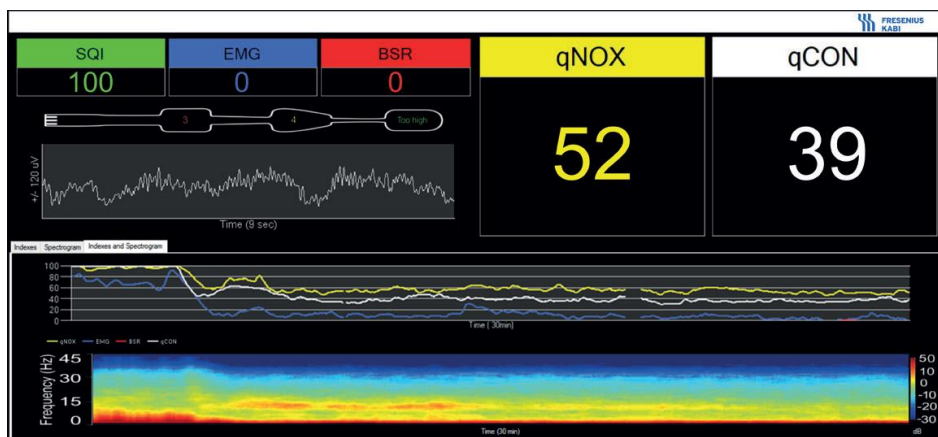


ConoxView PC v3.3

Instructions for Use



Abbreviations

EEG	Electroencephalogram
PC	Personal Computer
SQI	Signal Quality Index
BSR	Burst Suppression Index
EMG	Electromyogram Index
qCON	Conox consciousness index
qNOX	Conox Nociception index
FFT	Fast Fourier Transform

Table of Contents

1. GENERAL INFORMATION	5
1.1. About this manual	5
1.2. Contact address	5
1.3. Disclaimer	5
1.4. Copyright	5
1.5. Intended purpose	5
1.6. Indication for use	6
1.7. Contraindications	6
2. SOFTWARE REQUIREMENTS	7
3. INSTALLATION	7
3.1. Installation of the software	7
3.2. Pairing the Conox	13
4. SOFTWARE CHARACTERISTICS	14
4.1. System description	14
4.2. Controls and indicators	14
4.3. Tabs	15
4.4. Toolbar	15
4.5. Main Indexes	17
4.6. Secondary Indexes	17
4.7. Electrode Impedance	17
4.8. EEG waveform	17
4.9. Trends graph	18
4.10. Spectrogram	18
4.11. Recording Time	21
4.12. Annotations	21
4.13. Status bar	21
4.14. Notifications and warning messages	22
5. USING CONOXVIEW	26
5.1. View and record current Conox case	26
5.2. Replay saved case	27

5.3. Download a case	29
<u>6. CYBERSECURITY CONSIDERATIONS</u>	<u>32</u>
6.1. Data flows and user interactions diagram	32
6.2. Potential risks & vulnerabilities	32
6.3. Cybersecurity Requirements	35
6.4. Cybersecurity and IT-Network environment	37
6.4.1. Policy recommendations:	38
6.4.2. IT-Network recommendations:	38
6.5. Cybersecurity Features	39
6.5.1. Log visualization	40
6.6. Cybersecurity safety considerations	42
6.6.1. Network configuration	43
6.6.2. User Access Control (permissions management)	44
6.6.3. Login and passwords management	44
6.6.4. Hardening	46
6.7. Firewall configuration	46
6.8. Security Updates (Vulnerability management)	47
6.9. Data protection	47
6.10. Incident detection & response	48
6.11. Awareness and training	48

1. General Information

1.1.About this manual

This manual contains important information about the operation of the ConoxView (the "Software") PC v3.3. Here you will find how to install and operate the Software. It is important that you read and understand the manual fully before using the Software.

Ensure that all users of the Software are suitably trained and qualified, and make sure that the user has access to this manual.

1.2.Contact address

Manufacturer

Fresenius Kabi AG
Else-Kröner-Str. 1
61352 Bad Homburg
Germany
+49 (0) 6172 / 686-0
www.fresenius-kabi.com

1.3.Disclaimer

Manufacturer reserves all rights. No part of this document may be reproduced or published, in any format without written consent of the Manufacturer.

1.4.Copyright

This document is the sole copyright of Fresenius Kabi and must not be copied, distributed, or amended without the written consent of the Manufacturer.

1.5.Intended purpose

The ConoxView is intended to collect data from Conox in recording mode and/or download data stored on the Conox data repository, acting only as a remote display, and providing means for data storage.

1.6. Indication for use

ConoxView is intended to be used by healthcare professionals trained in anesthesia.

ConoxView is intended to be used in hospitals and medical facilities.

ConoxView displays and stores the data that are received from Conox device.

If ConoxView shows different or inconsistent values from the Conox device, the user shall rely on and use the Conox device values.



Refers to Conox device IFU for indication for use of the Conox device index and data.

1.7. Contraindications

Do not use the solely ConoxView for patient monitoring purpose.

Clinical decisions should not be taken relying on the data displayed on the ConoxView.

Refers to Conox device IFU for contraindications of the Conox device index and data.

2. Software requirements

The application ConoxView PC was designed to run on medical grade computers and monitors running Microsoft Windows Operating System, with the following minimum requirements:

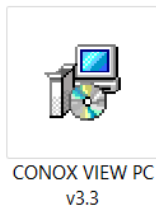
Minimum Requirements	
Operating System	Windows 10 or 11 (64 bits)
Connectivity	Bluetooth connectivity
Screen size	10 inches
Memory	ROM: 1024MB RAM: 1024MB
Processor	1GHz

Due to the wide variety of manufacturers and software, Fresenius Kabi cannot guarantee that the application will run on all computers that meet these requirements. Contact your Distributor for further information if encountering problems. It is recommended that no other programs are open during the functioning of the ConoxView to ensure a good performance.

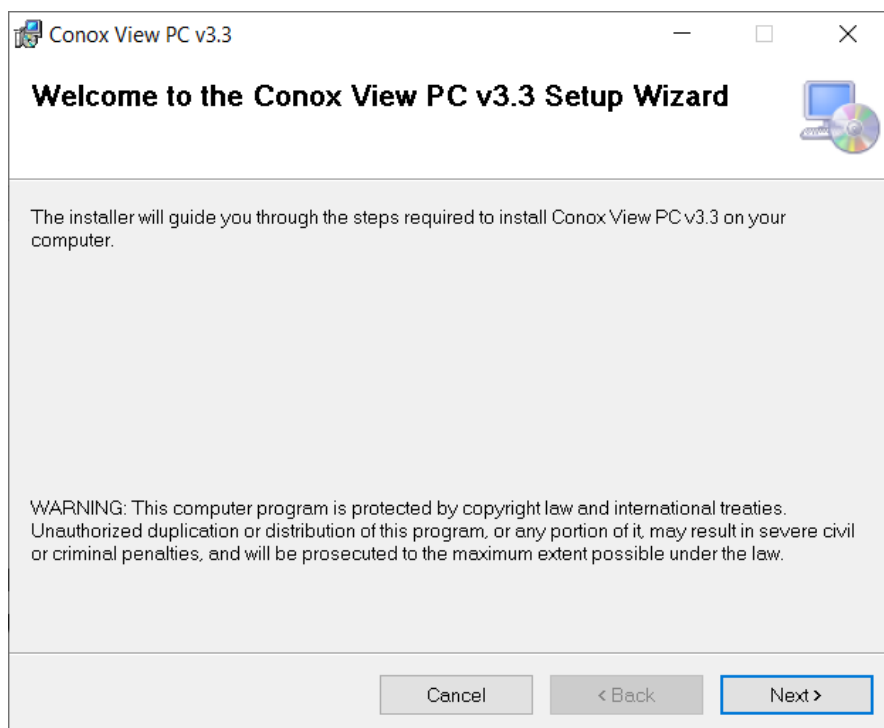
3. Installation

3.1.Installation of the software

Install the Software via the ConoxView PC v3.3 icon.

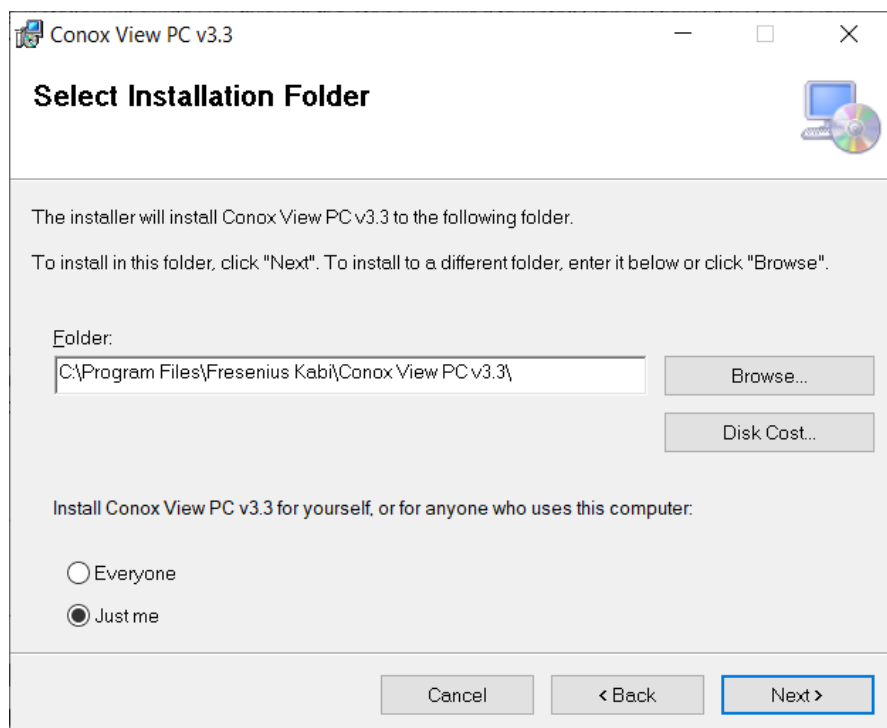


The installer will guide you step by step. Follow the recommendations and continue the installation. Click on "Next".

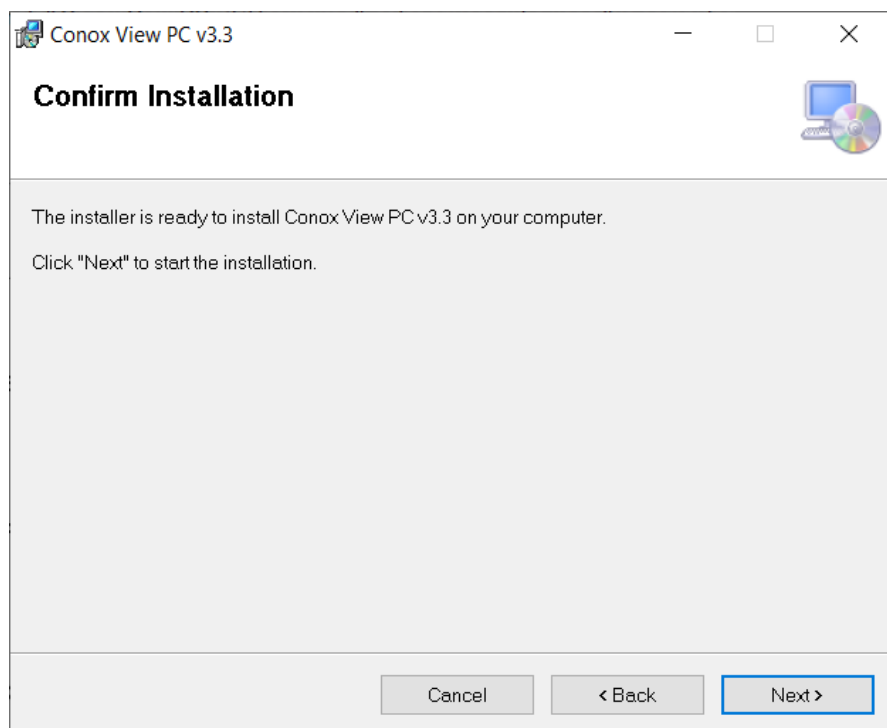


By default, the installer will propose a folder on the user's PC to save the program files.

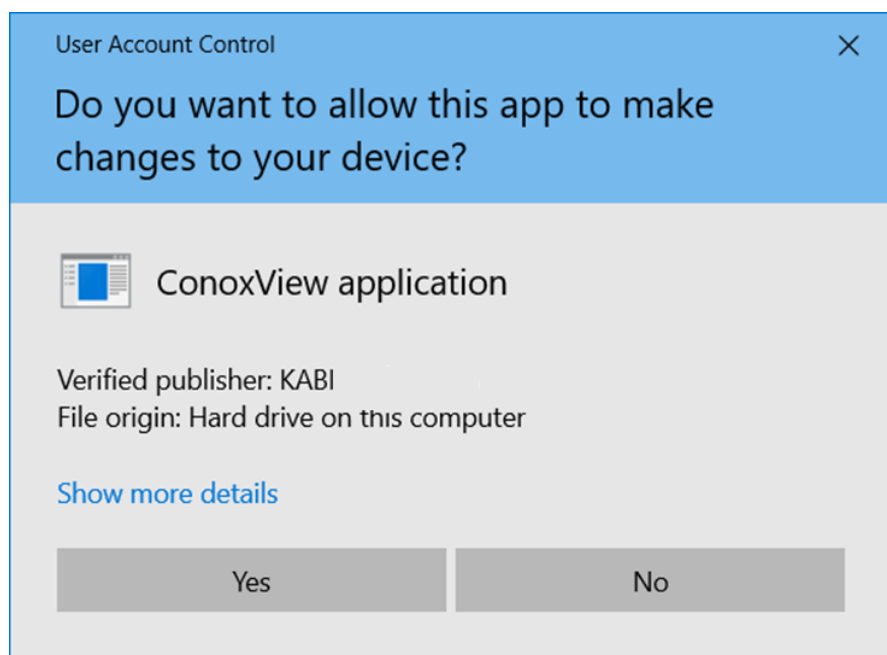
The user can change this by clicking on the "Browse..." button. Once the folder is selected, click on "Next".



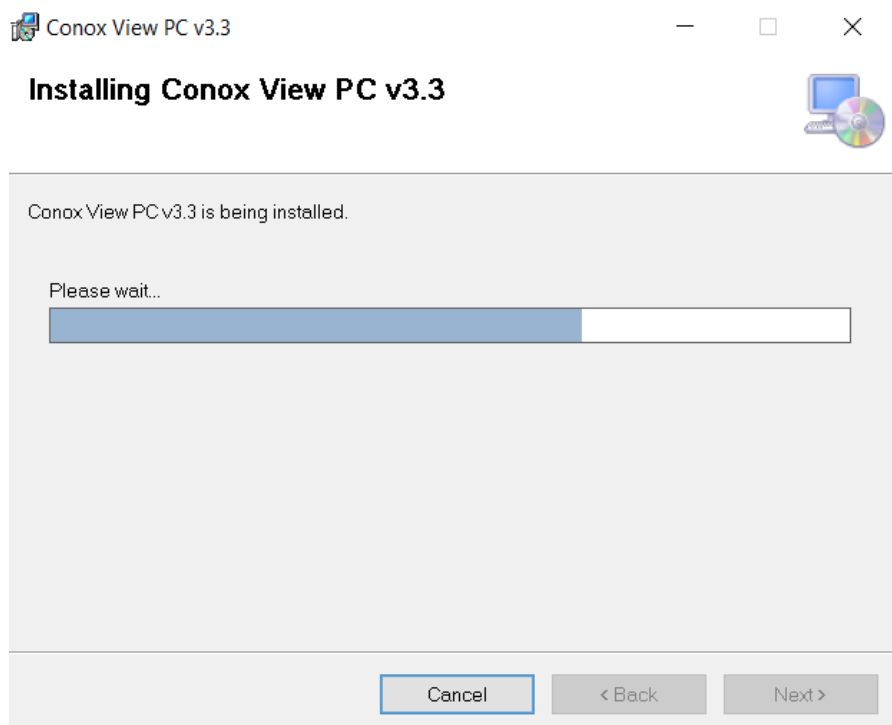
Confirm the installation.



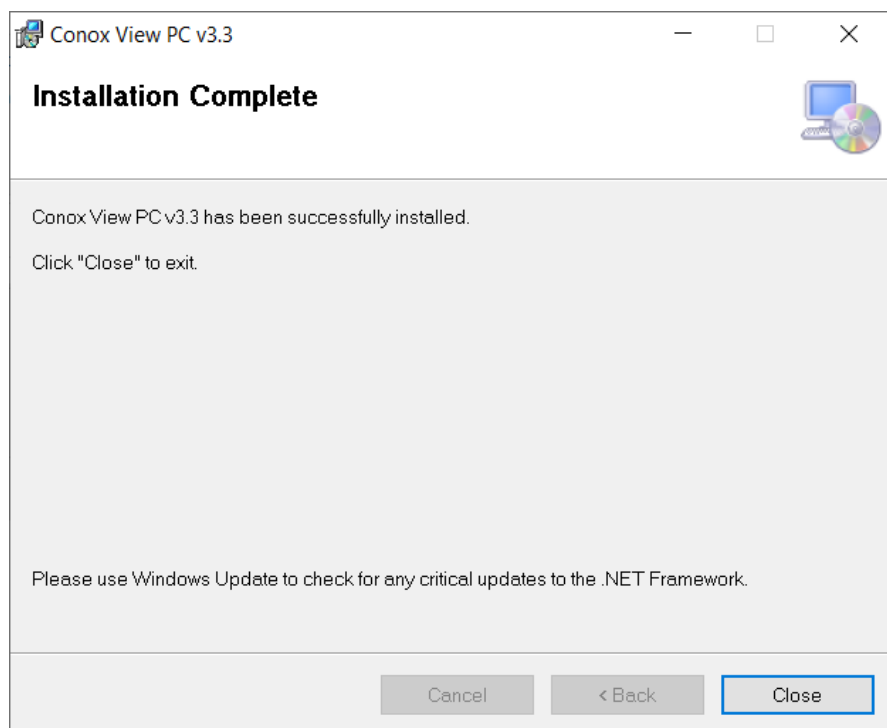
Click on the "Yes" button:



Wait until the installation is completed.




Once the installation is completed, the following notification will appear and a shortcut on the desktop will be created. Click on "Close". ConoxView software is now installed on your PC.



3.2. Pairing the Conox

1. Enable the Conox Bluetooth®.
2. Enable your device's Bluetooth® and find the Conox.
3. Select the Conox through the serial number.
4. Confirm the pairing key if required.

Note: If PC displays two devices with the same serial number, the PC shall be paired with the device that shows the  icon.

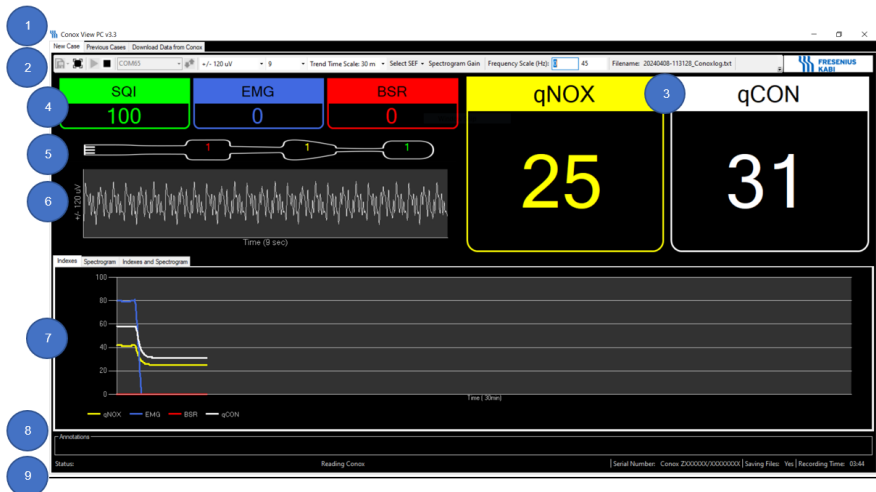
In Windows 11 if the device is not found in the pairing menu, the bluetooth devices discovery 'Advanced' shall be enabled.

4. Software characteristics

4.1.System description

The ConoxView reads data received from the Conox via Bluetooth and extracts information about the indices, impedances, Conox status and EEG signal. The Software allows the user to save annotations and notes while the Conox is recording patient data.

4.2.Controls and indicators



Description





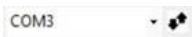

- | | |
|------------------------|---------------------------------------|
| 1. Tabs | 7. Trends graph and spectrogram image |
| 2. Toolbar | 8. Annotations |
| 3. Main indexes | 9. Status bar |
| 4. Secondary indexes | |
| 5. Electrode impedance | |
| 6. EEG graph | |

4.3.Tabs

Tab	Description
New case	Record and visualize a case in real time
Previous cases	Visualize the cases saved on the PC
Download data from Conox	Send recorded cases stored on the Conox to the PC

4.4.Toolbar

The toolbar contains buttons that allow the user to save and adjust the visualization of the case:

Tab	Icon	Description
Save		Allow recording while the case is being displayed. Options: Save file ON / OFF
Full screen		Display the case in full screen mode
Play		Start visualizing the case
Stop		Finish recording/visualizing the case
COM Port		Select serial port communication for Bluetooth® connection
EEG graph amplitude		Select EEG graph amplitude (µV). Options: +/- 25uV, +/- 50uV, +/- 120uV, +/- 250uV and +/- 475uV.

EEG graph time scale		Select EEG graph timescale. Options: 3, 6 and 9 seconds.
Select Index Trend		Select graphs to trend. Options: qCON, qNOX, EMG, BSR
Trend Time Scale		Select trends graph and spectrogram timescale. Options: 30 min, 2h, 6h.
Select SEF		Select Spectral Edge Frequency (SEF). Options: SEF50 (50%), SEF90 (90%), SEF95 (95%).
Spectrogram Gain		Select the color gain of the spectrogram. Options: Selectable Continuous (allows user to choose a custom Max dB and Min dB) or Default (allows user to choose a combination of Max dB and Min dB out of a list).
Frequency Scale (Hz)		Introduce the range of frequencies that the user desires in the Y-axis of the spectrogram in the Spectrogram tab.
Select Index Trend		Select which indexes the user wants to see displayed in the graph obtained in the Indexes tab. The unselected indexes will not be displayed in both the graph and the legend of it.
FFT win		Select Fast Fourier Transform (FFT) window. Options: FFT win 1s, FFT win 4s.
Filename		Name of file currently being recorded.
Information		Information window of the software.

4.5.Main Indexes

Index	Color	Range
qCON	White	0-99
qNOX	Yellow	0-99

4.6.Secondary Indexes

Index	Name	Color	Range
BSR	Burst Suppression Rate	Red	0-100
EMG	Electro- myogram	Blue	0-100
SQI	Signal Quality Index	Green	0-100

4.7.Electrode Impedance

Name	Electrode color	Range
Neg Imp	Red	0-10, Too High (TH)
Ref Imp	Yellow	0-10, Too High (TH)
Pos Imp	Green	0-10, Too High (TH)

4.8.EEG waveform

Graphical representation (downsampled) of the EEG waveform.

4.9.Trends graph

Graphical representation of the qCON, qNOX, BSR and/or EMG.

4.10. Spectrogram

Graphical representation of the EEG signal frequency content. The spectrogram is represented in a two-dimensional way as a function of time and frequency (1 – 45 Hz) and the power of the signal is color coded. Being the blue the lowest proportion of encephalographic waves and the red the highest.

The spectrogram is available in the 3-time scales: 30 min, 2 hours, and 6 hours, depending on the trend time scale user selection.

The spectrogram is a colored image which represents in the y axis the frequency f in the range $0 < f < 45$ Hz and in the x axis the last 30 minutes, 2 hours, or 6 hours of recording.

The user can select the view of index trend and spectrogram by three tabs (figure c) that show:

- only the index trend graph,
- only the spectrogram,
- both the index trend graph and spectrogram.

The “Indexes” tab contains only the index trend graph, the spectrogram tab contains a spectrogram box that shows only the FFT image, the index and spectrogram tab contain two boxes: one shows the index trend graph and the other shows the FFT image.

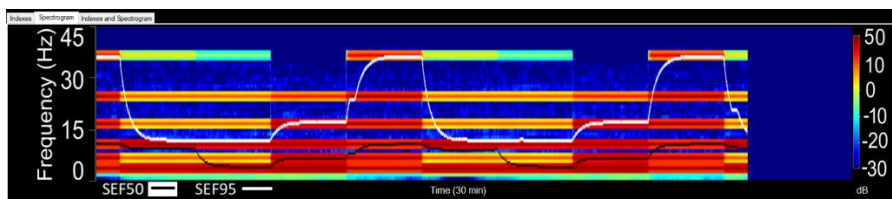


Figure a

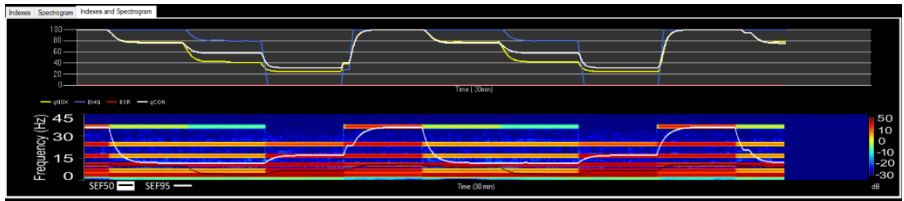


Figure b

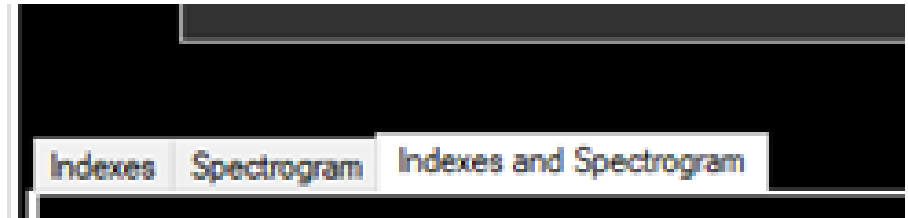


Figure c

The spectrogram image colors are proportional to EEG FFT Power. Color map unit is in dB (μV): 0 dB means a FFT power of 1 μV^2 which is equivalent to a sinusoid with amplitude $\sqrt{2} \mu V$

Association between the sinusoid amplitude in μV , the respective FFT power in μV^2 and dB and the color shown by the ConoxView in the default color gain scale (-30 to 50 dB):

Sine Amplitude (μV) peak to 0	FFT Power (μV^2)	FFT Power (dB)	Color
$320 \cdot \sqrt{2}$	102400	50	
$324 \cdot \sqrt{2}$	10.49	10	
$1 \cdot \sqrt{2}$	1	0	
$0.32 \cdot \sqrt{2}$	0.1024	-10	
$0.10 \cdot \sqrt{2}$	0.01	-20	
$0.031 \cdot \sqrt{2}$	0.00096	-30	

Spectrogram settings

The user can customize the spectrogram view in the "Spectrogram" with the following settings located in the menu bar:

- Trend Time Scale: allows the user to select the trends graph and spectrogram timescale. Options: 30 mins, 2h, 6h.
- SEF (Spectral Edge Frequency): allows the user to choose in between a 50% (SEF50), 90% (SEF90) and 95% (SEF95) of spectral edge frequencies, frequencies below which the 50%, 90% and 95% of the spectral energy is contained, respectively.
- Spectrogram Gain: allows the user to select the color scale of the spectrogram by changing the power range in dB:

- a) Selectable Continuous: allows the user to introduce a custom range of dB between a Min dB and a Max dB value.
- b) Default: allows the user to select from a variety of possibilities a range of dB between a Min dB and a Max dB value.

- Frequency Scale (Hz): allows the user to introduce the range of frequencies show in the Y-axis of the spectrogram. Frequency value digitated shall be integer.
- FFT window: allows the user to select the window of the Fast Fourier Transform (FFT). Options: FFT win 1s, FFT win 4s. When the user changes the Y-axis frequency scale, the FFT win is automatically set to 4s.

4.11. Recording Time

Indicates the time the ConoxView has been recording the case. It does not have to match with the elapsed time that it is shown on the Conox device.

4.12. Annotations

Text box to make notes and write any event occurrences during recording.



Annotations are stored in the txt file with the respective timestamps without processing.

WARNING

The data entered in annotation are stored in Conox log files, which are not encrypted in current design. In case the end-users enter personal or individual information (PII) or health information (PHI) data in the annotations, then the end-users shall ensure ConoxView data (i.e. log files) are protected in confidentiality to prevent leakage or exposure of those data.



4.13. Status bar

The status bar contains the following information:

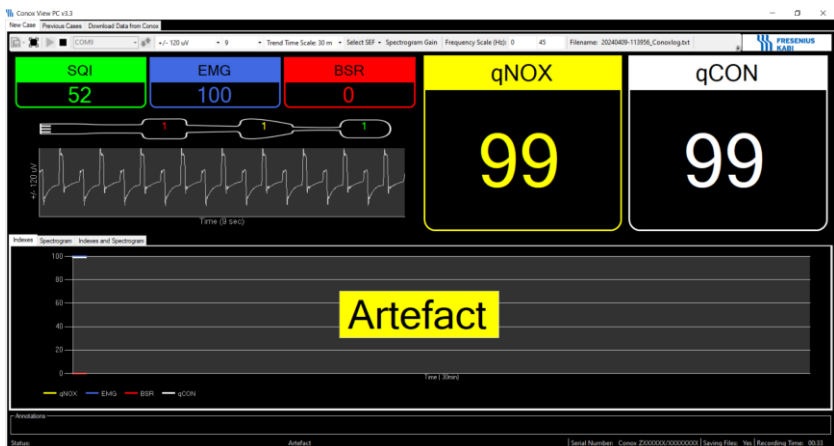
Name	Description
Status	Software operational status: Reading Conox, Artefact, Impedance Check, Lead Off, No Data Received from Conox.
Serial number	Serial number of Conox transmitting data
Saving files	Indicates whether the file displayed on the screen is being saved
Recording time	Time ConoxView has been recording the case displayed on the PC

4.14. Notifications and warning messages

The ConoxView PC displays the following notices and warning messages during data acquisition:

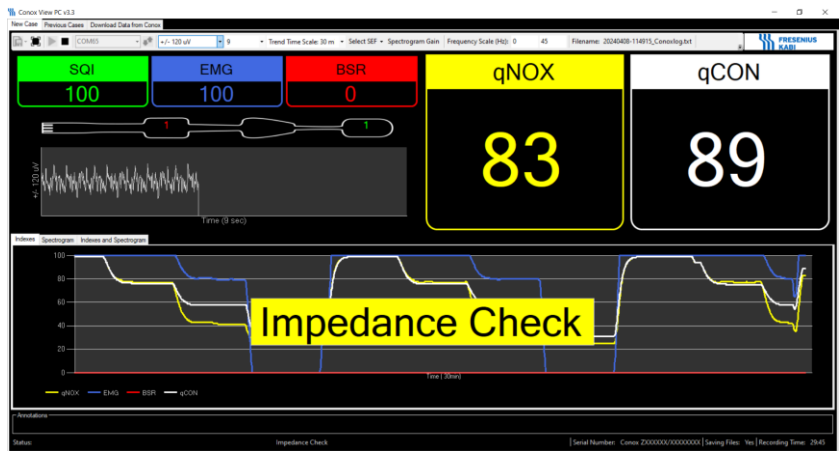
Artefact

Conox has detected an artefact.



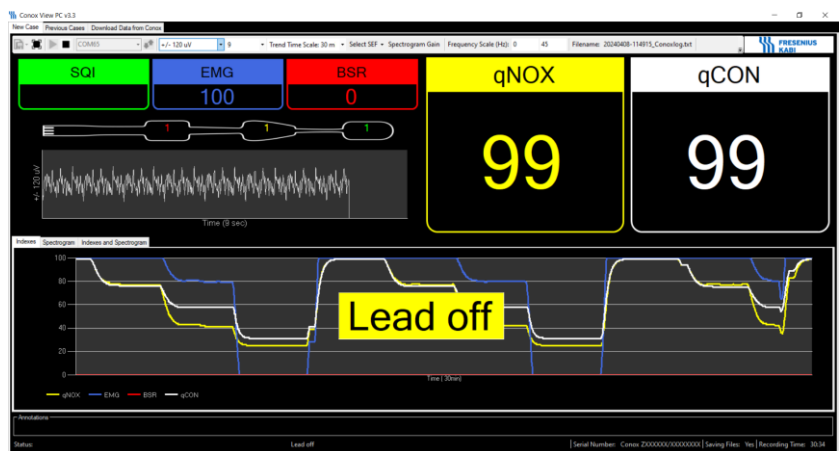
Impedance check

Conox performing an impedance check. During check the impedance readings for each electrode are not displayed.



Lead off

Conox has detected a lead off condition.



No data received from Conox

Conox is disconnected from the PC. Ensure the Bluetooth is enabled and PC and Conox are paired.

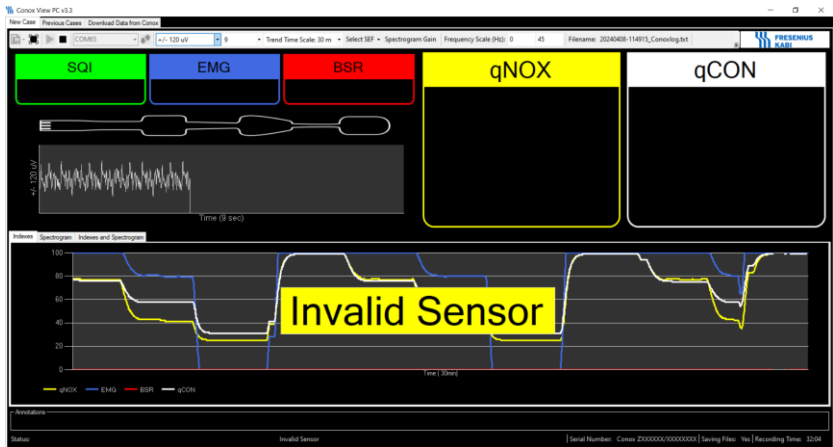


If ConoxView displays this message, use only Conox for patient monitoring.

If the communication is interrupted, ConoxView will automatically try to reconnect.

Sensor Invalid

The sensor connected to Conox is not valid (Sensor contains electronic identifier). Replace the actual sensor for a valid one.



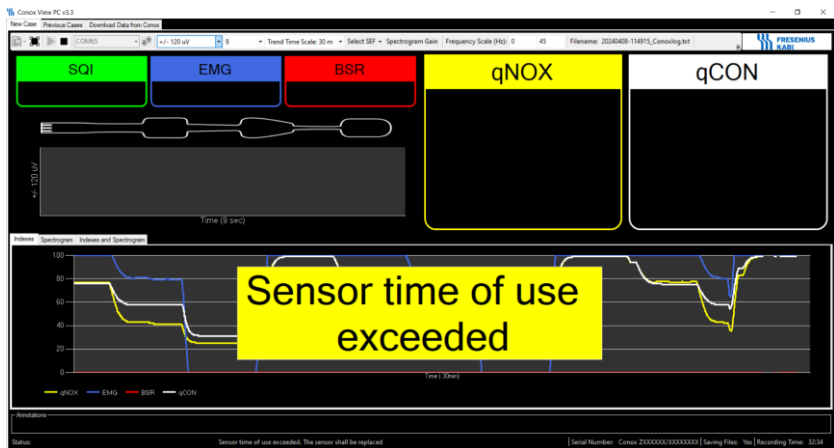
Sensor Expired

The sensor connected to Conox is valid, but it is expired.



Sensor Time of Use Exceeded

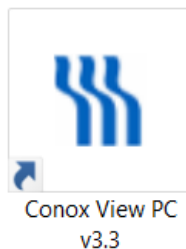
The connected sensor has been used for much longer than 24 hours.



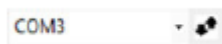
5. Using ConoxView

5.1. View and record current Conox case

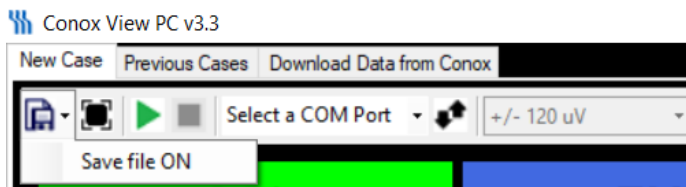
Click on the ConoxView PC icon in the Desktop.



Select a COM Port in the toolbar of the main screen:



Set "Save file ON" or "Save file OFF" on the toolbar and press "Play".



Press “Stop” to end the view/recording.

When recording, the user can add annotations. Annotation time will be saved automatically with the text.

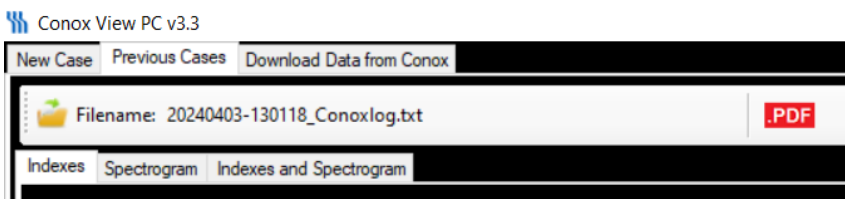
5.2.Replay saved case

Recorded session are stored as a .BIN file in the CONOX_Files folder. These files contain all the data uploaded by the Conox: raw EEG, qCON, qNOX, EMG, BSR and SQI indexes, serial number, firmware version, impedances values, date time, and device status. The Software also saves the indices, impedance values, device status and annotations introduced by the user in a .txt file.

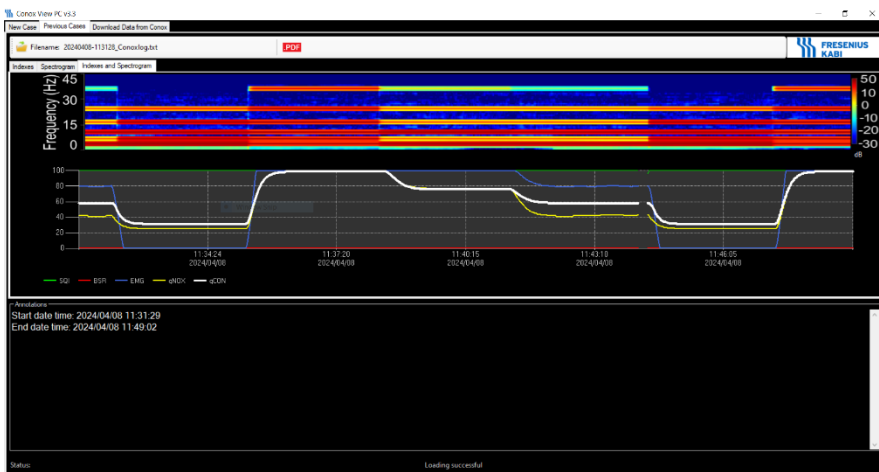
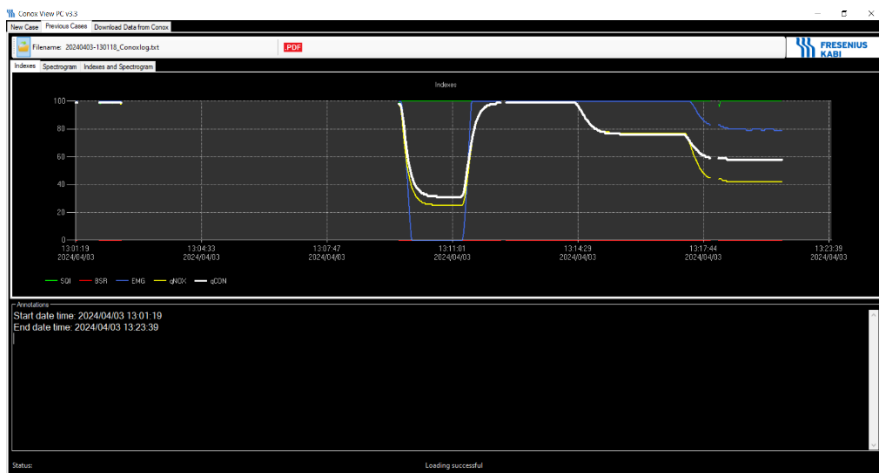
The name of both files is composed of: date (YYYYMMDD), hyphen, and recording start time. The .BIN file ends with “_Conox_stream” and the .txt file with “_Conoxlog”:

 20180926-161135_Conox_stream	9/26/2018 4:21 PM	BIN File
 20180926-161135_Conoxlog	9/26/2018 4:21 PM	Text Document

To visualize a previous case, press the “Previous cases” tab in the main screen and open the .txt file of the case you wish to display.



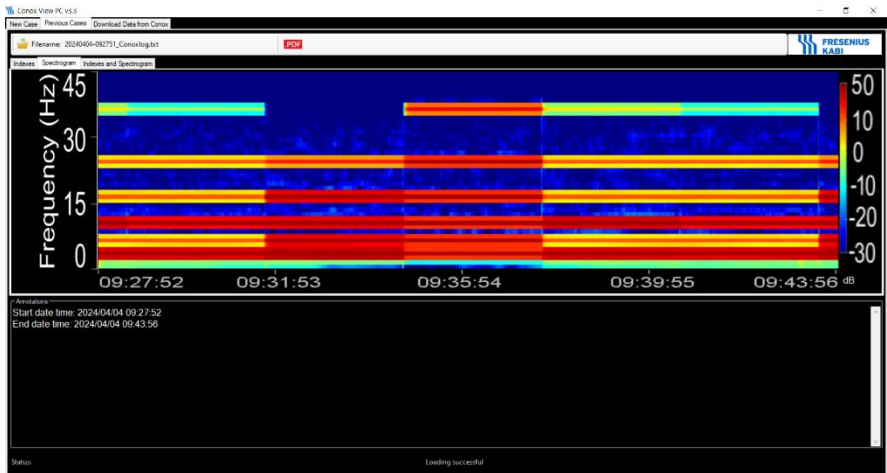
The entire case will be displayed, showing the trends of the four possible parameters and the start/end times.



A PDF file may be created by clicking on the PDF button:



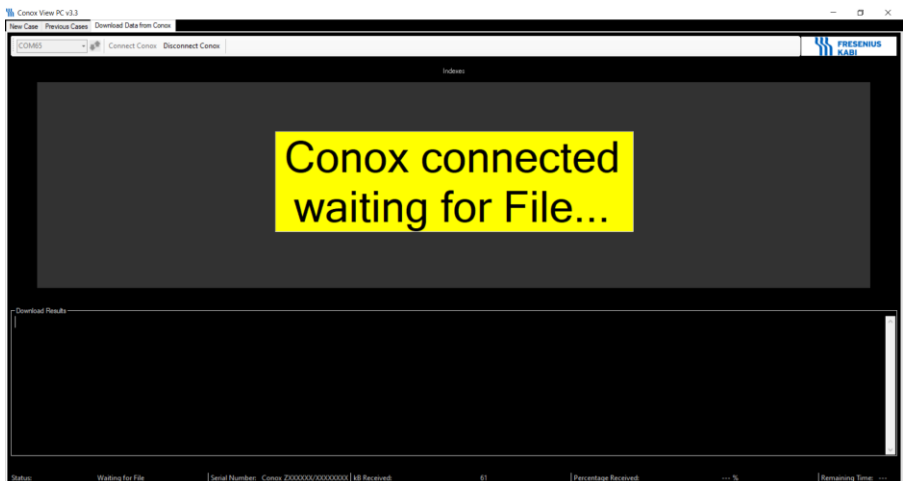
Spectrogram image is also stored on the user PC in the same folder as the ".txt" and ".bin" files. When the ".txt" of a previous case recorded with ConoxView 3.3 is loaded in the "Previous Case" tab, the spectrogram is also shown.



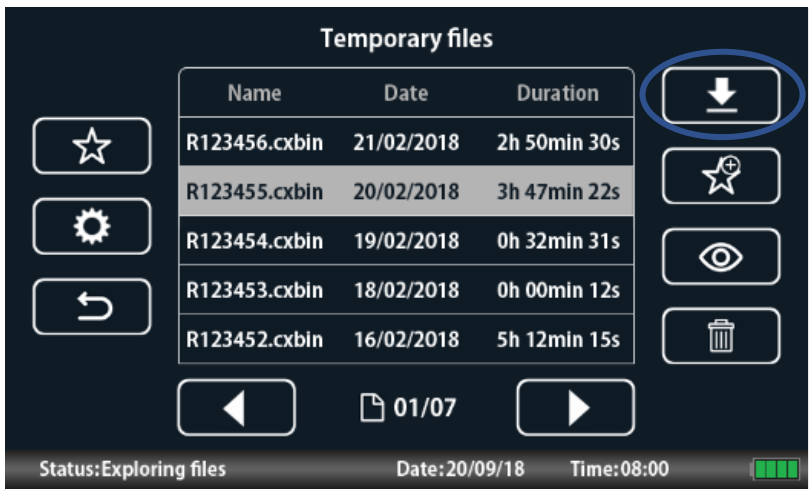
5.3.Download a case

To download a case, the user needs to access the “Download Data from Conox” tab. As when a case is being registered, the user is required to select the relevant COM port.

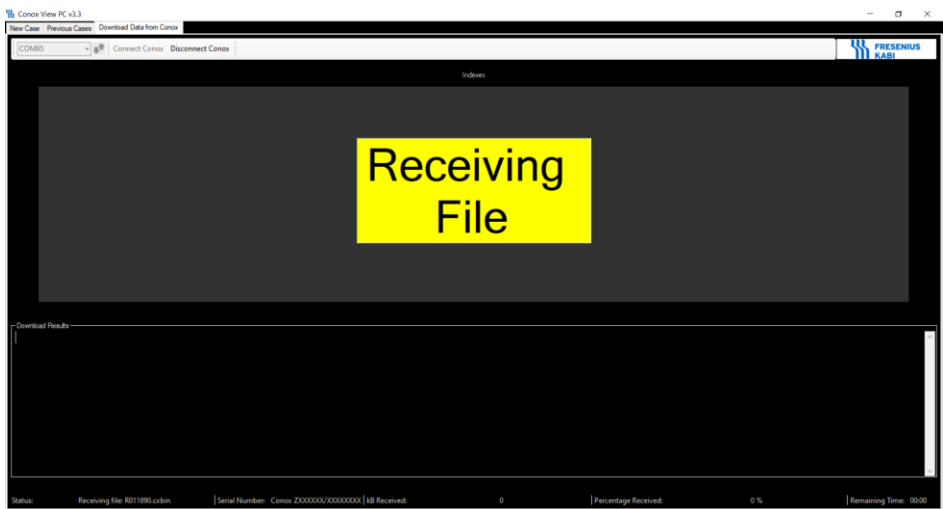
Before connecting, the user needs to access the data repository in the Conox and then, proceed to the connection of the Conox device with the “Connect Conox” button. If the process has been successful, a “Conox connected waiting for File...” message should be shown on ConoxView.



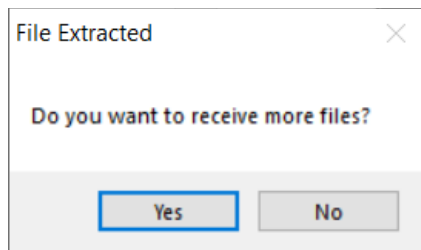
Once connected, the user is required to select the file to download and press the download button:



Once the file starts to download, a “Receiving file” message should be readable in ConoxView, as well as the file name, the kB received, the percentage received and the remaining time in the Status section of Conoxview:



Once file is downloaded, ConoxView will ask the user whether more downloads want to be made or not:



In case the user chooses "Yes" as an option, the "Conox connected waiting for File" message will be shown again.

In case the user chooses "No" as an option, ConoxView will show the download results, specifying the file name, the size of the downloaded file and the data loss percentage:

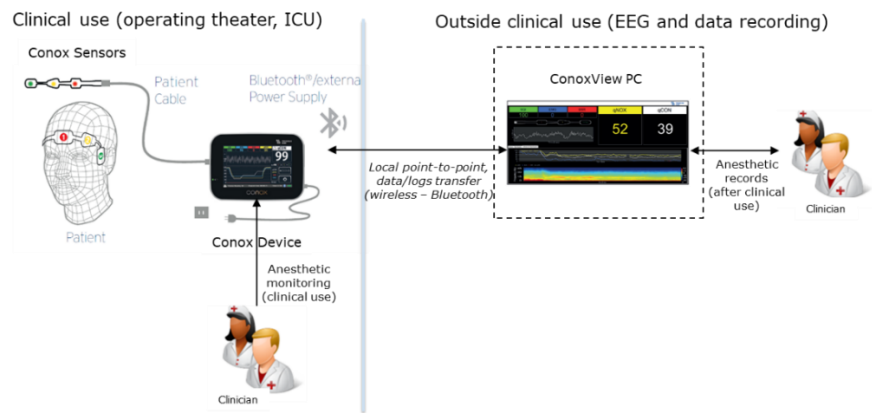


Download case is only available for Conox with Serial Number of 16 digits (ZXXXXXXX/XXXXXXX).

6. Cybersecurity Considerations

6.1.Data flows and user interactions diagram

Below diagram illustrates the ConoxView PC application, including assets inventory, data flows, communication protocols, and intended user’s interactions.



ConoxView PC data flow and user interactions diagram

6.2.Potential risks & vulnerabilities

The purpose of the subsequent cybersecurity recommendations is to allow proper mitigation of the commonly known threats and vulnerabilities. The following table includes description of commonly known vulnerabilities that could be found in typical IT network.

Vulnerability	Typical Threat Events
Communication and network configuration vulnerabilities	
Improperly configured or non-existent firewall or logical protective barrier	A lack of properly configured firewall could permit unnecessary data to pass between networks, such as device and facility networks, allowing adversary or malware to spread between networks, making critical or sensitive data susceptible to monitoring, eavesdropping and to be subjected to Man-in-the-Middle attack.

Standard, well-documented plain text communication protocol	Adversaries can use a protocol analyzer (commercially available) or other utilities to decode the data transferred by protocols, such as telnet, FTP, HTTP and NFS. It is relatively easier for adversaries to perform attacks on these communications.
Lack of integrity checking	Adversaries could manipulate communications undetected.
Inadequate authentication between wireless clients and access points	Strong mutual authentication between wireless clients and access points is needed to ensure that clients do not connect to a rogue access point deployed by an adversary.
Inadequate data protection between wireless clients and access points	Sensitive data between wireless clients and access point should be protected using strong encryption to ensure that adversaries cannot gain unauthorized access to the unencrypted data. Ensure protection from fraudulent Wi-Fi access points (Evil Twin) that appear to be legitimate but are set up to eavesdrop on wireless communications.
Poor remote access controls	Remote access capabilities must be adequately controlled to prevent unauthorized individuals from gaining access to the system.
Inadequate firewall and router logs	Without proper and accurate logs, it might be impossible to determine what cause a security incident to occur.
Unprotected ports or services	Unused ports (such as ForgedDoor) and services must be closed or turned off.
Physical Access	
Unauthorized personnel have physical access to devices	<ul style="list-style-type: none"> ■ Physical theft or damage of data ■ Unauthorized personnel add, remove or change resources of devices. Install unauthorized utilities (undetectable interception of data)
Unsecured physical ports	<ul style="list-style-type: none"> ■ Flash/thumb drives ■ Keystroke logger Other unauthorized utilities to exploit unsecure physical ports
Network Configuration and Communication	

A flat network with no zones (no segregation between corporate and device networks)	<ul style="list-style-type: none"> ■ Unauthorized access to Partner through facility's IT-network ■ Distribute malware across facility's IT-networks ■ Intercept or manipulate unencrypted messages (plain text)
Inadequate authentication between wireless clients and access points	<ul style="list-style-type: none"> ■ Phishing attack ■ Traffic injection (potentially modify content or affect communication)
Improperly selected and configured firewall (weak firewall rules)	<ul style="list-style-type: none"> ■ Phishing attack (spear phishing, mobile phishing) ■ Identity spoofing ■ Firewall bypassed ■ Man-in-the-middle attacks
Malware protection not installed or not up-to-date	<ul style="list-style-type: none"> ■ Disseminate virus, ransomware among networks ■ Plant spyware (for monitoring and eavesdropping) ■ Audit log manipulation or destruction
Software vulnerabilities	
Inadequately assess security of OTS	<ul style="list-style-type: none"> ■ A wide variety of security implications and vulnerabilities have been identified with various OTS operating systems or control protocols such as OLE, DCOM, RPC, OPC, etc.
Database vulnerabilities	<ul style="list-style-type: none"> ■ Databases with web interfaces may be vulnerable to typical web attacks like XSS, SQL injection. The information contained in database makes them high-value targets for any attacker.
Security Policies and Procedures	
Lack of or inadequate authentication, authorization, access control policies and incident detection and response plan or procedure	<ul style="list-style-type: none"> ■ Vulnerabilities regarding authentication, authorization, access control policies, incident detection and response plan or procedure could lead to multiple threat events (attacks) or more likely. ■ For example, incident detection (such as unusual CPU usage due to Cryptojacking) and response plans, procedures and methods are necessary for rapidly

	<p>detecting incident, minimizing loss and destruction, preserving evidence for later forensic examination, mitigating the weakness that were exploited, and restoring system services.</p> <ul style="list-style-type: none"> ■ Having an inadequately shared network between Medical Device Network and Corporate Network (for example, it does not have dedicated VLAN for medical devices) could make it possible for virus and worm to spread to Partner.
--	---

6.3.Cybersecurity Requirements

In order to protect the ConoxView PC installation from commonly known IT/Information Security cyber threats, please consider the below recommended cybersecurity requirements.

As a general requirement, for the download of Conox data from Conox Device using the ConoxView PC application, consider using a host machine dedicated to healthcare operations. This machine shall not be used to connect on the Internet, receive email, use person-to-person communications solutions.

Physical access to the ConoxView PC host machine shall be carefully managed and controlled, so to ensure only authorized user can interact with the ConoxView PC application hosting machine.

Table below provides a summary of recommended cybersecurity requirements for ConoxView PC host machine.

	Requirements
Network Security	<ul style="list-style-type: none"> ■ Consider Network Access Control mechanisms to enforce strong authentication of the ConoxView PC host machine allowed to connect on the Hospital IT network. ■ Ensure host firewall is enabled and configured so to only allow network accesses and traffic flows required. The ConoxView PC application is local desktop application only, no network communications required with external systems.
User Access Control	<ul style="list-style-type: none"> ■ Ensure only authorized user can physically interact with host machine. ■ Ensure separation of duties principle is applied (separation between Admin/Privileged user accounts and Standard user accounts).

User Rights	<ul style="list-style-type: none"> ■ Change default passwords when new software is installed and regularly after that. Define a strong password policy: <ul style="list-style-type: none"> – Encourage users to never reveal their passwords to others and use a password manager. – Use different passwords for different accounts. ■ Make passwords that are hard to guess but easy to remember. The longer a password is, the better. Use at least 8 characters for standard accounts, 12 or 16 characters whenever possible for privileged account. <ul style="list-style-type: none"> – To increase complexity, include upper- and lower-case letters, numbers, and special characters. A password should use at least 3 of these choices.
Secure Communications (Data in transit protection)	When supported, ensure secure communications are used and default certificates replaced by Hospital IT owned certificates.
Data (at rest) protection	<ul style="list-style-type: none"> ■ Avoid multiboot or boot only on hard drive. ■ Use hard disks encryption (i.e.: Bitlocker). ■ Use an up-to-date antivirus. ■ Use an up-to-date host firewall.
Host Hardening	<ul style="list-style-type: none"> ■ Prevent unauthorized use of removable media (e.g.: USB). ■ Ensure OS and application is up to date of the security patches.
Malware Protection	<ul style="list-style-type: none"> ■ Ensure that an up-to-date antivirus/antimalware protection solution is installed on the Partner host computer and configured to protect hard disk drives, removable media, memory for fileless malware.
Backup & Restore	<ul style="list-style-type: none"> ■ Perform regular backup of ConoxView PC host machine, including ConoxView PC installation and data files.

Ensure the application is installed on a trusted device (managed by organization IT department and conform to the IT / Information Security policies applicable within the end-user's organization).

Ensure the application is used by authenticated local users, logged in the hosting operating system.

Ensure the hosting operating system environment provides up-to-date malware protection (anti-virus) solution.

Ensure application is installed only from Fresenius Kabi provided installers executables. Check regularly for latest updates of the application from local Fresenius Kabi representative or Key2* platform.

6.4.Cybersecurity and IT-Network environment

Fresenius Kabi infusion systems including its software components are intended to be deployed primarily on a healthcare facility network with the following characteristics:

- Monitoring and control of access from outside of the network perimeter.
- Appropriate authentication and authorization of users on the network.
- Monitoring, prevention and containment of malware and computer viruses.
- Systematic data backup procedures.
- Periodically conducting audit trail.
- Well-defined IT segmentation and security perimeters.

In addition to these IT-Network characteristics, it is also recommended but not required that the IT-Network environment includes provision of dedicated medical device network (such as VLAN) for deployment of Conox device along with dedicated medical device applications only.

WARNING



Institutionalizing strong cybersecurity policies and following the industry best practices relative to IT security could minimize exposure to threats. These threats may include but are not limited to data leak, data corruption, data loss, network or service outage, network communications interception and manipulation, malware contamination, data tampering, network, or host machine compromise by an external adversary.

Fresenius Kabi strongly advises to follow IEC/ISO 80001 to manage risks regarding IT-Network and Cybersecurity as outlined below.

* <https://key2.fresenius-kabi.com>

6.4.1. Policy recommendations:

- Have top management strongly involved in the risk and the cybersecurity policies and role definition.
- Have a chain of responsibility for cybersecurity practices within the Hospital IT organizations; define who is capable to act for identification / protection / detection / response to cybersecurity vulnerabilities and potential incident.
- Have a risk management process led by a medical IT-Network risk manager.
- Use a medical IT-Network risk management file to provide traceability for hazards.
- Define who is in charge of gathering information around assets inventory and risks management; analyzing, assessing and storing them.
- Check for the correct functioning of Conox Device and ConoxView PC application at a regular interval.

6.4.2. IT-Network recommendations:

Even if ConoxView PC application is not connected to any network other than local point-to-point Bluetooth communication with Conox devices, Fresenius Kabi reminds healthcare organizations about recommended IT-Network security practices:

- Perform a full analysis of existing IT-Network, including detailed assets inventory and using different views (either relative to physical, data or process parts).
- Define the scope of each separated network and its needs to be isolated or not.
- Perimeter Network protection: define proper IT-Network security controls with goal to mitigate identified threats and risks (e.g.: segmentation and network traffic filtering strategy, enforcement of secure communications protocol where communications transit over network domain considered as "unmanaged" or "not properly controlled")
 - Use secure remote access methods: Implement secure methods for remote users to access your network. Require all remote users to connect and authenticate through a single, managed interface before conducting software upgrades, maintenance, and other maintenance or support activities.

- Set up measures for detecting compromises: Minimize the chances of compromise by monitoring and auditing system events 24/7. Use intrusion detection systems (IDSs), intrusion prevention systems (IPSs), antivirus software, and usage logs to help you detect compromises in their earliest stages. Have a plan in place to quickly detect the issue and respond. Refer to section 6.10 for further recommendations regarding incident detection & response.

INFORMATION



Fresenius Kabi strongly advises the use of host machine dedicated to healthcare purposes; those machines shall not be used for Internet browsing, person-to-person communications, email, or personal use.

6.5. Cybersecurity Features

The ConoxView PC application is designed to be a local, standalone, desktop application limited to the download of logs, history records, and anesthetic monitoring data from Conox Devices.

The application can not perform any configuration or calibration change of Conox devices.

The application does not process or transmit any sensitive data other than technical and physiological data related to Conox device and anesthetic monitoring.

No personal or patient data are present in the ConoxView PC data.

The application does not currently enforce user authentication and role-base access control.

The application is developed according to Secure Development Lifecycle (SDL) practices, including secure coding considerations, and regularly assessed during penetration testing campaigns of Conox system.

Also, the potential vulnerabilities related to third party software components are monitored. The Software Bill-of-Material (SBOM) can be obtained on-demand from Fresenius Kabi representative.

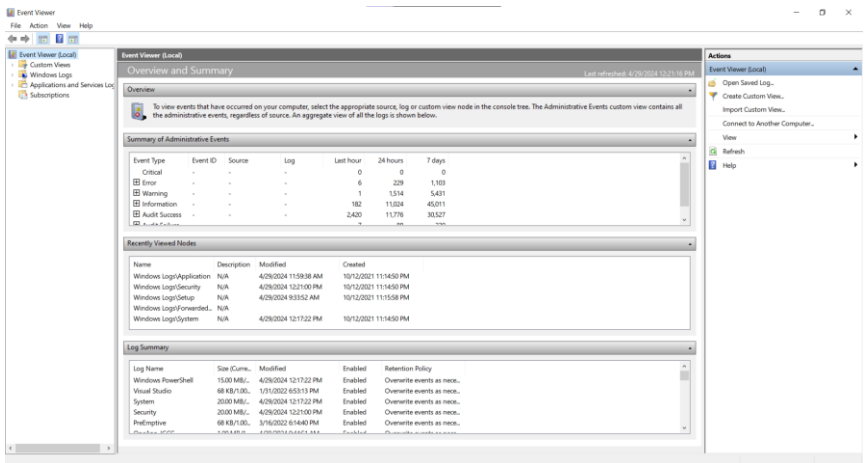
6.5.1. Log visualization

When using ConoxView v3.3, several events are logged and visualizable in the Windows Event Viewer. The events logged are the following:

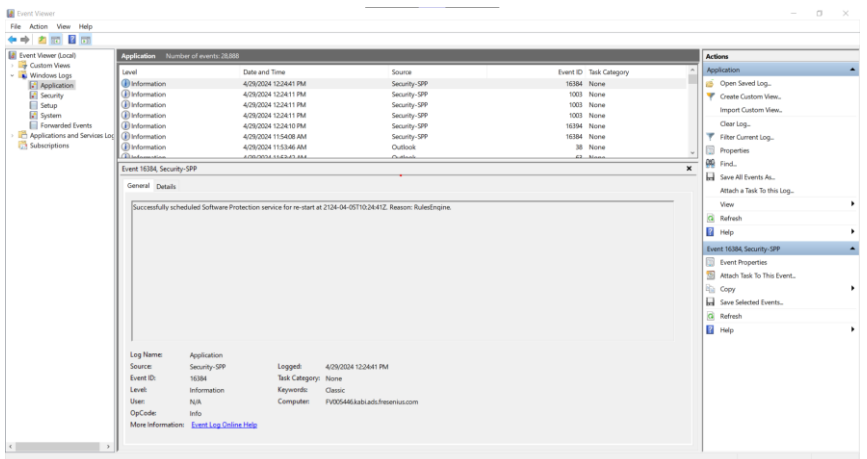
- "ConoxView loaded" when the application is opened.
- "ConoxView closed" when the user closes the application.
- "ConoxView recording started" when a recording is started by the user.
- "Conox connected" when data are received from Conox.
- "Conox Recording Stop" when a recording is stopped by the user.
- "Conox Annotation Entry" when the user enters a text into the Annotation box.
- "Conox CRC error" if CRC check of data received by the Conox fails.
- "Conox Offline Data Received and extracted" when the data are downloaded from the Conox in data repository mode.
- "Conox Packet lost: x" when x data packet is not received from the Conox, where x is the total number of packets lost.
- "Conox File Previous Case Open" when a .txt file of a previous case is loaded.
- "Conox File error loading: format error" when an error occurred during loading of previous .txt file: the format of the file is not corrected.
- "Conox File error loading: size too big" when an error occurred during loading of previous .txt file: the size of the file is above 1 Gb.

For the visualization of the events logged, the following steps need to be followed:

- 1) Open Event Viewer.



2) Navigate to the "Application" tab inside the "Window Logs" tab.



- 3) All the events of Conox View v3.3 (i.e. opening/closing the .exe) are listed in this view.
- 4) Taking as a reference the "Date and Time" and the "Source" variables, find the logged event.
- 5) Navigate to the "Details" tab inside the event description tab to visualize the information.

Application Number of events: 28,890 (1 New events available)				
Level	Date and Time	Source	Event ID	Task Category
Information	4/29/2024 12:29:39 PM	Application	0	None
Information	4/29/2024 12:29:18 PM	Application	0	None
Information	4/29/2024 12:24:41 PM	Security-SPP	16384	None
Information	4/29/2024 12:24:11 PM	Security-SPP	1003	None
Information	4/29/2024 12:24:11 PM	Security-SPP	1003	None
Information	4/29/2024 12:24:10 PM	Security-SPP	16394	None
Information	4/29/2024 11:54:08 AM	Security-SPP	16384	None
Information	4/29/2024 11:53:46 AM	Outlook	38	None
Information	4/29/2024 11:53:42 AM	Outlook	63	None
Information	4/29/2024 11:53:41 AM	Outlook	63	None
Information	4/29/2024 11:53:41 AM	Outlook	63	None
Information	4/29/2024 11:53:39 AM	Outlook	45	None
Information	4/29/2024 11:53:38 AM	Security-SPP	1003	None
Information	4/29/2024 11:53:38 AM	Security-SPP	1003	None
Information	4/29/2024 11:53:38 AM	Security-SPP	1003	None
Information	4/29/2024 11:53:38 AM	Security-SPP	1003	None

6.6. Cybersecurity safety considerations

Information for safety will recommend compliance with industry-wide IT policies, such as password complexity and mandatory periodic updates.



WARNING

Organization IT policy should be compliant with IEC 80001, Application of risk management for IT networks incorporating medical devices.

- Establish usage policies to help to proactively reduce the risk of security breaches as a result of employee negligence.
- Secure Internal Network.



WARNING

Conox devices and ConoxView PC application must be deployed within a secure IT-Network environment to prevent unauthorized accesses from external system(s) or adverse entities.

- Develop and maintain a Security Patch Management process to minimize system vulnerabilities.

**WARNING**

Ensure physical security of the premise and the connection to ConoxView PC application host computer.

Ensure that appropriate up-to-date virus/worm/malware protection mechanisms are in place to protect the system.

6.6.1. Network configuration

It is recommended that network installation and use be consistent with commonly accepted industry best practices related to cyber and information security.

**WARNING**

In order to avoid any loss of data, periodic backups of the ConoxView PC data are recommended. When installing or reinstalling ConoxView PC application, the data will be emptied of any previous content. Follow institutional SOPs for the appropriate backup intervals.



WARNING

- Ensure boundary protection devices (for example, VPN, firewall, VLAN, separated or out-of-band networks, etc.) are used appropriately.
- Perform and qualify the hospital network where ConoxView PC application is to be deployed.
- Design IT network to enable separation of medical devices from business applications.
- Ensure appropriate authentication (for example, password policy) and authorisation (for example, principle of least privilege) policy are in place to ensure only intended users have access to use the device.
- Have a policy in place to manage application of security updates to off-the-shelf components.
- Verify that the appropriate training requirements are met for a potential user before creating a user account.
- Monitor network traffic to identify and isolate devices suspected of generating malicious, excessive or unusual network traffic.
- Use strong authentication and encryption.

6.6.2. User Access Control (permissions management)

ConoxView PC application does not include user authentication authorization mechanism. In current design, it is assumed the application is used by authenticated local users, logged in the hosting operating system. Refer to next section for additional recommendations related to login and password management on the ConoxView PC host machine.

6.6.3. Login and passwords management

Individual institutional Information Technology (IT) policies should identify security controls that maintain the pairing of a login and password following IEC 80001-2.

- Change default passwords when new software is installed and regularly after that.
- Define a strong password policy.
- Encourage users to never reveal their passwords to others, and use a password manager.
- Use different passwords for different accounts.
- Make passwords that are hard to guess but easy to remember. The

longer a password is, the better.

- Use at least 8 characters for standard accounts, 12 or 16 characters whenever possible for privileged account.
- To increase complexity, include upper and lower case letters, numbers, and special characters. A password should use at least 3 of these choices.

It is also generally recommended to configure proper Microsoft Windows GPO for Password / Account login security.

- Account lockout duration - How long (in minutes) a locked-out account remains locked-out (range is 1 to 99,999 minutes). The MsDS-LockoutDuration value. (e.g.: 15min).
- Account lockout threshold - How many failed logons it will take until the account becomes locked-out (range is 1 to 999 logon attempts). The MsDS-LockoutThreshold (e.g.: 3 logons failure).
- Reset account lockout counter after - How long (in minutes) it takes after a failed logon attempt before the counter tracking failed logons is reset to zero (range is 1 to 99,999 minutes). The MsDS-LockoutObservationWindow value. (e.g.: 15min).

Microsoft Windows session automatic logoff can be configured with GPO[†]. The setting shall be applied to Interactive logon: 'Machine inactivity limit'

Location in Microsoft Windows 10 or Windows 11:

- *Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options*
- *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options (While creating and linking group policy on server)*

Possible values:

- *The automatic lock of the device is set in elapsed seconds of inactivity, which can range from zero (0) to 599,940 seconds (166.65 hours).*
- *If **Machine will be locked after** is set to zero (0) or has no value (blank), the policy setting is disabled and*

[†] <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-machine-inactivity-limit>

a user sign-in session is never locked after any inactivity.

Recommended value shall be set to 10minutes (600 seconds).


6.6.4. Hardening

Individual institutional Information Technology (IT) policies should identify security controls that maintain the pairing of a login and password.

Host PC hardening expectations:

- Encrypt the hard drive. Use Windows BitLocker or equivalent.
- Disable booting from removable media option in system BIOS.
- Disable all unused services.
- Close all unused inbound or output ports.
- Ensure removable media interface (e.g. USB Port) are disabled or blocked to prevent connection of unauthorized mobile devices.
- Commonly accepted Microsoft Windows hardening benchmarks shall be applied (e.g.: CIS-CAT benchmarks, Center for Internet Security Benchmarks - Microsoft Compliance <https://docs.microsoft.com/en-us/compliance/regulatory/offering-cis-benchmark>).

WARNING

- 
- Perform OS/Server hardening to the computer before ConoxView PC deploying.
 - Disable booting from removable media option for ConoxView PC host computer.
 - Disable all unused services.
 - Close all unused inbound or outbound ports.

6.7. Firewall configuration

Ensure that the ports specified during installation are allowed through the Windows firewall or your facility firewall. Also, ensure all unnecessary inbound or outbound traffic is blocked.

The ConoxView PC desktop application does not require any communications with any external IT systems.

6.8. Security Updates (Vulnerability management)

ConoxView PC software updates, including security updates, are delivered by Fresenius Kabi, and published on Key2[‡] platform. This platform is available and accessible for Fresenius Kabi customers only (restricted access, not public). It allows to release and distribute Fresenius Kabi approved software updates, with appropriate documentation and guidelines.

Users shall manually check the integrity of the downloaded files using the SHA-256 fingerprint published for the corresponding software package on the Key2 web page.

Ensure application is installed only from Fresenius Kabi provided installers executables. Check regularly for latest updates of the application from local Fresenius Kabi representative or Key2[§] platform.

Software updates are to be managed according to instructions provided in chapter 3 "Installation" of the present document.

6.9. Data protection

The ConoxView PC desktop application does not store, process, transmit neither personal or individual information (PII) nor health information (PHI).

Only technical data and physiological data (not linked to individual) related to anaesthetic monitoring operations are stored and processed by the application.

Once Conox data are transferred on the host operating system, end-users are responsible to ensure Conox data are protected from unauthorized access and tampering attempts which could lead to confidentiality or integrity compromise of those data.

Ensure Conox data are properly archived (backup) if required, depending on the use related to those data within end-users organization.

[‡] <https://key2.fresenius-kabi.com>

[§] <https://key2.fresenius-kabi.com>

6.10. Incident detection & response

If you suspect a cybersecurity attack occurred or a vulnerability related to the ConoxView PC application, please report this to your local Fresenius Kabi representative or submit a request to the Fresenius Computer Emergency Response Team (CERT, cert@fresenius.com).

For vulnerability reporting, please refer to Fresenius CVD portal: <https://www.fresenius.com/vulnerability-statement>.

For events logging, the application allows to retrieve history records from Conox devices. In case of suspicious behaviour observed on ConoxView PC application, it is recommended to check local Microsoft Windows Events logs.

INFORMATION



Fresenius Kabi strongly advice to report any suspected cybersecurity event or vulnerabilities related to Conox devices and ConoxView PC desktop application.

Please contact your local Fresenius Kabi representative or submit a request to the Fresenius CERT (cert@fresenius.com).

6.11. Awareness and training

Encourage secure workstation habits - everyone in your organization can contribute to cybersecurity efforts by keeping their workstations as safe as possible.

Provide cybersecurity training to your employees to help keep your organization secure. Explain phishing emails, infected attachments, malicious websites, and other methods that attack them directly.

General example: Be sure everyone gets into the habit of locking their screen when they aren't in use.

Require any contractors or managed services vendors to complete the equivalent cybersecurity training and ensure they are informed about information security policies applicable within your organization.

The Conox system (devices and ConoxView PC application) have to be used by trained healthcare professionals.

7. Release notes

Date	Software Version	IFU version	Modification
December 2022	ConoxView PC v3.2	0.0	First Release
May 2024	ConoxView PC v3.3	1.0	SW update
February 2025	ConoxView PC v3.3	2.0	Windows 11 compatibility

This document may not be reproduced in whole or in part without the written consent of Fresenius Kabi. Conox® is a registered trademark in the name of Fresenius Kabi in selected countries.

Made in France

Revision date: FEB 2025

<http://www.fresenius-kabi.com>



**FRESENIUS
KABI**

caring for life



Fresenius Kabi AG
Else-Kröner-Str. 1
6352 Bad Homburg, GERMANY
Tel.: +49 (0) 6172 / 686-0
www.fresenius-kabi.com



Fresenius Vial S.A.S.
Le Grand Chemin
38590 Brézins - FRANCE