Mobile Launcher User Manual

Revision 2.0

28/06/2019

Ascom UMS s.r.l. Unipersonale
Via Amilcare Ponchielli 29, 50018, Scandicci (FI), Italy
Tel. (+39) 055 0512161 – Fax (+39) 055 829030
www.ascom.com

Contents

1. Using the manual

This User Manual shall be used in combination with the Product User Manual and other module-specific manuals listed in Section 1

1.1 Aims

The effort which has gone into creating this manual aims to offer all the necessary information to guarantee a safe and correct use of the Mobile Launcher Application (hereafter “Product”). Furthermore, this document aims to describe every part of the Product, it also intends to offer a reference guide to the user who wants to know how to perform a specific operation and a guide for the correct use of the Product so that improper and potentially hazardous uses can be avoided.

1.2 Characters used and terminology

The use of Product requires a basic knowledge of the most common IT terms and concepts. In the same way, understanding of this manual is subject to such knowledge.

Remember that the use of Product must only be granted to professionally qualified and properly trained personnel.

When consulting the online version as opposed to the paper version, cross-references in the document work like hypertext links. This means that every time you come across the reference to a picture (e.g. “Fig 10”) or to a paragraph / section (e.g. “figure 5.4”), you can click the reference to directly go to that particular figure or that particular paragraph / section.

Every time a reference is made to a button, this is written “**Bold**” and if possible a small picture of the button is reported. For example, in expressions like:

- Click the “**Update**” button,

“**Update**” is a button featured on the screen being described. Where possible, it is clearly indicated in a figure (with cross references as “See Fig 12 **A**”).

The character ➢ is used to indicate an action which the user must perform to be able to carry out a specific operation.

The character ● is used to indicate the different items of a list.

1.3 Symbols

The following symbols are used in this manual.

Useful information

This symbol appears alongside additional information concerning the characteristics and use of Product. This may be explanatory examples, alternative procedures or any “extra” information considered useful to a better understanding of the product.

Caution!

The symbol is used to highlight information aimed at preventing improper use of the software or to draw attention to critical procedures which might cause risks. Consequently, it is necessary to pay extreme attention every time the symbol appears.

The following symbols are used in the Product information box:

The manufacturer’s name and address

Attention, consult accompanying documents

2. Mobile Launcher

Mobile Launcher is a mobile application designed to bring some of the Product suite functionalities directly “in the hands” of nurses and clinicians. Mobile Launcher acts as a container for a set of modules, each one designed to provide specific information and presenting it to the staff in a clear and concise way.

2.1 Information for the user

Please read carefully the following warnings.

	In case of disconnection of the Mobile Launcher application a specific notification is generated, consisting of a characteristic and persisting sound and vibration. Sound duration is configurable. The sound is repeated until the connection is reestablished. Connection is automatically reestablished as soon as possible.
	The mobile device shall always be kept by the user either in direct contact or close enough to be clearly audible.
	The Mobile Launcher application may display personal and/or confidential information. It is therefore recommended to not leave unattended the handheld device on which the Mobile Launcher application runs or, in case, to always logout before leaving it unattended.
	Mobile Launcher can be closed by the user. After which time the application will not send any other notification.
	Because of the Android architecture, in exceptional cases, which are hard to foresee, the operating system can close the Mobile Launcher application. After such event, the application will not send any other notification.
	If the generic Alaris® Driver is in use it is necessary to wait at least ten seconds after disconnecting an infusion pump before connecting another.
	The mobile device shall support the vibration mode.
	Use the sound check procedure to verify if the audio on the workstation/handheld device is correctly working (see related paragraph for the procedure).
	The Product acquires the information generated by the primary medical devices and displays them. Therefore, the Product always reports what the primary medical devices communicate. The

assignment of alarm priorities is decided according on the primary medical device. On the Product it is possible to decide the order of the medical devices, for every bed, in accordance to the customer preference: per device type, model / manufacturer. This kind of ordering is setup in the Product during deployment of the product according to the user request/preference. The color of every bed card (i.e. bed-area) is always the color of the highest priority alarm among all alarms occurring on that bed.

2.2 Start-up

Although the contents are the same, on Myco1/Myco2 devices it is possible to configure the product to appear on the third page of the custom launcher. Start-up layout is slightly different in this case compared to other Android handheld devices (or Ascom Myco when not running on Ascom Myco Launcher third page).
The layout displayed in Fig 7 is referring to a scenario where the Ascom Myco is integrated with Unite.
A further layout difference can be present according to adopted login procedure: see Paragraph 2.3 for further details.

2.2.1 Authorizations for proper functioning

This section applies only to Android 6.0+ devices i.e. not to Myco1/Myco 2.

In order to perform the expected functioning, the Mobile Launcher application at its first use asks to provide some basic authorizations. All the requested authorization have to be provided.

In Fig 1 is reported the screen shown to ask the user the authorization to access the device's location. The user has to tap the label "Allow":

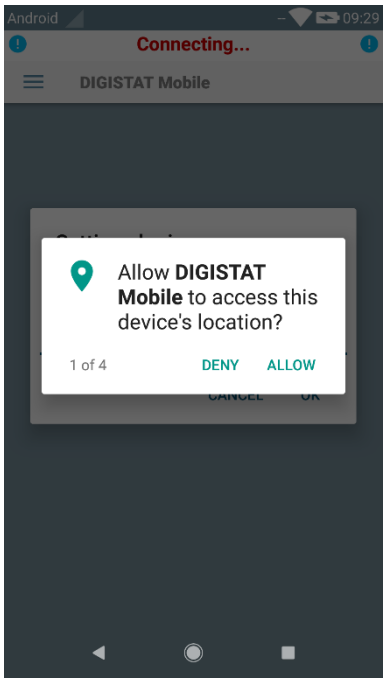


Fig 1

In Fig 2 is reported the screen shown to ask the user the authorization to take pictures and record video. The user has to tap the label "**ALLOW**":

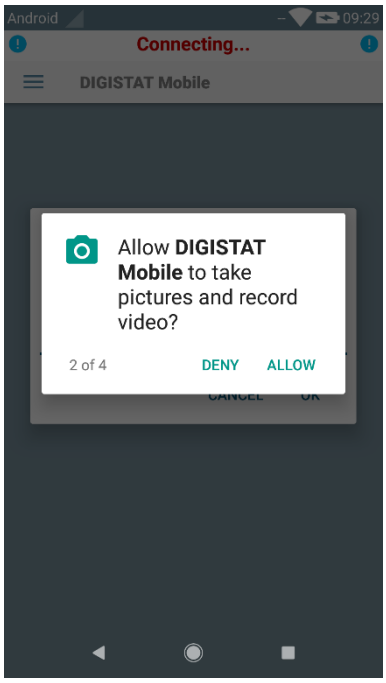


Fig 2

In Fig 3 is reported the screen shown to ask the user the authorization to access photos, media and files on the device. The user has to tap the label "**ALLOW**":

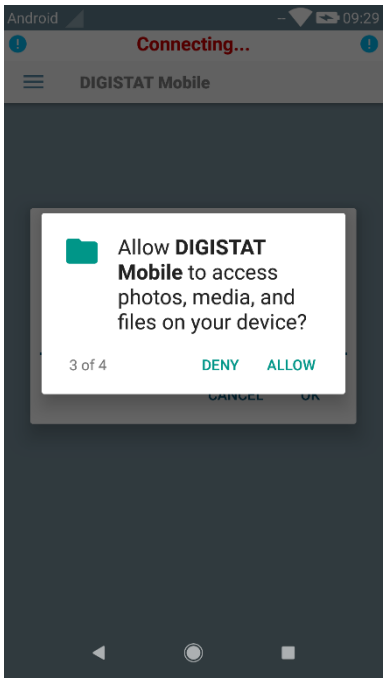


Fig 3

In Fig 4 is reported the screen shown to ask the user the authorization to record audio. The user has to tap the label "**ALLOW**":

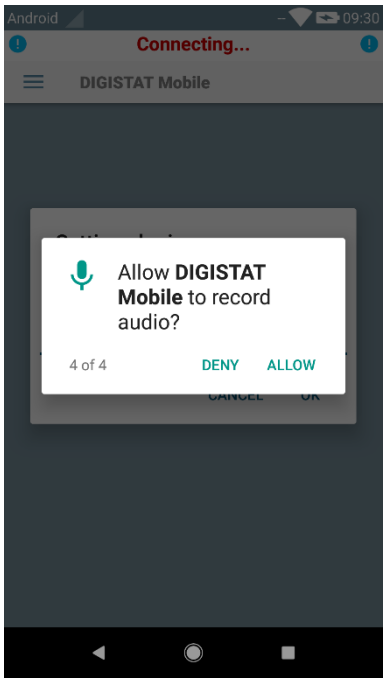


Fig 4

On Myco3 devices is requested in addition the authorization to read the device ID.

If at least one of the requested authorization is not granted, the Mobile Launcher application raises a toast message for the user (Fig 5):

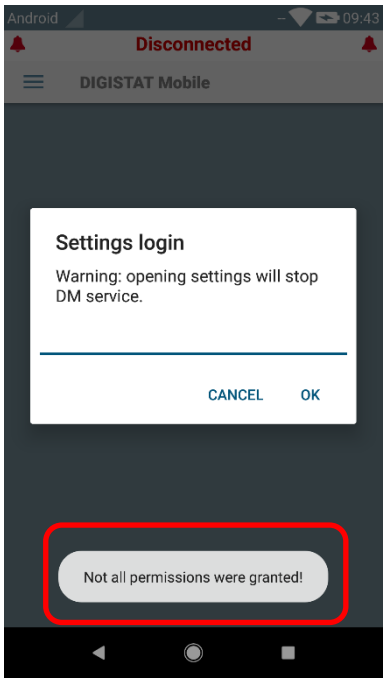


Fig 5

In addition, once the configuration of the application is correctly performed (see Paragraph 2.2.1) the Mobile Launcher application asks again to provide the missing authorization (Fig 6):

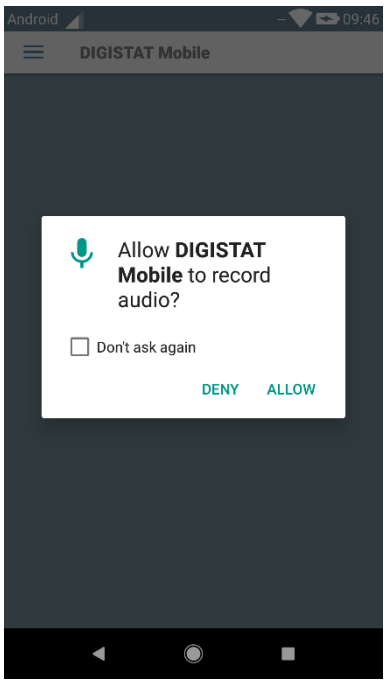


Fig 6

If the requested authorization is again not granted, the Mobile Launcher application raises furthermore the same toast message for the user shown before (Fig 5):

2.2.2 Start-up with Myco launcher

On the Ascom Myco device, when integrated with Myco launcher, the Mobile Launcher can run on the rightmost page of the launcher.

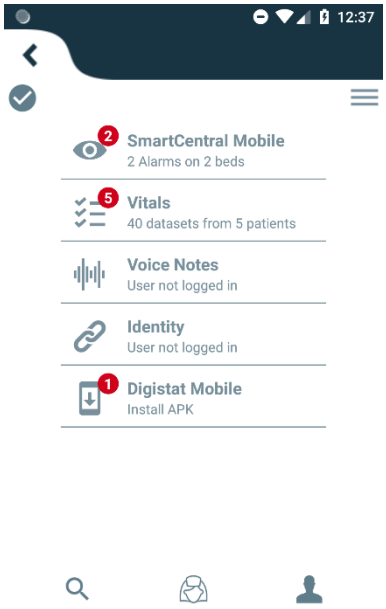


Fig 7

The available modules are listed on the page. Touch the row corresponding to the module to open it.

The **Settings** option makes it possible to access some configuration options. A specific password is required to access this area (Fig 8).

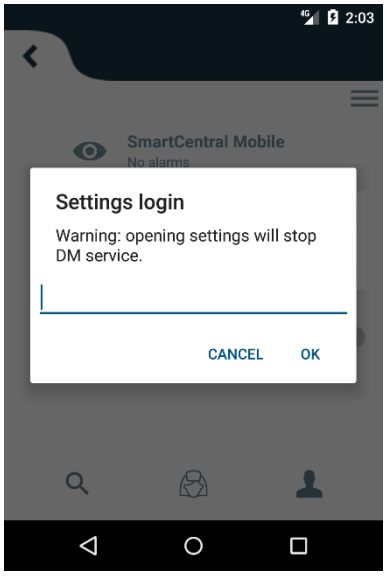


Fig 8

- Insert password and touch **"OK"** to access these options. The following screen will be displayed.

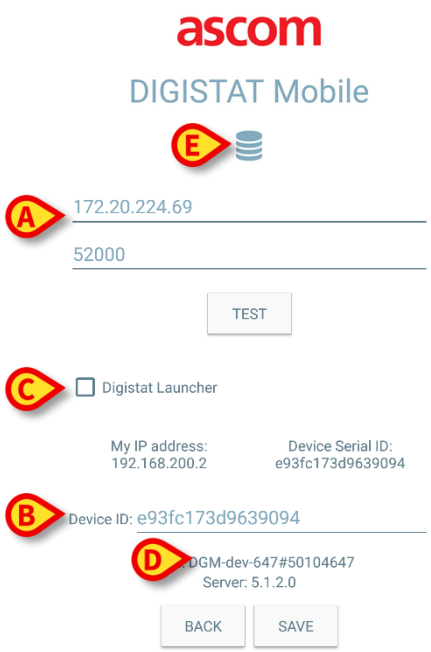


Fig 9

If Myco launcher integration is used, please deselect the checkbox in Fig 9 **C**; the home screen will be colored as the one in Fig 10.

It is here possible to specify the IP address of the server and the server port (Fig 9 **A**).

After editing:

- touch the **Test** button to test the new settings
- touch the **Save** button to save the changes made,

The lower field (Device ID - Fig 9 **B**) makes it possible to change the device id code.

Since the Device ID is changed, to recover the default value the user has to do the following steps:

- Insert an empty value in Fig 9 **B** and then save.
  The Mobile Launcher will signal by means of a message that in this way the Device ID will be restored; in addition, a confirmation is requested by the user.

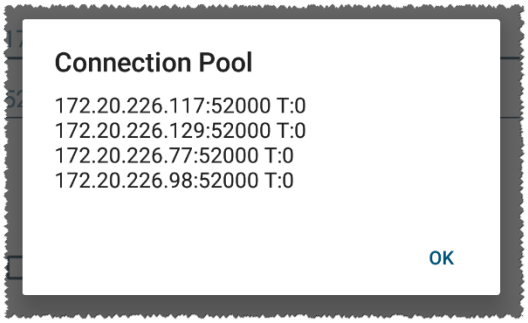
- Press **OK** to confirm the required actions.

The default Device ID is now recovered (Fig 9 **B**).

Please note only one device ID can be connected at the same time.

The server version is indicated (Fig 9 **D**) since the device had previously connected with the server i.e. it is empty at the first use. The Client Version is also indicated.

The button (Fig 9 **E**) opens a window showing the connection pool received by the mobile server.



Connection pool contains all servers at which the mobile client can connect.

2.2.3 Start-Up without Myco Launcher

On the handheld device,

➢ Touch the  icon.

The following screen will be displayed (Fig 10).

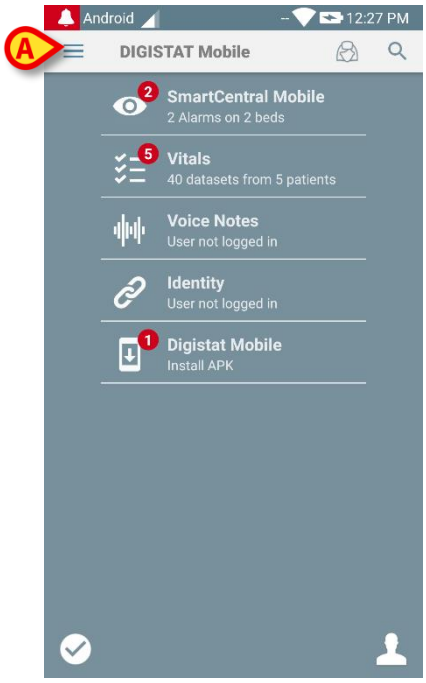


Fig 10

The available modules are listed on the page. Touch the row corresponding to the module to open it.

➢ To access the “Settings” area, touch the  icon on the top-left corner.

The following options will open (Fig 11 - see paragraph 2.3.1 for the full list of options).

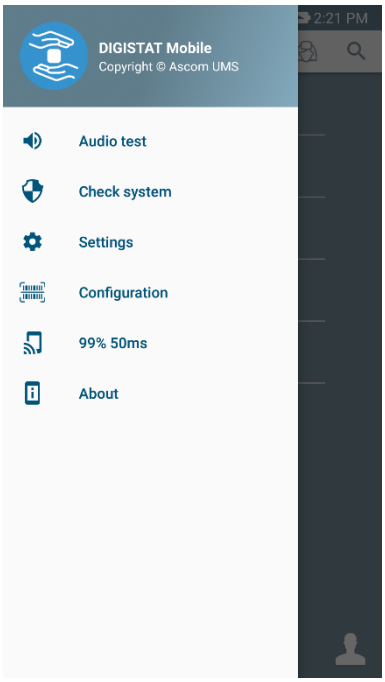


Fig 11

- Touch **Settings** to access the settings management screen. A specific password is required to access this area.

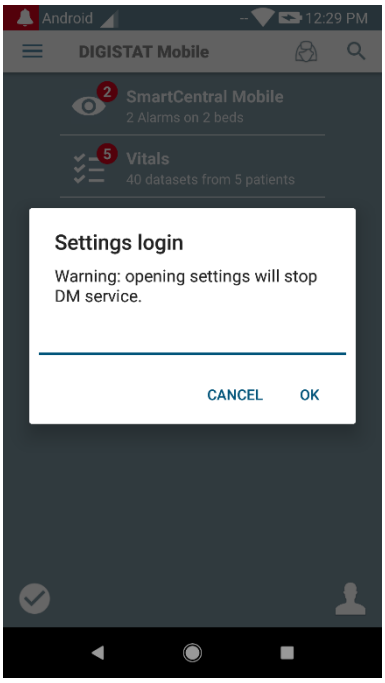


Fig 12

- Insert password and touch **OK** to access these options. The following screen will be displayed.

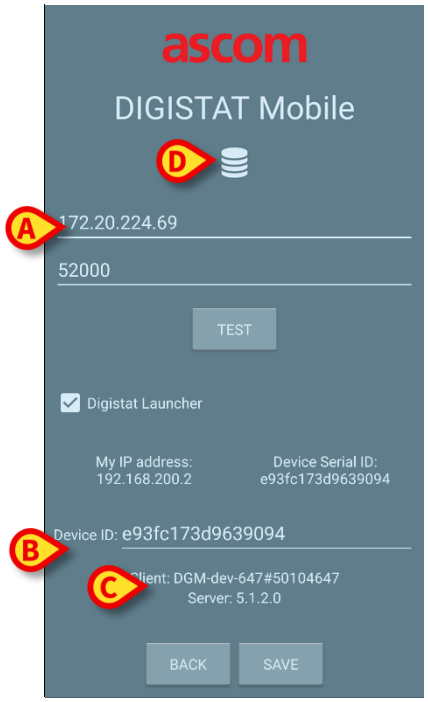


Fig 13

It is here possible to specify the IP address of the server and the server port (Fig 13 **A**). After editing:

- touch the **Test** button to test the new settings
- touch the **Save** button to save the changes made,

The lower field (Device ID - Fig 13 **B**) makes it possible to change the device id code.

Since the Device ID is changed, to recover the default value the user has to do the following steps:

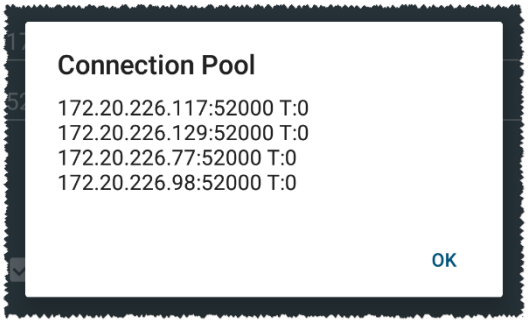
- Insert an empty value in Fig 13 **B** and then save.
  The Mobile Launcher will signal by means of a message that in this way the Device ID will be restored; in addition, a confirmation is requested by the user.
- Press **OK** to confirm the required actions.

The default Device ID is now recovered (Fig 13 **B**).

Please note only one device ID can be connected at the same time.

The server version is indicated (Fig 13 **C**) since the device had previously connected with the server i.e. it is empty at the first use. The Client Version is also indicated.

The button (Fig 13 **D**) opens a window showing the connection pool received by the mobile server.



Connection pool contains all servers at which the mobile client can connect.

2.3 Login

Login procedure can be handled from Mobile Launcher application itself or from Unite Product, if present on mobile device.

For application versions until 5.1.3, login procedure is strictly related to Myco launcher integration: if mobile application login comes from Unite, only the Myco launcher mode is available.

Application versions later than 5.1.3 allow login procedure separated from Myco launcher: Mobile Launcher or Unite login can be used indifferently if mobile application is running with Myco launcher or not.

The procedure described below is referred to the case in which the Login is performed by means of Mobile Launcher. Such a feature is signaled by the presence in the home page of the usual icons for login and logout:

To login to Mobile Launcher

- Touch **Login** on the lower-right corner of the “Applications list” screen (Fig 14 **A** or Fig 15 **A**)

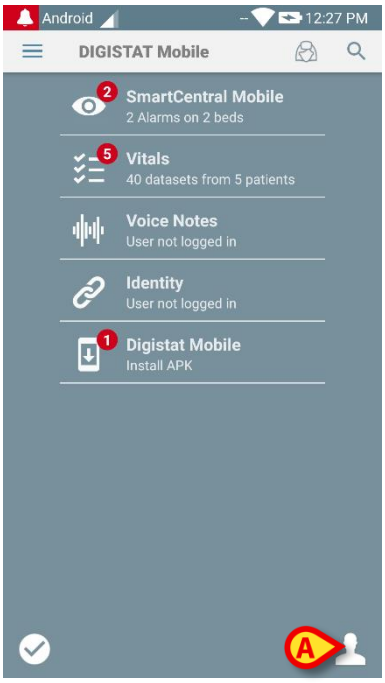


Fig 14

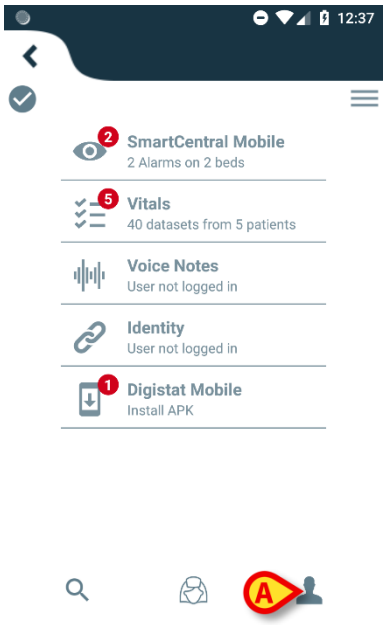


Fig 15

The following screen will be displayed (Fig 16 or Fig 17):

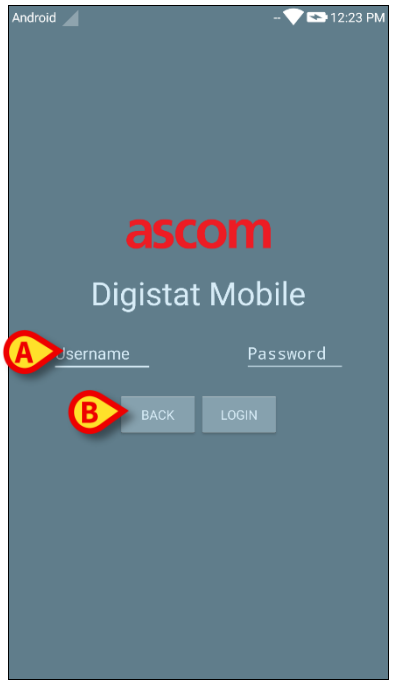


Fig 16

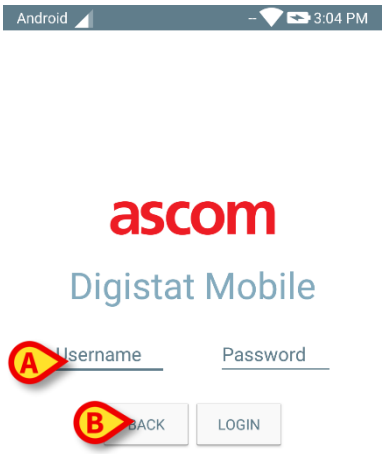


Fig 17

- Insert username and password (Fig 16 **A** or Fig 17 **A**).
- Touch the **Login** button (Fig 16 **B** or Fig 17 **B**)

The acronym indicating the logged user will then be displayed either on the upper notification bar (for generic android handheld devices - Fig 18 **A**), or on the "Applications list" screen (for Myco/UNITE version - Fig 19 **A**).

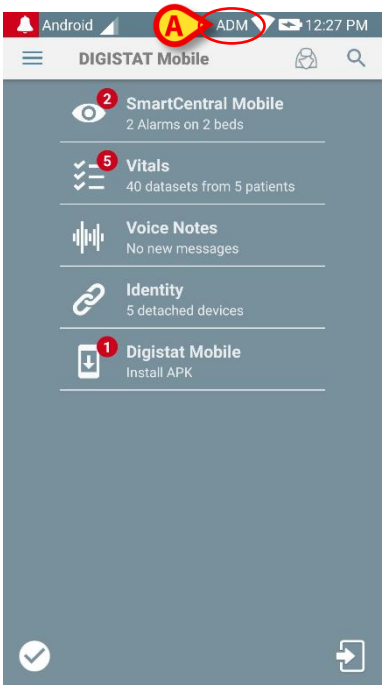


Fig 18

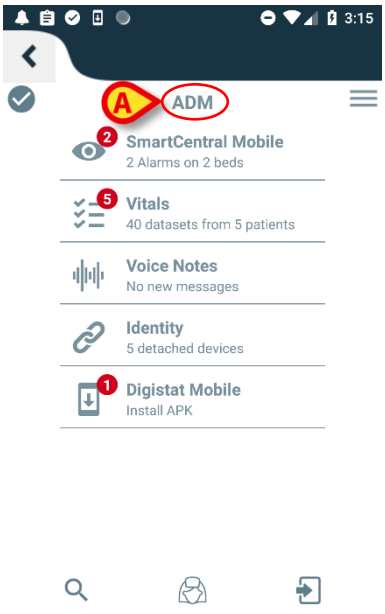


Fig 19

2.3.1 Login with PIN code

The present procedure can be performed only if the login procedure is managed by Mobile Launcher i.e. NOT with Myco Launcher.

The “Login with PIN code” is a login procedure quicker than the usual one. For this purpose the system administrator provides the user with:

- a NFC tag, whose scheme triggers the procedure;
- a PIN code i.e. a numeric code generated when the user account is created.

To Login via PIN code:

➢ Put the NFC tag close to the back of the mobile device.

The following window is shown (the “admin”):

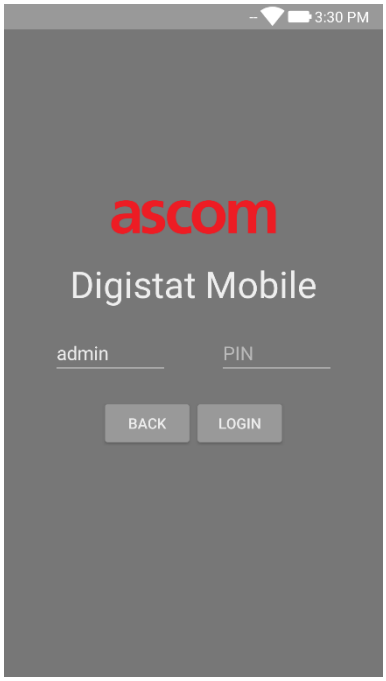


Fig 20

➢ Touch the “PIN” text field.

The numeric keyboard allowing the PIN code insertion is shown:

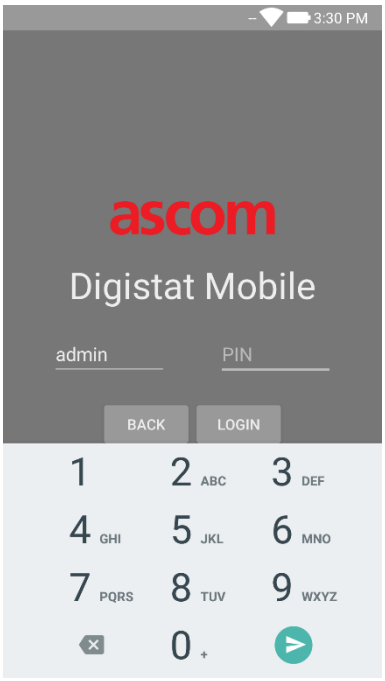


Fig 21

➢ Insert the PIN code and touch the **LOGIN** button.

Specific messages alert the user if:

- The procedure is attempted even if the mobile application is not running;
- The user is already logged in.

2.4 Lateral Menu

The  icon on the home page opens a menu containing different options (Fig 22 or Fig 23).

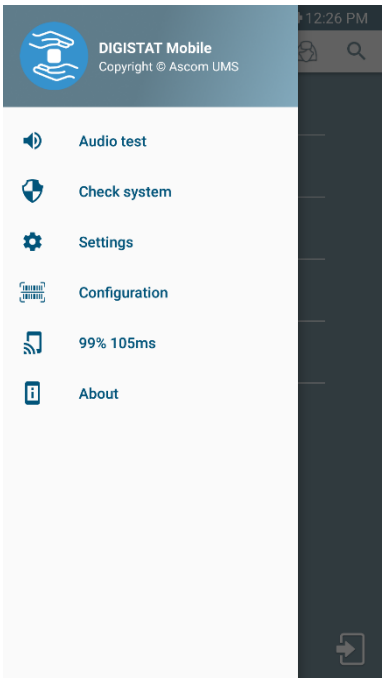


Fig 22

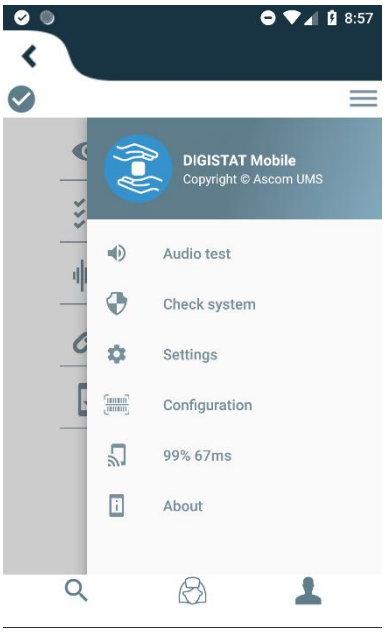


Fig 23

These are:

Audio test
Touch the **Audio Test** button to test the sound-vibration associated to the notifications (see paragraph 2.7.1).

Check system
Touch this item to perform the Check System procedure (see paragraph 2.7.2).

Settings
Touch this option to access the Settings screen (see paragraph 2.2.1).

Configuration
Touch this item to access the configuration update feature via QR code (see Paragraph 2.6.1)

Wireless connection status
Indicating the wireless connection status.

About
Touch this option to open a screen containing general info about the Product and Manufacturer. Please read the Product Manual for a complete information on this topic.

2.5 Upper notification bar

The upper notification bar (Fig 24 **A**) is always visible and displays general information. It is not available when running on Myco launcher.

Fig 24

The red bell icon placed on the top-left corner (only visible in non-Myco/UNITE devices - Fig 24 **A**) is displayed if there are notifications for one of the patients, coming from any module. It is as well displayed if the module is not active.

On the top-right corner the following information is displayed (Fig 24 **B**):

- Acronym of the logged user (non-Myco/UNITE devices);
- Wi-Fi connection status;
- Battery charge status;
- Time.

2.6 Distribution of Configuration Updates

In case the Healthcare Structure should distribute for all mobile devices a Configuration Update (i.e. mobile server address and port) to many mobile devices used by the personnel, the Product offers some different procedures to do this in the fastest and simplest way. These procedures are explained as follows.

2.6.1 Configuration Update via QR Code

The Product configuration can be updated via QR Code, if devices supports such a technology i.e. have photo camera. The configuration to be loaded has to be previously coded in a QR Code: each mobile willing to update has to shot the QR Code itself and the Product will automatically read the new configuration.

	Please note such a procedure stops the Product service until the Product itself restarts and newly connects to Mobile server. During this time no alarms are shown.

The steps one should do are below detailed:

- Access the Lateral Menu and touch the **Configuration** label (Fig 25 **A**);

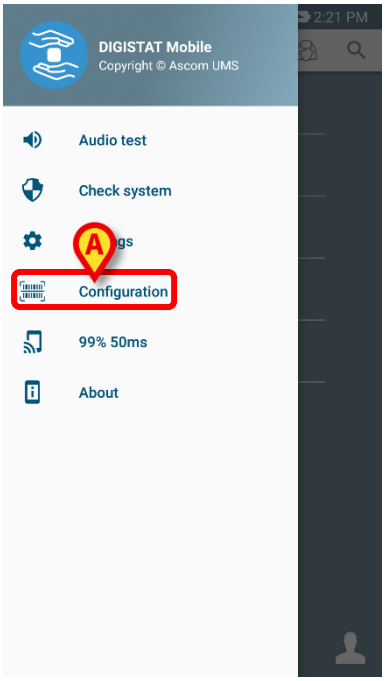


Fig 25

An authentication is requested with same credentials of Settings page (Paragraph 2.2.3). Please note during this procedure the Product service is stopped.

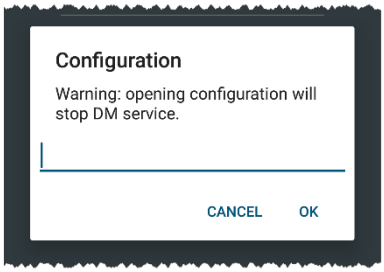


Fig 26

The following window will appear (Fig 27):

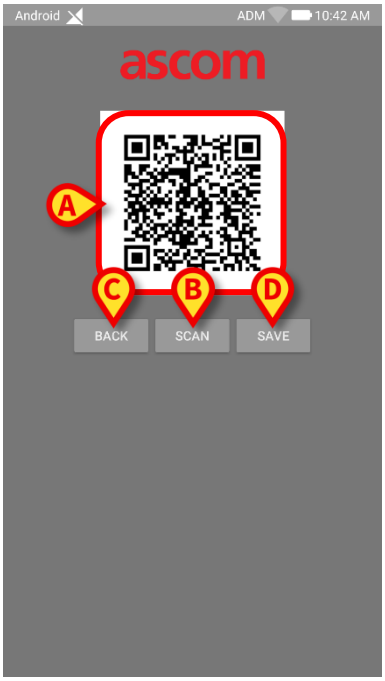


Fig 27

The QR code shown in Fig 27 **A** details the currently saved configuration. In such a way, by following the present procedure it is possible to transfer a valid configuration from a device to another one showing the QR code of a device to another device.

- Touch the **BACK** button (Fig 27 **C**) to stop the procedure and go back to launcher home page;

- Touch the **SCAN** button (Fig 27 **B**) to acquire a new QR code;

The following window opens (Fig 28). At the same time, the device flash light turns on helping the user to shoot the QR code containing the configuration. This happens only on Myco3 devices, despite other devices will display the camera stream.

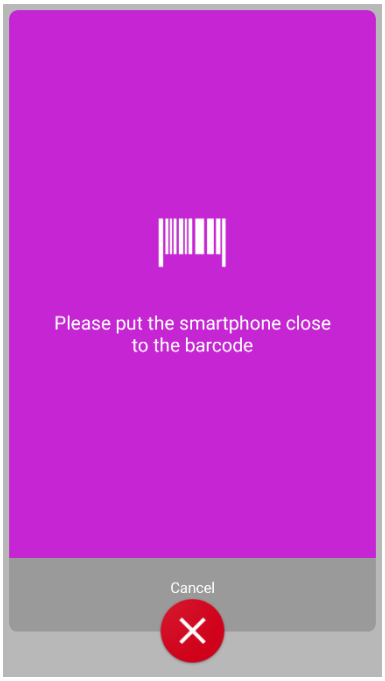


Fig 28

The QR code is automatically decoded and a connection test is moreover performed. If such a test is successful, then the following message is shown to the user (Fig 29):

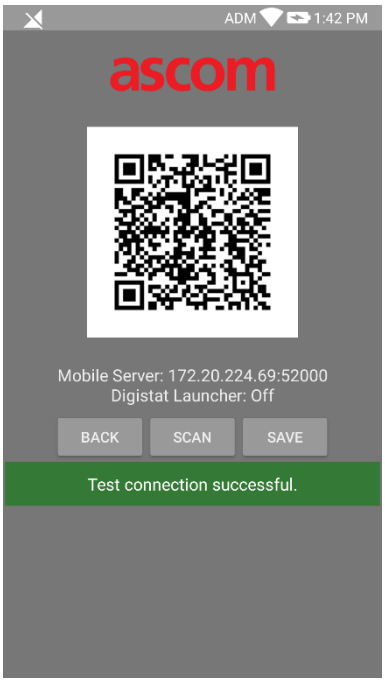


Fig 29

Otherwise, if connection test fails then a specific message is shown (Fig 30):

Fig 30

It can also happen the configuration read from the QR code is invalid or missing. A specific message is foreseen to notify such an occurrence to the user (Fig 31):

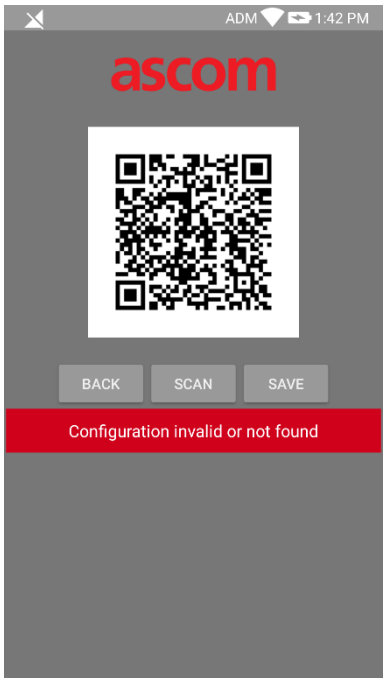


Fig 31

- Touch the **SAVE** button (Fig 27 **B**) to save the acquired QR code.

2.6.2 Configuration Update via NFC

The Product configuration can be updated via NFC, if device supports such a technology i.e. has NFC sensor. The configuration to be loaded has to be previously written on an NFC tag: each mobile willing to update has to put the mobile device close to the tag and the Product will automatically read the new configuration.

⚠	Please note such a procedure stops the Product service until the Product itself restarts and newly connects to Mobile server. During this time no alarms are shown.

⚠	Please note at the end of the present procedure the Product service is restarted only if it was previously running.

⚠	Please note such a procedure does not require administrator credentials so it should be done only by system administrator.

The steps one should do are below detailed:

- Be sure the NFC is activated on the device to be updated;
- Put the mobile device close to the NFC tag containing the details of the new configuration i.e. server address and port.

The following window is shown (Fig 32):

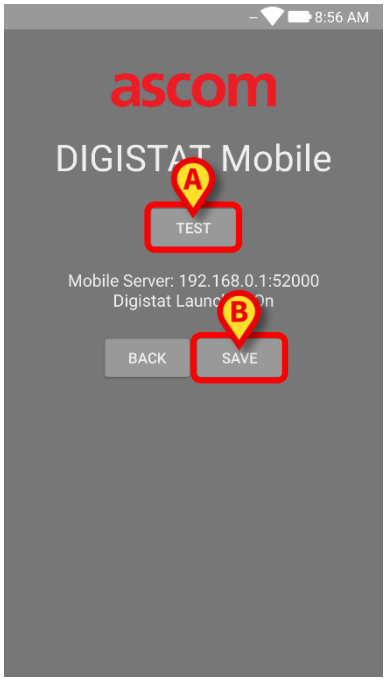


Fig 32

- Press the **TEST** button (Fig 32 **A**) to test the connection to Mobile server.

If the connection test is successful, then a message is shown to the user (Fig 33):

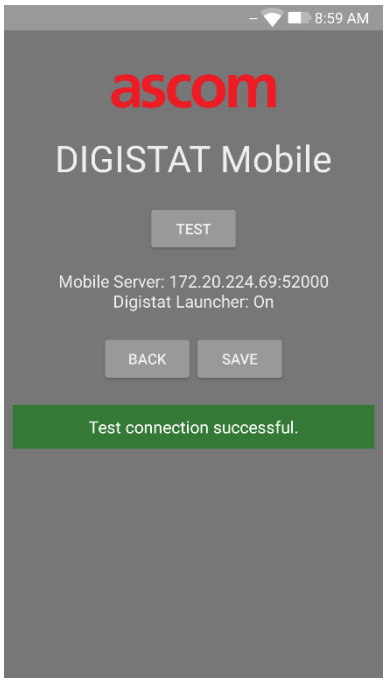


Fig 33

A notification message is shown even in case the connection test fails (Fig 34):

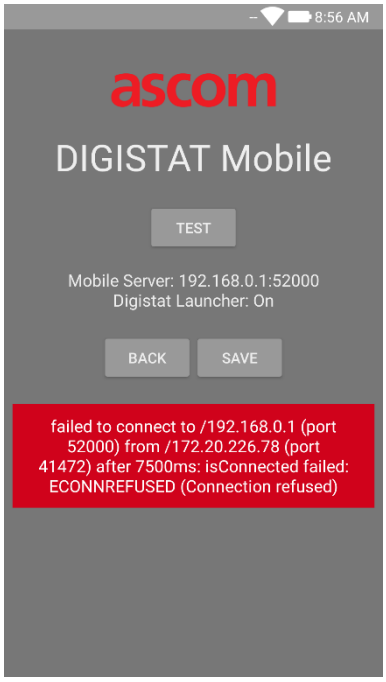


Fig 34

- Touch the **SAVE** button (Fig 32 **B**) to save the configuration read from NFC Tag.

2.7 General System Notifications

Mobile Launcher provides short notifications of alarms/messages coming from any installed module when the application is not active as well (Fig 35 **A**). The highest level notification indicates the overall alarm level of the Mobile Launcher application. Actually are implemented three levels of severity for the notifications, each of them corresponding to a different color (red = high priority – yellow = medium priority – cyan = low priority); in addition a purely informative notification is foreseen just as reminder for the user (purple).

For each module a row in the notification area is foreseen. Any change in the notifications is performed within the row related to the module triggering notification change.

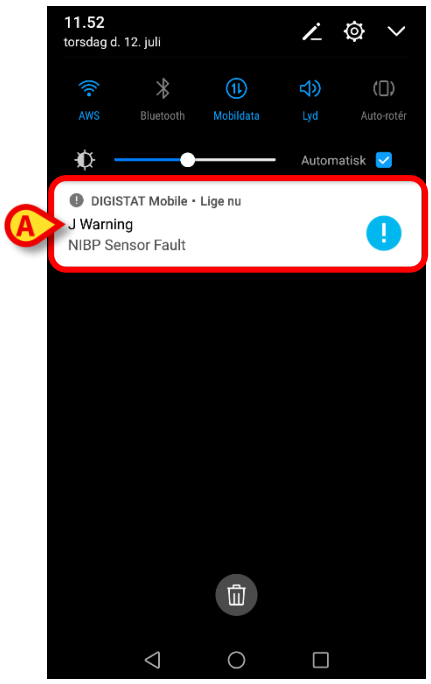


Fig 35

- Swipe the notification to make it disappear.

- Touch the notification to directly access the relevant module/patient (see an example in Fig 36; see further paragraphs for a description of the specific modules).

If the alarm notification from a module is related to one patient, then by touching it the alarmed patient tab is displayed; moreover, if the alarm notification is raised for more than one patient, by touching it the list of alarmed patient is displayed.

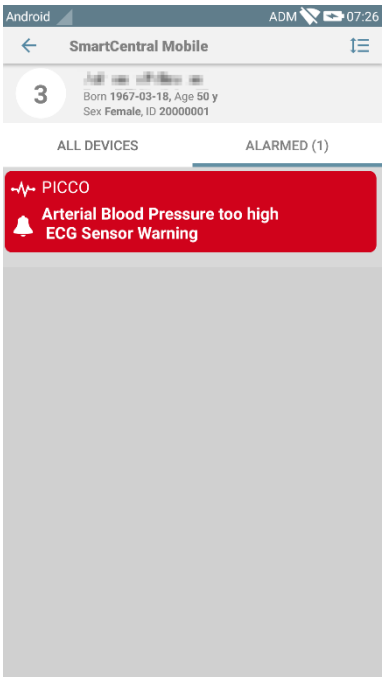


Fig 36

According to the device type, notifications concurrently coming from different applications of the Product mobile suite have a different LED color behavior

- **Myco 3**. The LED always reflects the higher priority alarm at any time;
- **Non – Myco 3**. The LED reflects the latest notification color.

This means in case of multiple notifications, when swiping the higher priority one on a Myco3 device, the LED color is the one of the next notification. On non Myco3 devices, the LED is disabled after a swipe.

In addition to screen notifications, the Product is able to handle sound notifications by means of the device speaker and light notifications by means of the notification led.

In the case of sound notifications, the Product ever plays the notification with higher priority; if a notification is being executed and a new alarm has to be raised, then the Product restarts the notification with higher priority. Notifications with low priority level don’t have any sound associated.

In case of service stop, a notification is provided to the user: it has the highest level of severity and it’s not swipable.

In case of disconnection, the Product mobile client attempts to reconnect to the Product server. If this attempt fails, a not-swipable system notification is provided to the user, according to the following two different options:

- **Android previous than 8.0**. One notification, non swipable, highest priority level. The user can mute it by pushing the **Mute** button;
- **Android 8.0 and later**. Two notifications, one non swipable without sound or LED color, the second one swipable with the highest priority level, reporting useful information about the cause of the disconnection. Moreover, the second notification will not be shown anymore since the user pushes the **Mute** button.

2.7.1 Sound Check procedure

The Sound Check procedure shall be performed at least once per shift.

The Sound Check Procedure makes it possible to verify if the sound notification of alarms is working properly.

To perform the “Sound Check” procedure

➢ Activate the main screen of Mobile Launcher application (Fig 37).

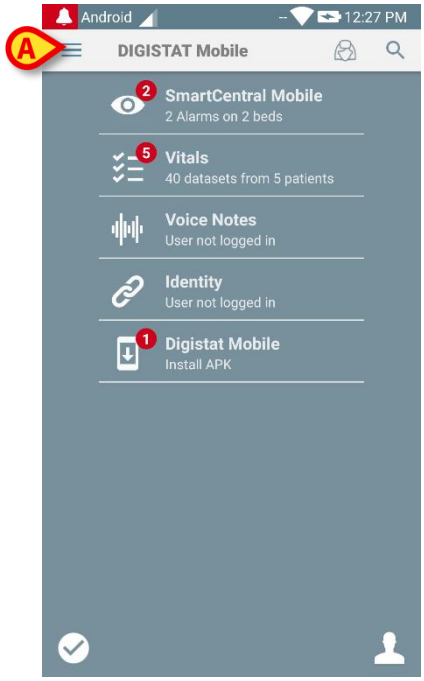


Fig 37

➢ Touch the ☰ icon on the top-left corner of the screen (Fig 37 **A**)

The following menu will be displayed (Fig 38).

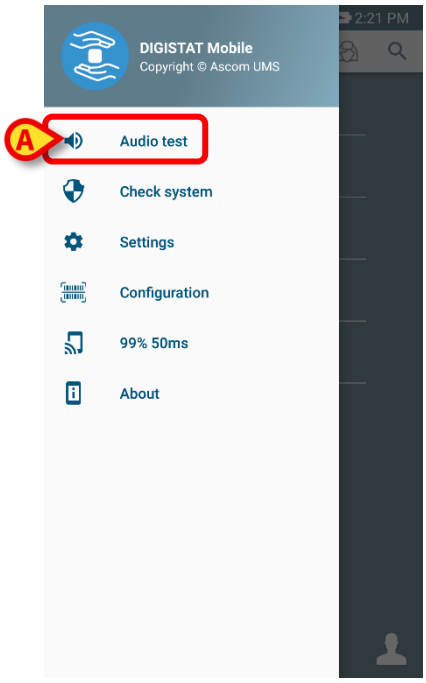


Fig 38

➢ Touch the **Audio test** option (Fig 38 **A**).

A test notification/sound will be this way provided (Fig 39 **A**).

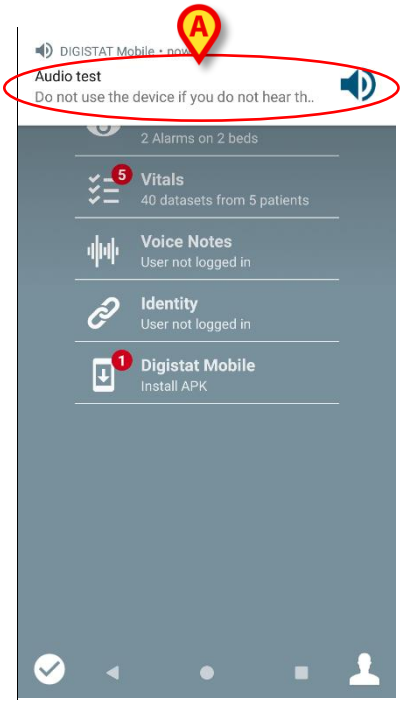


Fig 39

⚠	Do not use the device if you do not hear the alarm sound and/or feel the device vibration.

2.7.2 Check System procedure

It is highly recommended to perform the Check System procedure at first installation or every update of Mobile Launcher application.

Only Myco3 devices perform the full test suite. Some tests needing Android 6.0+ devices (not available on older Android versions) are not run on Myco 1 or Myco 2.

The Check System menu item checks if the device running the product is properly configured and operating (i.e. all the authorizations required by Mobile Launcher application to work properly were correctly provide, if the battery health is good, etc). Moreover, the proper firmware version of the device is also checked.

In the Paragraph 2.2.1 were described the authorization requested for the proper functioning of the Mobile Launcher application.

To perform the Check System

- Activate the main screen of Mobile Launcher application (Fig 40).

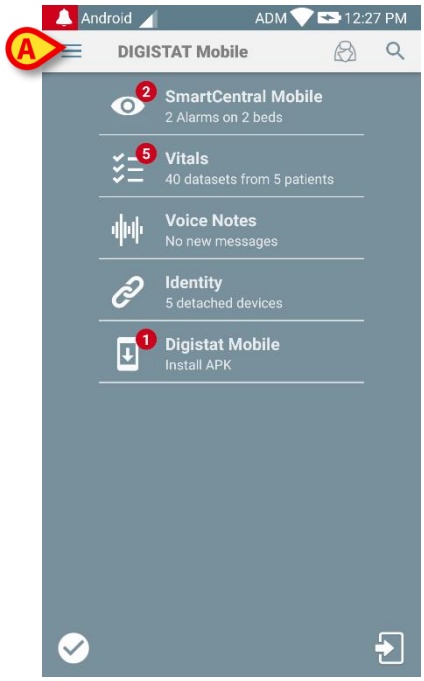


Fig 40

- Touch the ≡ icon on the top-left corner of the screen (Fig 40 **A**)

The following menu will be displayed (Fig 41).

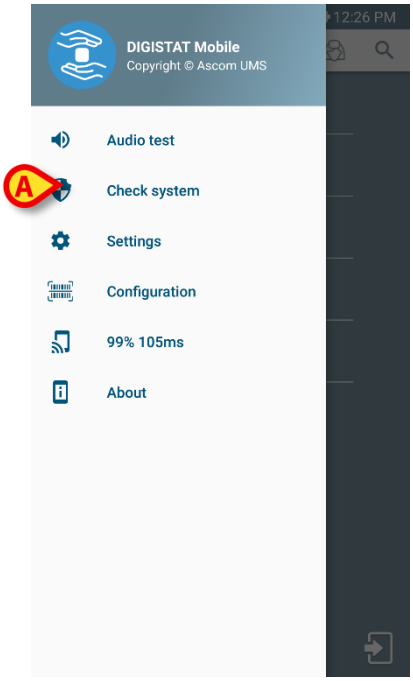


Fig 41

- Touch the **Check System** option (Fig 41 **A**).

A test notification will be this way provided, showing a reference to the missing authorizations (Fig 42). Please provide the requested authorization.

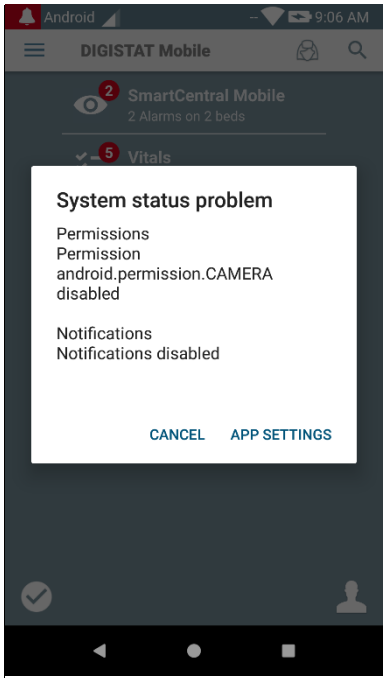


Fig 42

In addition to the above mentioned checks, the Check System raises an alert message to the user if the timestamp of Mobile client differs from the one of Mobile server. If the user touches the alarm notification related to timestamp not synchronized, then triggers the redirection to Android Settings.

	The Check System Procedure is also in charge to perform the Check Application Whitelist procedure. Please see paragraph 2.7.3 for any details.

	Do not use the device if you do not have previously provided all the requested authorizations.

2.7.3 Check Application Whitelist Procedure

	The Check Application Whitelist procedure is performed in the following cases: • During the Check System Procedure; • Each time the Main Screen of Mobile Application is displayed.

Because on some devices (i.e. Android 6.0 and later, thus NOT on Myco 1 / 2) an aggressive battery optimization policy is in place, foreground services might be frozen: this may also occur to mobile Product applications. The Check Application Whitelist procedure is in charge to verify that Mobile Launcher is in the battery optimization whitelist:

- Since this check has a negative result, a message is raised to the user suggesting to insert Mobile Launcher in the battery optimization whitelist.

	Do not use the device if you do not have previously provided all the requested authorizations.

2.8 Patient's search functionalities

The Product implements several patients search tools. These tools can be accessed from the Patients List screen.

To access the search functionalities

➢ Touch the icon indicated in Fig 43 **A** for devices without Myco/Unite integration or in Fig 44 **A** for devices with Myco/Unite integration.

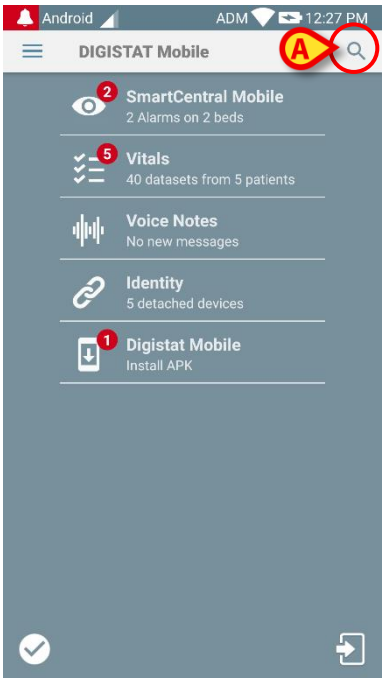


Fig 43

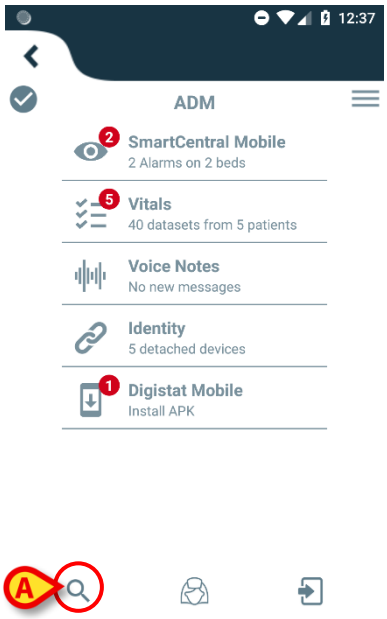


Fig 44

The following screen will open (Fig 45).

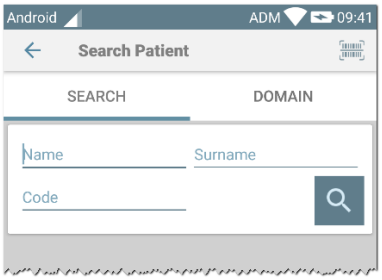


Fig 45

Three search options are available:

1. Textual search (see paragraph 2.8.1);
2. Barcode scan (see paragraph 2.8.2);
3. NFC code scan (see paragraph 2.8.3).

2.8.1 Textual search

➢ Insert patient data in the fields indicated in Fig 46 **A** (name, surname, code), then click the **Search** button (Fig 46 **B**). Partial information is allowed.

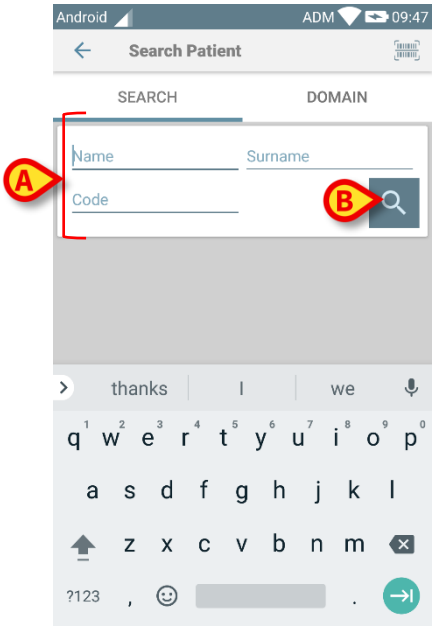


Fig 46

The list of patients whose data match those specified will be displayed (Fig 47).

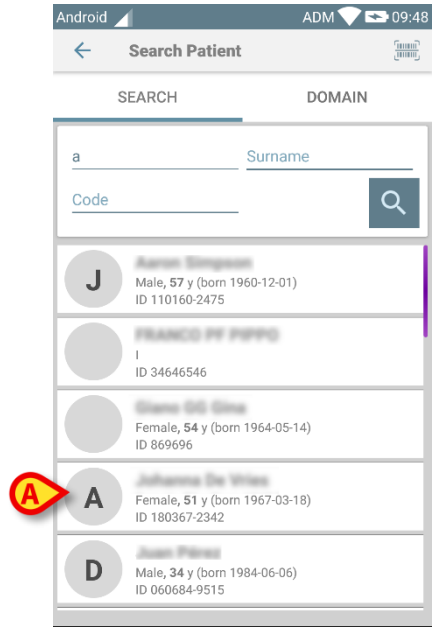


Fig 47

The search is performed among all patients, both belonging and not belonging to the device domain. If the patient is currently in bed, the bed number is displayed on the left.

➢ Touch the box corresponding to a patient to select the patient. User confirmation is required (Fig 48).

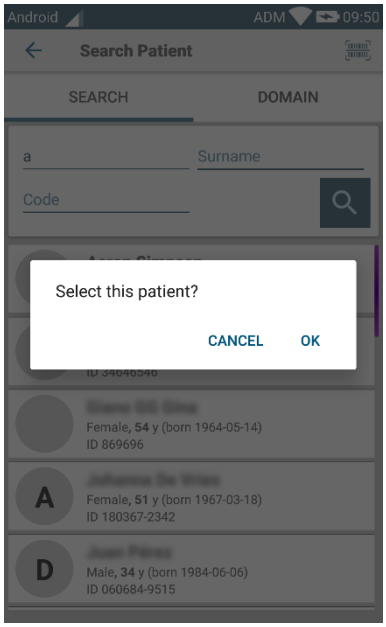


Fig 48

- Touch **Ok** to confirm.

The patient will be this way selected (Fig 49).

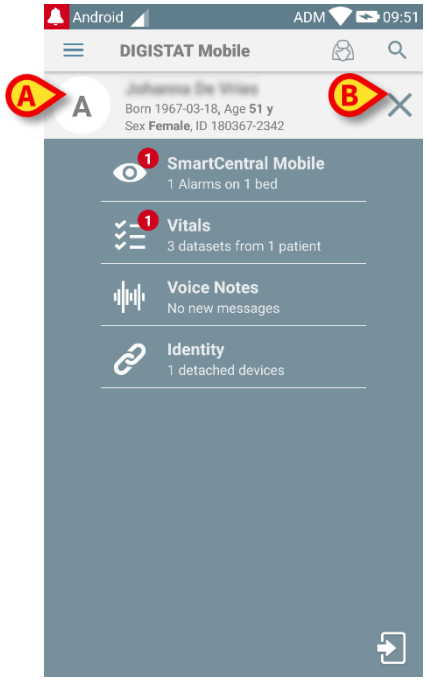


Fig 49

Patient data are on top of the page (Fig 49 **A**). All the data in all the Mobile Launcher modules are now filtered by patient (i.e. all and only the selected patient alarms/notifications are displayed).

- Touch the cross indicated in Fig 49 **B** to deselect the patient and turn to “All Patients” mode again.

2.8.2 Barcode Scan search

The Barcode Scan functionality makes it possible to select a patient by scanning his/her code.

To access the Barcode Scan functionality on non-Myco 3 devices:

- Access the search page as described in paragraph 2.8.
- Touch the  icon indicated in Fig 50 **A**

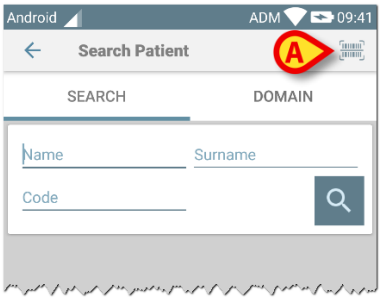


Fig 50

The device camera will be in this way activated.

- Scan the wanted patient's barcode.

To access the Barcode Scan functionality on Myco 3 devices:

- Access the search page as described in paragraph 2.8.
- Touch the side button dedicated to barcode scan (the button indicated in Fig 50 **A** is not present in this case);

The flash camera turns on to help the user to shoot the barcode. At the same time, a message is shown to the user signaling the barcode scanning (Fig 51 **A**):

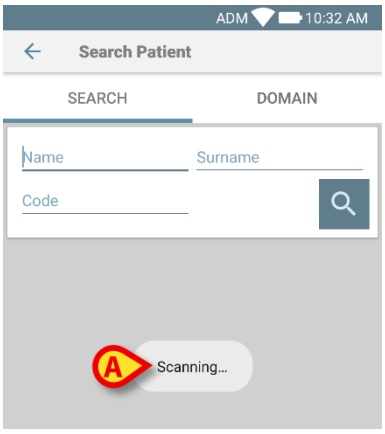


Fig 51

The patient will be this way selected. The screen shown in Fig 49 (example) will be displayed.

The barcode scanning can be done within a certain configured time; if such a time elapses and no barcode is recognized then a message is shown to the user (Fig 52 **A**):

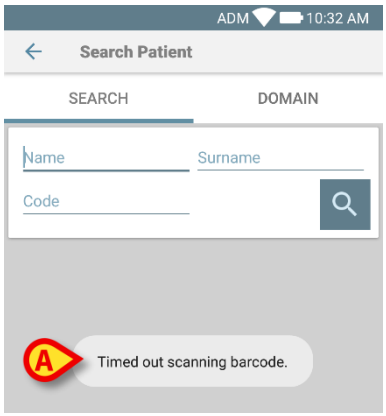


Fig 52

2.8.3 NFC Reader search

The NFC Scan makes it possible to select a patient using the device's own Near Field Communication sensor.

To do that:

- Access the search page as described in paragraph 2.8.

The device NFC reader will be this way activated.

- Position the device close to the patient's Tag.

The patient will be this way selected. The screen shown in Fig 49 will be displayed.

2.8.4 Single Patient Selection

To select a single patient:

- Touch the icon indicated in Fig 43 **A** for devices without Myco/Unite integration or in Fig 44 **A** for devices with Myco/Unite integration. The following screen will appear (Fig 53 **A**):

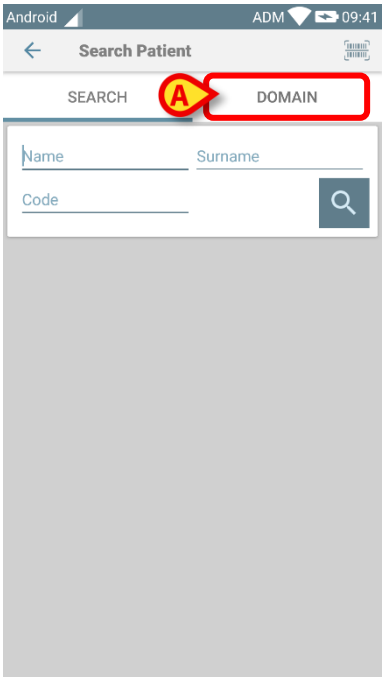


Fig 53

- Touch the "**DOMAIN**" tab. The following window shall appear (Fig 54)

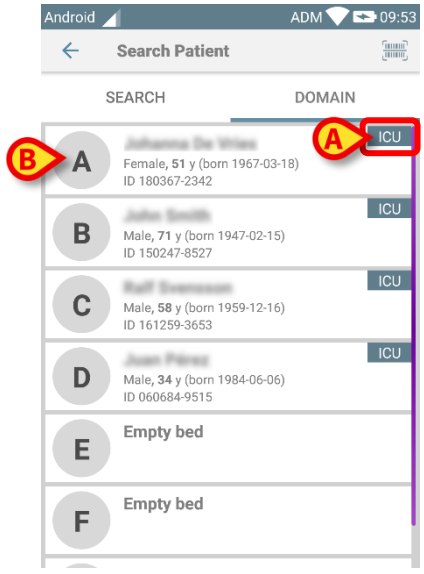


Fig 54

In Fig 54 all the patients are listed, without regard to their domain. The label on the top right corner of each tile highlights the domain of the patients (Fig 54 **A**).

One single patient can be selected by touching the tile corresponding to his/her bed. Just for example:

- Touch the tile indicated in Fig 54 **B**. User confirmation is required (Fig 55).

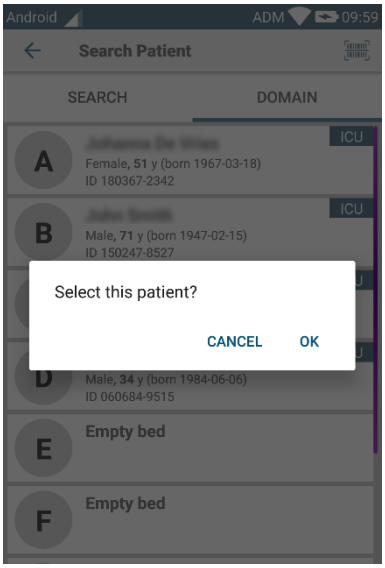


Fig 55

- Touch **Ok** to confirm. After confirmation, the following screen is displayed.

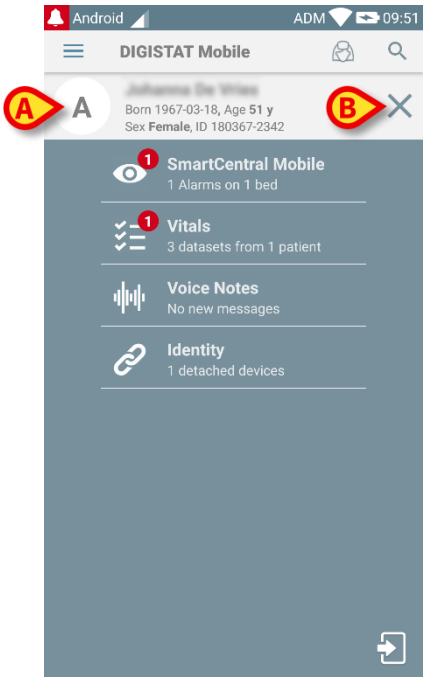


Fig 56

Patient data are on top of the page (Fig 56 **A**). All the data in all the Mobile Launcher modules are now filtered by patient (i.e. all and only the selected patient alarms/notifications are displayed).

- Touch the cross indicated in Fig 56 **B** to deselect the patient.

2.9 Patients Assignment Functionality

Patient's assignment makes it possible for a user to select one or more patients and create a group of patients who are under his charge. The name of this group in the Mobile Launcher application is "My Patients".

Since the user assigns himself some patients, the following notifications can be displayed on the handheld device:

a) The notifications related to the patients assigned (i.e. in the group "My patients");
b) The notifications related to the patients assigned (i.e. in the group "My patients") and those related to the patients that no one has explicitly taken in charge;
c) The notifications related to the patients assigned (i.e. in the group "My patients"), those related to the patients that no one has explicitly taken in charge and those related to other patients if the devices which had them in charge "lose" them (for any reason, low Wi-Fi signal for instance).

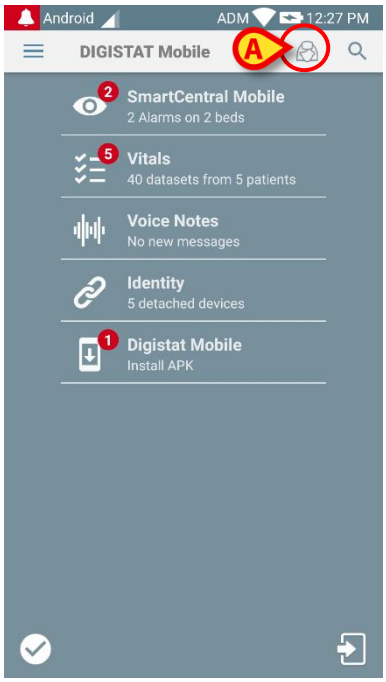


Fig 57

To select the list of patients a user assigns himself and forming "My patients" list, on Mobile Launcher Central screen,

- Touch the icon (Fig 57 **A**).

The following screen will be displayed (Fig 58 - "Setup My Patients").

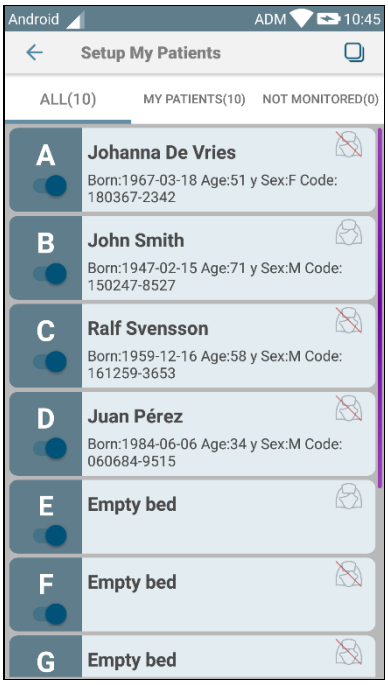


Fig 58

A patient can be selected/deselected by touching the corresponding “tile”. Each tile corresponds to a bed. In addition, the user can select or deselect all the patients by checking the box on the top right corner (Fig 59 **D**).

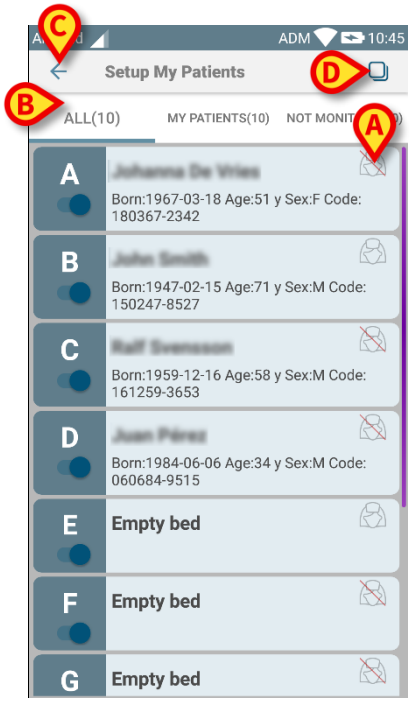


Fig 59

The icons on the right of the patient names (Fig 59 **A**) have the following meanings:

- Patient is part of “My patients” of another user. It is still possible to select the patient. If two users select the same patient, the patient will be grouped under “My patients” for both users.

 - Patient is not monitored. I.e. another user has him/her in charge, but at the moment, due (for example) to Wi-Fi connection failure, no one is monitoring him/her. No icon means that no one has the patient in their “My patients” list, so the patient is not monitored.

The filters indicated in Fig 59 **B** make it possible to display:

- All patients;
- Only the assigned patients;
- Only the patients that are not monitored.

The  icon indicated in Fig 59 **C** makes it possible to go back to “My Patients” list screen.

2.10 Patient selection/assignment, modules and domain

In the present document the phrase “patient selection/assignment” was used to generically refer to the operations in which a patient is selected in order to perform some operations on him within the Mobile Launcher environment. Nonetheless, for some of the modules detailed below it would be preferable to talk about “bed selection/assignment”.

The main differences are detailed as follows:

- An application can operate within the domain or without the domain;
    - The Smart Central, Vitals and Voice Notes module operate within the domain. This implies that they can select beds or patients within the same domain of the user;
    - The Identity module operates without the domain. This means that Identity can establish an association patient/device even for patients outside the user domain;
- An applications operating in the domain can handle beds or patients;
    - The Smart Central module handles a bed selection (because it could be important to track data from devices coming from a bed occupied by a patient not yet identified). This implies that Smart Central can select or assign empty beds;
    - The Vitals and Voice Notes modules handle a patient selection (because it is supposed that planned parameter acquisition is performed on patients yet admitted and identified). This implies that Vitals and Voice Notes cannot select an empty bed.

2.11 Device Availability

The setting of device availability is useful if the user has to be considered as “unavailable” for a temporary condition. This can be triggered from the user by proper actions in the mobile application or (if configured) by placing the device in its Docking Station.

2.11.1 Setting by the User

Within the product mobile application the user can set the device as “unavailable”. For all devices of its ward, the beds owned by the “unavailable” device will be considered as “unattended”. Nonetheless, the device set as “unavailable” continues receiving alarms and messages. In this case such alarms will continue triggering sounds and/or vibration.

- Touch the symbol in Fig 60 **A** or Fig 61 **A** to set the device as “unavailable”;

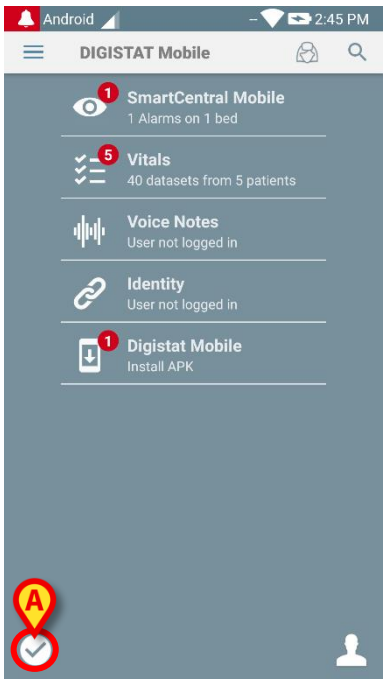


Fig 60

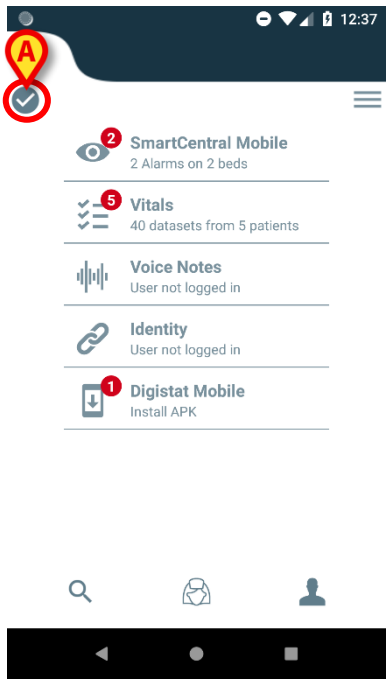


Fig 61

The following dialog message will appear, asking a confirmation from the user:

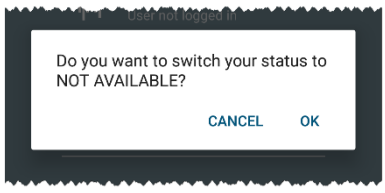


Fig 62

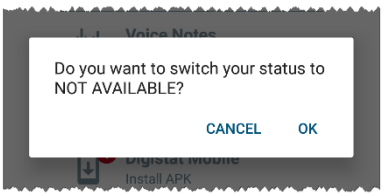


Fig 63

- Touch **OK** to set the device as unavailable.

The launcher home page will change as shown in Fig 64.

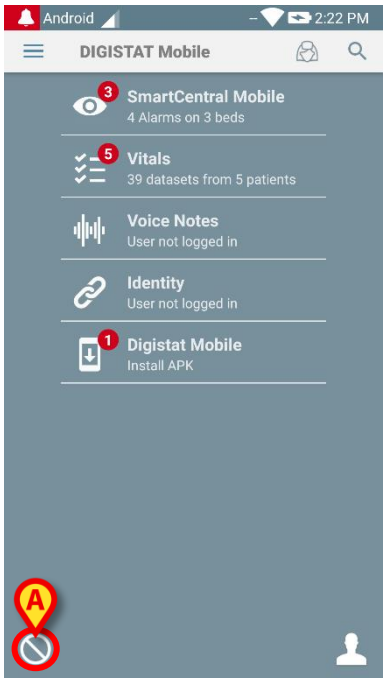


Fig 64

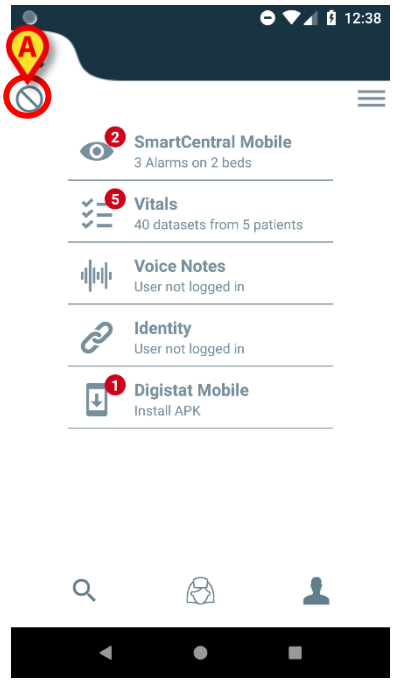


Fig 65

- Touch the symbol in Fig 64 **A** or Fig 65 **A** to set the device as “available”;

The following dialog message will appear, asking a confirmation from the user:

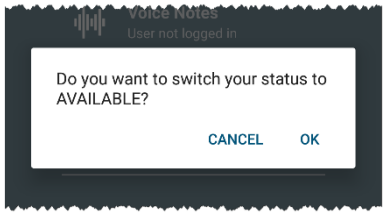


Fig 66

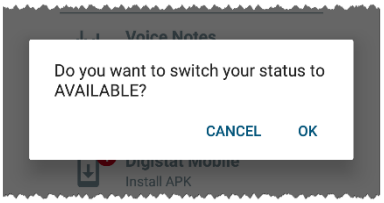


Fig 67

- Touch **OK** to set the device as unavailable.

The launcher home page will change as shown in Fig 60.

2.11.2 Setting by Docking Station

The Docking Station is an accessory device able to charge mobile devices and maintain network connection. It can host a certain number of mobile devices, thus allowing the user to change an uncharged device with a full charged one.

A specific configuration parameter has to be set in order to consider the device as “unavailable” if placed in the Docking Station.

The beds owned by the “unavailable” device will be considered as “unattended” and user will be logged out. Nonetheless, the device set as “unavailable” remains connected to mobile server and continues receiving alarms and messages.
In this case such alarms will not trigger any sound or vibration.

2.12 Updates installation (APK files)

Whenever a software update is available, an additional row is displayed on the start page (Fig 68).

Fig 68

In this situation a warning message is also displayed for the user (Fig 69):

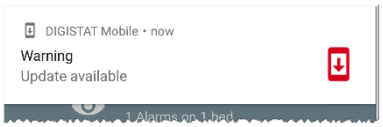


Fig 69

To install the software updates

- Touch the row indicated in Fig 68 **A**.

On Myco 1 and Myco 2 devices this is sufficient to complete the update process.

In all other cases and in particular on Android 7+ devices, the Mobile Launcher application firstly checks if the user has authorized it to install applications from unknown sources (Fig 70):

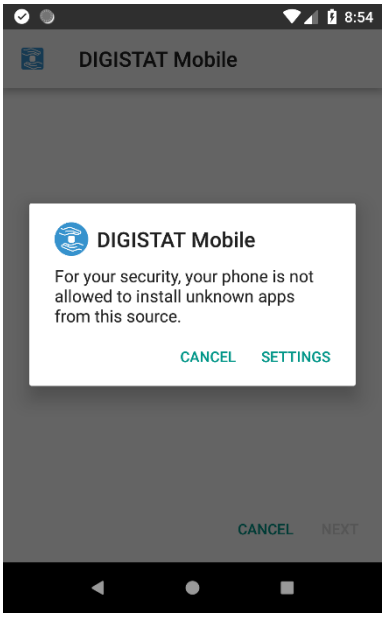


Fig 70

- Press the button **“SETTINGS”** in Fig 70 to authorize the installation of the update, or press the button **“CANCEL”** to stop the updates installation process.

The following screen will be shown (Fig 71).

- Toggle the switch in Fig 71 A with the label “Allow from this source” and then press the **“Back”** button on the device (it’s a system button and it’s not described in this User Manual).

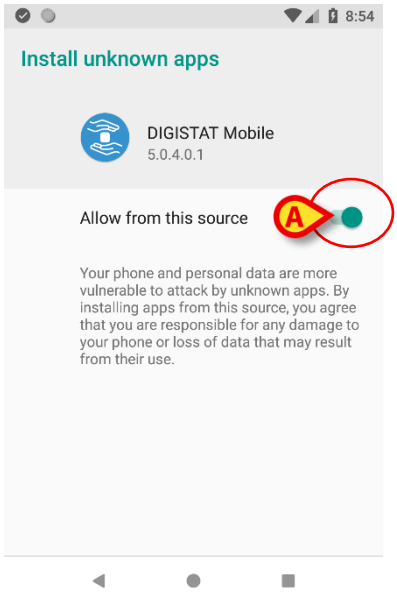


Fig 71

If all permissions requested during the first installation of Mobile Launcher application were granted, the following screen will be shown (Fig 72):

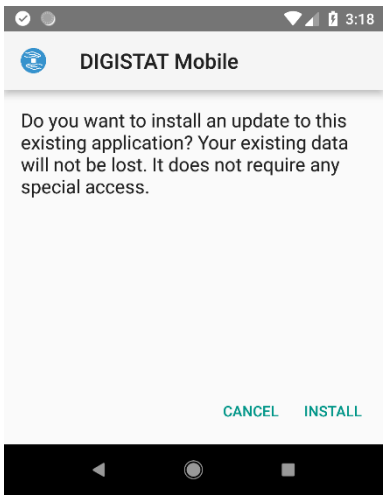


Fig 72

- Press the button **“INSTALL”** in Fig 72 to complete the updates installation process or the button **“CANCEL”** in Fig 72 to cancel the updates installation process.

2.13 Widgets

The Product implements a set of widgets i.e. graphic controls intended to facilitate some specific actions from the user.

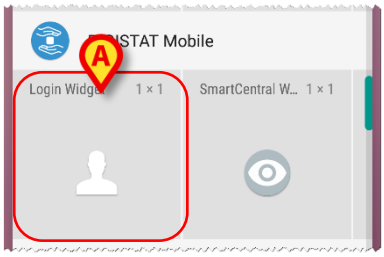


Fig 73

In the present paragraph will be showed the widget related to the overall Product mobile environment.

2.13.1 Login Widget

The Login Widget allows the user to authenticate in the Product mobile application and to search and select patients. To use such a feature the user has to do the following actions:

- Push the icon shown in Fig 73 **A** and release it on the device screen.

The Login Widget as default will be placed on the device screen with size 1 x 1 (Fig 74)

Fig 74

- Push the icon in Fig 74 **A** to authenticate in the Product (Fig 75).

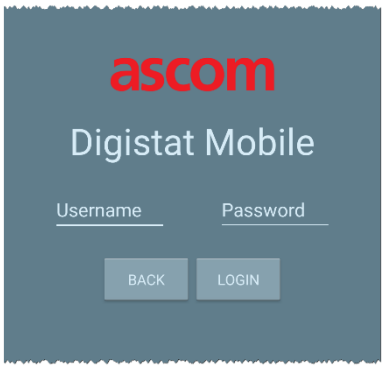


Fig 75

After the authentication, the Login Widget shows the user currently logged in:

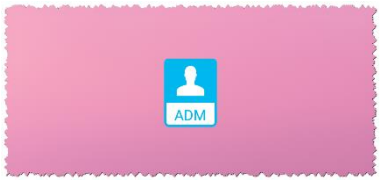


Fig 76

- Long press the icon in Fig 74 **A** or Fig 76 **A** and then release to show grab points for widget resize (Fig 77 – left if user is not logged, right if user is logged):

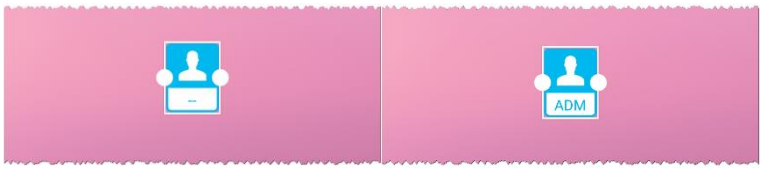


Fig 77

- Touch and move one of the two grab points and then push the desktop background to resize the widget to the size 2 x 1:

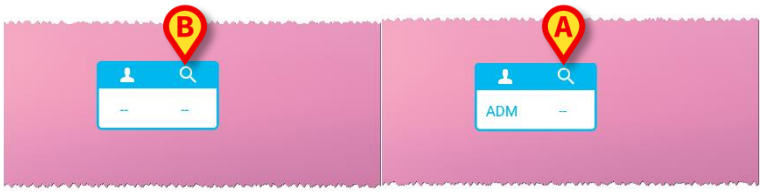


Fig 78

- Touch the icon in Fig 78 **A** to access the Patient Search & Selection functionality (Fig 79).

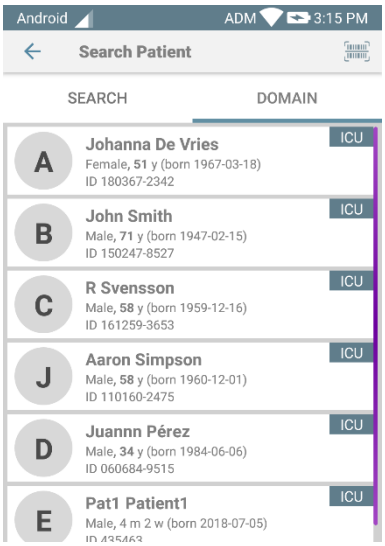


Fig 79

Such a feature is accessible only if the user is logged in. If the user is not logged in and the icon in Fig 78 **B** is pressed, then the authentication window is moreover displayed.
After the Patient Selection, the Login Widget shows the patient currently selected (Fig 80):

Fig 80

- In this situation, touch again the Login Widget to show the main page of the Mobile Application (Fig 81):

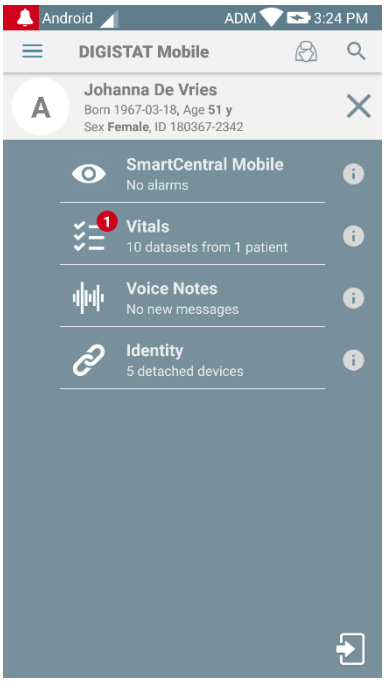


Fig 81

Please note that in the Widget's size 2 x 1 some patient names could result too long to be correctly displayed. In this case, it is suggested to extend again the size of the Widget. The Login Widget can be indeed resized to 3 x 1, 4 x 1 and 5 x 1:

Fig 82

If the user logs out while a patient is currently selected, the Login Widget will show a "blank view" i.e. no user and no patient will be shown.