OMM to the new OMM. The new OMM initiates a SIP registration on the configured SIP server, while the old OMM unregisters the DECT phone from its SIP server.

For more information, see the *Multi-OMM Manager Configuration and Administration Guide*.

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 41 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 45 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 authenticated. This features allows the provisioning server to provide user-specific settings on demand, using one file name based on the specific user credentials.

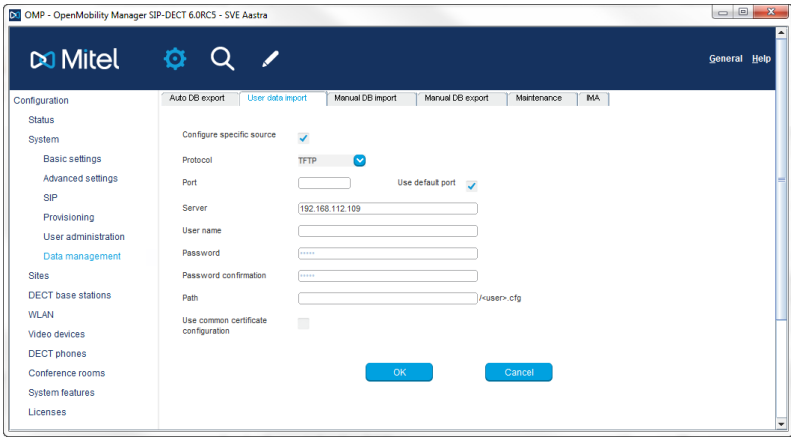
To remain in sync with the server’s data, the common configuration and the user data file can contain parameters for an update interval (default are 24 hours for both if not explicitly set):

- 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 requires 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.

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

- At start-up, the OMM reads the default “user_common.cfg” file. In the above example, the “tftp://192.168.112.109/user_config/user_common.cfg” is loaded.
- When a new user logs in, the OMM loads a user-specific configuration file. 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 for the newly logged in user. You can set, for example, a common login PIN code that is valid for all users (user_common.cfg). You can then provide more specific settings, for example by specifying a arbitrary display name for the 4711 user in the <4711.cfg> file.

See “External User Data Server File Specifications” on page 41 for two example files.

OMM DATABASE PROVISIONING DEPENDENCIES

Note the following dependencies 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 retain data changed by the user between logout and login.
- At startup, the OMM loads the "userCommon.cfg" configuration file. User configuration files (“<user>.cfg” or “<LoginID>.cfg”) are loaded when the individual timer elapsed. If the users are removed from the server, the associated user data sets are also removed from the OMM database. Removing a user data set forces a logout on all affected DECT phones.
- The login status is not restored by an OMM database restore operation. Users must login again.
- When a start up with a database restore occurs, external users are automatically logged out. You can prevent the automatic logout by enabling the "Preserve user device relation at DB restore" parameter in the OMM. See the *SIP-DECT System Manual* for more information.

Note the following restrictions for user and device data changes via the OMP interface:

- 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 cannot be administered through the OMM Web service. They are displayed as read-only. They can only be deleted at the OMM Web service to force an administrative logout.

DEPENDENCIES FOR DYNAMICALLY LINKED DEVICES

Additional procedures are required to operate unbound DECT phones (e.g., user login and logout). For security reasons, the user must authenticate through a user ID and PIN code before executing any such procedures. The DECT user authentication mechanism is specified in the DECT standard, and ensure that the PIN is not sent over the air interface. All DECT phones support this authentication 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

On Mitel 600 DECT phones, this information is deleted when the user logs out, for privacy protection. This is not supported on GAP devices.

- The DECT phone maintains a local configuration. 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 DECT phone (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 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 in alphabetic order:

UD_AllowBargeIn=	One of "On", "Off" or "Global" / Controls the behaviour how the PP handles incoming calls while the phone is on an active call.
UD_AllowMsgSend=	BOOL, if TRUE admission to send messages for the user shall be activated per default.
UD_AllowVcardRecv=	BOOL, if TRUE admission to allow vcard receive at the PP.
UD_AllowVcardSend=	BOOL, if TRUE admission to allow vcard send from PP.
UD_AllowVideoStream=	BOOL, if TRUE video streaming is enabled.
UD_AuthenticateLogout=	BOOL, if TRUE the user logout procedure requires an authentication to logout from the DECT phone, otherwise the logout is done without any PIN input. The default value is "false".
UD_AutoAnswer=	One of "On", "Off" or "Global" / Allows auto answering for an call.
UD_AutoLogoutOnCharge=	BOOL, if TRUE automatic user logout when users PP is in charger is enabled.
UD_BTLocatable=	BOOL, if TRUE the user shall be locatable by Bluetooth per default, setting this value requires also to set the "UD_Locatable" parameter.
UD_BtSensitivityType=	One of "Low", "Medium" or "High" to set Bluetooth sensitivity type.

UD_ConferenceServerType=	Selection the conference server type - one of "Off", "Global", "External", "ExternalBlindTransfer", "Integrated".
UD_ConferenceServerURI=	Conference server URI.
UD_HotDeskingSupport=	BOOL, if TRUE the user is registered as a 'Hot Desking user' at the call server (user's capability for Hot Desking support).
UD_KeepLocalDir=	BOOL, if TRUE admission to keep the local directory after PP logoff.
UD_KeyLockEnable=	"TRUE", if the keylock management of the DECT phone user shall be enabled. The user can activate the automatic keylock, if the UD_KeyLockTime is unequal to 0. The keylock setting by hand is activated then too. Set "0" or "false", if the keylock management of the DECT phone user is disabled. Any keylock is disabled on the users DECT phone. Default value is "true".
UD_KeyLockPin=	Key-Lock-PIN number to unlock the DECT phone. This is encrypted with the public key. Default value is "0000".
UD_KeyLockTime=	If UD_KeyLockEnable is "true", the keylock can be activated by setting the UD_KeyLockTime for the DECT phone user. The valid activation values are 10, 20, 30, 60, 90 or 120 seconds. The deactivation value is 0. Default setting is 60 seconds.
UD_Locatable=	BOOL, if TRUE the user shall be locatable per default.
UD_LocatingPermission=	BOOL, if TRUE localisation for the user shall be allowed per default.
UD_ManDownNumber=	Common ManDown number when needed.

UD_MicrophoneMute=	One of "On", "Off" or "Global" / Microphone controlling for calls made by the originating caller.
UD_Pin=	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 crypted form.
UD_PpProfileId=	Id of the PP configuration profile data (setting to 0 means no profile to use).
UD_ServiceAuthName=	It is the user individual authentication name for all supported XSI corporate directory services.
UD_ServiceAuthPasswd=	It is the user individual authentication password for all supported XSI corporate directory services.
UD_ServiceUserName=	It is the user individual name for all supported XSI corporate directory services.
UD_SosNumber=	Common SOS number when needed.
UD_Tracking=	BOOL, if TRUE life tracking localization for the user shall be activated per default.
UD_UpdateInterval=	Interval to re import user data files in hours / default=24 hours when not set.
UD_UserMonitoring=	One of "Off", "Active" or "Passive" to set one user monitoring mode.
UD_UseSIPUserAuth=	One of "On", "Off" or "Global" / the service authentication name and password for XSI corporate directories are taken from users SIP data.
UD_UseSIPUserName=	One of "On", "Off" or "Global" / the service user name for XSI corporate directories is taken from users SIP data.
UD_Vip=	BOOL, if TRUE SIP Periodization is enabled.
UD_VoiceMailNumber=	Common VoiceMail number when needed.

UD_WarningTone=	One of "On", "Off" or "Global" / Controls warning tone to play when the PP receives an incoming call on an active line.
UDS_CommonUpdateInterval=	Interval to re import this file in hours / default=24 hours when not set.
UDS_CommonUserFileName=	BOOL, enables / disables use of common file name (user.cfg) for user configuration files when account/password authentication is used to access these files from the server.

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 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
UD_Number=4711              # Subscriber number or SIP call name,
                            # ignored when DECT phone user login type
                            # is set to “Number”.
                            # (See System settings in Web or OMP.)
UD_Name=Julian              # Displayed name
UD_SosNumber=112            # Common SOS number when needed
UD_ManDownNumber=112        # Common ManDown number when needed
                            # Only for FFSIP:
UD_SipAccount=4711          # SIP account
UD_SipPassword=0815         # SIP password
UD_Locatable=FALSE          # BOOL, if TRUE the user is locatable,
                            # default is FALSE (licensed)
UD_LocatingPermission=0     # 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=0         # BOOL, if TRUE permission to send
                            # vcard from DECT phone user is activated
```

UD_AllowVCardRecv=0	# 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