SIP - DECT
OM Handset Sharing & Provisioning
Installation & Administration

User Guide

AASTRA

Welcome to Aastra

Thank you for choosing this Aastra product. Our product meets the strictest requirements with regard to quality and design.

The following user guide will assist you in using the SIP - DECT OM Handset Sharing & Provisioning and provide answers to all your most important questions.

If you should require further technical support or information about other Aastra products, please contact the person responsible for your system or get in touch with your local dealer.

You can also find information about this device and other products on our website at **http://www.aastra.de** or **http://www.aastra.com**.

We hope you enjoy using your SIP - DECT OM Handset Sharing & Provisioning.

Contents

OpenMobility Provisioning

This document describes the Handset Sharing and Provisioning which has been enhanced for the OpenMobility SIP - DECT solution release 2.1 or higher. The enhanced DECT Handset Sharing and Provisioning concept enables you to comfortably manage a large amount of DECT handsets and provides a more flexible subscribing model than it's predecessor. With this, the SIP - DECT system supports new features such as logging in and out with a personalized user account on different DECT handsets, automatically subscribe new DECT handsets or control subscription specific system functions from DECT handsets.

Features and Benefits

- "Auto-create on subscription" feature: Reduces administration effort by automatically created handset data in large systems during subscription (OMM SIP 2.1 supports up to 2,048 RFPs with up to 4,500 DECT handsets).
- Moving one DECT handset from one user to another one must not be administrated any longer (as with OMM versions < release 2.1).
- Provisioning/Import of user data from an external source ("external provisioning server"), no redundant OMM administration required.
- Splitting of user data and handset data is supported which allows to create a dynamic relation between a DECT handset and a registered user.

These features support the following use cases:

- One handset can be shared by different users at different points in time ("free seating"). The handset is linked/unlinked by the user's login/logout.
- A login with credentials of a user account that is administrated externally is also possible.

Basic Concepts

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

Alternatively, is possible to split the PP data into handset data and user data in the OMM database. This enhanced Handset Sharing and Provisioning concept introduces a new data model that is used to add flexibility.

Data Model

Data sets
While the previous OpenMobility SIP - DECT solution release manages user data and handset data in a single and fixed data set, the current version supports two different data sets:

- A handset data set, that stores data for the known handsets, 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 handset data set is used to convert existing subscriptions from previous versions of the OpenMobility SIP - DECT solution or if you create subscription data with the OMM Web service.
- A **dynamic relation** which supports e.g. login in and out is created if you use the "OM Management Portal" Java tool to create new subscriptions.

Note

A database upgrade/migration (OMM release 1.5 to OMM release 2.1 or higher) leads also to fixed relations of user and device data sets. If you want to switch an imported subscription from a fixed to a dynamic relation, you have to re-subscribe the handset.

Feature Access Codes

To control subscription specific features from a DECT handset, feature access code (FAC) can be used. You can call a special phone number which accepts additional code digits to trigger a feature. This basically includes:

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

By using an FAC, you may activate the subscription of new DECT handsets, deactivate subscription, or login / logout a user.

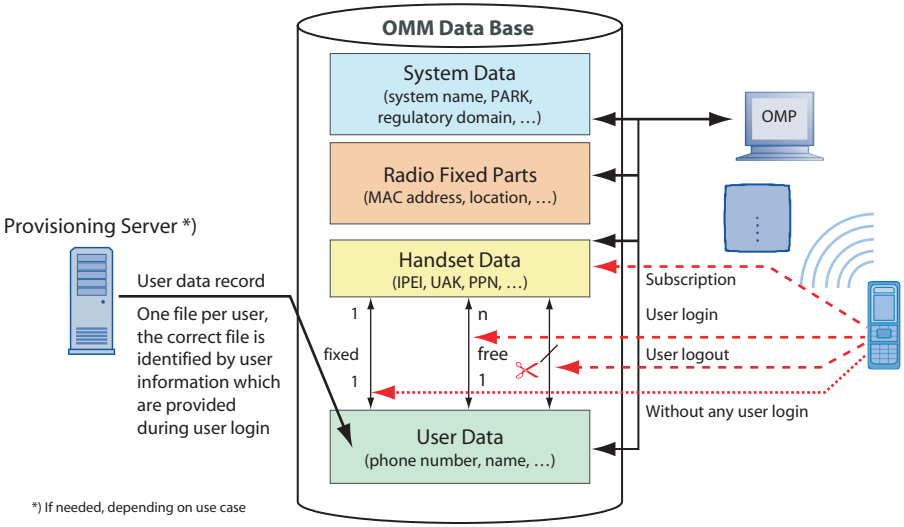
Other Valid Documentation

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

- SIP - DECT; OM System Manual
  Describes the installation, administration, and maintenance of the SIP - DECT system.
- SIP - DECT; OM Locating Application
  If you have also purchased the “OpenMobility Locating” application, please refer to this user guide which describes the installation, administration, and usage of the OM Locating application.
- SIP - DECT; OM Integrated Messaging & Alerting Application
  This user guide describes the messaging features and the integrated messaging solution.
- SIP - DECT; Aastra 610d, 620d, 630d Messaging & Alerting Applications
  This user guide describes the special messaging features of the Aastra 6x0d DECT terminal series and how to use them.

OMM Administration Infrastructure

There are different instances that take effect to the user and device data set administration in the OMM database release 2.1 or higher. The following picture gives an overview:



"OM Management Portal" (OMP)
By using the "OM Management Portal" (OMP) you can

- create or delete fixed data sets,
- create or delete unbound user data sets,
- create or delete unbound device data sets.

DECT handset
During the subscription process the DECT handset 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 dynamic configured DECT handset 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 neccessary 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/retrieved by the OMM

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

The provisioning server also provides a user file per user for the OMM ("user.cfg" or "LoginID.cfg"). These files are queried/retrieved by the OMM

- when a user login is done at a handset,
- when a specified update interval elapsed during a login session,
- when a user data set in the OMM database is built,
- or when 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 noticed at login time or when an update interval elapses.

For more information on the provisioning server please refer to the chapter entitled Using External User Data starting on page 27.

For the user data file format description please refer to the chapter entitled External User Data Server File Specifications starting on page 32.

Subscription Handling

In the OMM release 1.5 the “manual” and “wildcard subscription” methods were supported. These methods are also supported in OMM release 2.1 and higher with some conditions described below. Additionally a new “Auto-create on subscription” method is available since OMM release 2.1.

After startup of the system, as long as no device has been successfully completed the subscription process, “manual subscription” including “Auto-create on subscription” are enabled permanently. When the first subscription was successfully done, further subscriptions are possible for the next 24 hours or until the subscription mode is disabled by Feature Access Code (FAC), via the OMM Web service, or via the “OM Management Portal” tool (OMP).

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

Manual Subscription

The manual subscription method is characterized by managing user and device data in the OMM database that have a fixed relation. Here both, user and device data are configured in one step.

Since OMM release 2.1, either a fixed or a dynamic relation between a user and a device data set are possible, this depends on the administration:

- OMM Web service: this administration tool supports only fixed relations between user and device data sets.
- “OM Management Portal” tool (OMP): this administration tool supports fixed relations as well as dynamic relation between user and device data sets.
- External user data server (see also page 27): only dynamic relations between user and device data sets are supported.

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

Wildcard Subscription

The wildcard subscription method is a comfortable method to assign devices to users without any device administration. Wildcard subscription only works for fixed relations between user and device data sets and does not work if "Auto-create on subscription" is enabled.

If wildcard subscription is enabled, the IPEI of the DECT handset which is performing the subscription procedure must not be stored in the OMM database. The additional ID that is entered at the DECT handset identifies the desired user data set. Because only fixed relations between user and device data sets are supported, the new DECT handset's device data overwrite previously stored device data.

"Auto-create on subscription" Method

This subscription method allows to subscribe DECT handsets automatically without any device administration. This subscription method creates an unbound device data set. The mapping to a certain 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 "OM Management Portal" (OMP, see page 16). To activate this feature, you need to enable the **Auto-create on subscription** option and also switch on the subscription mode, either by FAC, Web service, or OMP.

If the IPEI of a DECT handset 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 with the OMM system settings needs to be entered on the DECT handset.

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

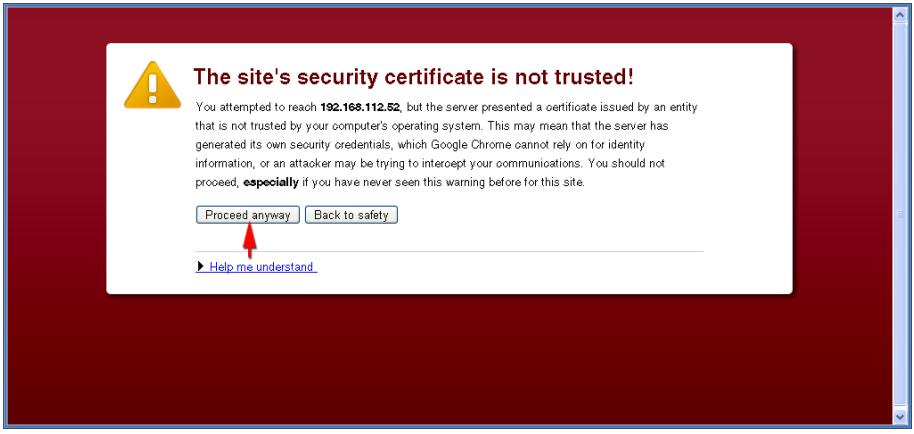
Feature Access Codes

The Feature Access Codes or short FAC allow you to control certain functions from a DECT handset. The functions available as FAC are basically related to the management of DECT handset subscriptions.

Configuring via OMM Web Service

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

1. Start a web browser. Enter the DNS name or IP address of the OMM in the browser's address input. The OMM Web server switches to the secured HTTPS protocol and you will typically see a browser display like the following one.



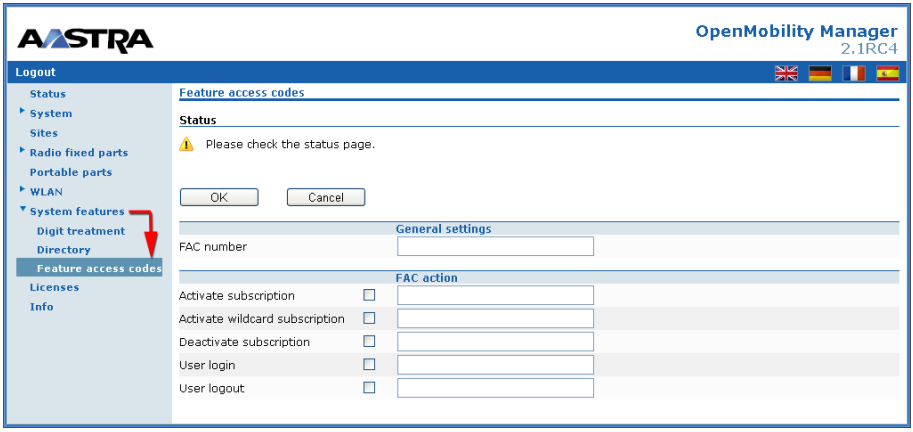
Certificate warning (Google Chrome Browser)

   To overcome the browser warning automatically, a regularly re-paid validation certificate for the OMM's network address needs to be issued by a third party. For connecting to the web user interface of the OMM in your LAN you can safely ignore this message and store a permanent exception in your browser.

   After accepting the certificate warning, the browser displays the OMM's login page.

2. Enter the **User name** that is configured at the OMM for the "Full access" account type. This is "omm" by default, but you may have changed this setting at the OMM. Enter the **Password** for the respective account. Confirm with **OK**.

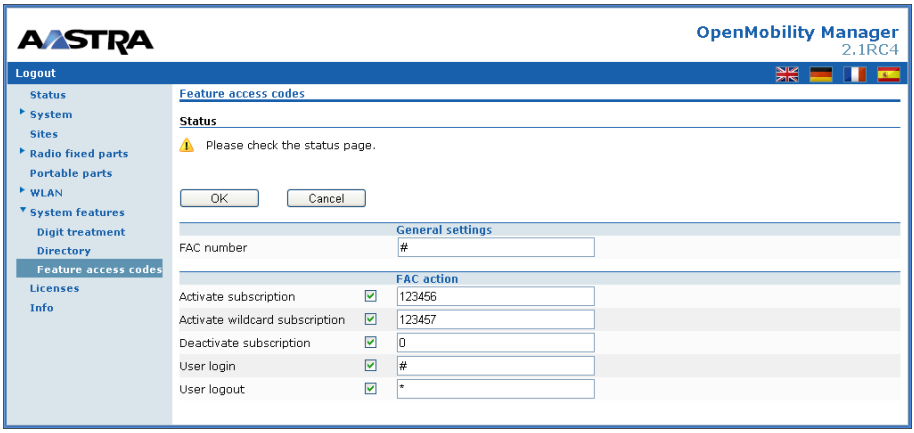
3. The OMM Web service main page is displayed. In the menu tree on the left, navigate to the **System features**: **Feature access codes** page.



OMM Web Service: Configuring Feature Access Codes

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

5. Enable the desired feature access codes by activating the respective check box. Enter the desired **FAC action** number code as well (0-9, *, or #). Protect critical functions with a longer sequence. To trigger a feature on the handset later on, the handset user has to dial the FAC number followed by the desired FAC action number code. The following screenshot depicts an example configuration.



OMM Web Service: Feature Access Codes Example

6. Confirm your settings with the **OK** button.

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

Note

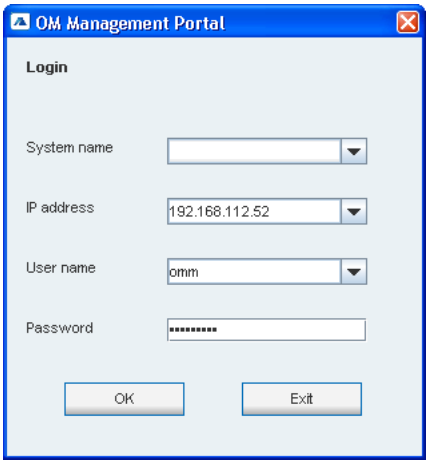
While you are free to choose any valid sequence as Feature Access Code, you should ensure that the resulting FAC is compatible to the connected PABX system and that there are no conflicts. In the example above, an OpenCom 100 system is connected as SIP back-end. The OpenCom 100 PABX offers dialling codes 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

As alternative to the OMM Web service, you can configure Feature Access Codes by using the “OM Management Portal” tool (OMP).

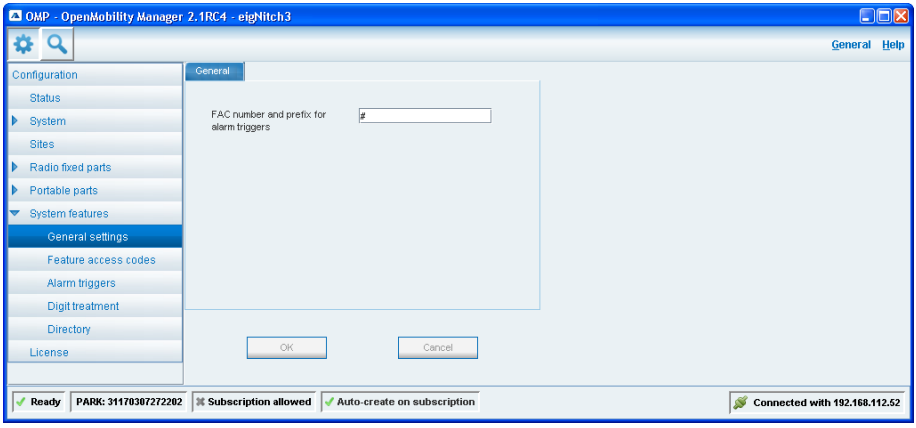
1. Double click the “OMP.jar” to start the Java-based “OM Management Portal” tool. Note, that you need a recent version of the “Sun Java Runtime” installed on your PC to execute Java programs.

The “OM Management Portal” tool starts and displays a login dialogue. Note, that the **System name** drop-down list is empty if you started the tool for the first time.



2. In the **IP address** input field, enter the DNS name or IP address of the OMM. Enter the **User name** that is configured at the OMM for the "Full access" account type. This is "omm" by default, but you may have changed this setting at the OMM. Enter the **Password** for the OMM. Confirm with **OK**.

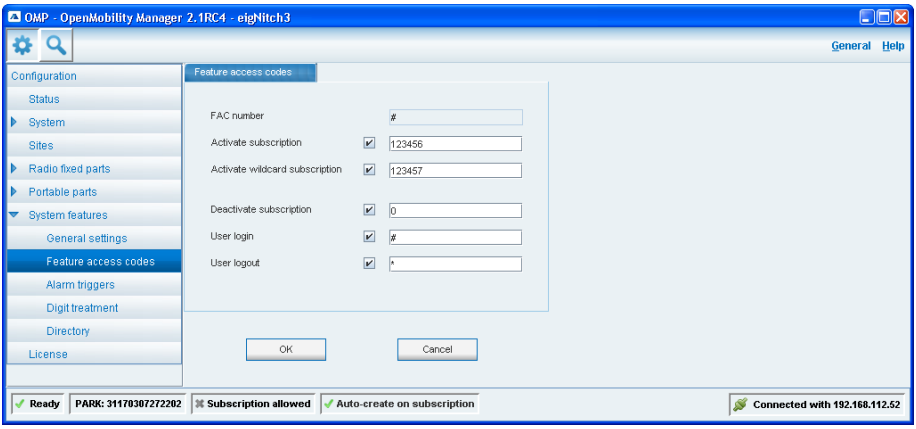
3. The **OpenMobility Manager** window opens. Navigate to the **System features**: **General settings** page.



"OM Management Portal" Tool: Configuring Feature Access Codes

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

5. Confirm with the **OK** button and navigate to the **System features**: **Feature access code** page.



"OM Management Portal" Tool: Feature Access Codes Example

6. Enable the desired feature access codes by activating the respective check box. Enter the desired FAC action number code as well (0-9, *, or #). Protect critical functions with a longer sequence. The following screenshot depicts an example configuration.

7. Confirm your settings with the **OK** button.

Using FACs on the Handset

You can use FACs from any DECT handset which is subscribed to the OMM.

1. In the idle state of the (subscribed) DECT handset, enter the **FAC number** on the handset's keyboard. Add the digits of the desired **FAC action**.

   Note, that you cannot activate a feature access code by dialling digit-by-digit. You need to use block-dialling for this.

2. Press the call key  to activate the feature access code.

   – If you dialled the correct code, you will hear an acknowledgement sequence which consists of a deep tone followed by a high-pitched tone.

   – If you dialled the correct **FAC number** but an unknown **FAC action** code, you will hear a negative acknowledgement.

   – Otherwise, you hear the busy tone.

Note

The dialled feature access codes are not added to the DECT handset's re-dial list.

Available FACs

The following feature access codes are available. The listed dialling sequences (shown in parenthesis) are examples which are valid with the example configuration depicted in the chapter entitled Configuring via OMM Web Service starting on page 8.

Subscription FACs

Activate subscription (#123456)
Enables or elongates the standard subscription period for 24 hours. Completing the subscription is possible only for DECT handsets for which a subscription entry exists which includes the IMSI number in the OMM's handset 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 (#123457)
Enables or elongates the wildcard subscription period for 1 hour. Completing the subscription is possible from any DECT by using the correct access code (refer to the **DECT authentication code** field on the **System**: **System settings** page of the OMM Web service). Note, that 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 this, the standard subscription mode is active for one hour.

Note, that the **Auto-create on subscription** option available on the **System**: **System settings** page of the "OM Management Portal" tool is inactive while wildcard subscription is enabled (see page 16).

Deactivate subscription (#0)
Switches off the subscription mode immediately. DECT handsets cannot subscribe to the OMM in this operating mode.

Login / Logout FACs

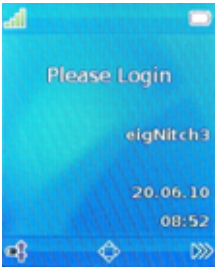
Dynamic devices need a user login procedure to be used and a logout procedure to detach the device from a user and make it ready for a new login for e.g. a different user. To login/logout on an unbound device, a feature access code followed by the users telephone number must be dialled en-bloc.

The login/logout procedure is implemented by using the DECT user authentication mechanism which is defined in the DECT standard. Therefore security aspects are covered. Optional encrypted data transfer can be used over the air interface. For more information on data encryption please refer to the “SIP - DECT; OM System Manual”.

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

This feature access code can be executed only on DECT handsets which have a dynamically linked handset data set. If this FAC is received, the user login procedure is started. After the DECT user authentication is completed successfully, the handset data set is linked to the desired user data set. Phone calls to the user’s phone number are signalled on the DECT handset.

FAC Login Procedure

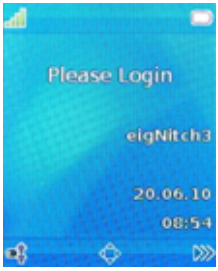
			
Display of an unused phone.	Dial FAC plus user number.	Enter the PIN to gain access.	You are logged in right now.

User logout (#*)
Enter this feature access code to log out. Press the call key and enter the users’s PIN to complete.

This feature access code can be executed only on DECT handsets with a dynamically linked handset data set. If this FAC is received, the OMM will mark the corresponding handset data set as unused which un-links it from the user data set.

Phone calls to the user's phone number are not signalled on the DECT handset any more. Also, another user may log in to the DECT handset.

FAC Logout Procedure

			
Dial FAC to initiate logout.	Enter PIN to proceed.	System confirms the process.	Display of an unused phone.

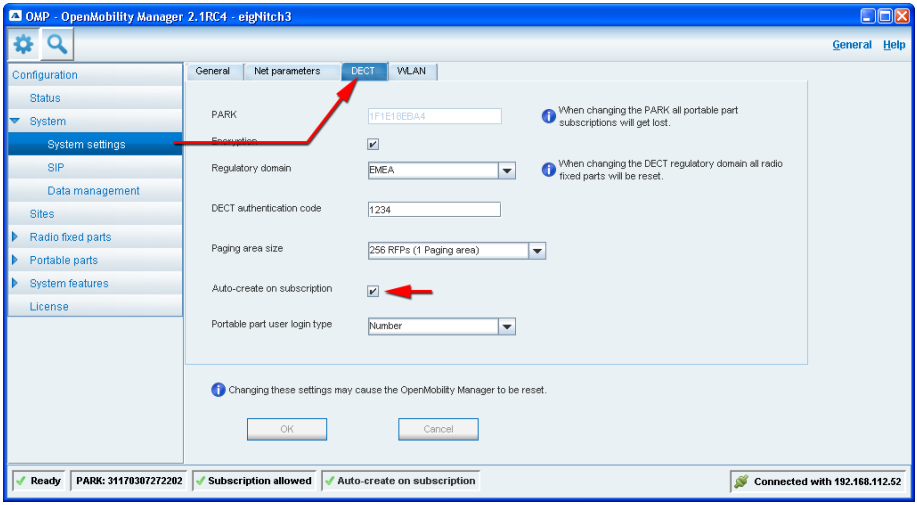
Log in / Log out

The standard relation between a DECT handset and the user is a fixed subscription. With this, the relation between the handset data set (IPEI, encryption data) and the corresponding user data set (phone number, name) is fixed. If another user wants to use the DECT handset, you normally need to un-subscribe and then re-subscribe the DECT handset for the new user.
To support new use cases, the OpenMobility SIP - DECT solution supports a dynamic relation between the handset data set and arbitrary user data set. To do so, you need to subscribe a DECT handset in a special way. A DECT handset with a dynamic subscription can be linked to a user data set by means of a login procedure. Also, you can free the handset data set with a logout procedure.

Creating Device Data Sets

While you manage fixed subscriptions with the OMM Web service, you need to use the Java-based "OM Management Portal" tool. By using this tool, you can create and manage dynamic subscriptions. The following step-by-step description explains the procedure.

1. Creating a dynamic handset subscription is possible when using the "auto-create on subscription" feature. To switch on this feature, navigate to the **System**: **System settings** page and select the **DECT** tab. Enable the **Auto-create on subscription** option.



"OM Management Portal" Tool: Enabling "Auto-create on subscription"

With the “auto-create on subscription” feature switched on, a dynamic data set is automatically created when a new and unknown DECT handset subscribes to the OMM. Because you do not add a data set manually, you cannot assign individual authentication codes for each DECT handset. Instead, the authentication code configured in the **DECT authentication code** input field can be used to subscribe DECT handsets.

Confirm the desired settings with **OK** to activate the “auto-create on subscription” feature. Note, that the **Auto-create on subscription** status indicator displayed at the bottom of the “OM Management Portal” tool window should show a green tick to indicate the activated function.

2. **Portable part user login type**: Two kinds of login types are supported. During the login the user can either be determined by the telephone number (**Number**) or by the unique user login ID (**Login ID**). Both elements are part of each user data set. The **Portable part user login type** setting specifies the system wide login variant.

   Note: Changing this setting forces an automatic logout of all logged in DECT handsets.

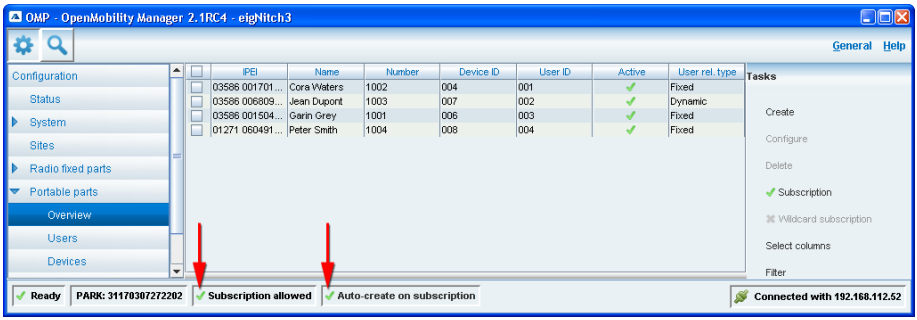
3. For security reasons, the subscription feature is turned off initially. To subscribe a new DECT handset and thereby creating a dynamic subscription, you need to enable the **Subscription allowed** status. Three different methods exist for this:

   – In the “OM Management Portal” tool, navigate to the **Portable Parts**: **Devices** page. On this page, a **Tasks** pane displayed on the right gives access to various commands. Click the **Subscription** command to enable the subscription allowed mode.

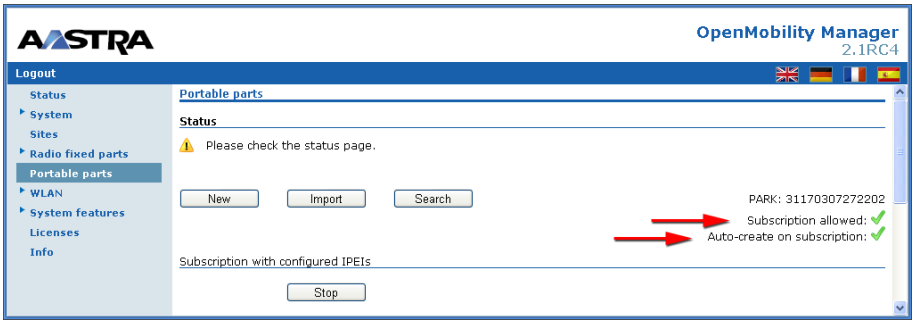
   – Use a Feature Access Code to enable the subscription from a DECT handset (see Activate subscription (#123456) starting on page 13). With the example configuration, you dial the desired FAC code and trigger it by pressing the call key  . You should hear the positive acknowledgement sequence.

   – You can also use the OMM Web service. Log in and navigate to the **Portable parts** page. Below the **Subscription with configured IPEIs** heading, click the **Start** button.

   The active subscription mode is indicated either by the “OM Management Portal” tool or on the OMM Web service as shown in the following screenshots.



"OM Management Portal" tool – "Auto Create on subscription" Activated



OMM Web Service – "Auto Create on subscription" Activated

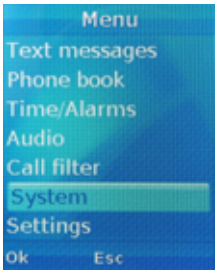
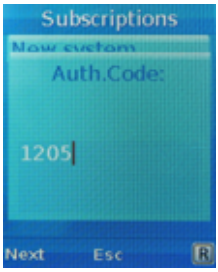
4. Initiate the subscription on the desired DECT handsets. For this, open the DECT handset's system menu and select the **Subscriptions** command. Proceed as follows:

– When asked for the system PARK, you may optionally type in the14 digit decimal PARK number of the desired SIP - DECT system. This number is visible in the OMM Web service on the **System**: **System settings** page.

– When asked for the access code, you need to enter the SIP - DECT systems DECT authentication code. This decimal number is visible and can be changed from the OMM Web service on the **System**: **System settings** page. Alternatively, the "OM Management Portal" tool shows this number on the **Configuration**: **System**: **System settings**: **DECT** page – **DECT authentication code** setting.

Complete the subscription process as usual. The DECT handset should indicate a successful subscription by showing the appropriate message. The following images illustrate an example performed with the Aastra 630d DECT phone.

Dynamic Subscription

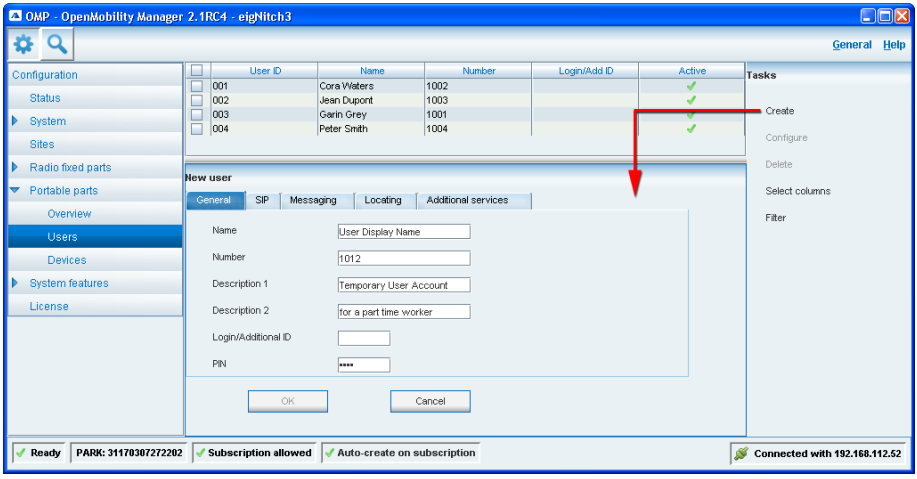
			
Call up **System** menu on the phone	Select **System**: **Subscription**: **New** command	Enter required authentication code	Wait for the subscription to complete

If the subscription completes successfully, the DECT handset should show a "Please Login" home screen. You may repeat these steps for an arbitrary number of DECT handsets. After this, you need to create at least one user data set in order to perform a successful login (see next section).

Adding User Data Sets

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

1. Open the “OM Management Portal” tool. Navigate to the **Portable Parts**: **Users** page.



“OM Management Portal” tool – Create New PP User

2. In the **Tasks** menu on the right, click the **Create** command. This opens a new pane where you can enter parameters for the **New user**.
3. Switch to the **General** tab and enter general user data:

   – **Name**: This name is displayed on the DECT handset home screen after the user successfully logged in.

   – **Number**: Determines the phone number for the user. After a successful login, this number can be called by other DECT phones to reach the user.

   – **Description 1** / **Description 2**: Enter any arbitrary text to describe the user data set.

   – **Login/Additional ID**: This unique ID can be used 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** field of the OMP **System**: **System settings** page, **DECT** tab (see page 17).

– **PIN**: To log in and out, the user has to provide a PIN code when entering the respective feature access code (see User login (##[user phone number / login ID]) starting on page 14 and User logout (#*) starting on page 14).

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

   – **User name**: Enter the authenticating user name for the SIP account. For example, if an Aastra OpenCom 100 PABX system is used, enter the user name configured on the **User Manager**: **User** page of the OpenCom 100 Web console.

   – **Password**: Enter the SIP password that should match the **User name** setting.

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

   Note, that all SIP - DECT users will use the same SIP server. The SIP server settings are available on the **System**: **SIP** page of the "OM Management Portal" tool.

   Switch to the **Messaging** tab if you want to configure the OM Integrated Messaging and Alerting service for the user data set. For information on the settings in this tab please see the SIP - DECT; OM System Manual.

5. Switch to the **Locating** tab if you want to change the settings for the locating application. Refer to the "SIP - DECT; OM Locating Application" user guide for details. Basically, these settings determine if the DECT handset is locatable from the locating application if the user is logged in.

6. Switch to the **Additional services** tab to configure extra configuration items for the user data set.

   – **SOS number**: This number is called if the logged in user presses the SOS key on the phone (e.g. on an Aastra 630d).

   – **ManDown number**: This number is called if the DECT handset (e.g. an Aastra 630d) determines the ManDown condition.

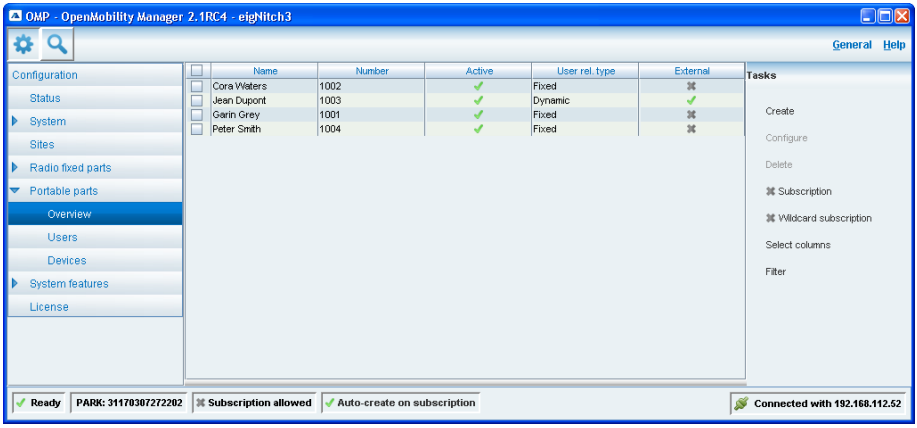
   – **Keep personal directory**: Activate this option to keep the personal directory data in the handset if the user logs out.

7. Click the **OK** button to create the new PP user data set.

You may repeat these steps for an arbitrary number of user data sets. Alternatively, you can import user data sets from an external server (e.g in case of a large number of data sets, see the chapter entitled External User Data Provisioning starting on page 27).

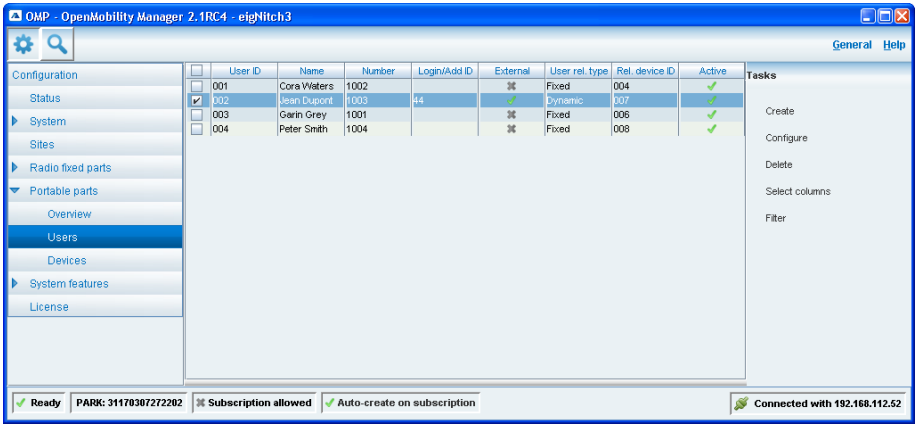
Viewing User and Device Data

“OM Management Portal” tool (OMP)
Associated users and devices are listed on the **Overview** page of the **Portable parts** menu. Data sets with imported user data are marked with a tick in the **External** column.



“OM Management Portal” tool: Portable parts – Overview

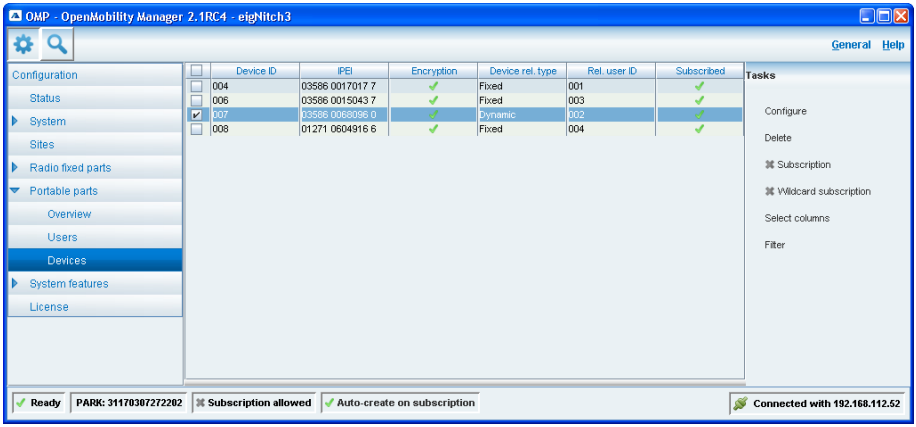
Imported user data are also listed in the on the **Users** page of the **Portable parts** menu and marked with a tick in the **External** column. For the import of user data see the chapter entitled External User Data Provisioning starting on page 27.



“OM Management Portal” tool: Portable parts – Users

Note: The screenshot above shows the user “Jean Dupont”. He can login either with the telephone number “1003” if the **Portable part user login type** setting (see page 17) is set to **Number**. Or he can login with the login user ID “44”, if the **Portable part user login type** setting is set to **Login ID**.

If the login was successful, then the user and device are associated. This is displayed on the **Device** page of the **Portable parts** menu. The **Device rel type** column shows the dynamic relation type.



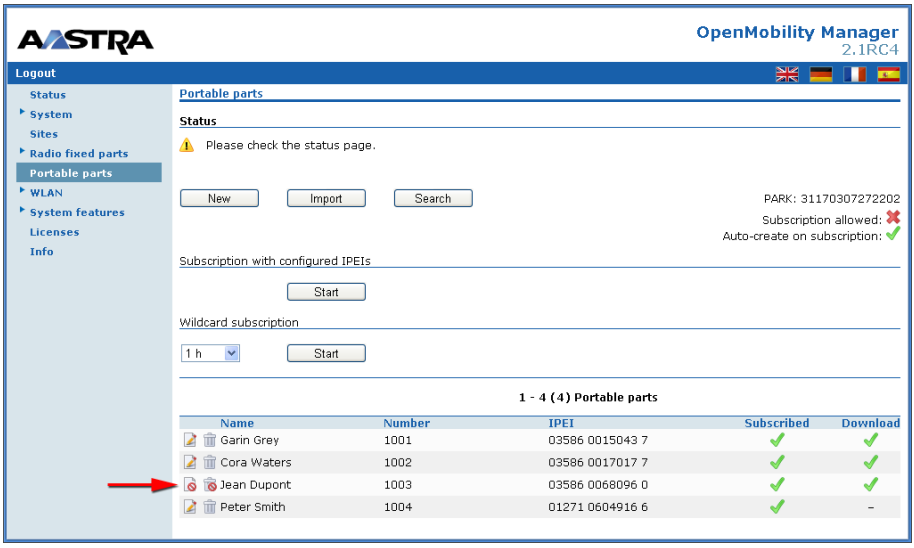
“OM Management Portal” tool: Portable parts – Devices

OMM Web service

User and device data are combined to PP data in the Web service as known in precedent OMM releases. This is not changed in the OM Web service for OMM release 2.1 and higher.

External or unbound user data sets (configured with OMP) do not have a dedicated device (PP). They have to login at a device first.

All PP data that are configured as unbound (split into device and user data) are also listed at the OM Web service when user are logged in at the device, but they can not be deleted or changed. These data sets are marked with the icons displayed in the following screenshot.



OMM Web Service: Portable parts – Overview

Troubleshooting Dynamic Subscriptions

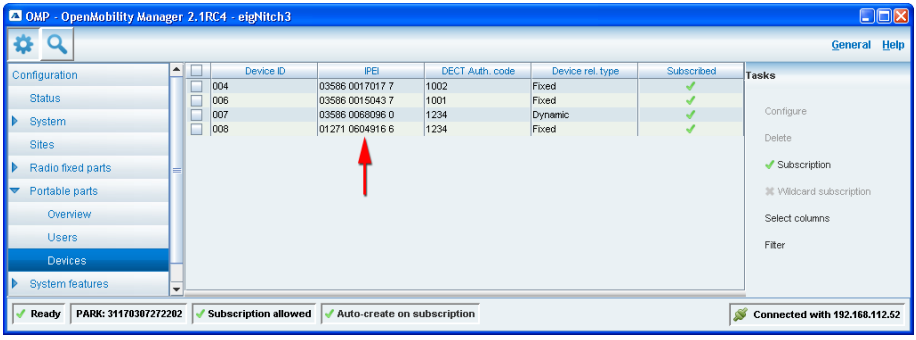
If you cannot dynamically subscribe a new DECT handset to the SIP - DECT system, you should check the following points.

Check DECT Handset's IPEI

You cannot re-subscribe a known DECT handset to the SIP - DECT system. If you have a single DECT handset 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. For this, display the DECT handset's IPEI number which is available on the DECT handset in the **System**: **Show IPEI** command. Verify, that the particular IPEI number is unknown to the SIP - DECT system:

1. Display the list of known DECT handset's IPEI numbers. For this, call up the **System**: **Show IPEI** command on the DECT handset. This will display the unique IPEI number, for example "03586 0017017 7".
2. Start the "OM Management Portal" tool. Navigate to the **Portable parts**: **Devices** page. Click on the **IPEI** table heading to sort the display by number.



"OM Management Portal" tool – List of known IPEIs

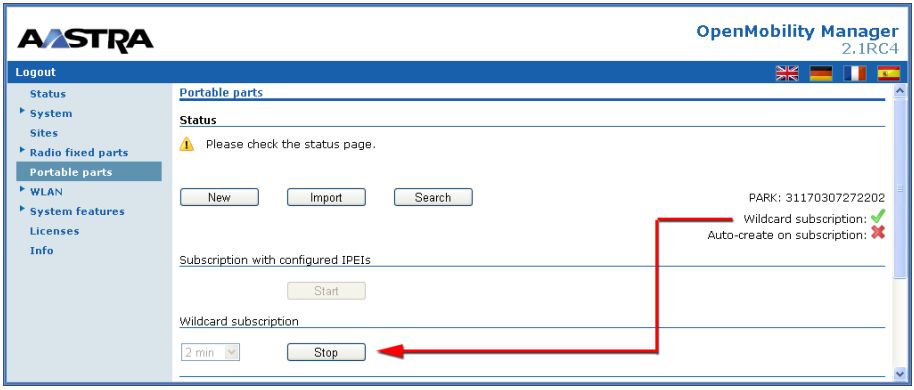
3. If the IPEI in question is visible in the list, you need to remove the subscription in order to proceed later on. Do to so, highlight the desired device item. Select the **Delete** command from the **Tasks** menu available to the right.
4. A confirmation dialogue is displayed to notify you that you are about to remove a known device. Click the **OK** button to confirm.

To create a dynamic subscription for the DECT handset proceed as described in the section entitled Creating Device Data Sets starting on page 16.

Wildcard Subscription Enabled

By using the wildcard subscription feature, you can subscribe an arbitrary DECT handset without entering the expected IPEI number. This “first comes – first served” approach conflicts with the dynamic subscription feature.

1. Start a browser an navigate to the OMM’s login page.
2. Login to the OMM Web service and navigate to the **Portable parts** page. Make sure, that the **Wildcard subscription** option is disabled. If the feature is enabled, click the **Stop** button below the **Wildcard subscription** heading.



OMM Web Service: Indicate and Disable Wildcard Subscription

3. Call up the **System**: **System settings**: **DECT** page in the “OM Management Portal” tool. Enable the **Auto-create on subscription** option and confirm with **OK**.

After following the above steps, you can proceed to subscribe new DECT handsets while creating a dynamic subscription.

External User Data Provisioning

Whereas you need to subscribe the DECT handset to the SIP - DECT system manually, the process of creating new user accounts can be automated. By using this feature you can manage a large amount of users that can log-in to the subscribed DECT handsets.

Scenario
Suppose, you have registered a larger number of DECT handset while creating a dynamic subscription. All those DECT handsets are waiting for their users to log in. You do not want to create a large set of user accounts, e.g. because the "OM Management Portal" tool GUI needs a lot of clicks for each single user account. The solution to this DECT handset user management task is to use external configuration files which 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

Since OMM release 2.1 it is possible to import user data from an external server. On the external server a specific file has to be provided for each user.

Additional a common configuration file (e.g. for default user data) can optionally be requested from the server for all external users. Same data sets in a user data file will overwrite the data of the common configuration file.

All additional user data values which can be changed at the handset (call forwarding, …) will be 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 will also be entirely deleted in the OMM database. The device gets unlinked from the user (automatically logged out).

Common file name conventions have to 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 for all users. For the file format description see the chapter entitled Example: "user_common.cfg" starting on page 32.

- user data files: "user.cfg" or "LoginID.cfg"

Each user configuration settings are stored in a user specific file where the file name represents the call number of the user. For the file format description see the chapter entitled Example: “user.cfg” or “LoginID.cfg” starting on page 34.

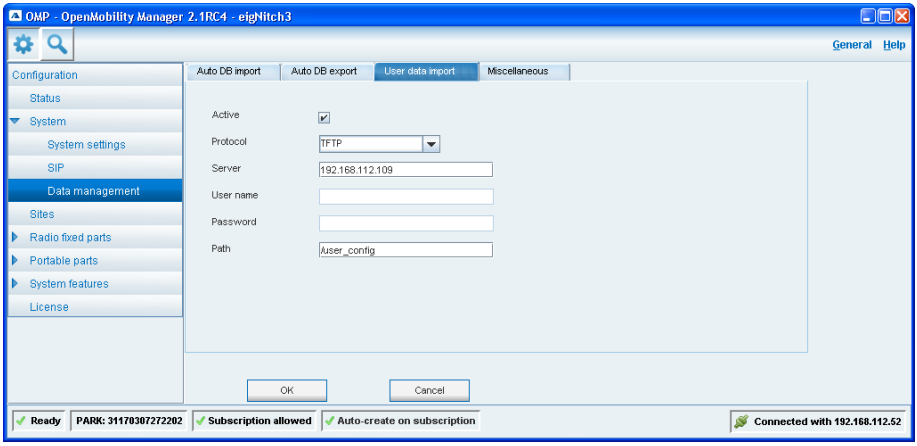
To be in sync with the server’s data the common configuration and the user data file can contain parameters for an update interval (default are 24 hours for both if un-set):

- For the common configuration file the timer starts when the file is imported.
- For the user data files the timer starts at login. Additionally to the timer update, the user data file will be re-imported at any login.

Activating External User Data

To deploy external user data configuration files to the SIP - DECT system, an external TFTP, HTTP or FTP server is required. Secure protocols can optionally be used for security reasons (FTPS or HTTPS). The configuration for the external user data server is done with the “OM Management Portal” tool.

1. Start the “OM Management Portal” tool. Navigate to the **System**: **Data management** page. Switch to the **User data import** tab.



“OM Management Portal” tool – Enable External User Data

2. The above example features a TFTP server with the following properties:

   – To switch on the external user data feature, enable the **Active** option.

   – Select the **Protocol** to use TFTP. Other possible choices include FTP, FTPS, HTTP, or HTTPS.

– The example uses a **Server** IP address of 192.168.112.109. On this external machine, the TFTP server runs waiting for requests. Enter an IP address or the corresponding DNS name of the server.

– If you have 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 these data. For this reason, the **User name** and **Password** fields are left empty in this example.

– The configuration files are kept in a subdirectory below the TFTP server's root. The **Path** setting determines the name of the sub-directory.

3. Confirm the setting with **OK** in order to activate the configuration.

External User Data during Runtime

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

- When the SIP - DECT server starts, it will read in the defaults file named "user_common.cfg". With the above configuration, 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 PIN code for logging in valid for all users (<user_common.cfg>). Then you narrow down the users configuration, for example by specifying a arbitrary display name for the 4711 user in the <4711.cfg> file.

Two example files are shown in the chapter entitled External User Data Server File Specifications starting on page 32.

OMM Database Provisioning Dependencies

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

- Dynamic links between user and device 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 to keep data changed by the user between logout and the next login.
- All external user data are re-imported at startup. When they do not exist on the server any more, the respective user data sets are also removed from the OMM database. Removing a user data set also forces a logout on all affected handsets.
- The login status is not restored by an OMM database restore operation. Users have to login again in this case.

The “OM Management Portal” interface can also have influence on user and device data:

- When a dynamically linked device data set is deleted, the bound/linked user data set will be set to logged out.
- When a dynamic linked user data set is deleted, the respective handset is logged out and a login mask is displayed.
- Dynamic user/device data sets can not be administrated with the OMM Web service. They are displayed read-only.

Dependencies For Dynamic Linked Devices

Dynamic linked devices have to perform certain procedures to operate, e.g. “login”, “logout”. For security reasons, an authorization is required when a user executes such a procedure. Therefore each procedure is secured by entering the user identification and a PIN code. This authentication is done with the “DECT user authentication” mechanism which is specified in the DECT standard. This mechanism assures, that the PIN is not exchanged on the air interface. All DECT devices are able to handle this mechanism.

The following dependencies exists for devices which are dynamically linked to users:

- DECT user authentication is not supported with Aastra 600d feature pack 1.

- The “login” and “logout” procedures are available on all GAP phones by initiating a call. To separate those from other call activities, certain FAC numbers are used.
- On GAP DECT devices it is not possible to manipulate the display when the device is not in call state. Therefore the “login” mask can not be displayed when the GAP phone is logged out. The OMM implementation will send the “Please login” display to a GAP phone when you hook off the device.
- The “message list”, “message icon”, “received call list”, “caller list”, “local phone book”, and “call forwarding icon” are stored locally on a DECT device. To protect the users privacy, these will be deleted when the user logs out. **This is only possible for Aastra 600d handsets – but not available for GAP devices.**
- Note, that the DECT handset also manages a local configuration. The local configuration data is not cleared if a new user logs in.
- **GAP devices and Aastra 142d devices**: User name and number must be manually set on the handset after login. Local lists e.g. redial list must be manually cleared after logout.
- **Aastra 600d devices**: User name and number are automatically set on the handset after user login. Local lists on the handset e.g. redial list are automatically cleared after logout.

External User Data Server File Specifications

This chapter 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> file is an ASCII file. The file is read in line by line while ignoring any content that follows a hash sign thereby treating such text as a comment. Note, that you should use the UNIX style line end convention (UTF-8 encoded).

The usage of the <user_common.cfg> configuration file is optional.

```
#####################################################################
# sample configuration file for the OpenMobility system retrieved via the net
# using file transfer protocols like tftp, ftp or http
#####################################################################
# comments are starting with the hash sign: "#"
#####################################################################
# BOOL variables support the following values
# YES Y 1 TRUE (case does not matter)
# 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
#                               #
# OM_UniqueId=                  # What will be the unique user identification
#                               # in the system, e. g. NUMBER or UID (login
#                               # user id) / default=NUMBER
#                               # <user>.cfg" <--> "<NUMBER>.cfg" or
#                               # <UID>.cfg"
#                               # if UID is used, it must be for sure, that all
#                               # login user ids are different from all OMM
#                               # internal user ids!
#                               # The login user id will be stored in the
#                               # 'additional id' data element of the user
#                               # data set within the OMM data base.
# UDS_CommonUpdateInterval=     # Interval to re import this file in hours /
#                               # default=24 hours when not set
# UDS_UseExternalUsers=         # Enables / disables user data import - when
#                               # disabled all users are deleted in the OMM
#                               # (incl. private data) and gets unlinked from
#                               # the handset / default=yes
```

```
# UD_SosNumber=                 # Common SOS number when needed
# UD_ManDownNumber=             # Common ManDown number when
#                               # needed
# 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 encrypted form
# UD_UpdateInterval=            # Interval to re import user data files in
#                               # hours / default=24 hours when not set
# 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_Tracking=                  # BOOL, if TRUE life tracking localisation for
#                               # the user shall be activated per default
# UD_AllowMsgSend=              # BOOL, if TRUE admission to send
#                               # messages for the user shall be activated
#                               # per default /
#                               # Supported >= OMM release 2.1
# UD_AllowVcardSend=            # BOOL, if TRUE admission to allow vcard
#                               # send from PP / Supported >= OMM
#                               # release 2.1
# UD_AllowVcardRecv=            # BOOL, if TRUE admission to allow vcard
#                               # receive at the PP / Supported >= OMM
#                               # release 2.1
# UD_KeepLocalDir=              # BOOL, if TRUE admission to keep the local
#                               # directory after PP logoff / activated per
#                               # default / Supported >= OMM release 2.1
#####################################################################
# Common User data settings
OM_UniqueId=                    NUMBER
UDS_CommonUpdateInterval=       6
UDS_UseExternalUsers=           YES
OM_SosNumber=                   110
OM_ManDownNumber=               110
UD_Pin=                         0815
UD_UpdateInterval=              4
UD_Locatable=                   TRUE
UD_LocatingPermission=          TRUE
UD_Tracking=                    TRUE
UD_AllowMsgSend=                TRUE
UD_AllowVcardSend=              TRUE
UD_AllowVcardRecv=              TRUE
UD_KeepLocalDir=                TRUE
UD_Tracking=                    TRUE
```

Example: “user.cfg” or “LoginID.cfg”

The user data configuration file “user.cfg” file (e.g. “4711.cfg”) or “LoginID.cfg” is an ASCII file. The file is read in line by line while ignoring any content that follows a hash sign thereby treating such text as a comment. Note, that 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 which are specified in the common user configuration file (“user_common.cfg”). A user configuration file sample for the user “4711” follows:

```
#####################################################################
# sample configuration file for the OpenMobility system retrieved via the net
# using file transfer protocols like tftp, ftp or http
#####################################################################
# comments are starting with the hash sign: "#"
#####################################################################
# BOOL variables support the following values
# YES Y 1 TRUE (case does not matter)
# NO N 0 FALSE (case does not matter)
# other values are interpreted as false
#####################################################################
# Possible user data configuration settings:
#
# UD_PinDel=                    # BOOL, if TRUE the user PIN will be deleted
#                               # in OMM private data to default "0000"),
#                               # must be set to FALSE after the file is
#                               # processed to have the possibility to set a
#                               # new user PIN at the linked handset!
# UD_Pin=                       # User PIN to login and logout / this can only
#                               # be used until PIN change is implemented
#                               # at the handset!
#                               # Can also be given in a public key
#                               # encrypted form
# UD_UpdateInterval=            # Interval to re import user data files in
#                               # hours / default=24 hours when not set
# UD_Number=                    # Subscriber number, ignored when
#                               # NUMBER is unique
#                               # (OM_UniqueId=NUMBER)
# UD_Name=                      # Displayed name
# UD_SosNumber=                 # Common SOS number when needed
# UD_ManDownNumber=             # Common ManDown number when
#                               # needed
# Only for FFSIP:
# UD_SipAccount=                # SIP account
# UD_SipPassword=               # SIP password
# UD_Locatable=                 # BOOL, if TRUE the user shall be locatable,
#                               # default is FALSE
# UD_LocatingPermission=        # BOOL, if TRUE localisation for the user
#                               # shall be allowed, default FALSE
```

```
# UD_Tracking=                    # BOOL, if TRUE life tracking localisation for
#                                 # the user shall be activated, default is
#                                 # FALSE
# UD_AllowMsgSend=                # BOOL, if TRUE admission to send
#                                 # messages for the user shall be activated
#                                 # per default / Supported >= OMM
#                                 # release 2.1
# UD_AllowVcardSend=              # BOOL, if TRUE admission to allow vcard
#                                 # send from PP / Supported >= OMM
#                                 # release 2.1
# UD_AllowVcardRecv=              # BOOL, if TRUE admission to allow vcard
#                                 # receive at the PP / Supported >= OMM
#                                 # release 2.1
# UD_KeepLocalDir=                # BOOL, if TRUE admission to keep the local
#                                 # directory after PP logoff / Supported >=
#                                 # OMM release 2.1
# UD_HierarchyName1=              # Optional 1. hierarchy name of a user, to
#                                 # make groups of users up to 16 bytes
# UD_HierarchyName2=              # Optional 2. hierarchy name of a user, to
#                                 # make groups of users up to 16 bytes
#####################################################################
# User data configuration settings for user "4711":
UD_PinDel=                        n
UD_UpdateInterval=                1
UD_SipAccount=                    SIP.4711
UD_SipPassword=                   password
UD_Name=                          Name-4711
UD_Number=                        4711 # ignored when number is unique
UD_Locatable=                      FALSE
UD_LocatingPermission=            FALSE
UD_Tracking=                      FALSE
UD_HierarchyName1=                Company1
UD_HierarchyName2=                Departement1
UD_SosNumber=                     110
UD_ManDownNumber=                 112
```

Index

Notes