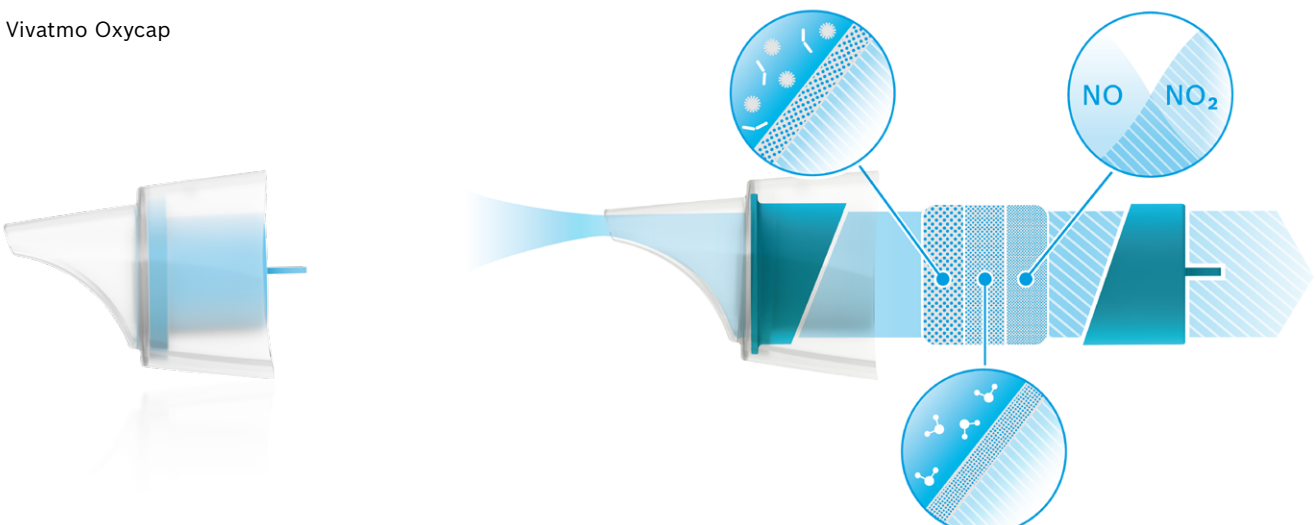
BOSCH

Vivatmo pro

Administration instructions

Vivatmo Oxycap



en

Content

1 Administrator settings 4

2 Device settings 4

2.1 Setting the language 5

2.2 Setting date and time 5

2.3 Setting Auto-Lock 6

3 Quality Control (QC) settings 7

4 Printer configuration 7

5 Network and interfaces 9

5.1 Handheld 9

5.1.1 Assigning the handheld 9

5.1.2 Release the handheld 10

5.2 Network configuration 10

5.2.1 Supported configuration of an ethernet connection 12

5.2.2 Supported installation of a WLAN connection 13

5.2.3 Manual ethernet configuration 14

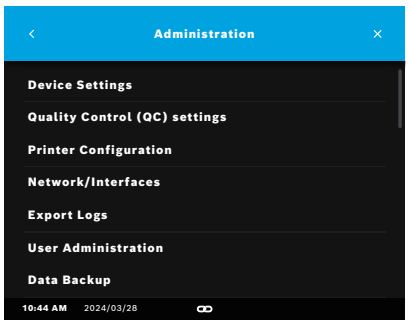
5.2.4 Manual WLAN configuration 15
5.3 Order/result interface 16
5.4 Export and Backup file configuration 18
5.5 Vivasuite configuration 19
6 Export Logs 21
6.1 Reading out audit log files 21
6.2 Reading out system log files 22
7 User administration 23
7.1 Add new user 24
7.2 Editing and reset user accounts 25
7.3 Enable/Disable user account 25
7.4 Deleting user accounts 26
8 Data backup 26

 © Bosch Healthcare Solutions GmbH

en

1 Administrator settings

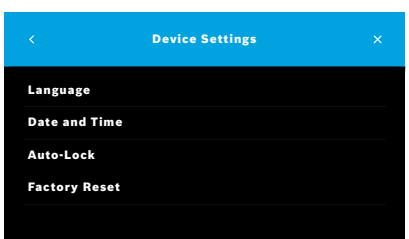
These Administration instructions supplement the Vivatmo *pro* instructions for use explaining all administrator settings of the settings menu.



INFORMATION	Administration settings are activated only if you are logged in as administrator.

1. Log in as administrator.
2. In the Settings menu, select **ADMINISTRATION**.

2 Device settings

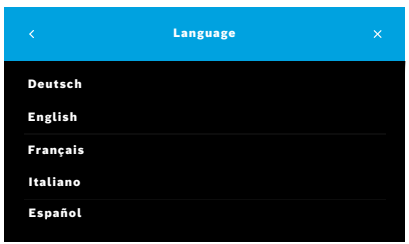


3. On the **Administration** screen, select **Device Settings**.
   The **Device Settings** screen opens for changing Language, Date and Time, Auto-Lock or Factory Reset. Factory Reset resets all stored data and settings.

© Bosch Healthcare Solutions GmbH

2.1 Setting the language

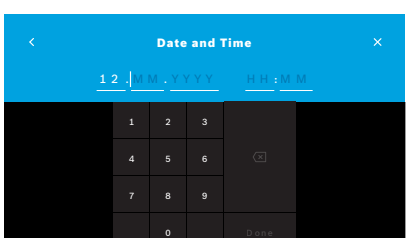
The language selection depends on the selected region.



1. On the **Device Settings** screen, select **Language**.
2. Select the desired language.

2.2 Setting date and time

The time format is <dd/mm/yyyy>, <hh:mm> 0-24 h.

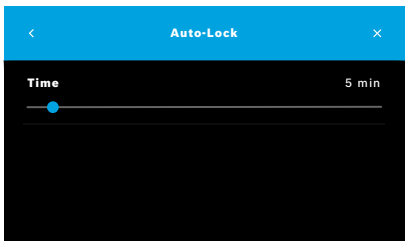


1. On the **Device Settings** screen, select **Date and Time**.
2. Enter day, month, year and the time.
3. Confirm with **DONE**.
4. Select the **CONTINUE** button to confirm your settings.

© Bosch Healthcare Solutions GmbH

en

2.3 Setting Auto-Lock



When Auto-Lock is activated, the system shuts down to save energy and protect patient data. The user needs to log in again after an automatic lockoff.

You can set the interval according to the needs in the clinical environment.

1. On the **Device Settings** screen, select **Auto-Lock**.
2. Select and hold the blue point and move it to the desired Auto-Lock time.

Factory reset

Factory reset removes all stored measurements from the basestation and all data of patients and users. Date and time are reset and no handheld will be connected afterwards.

INFORMATION	Use factory reset prior to disposal or service returns only.

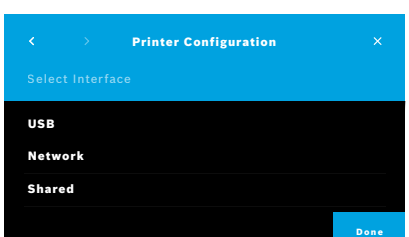
3 Quality Control (QC) settings

External QC tests are used to control the measurements of the Vivatmo *pro* handheld in comparison to reference concentrations of nitric oxide (NO).

Quality control settings can only be accessed by administrators. The QC settings contain QC status, interval and number of measurements.

For further information see “6.2 Quality control (QC)” in General manual.

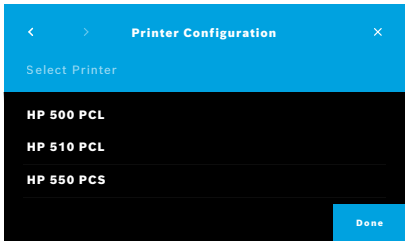
4 Printer configuration

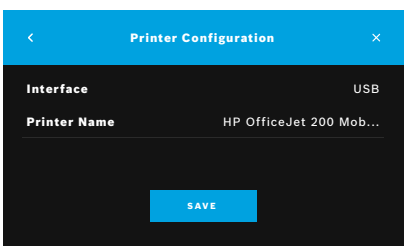


1. On the **Administration** screen, select **Printer Configuration**.
   The **List of Printers** screen opens. The standard printer is highlighted.
2. Select **Add printer**.
3. Select the desired printer interface:
   - USB
   - Network
   - Shared

   Select the **Right Arrow** to move to the **Select Printer** screen.

 © Bosch Healthcare Solutions GmbH





INFORMATION	Printing data is transmitted unencrypted.

4. On the **Select Printer** screen, select the desired printer.
5. Select the **Right Arrow** to move to the **Select Printer Driver** screen.
6. Select the **printer driver**.

   The **Printer Configuration** screen is displayed.
7. Confirm with **SAVE** to save the printer configuration.
   The list of printers is shown.

Elements in the list of printers:

8. Mark a printer to select your standard printer.
9. Select the **Delete** button to delete a printer from the list.
10. Select the **x** button to close the list.

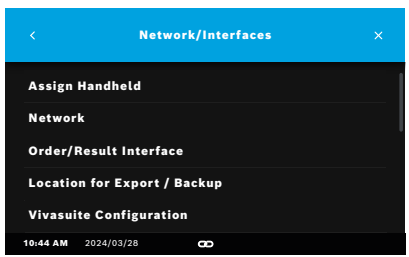
 © Bosch Healthcare Solutions GmbH

en

5 Network and interfaces

5.1 Handheld

5.1.1 Assigning the handheld



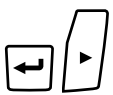
1. On the **Administration** screen, select **Network/Interfaces.**
2. On the **Network** screen, select **Assign Handheld**.
3. Turn on your handheld.
4. Select **SCAN FOR HANDHELDS**.
5. Wait until the scan procedure is completed.
   You see the list of active handhelds.
   If no handheld is active, you see the message: “No handhelds available”.
6. Compare the number of the Vivatmo *pro* handheld in the list with the serial number beneath the symbol SN on the handle of the handheld.
7. From the list, select the Vivatmo *pro* handheld which shall be installed with your Vivatmo *pro* basestation.
8. The Configuring device screen opens.The handheld and the basestation connect automatically.

The Vivatmo *pro* handheld and the Vivatmo *pro* basestation show the same date and time now.

INFORMATION	If QC is activated, perform a QC-measurement after assigning a new handheld. The basestation software stores the QC status of the handheld with each measurement.

5.1.2 Release the handheld

In case another handheld was installed before, it is disconnected by tapping the **Release Handheld** button. If you want to dispose the old handheld, clear memory and take out the battery.



1. Keep the **ENTER** button and the **Arrow right** button pressed for 3 seconds.

The **Clear memory** icon is selected.

2. Use the **Arrow** buttons to select the check mark.

3. Press the **ENTER** button to confirm the clear memory.

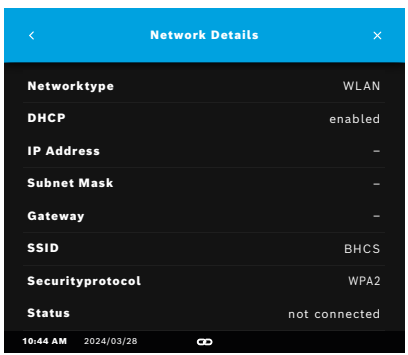
An animation is shown while the **Clear memory** icon flashes.

4. Press the **ENTER** button to return to the main screen.
5. Switch off the handheld.

5.2 Network configuration

Vivatmo *pro* can be connected to a local area network to receive measurement orders, send back measurement results, export patient related measurement data, or use a network printer. Vivatmo *pro* supports Ethernet and Wireless via WLAN connection.

INFORMATION	**Vivatmo *pro* shall not be used in unprotected networks.** Data security using user credentials shall be used in accordance with the local data security policies. Data is transmitted unencrypted.

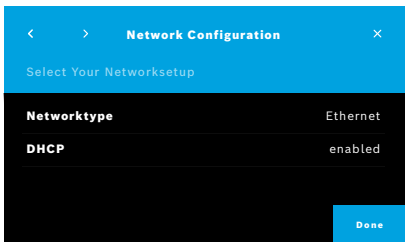


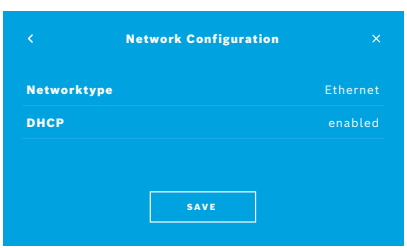
1. On the **Network/Interfaces** screen, select **Network**.
2. If a network access is configured already, select **Show Network Configuration.**
   The **Network Details** are:
   - **Networktype:** WLAN or Ethernet
   - **DHCP**: **D**ynamic **H**ost **C**onfiguration **P**rotocol
     When DHCP is enabled, the device supports the configuration of the network.
   - **IP Address:** Internet Protocol (IP) address uniquely identifies a device on a network. It needs to be set when DHCP is disabled.
   - **Subnet Mask:** Defines the network and host portions of an IP address. It must be configured when DHCP is turned off to ensure proper network segmentation.
   - **Gateway:** Connects different networks. It should be specified when DHCP is disabled to enable access to external networks, such as the internet.
   - **SSID**: **S**ervice **S**et **Id**entifier
     Shows the name of the WLAN network.
   - **Status:** Status can be “connected” or “not connected”

 © Bosch Healthcare Solutions GmbH

en

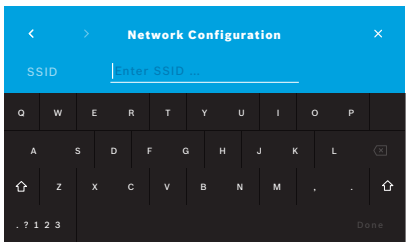
5.2.1 Supported configuration of an ethernet connection

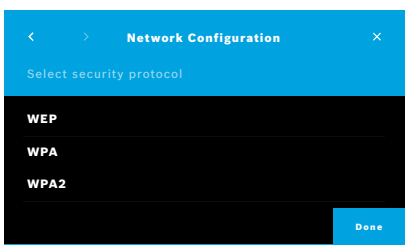




1. Plug in the ethernet cable in the ethernet port on the rear of the Vivatmo *pro* basestation.
2. On the **Network** screen, select **Configure Network**.
3. Select the Networktype **Ethernet** in the drop down menu.
4. Enable **DHCP**.
5. Confirm with **SAVE**.

5.2.2 Supported installation of a WLAN connection



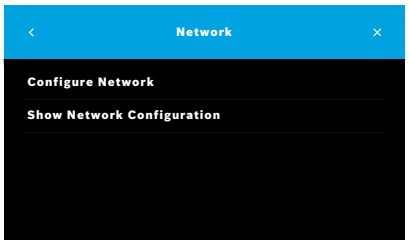


1. On the **Network** screen, select **Configure Network**.
2. Select the Networktype **WLAN**.
3. Enable **DHCP**.
4. On the **Set network SSID** screen, enter the name of the WLAN.
5. Select the **Right Arrow** or the **DONE** button to leave the screen.
6. Select the security protocol activated in your WLAN.
7. Select the **Right Arrow** button to leave the screen.
8. On the next screen, enter the WLAN Password of your WLAN.
9. Select the **Right Arrow** or confirm with **DONE** to leave the screen.
10. Confirm with **SAVE**.

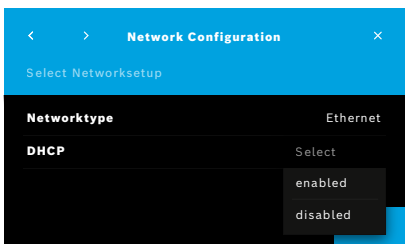
 © Bosch Healthcare Solutions GmbH

en

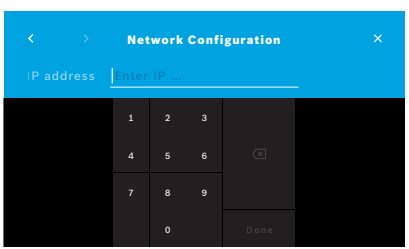
5.2.3 Manual ethernet configuration



1. Plug in the ethernet cable in the ethernet port of the basestation.
2. On the **Network** screen, select **Configure Network**.



3. Select the **Networktype Ethernet**.
4. Disable **DHCP**.



5. Enter the **IP-Address** of your network and the **Subnet Mask** of your network.
6. Enter the **Gateway ID**.
7. Select the **Right arrow** or confirm with **DONE** to leave the screen.

8. Confirm with **SAVE**.

5.2.4 Manual WLAN configuration

1. On the **Network** screen, select **Configure Network**. The **Network Configuration** screen opens.
2. Select the Networktype **WLAN**.
3. Disable **DHCP**.
4. Follow steps 4 to 8 of “5.2.2 Supported installation of a WLAN connection”.
5. Follow step 5 to 8 of “5.2.3 Manual ethernet configuration”.
   After a successful configuration, the **Network Configuration** screen is displayed.
6. Confirm with **SAVE**.

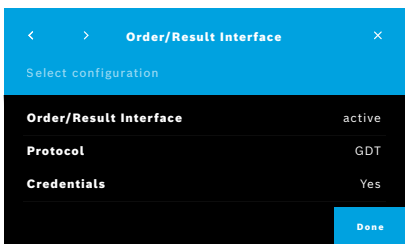
 © Bosch Healthcare Solutions GmbH

en

5.3 Order/result interface

Vivatmo *pro* can receive measurement orders from and send results to an electronic patient record system (EPR), if the network is configured. The interface standards GDT (German Data Transfer) and HL7 are supported.

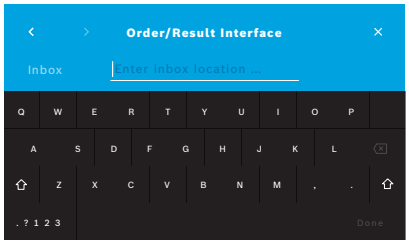
To configure the interface to your patient management system follow the installation wizzard:

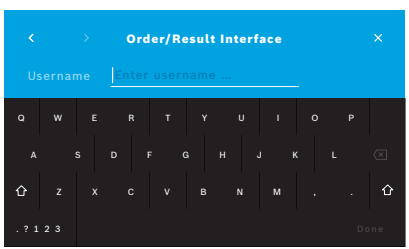


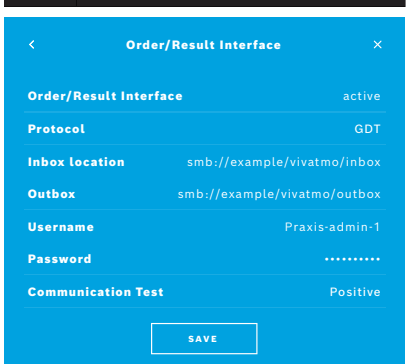
1. On the **Administration** screen, select **Network/Interface**.
2. On the **Network and Interface** screen, select **Order/Result Interface**. You can select:
   - **Configure Interface** to change the settings.
   - **Show Interface Configuration** to display the current settings.

Select **Configure Interface** to change settings.

3. Activate the **Order/Result Interface**. The system keeps the interface settings when deactivated.
4. Select the **Arrow Right** button to move to the next screen. Select the desired protocol standard: **HL7** or **GDT**.
5. Select **Yes** for Credentials when the **Order/Result Interface** is access controlled by user name and password.







6. In accordance to IT definitions in your organization, define the location for the inbox for incoming measurement orders.
7. Repeat the procedure for the location of the outbox.
8. Confirm with **DONE**.

When credentials are required, follow steps 9 to 13.

9. Enter the user name required to access the data from the EPR system.
10. Confirm with **DONE** to move to the next screen.
11. Enter the password required to access the data from the EPR system.
12. Confirm with **DONE**.

    The settings for the **ORDER/RESULT INTERFACE** are displayed including the result of a Communication Test.
13. Check the data and confirm with **SAVE** when the data are correct.

    On your home screen, you see the order button, see “2.1 Screen elements” in General manual.

    If you delete the inbox and the outbox, the order button disappears from the home screen.

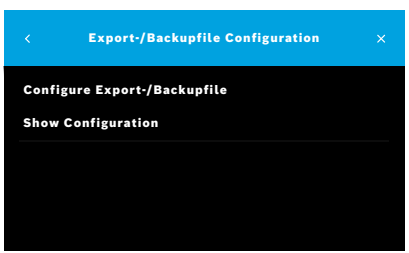
 © Bosch Healthcare Solutions GmbH

en

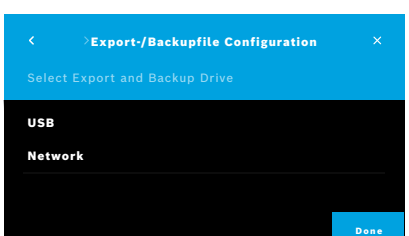
5.4 Export and Backup file configuration

You can export data from patient records (see “5.1 Patient records”in General manual) or backup the entire measurement and patient data (see “8 Data backup”) to a defined storage location. The storage location can rather be a USB drive or a network drive. Export files of a patient can be identified by the time stamp and the patient name. Export data are transmitted unencrpyted. The backup file is stored encrypted and can be imported to the same basestation only.

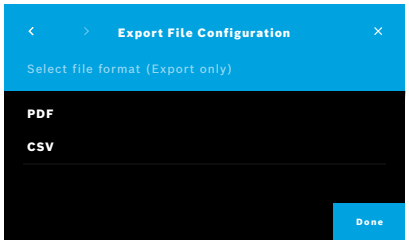
For configuration follow the configuration wizard:



1. On the **Administration** screen, select **Network/Interfaces**.
2. On the **Network and Interfaces** screen, select **Location for Export/ Backup**.



3. Select **Configure Export/Backup File** to change the settings.
4. In accordance to IT definitions in your organization, define the location for the storage of the export and backup files on USB or network drive. End the location path always with “/”-symbol.



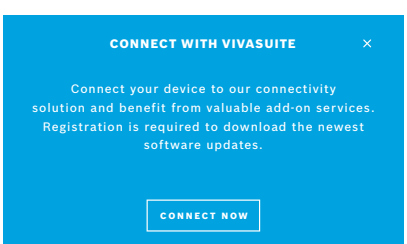
5. Select **CSV** or **PDF** as export format.
   The settings for the **Location for Export/Backup** are displayed.
6. Check the data and confirm with **SAVE** button when the data are correct.

5.5 Vivasuite configuration

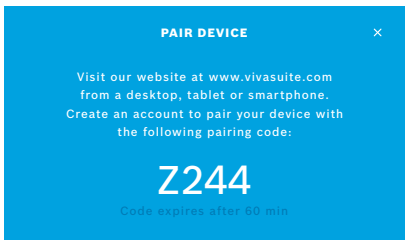
Vivasuite is the digital Vivatmo ecosystem allowing to use services such as device management and remote software update. Vivasuite runs in the Bosch managed Cloud and applies highest standards regarding IT security and data privacy. The Vivasuite service is not available in all countries. Ask your local distributor.

A registration to Vivasuite and pairing of your device is required. Your device must be connected to an internet-enabled network.

To connect Vivatmo *pro* to Vivasuite perform the following steps:

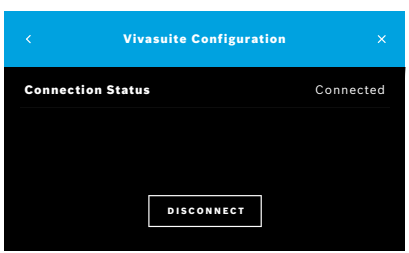


1. Vivasuite: Register an account on www.vivasuite.com and log into your account.
2. Vivatmo *pro*: On the Administration Screen select **Network/Interfaces**. On the **Network/Interface**s screen, select **Vivasuite configuration**.
3. Vivatmo *pro*: Click through introduction and configure your network connection (for details see “5.2 Network configuration”) until devices show screen with the pairing code.



4. Vivasuite: Click **Add device**.
5. Vivasuite: Enter the pairing code shown on the Vivatmo *pro*.
6. Vivatmo *pro*: Confirmation screen is shown.

To disconnect Vivatmo *pro* from Vivasuite perform the following steps:



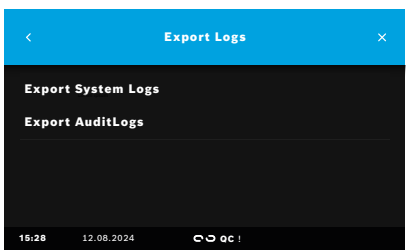
1. Vivatmo *pro*: On the **Network/Interfaces** screen, select **Vivasuite Configuration.**
2. Vivatmo *pro*: Select **Disconnect**. You are asked to confirm before device gets disconnected.

 © Bosch Healthcare Solutions GmbH

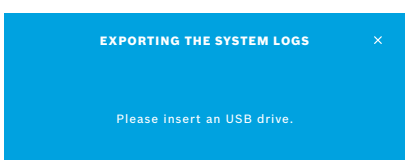
6 Export Logs

6.1 Reading out audit log files

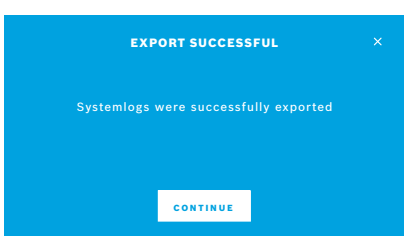
Administrators can read-out audit log files for quality management purposes.



1. Log in as administrator.
2. Go to **Settings** and **Administration**.
3. Click on Export Logs.
4. Choose **Export Audit Logs**.



5. Insert USB drive and copy audit logs.

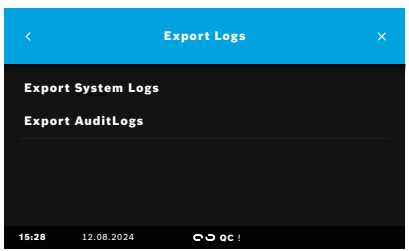


 © Bosch Healthcare Solutions GmbH

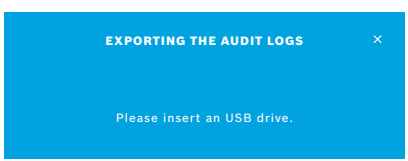
en

6.2 Reading out system log files

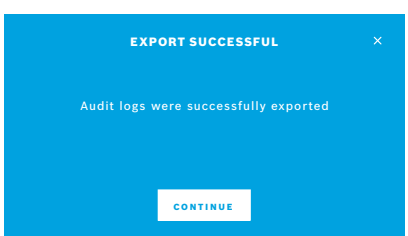
The system is recording any internal system events. Administrators or technicians can export system log files to USB drive for the exchange with the customer support.



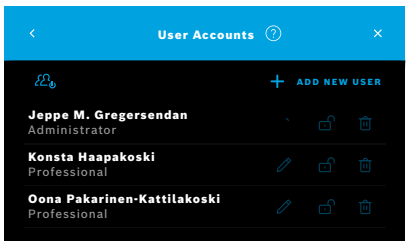
1. Log in as administrator.
2. Go to **Settings** and **Administration**.
3. Click on **Export Logs**.
4. Choose **Export System Logs**.



5. You will be asked to insert an USB drive. Insert USB drive and copy system logs.

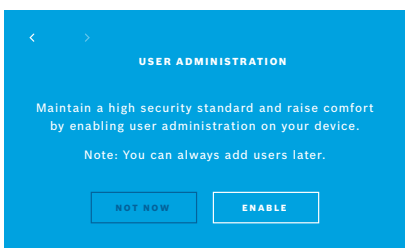


7 User administration



1. On the **Administration** screen, select **User Administration**.

   Access control by user accounts can be disabled by the button .



When **USER Administration** is not enabled in the setup procedure, the **User Accounts** screen opens to **ENABLE** individual user accounts.

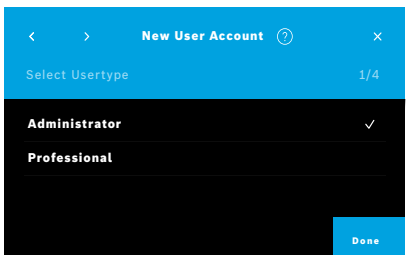
INFORMATION	By disabling the User Administation the user settings are kept for later use. See also “3.2.1 User concept” in General manual.

INFORMATION	The system needs at least 1 administrator login. If the administrator passcode is forgotten, Vivatmo *pro* needs to be reset by a service technician.

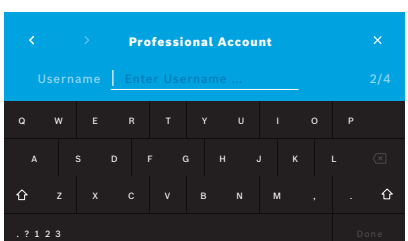
en

7.1 Add new user

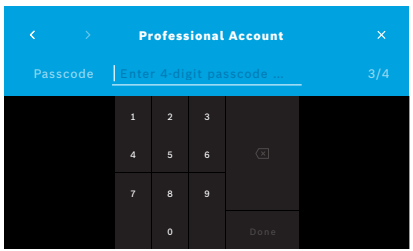
For adding a new user, follow the configuration wizard:



1. On the **User Accounts** screen, select the **+ ADD NEW USER** button.
2. Select the desired user type, see “3.2.1 User concept” in General manual
   - Administrator
   - Professional



3. Enter the **name** of the user.



4. Enter the respective **passcode**:
   - a 4 digit passcode for a professional user.
   - an 8 digit passcode for an administrator account.
5. Repeat the passcode.
6. Confirm with **DONE**. The user is successfully added.

7.2 Editing and reset user accounts

1. On the **User Accounts** screen, select the user you want to edit.
2. Select the **Pencil** button.
3. Enter your changes to user name and passcode.
4. Confirm with **DONE**.

7.3 Enable/Disable user account

1. On the **User Accounts** screen, select the user you want to enable/ disable.
2. Select the **Enable/Disable user** button. When lock is open, the user access is enabled.

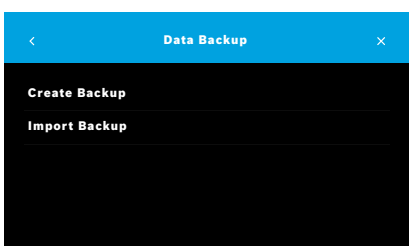
© Bosch Healthcare Solutions GmbH

7.4 Deleting user accounts

1. On the **User Accounts** screen, select the user you want to delete.
2. Select the **Delete** button.
   The account is deleted.

8 Data backup

Data backup stores the entire measurement and patient data encrypted at the defined storage location, see “5.4 Export and Backup file configuration”. Due to the encryption mechanism the Backup data can be imported to the same basestation only. The import of the backup overwrites the data stored on the basestation.



1. On the **Administration** screen, select **Data Backup**.
2. Select between:
   - **Create Backup**
   - **Import Backup**

   The backup procedures might take up to 5 minutes.

UK CA	UKCA mark refers to compliance with UK regulation “Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 (as amended).”

CH REP	Decomplix AG Freiburgstrasse 3 3010 Bern Switzerland

Approved by Ministry of Communications of Israel
התאמת מספר אישור מטעם הישראלי
משרד התקשורת: 51-89211

חל איסור לבצע פעולות במכשיר
שעלולים לשנות את התכונות האלחוטיות של המכשיר,
כולל שינויים בתוכנה, החלפת א
אנטנה מקורית או הוספת אפשרות חיבור
לאנטנה חיצונית, ללא קבלת אישור
ממשרד התקשורת, מחשש ל
התערבות עובדים.

ift IFT TEBOVI24-01350 NOM NYCE	La operación de este equipo está sujeta a las siguientes dos condiciones: (1) es posible que este equipo o dispositivo no cause interferencia perjudicial y (2) este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.

MCMC HIDF24000106	Certification for telecommunications or multimedia products that meet the standards set by the Malaysian Communications and Multimedia Commission (MCMC) for use in Malaysia.

CCAF24LP145AT5 CCAF24LP1330T6	Without permission granted by the NCC, any company, enterprise, or user is not allowed to change frequency, enhance transmitting power or alter original characteristic as well as performance to a approved low power radio-frequency devices. The low power radio-frequency devices shall not influence aircraft security and interfere legal communications; If found, the user shall cease operating immediately until no interference is achieved. The said legal communications means radio communications is operated in compliance with the Telecommunications Management Act. The low power radio-frequency devices must be susceptible with the interference from legal communications or ISM radio wave radiated devices.

กสทช.

เครื่องวิทยุคมนาคมนี้ ได้รับยกเว้น ไม่ต้องได้รับใบอนุญาตให้มี ใช้ซึ่งเครื่องวิทยุคมนาคม หรือตั้งสถานีวิทยุคมนาคมตามประกาศ กสทช. เรื่อง เครื่องวิทยุคมนาคม และสถานีวิทยุคมนาคมที่ได้รับยกเว้นไม่ต้องได้รับใบอนุญาตวิทยุคมนาคม ตามพระราชบัญญัติวิทยุคมนาคม พ.ศ. 2498

กสทช. โทรคมนาคม
ก้ากับดูแลเพื่อประชาชน
Call Center 1200 (โทรฟรี)

TRA
REGISTERED No.
ER92285/20
DEALER No.
DA97534/20

Complies with
IDMA standards
DA105282

72413/SPDDI/2021
10325

72412/SPDDI/2021
10325

BOSCH

Bosch Healthcare Solutions GmbH
Stuttgarter Straße 130
71332 Waiblingen
Germany

CE IVD

F09G100560_03
Latest change: 2024-12-06

Bosch Healthcare Solutions GmbH
Stuttgarter Straße 130
71332 Waiblingen, Germany