SIbEL

ANNE View ADMIN IFU

Installation, Configuration, Service & Maintenance

support.sibelhealth.com

IFU P/N 443-00005-J

Table of Contents

Section 1. Important Safety Information

1.1 Device Description

The ANNE View Tablet is a bedside patient monitoring device that receives vital signs and physiological data from compatible devices for display and transmission to central monitoring platforms. The ANNE View application operates on the ANNE View Tablet. When connected to the ANNE Chest Sensor, the ANNE View application displays electrocardiography (ECG), skin temperature, heart rate, respiratory rate, fall detection, and body position data. When connected to the ANNE Limb Sensor, the ANNE View application displays photoplethysmography (PPG), SpO2, pulse rate, and perfusion index data. The ANNE View application is also compatible with optional third-party devices for SpO2, non-invasive blood pressure, and body temperature measurements. The ANNE View application alarms when physiological data are outside of the configured thresholds.

1.2 Indications for Use

The ANNE View application is intended for the display of physiological data from the ANNE Chest and ANNE Limb devices. The application is also compatible with third-party, FDA-cleared devices for the display of noninvasive blood pressure, SpO2, pulse rate, and body temperature measurements. The ANNE View application notifies healthcare professionals when physiological data fall outside selected parameters. The ANNE View application displays the orientation of patients to aid in the prevention of pressure ulcers for at-risk patients. The system notifies the user when the patient's position has not changed for a preset threshold of time. The ANNE View application communicates to compatible central monitoring platforms, including the Central Hub, for the display and storage of multiple patients' physiological data. The Central Hub has the ability to notify healthcare professionals when physiological data fall outside selected parameters.

The ANNE View and Central Hub are intended for use by trained, qualified healthcare professionals in the clinical or home healthcare environment. The device is not intended for use on critical care patients.

1.3 Contraindications

- ANNE View is not intended for use on critical care patients and is not a remote diagnostic device.
- While the data displayed by ANNE View may be applicable for use as an aid to diagnosis and treatment, ANNE View does not provide diagnostic or interpretive statements to either the patient or the clinician.
- The electrocardiogram is not for diagnostic or interpretative purposes. It should not be relied on for assessing QRS morphology.

1.4 Warnings

- For US Customers: Federal law restricts this device to sale by or on the order of a licensed healthcare practitioner.
- ANNE View should not be used in the presence of strong electromagnetic fields such as high frequency surgical equipment.

- ANNE View is not intended to be used as an apnea monitor. Do not rely on the respiration monitoring to detect cessation of breathing.
- Setting alarm limits to extreme values may prevent certain alarm conditions from being detected and from being enunciated with audible and visual alarm signals.
- Do not attempt to disassemble, repair, or modify the device.
- Do not plug in any unauthorized cables to the hardware ports located on the tablet device.
- Turning all audio alarms off may result in clinically actionable physiological conditions to be missed. Ensure that audio alarms are re-enabled upon leaving the bedside if there is no connected central monitoring system.
- Use proper clinical judgement when determining the prioritization of concurrent physiological and technical alarm conditions.
- Ensure that a new monitoring session is started for each patient. Continuing the previous monitoring session with a new patient will result in physiological information to be associated with the previous patient. Continuing the previous monitoring session with a new patient may result in inappropriate alarm setting for the new patient, resulting in false positive or false negative alarm generation.
- The ANNE View Tablet is intended to be located at the patient bedside. Placing the device away from the patient bedside may result in communication drops with wireless sensors. Placing the device away from the patient bedside may decrease the effectiveness of the alarm system.

1.5 Precautions

- Do not use this product if the ANNE View Tablet is damaged.
- Temporary interruption of data streaming is possible. Similar devices may cause signal interference during data transmission. If you experience this effect, avoid operating near interfering devices.
- The battery used in the tablet may present a risk of fire, explosion, or chemical burn if mistreated. Do not expose the sensors or tablet to excessive heat or fire. Do not crush, puncture, or incinerate as doing so can result in fire, explosion, or the release of toxic gasses. Do not use or charge if the sensors appear to be leaking, discolored, deformed, or in any way abnormal.
- For US customers: Return all non-consumable components to Sibel Health for disposal following all state and federal laws governing the disposal of routine, non-hazardous electronic waste.
- For EU customers: Return all non-consumable components to your authorized distributor for disposal. Sibel Health's European distributors have been registered as a B2B (business-to-business) producer of Category 8 (Medical Equipment without implanted or infectious devices).
- ANNE View is intended to be operated by a qualified healthcare professional. The patient is not an intended operator.
- ANNE View has no cardiac arrhythmia detection capabilities.
- In order to maintain monitoring of the patient the ANNE View Tablet should be transported with the patient during transfers.

1.6 Glossary

Table 1: Glossary

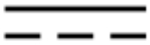
Abbreviation	Definition
ADT	Admission-discharge-transfer
AFE	Analog Front End

AVOP	On Premises Configuration
AVSC	Standalone Configuration
BLE	Bluetooth Low Energy
BPM	Beats Per Minute
BRPM	Breaths Per Minute
DIA	Diastolic
ECG	Electrocardiogram
EMC	Electromagnetic Compatibility
FHIR	Fast Healthcare Interoperability Resources
HR	Heart Rate
ID	Identifier
IP	Ingress Protection
IT	Information Technology
LED	Light-emitting diode
ME	Medical Equipment
MRI	Magnetic Resonance Imaging
NFC	Near Field Communication
NIBP	Non-Invasive Blood Pressure
PI	Perfusion Index
PIN	Personal Identification Number
PLETH, PPG	Photoplethysmogram
PM	Patient Monitor
PR	Pulse Rate
RF	Radio Frequency
RH	Relative Humidity
RR	Respiratory Rate
RSME	Root mean square error
SDC	Service-oriented Device Connectivity
SpO2	Oxygen Saturation
SYS	Systolic

TEMP	Temperature

1.7 Symbols and Markings

Table 2: Symbols and markings

Symbol	Title	Description
	eIFU	Indicates the need for the user to consult the instructions for use or the electronic instructions for use.
	Refer to instruction manual/booklet	To signify that the instruction manual/booklet must be read
	Class II Equipment	Equipment meets the safety requirements specified for Class II equipment according to IEC 61140
	MRI Unsafe	This device is not safe for use with MRI equipment
Rx ONLY	Prescription Use Only	Federal law restricts this device to sale by or on the order of a licensed healthcare practitioner
	Does not contain natural latex rubber	Natural rubber latex was not used as a material in the manufacture of this medical device, its container, and/or packaging
	Manufacturer	Indicates the medical device manufactured, as defined in EU Directives 90/385/EEC, 93/42/EEC and 98/79/EC
	Direct current	Direct current
	Alternating current	Alternating current
	Do not use if package is damaged	Indicates a medical device that should not be used if the package has been damaged or opened
	Federal Communications Commission Mark	FCC marking indicates the electronic device, which sold in the United States, is certified and the electromagnetic interference from the device is under the limits that are approved by the Federal Communications Commission
	Batch code	Indicates the manufacturer's batch code so that the batch or lot in which the device was manufactured can be identified
	Date of Manufacture	Indicates date when medical device was manufactured
	Catalogue number	Indicates the manufacturer's catalogue number so the medical device can be identified
	Serial Number	Device serial number

	WEEE (Waste Electrical and Electronic Equipment)	Electrical and electronic items should not be disposed of in your dustbin or wheelie bin but should be recycled
	TELEC Certification	The classification and technical standards for the specified radio equipment listed in the official online technical regulations compliance certification system
IPN_1N_2	Ingress Protection	N1 0 Non-protected 1 Protected against solid foreign objects of 50 mm diameter and greater 2 Protected against solid foreign objects of 12.5 mm diameter and greater 3 Protected against solid foreign objects of 2.5 mm diameter and greater 4 Protected against solid foreign objects of 1.0 mm diameter and greater 5 Dust-protected 6 Dust-tight N2 0 Non-protected 1 Protection against vertically falling water drops 2 Protection against vertically falling water drops when enclosure tilted up to 15° 3 Protected against spraying water 4 Protected against splashing water 5 Protected against water jets 6 Protected against powerful water jets 7 Protected against the effects of temporary immersion in water 8 Protected against the effects of continuous immersion in water When a characteristic numeral is not required to be specified, it is replaced by the letter "X" ("XX" if both numerals are omitted).
RoHs compliant	RoHs (Restriction of Hazardous Substances)	Regulates the use of toxic materials with the purpose of making electronics manufacturing safer at every stage of its life cycle
	Non-sterile	Indicates a medical device that has not been subjected to a sterilization process
	Bluetooth®	Indicates that the sensors use Bluetooth® as the wireless communication protocol
	Caution	Indicates the need for the user to consult the instructions for use for important cautionary information such as warnings and precautions that cannot, for a variety of reasons, be presented on the medical device itself
	Temperature limits	Operating temperature range
	Atmospheric pressure limitation	Operating pressure range

	Humidity limitation	Operating humidity range
	Non-ionizing electromagnetic radiation	Equipment includes RF transmitters that generate non-ionizing electromagnetic radiation
	Indoor use only	Identifies electrical equipment designed for indoor use
	Audio On	Indicates audible alarm tone is on.
	Audio Pause	Indicates audible alarm tone is paused temporarily.
	Audio Off	Indicates audible alarm tone is turned off permanently.
	Keep Away From Rain / Keep Dry	The transport package shall be kept away from rain and in dry conditions or keep dry when applied to a device.
	Acknowledgement	To identify the control whereby a bell may be acknowledged or to indicate that the bell has been acknowledged. The alarm condition may be indicated below or beside the bell.
	Alarm off	To identify the control for alarm off or to indicate that the alarm system is in the alarm off state.
	Quantity Symbol	Indicates the number of units or pieces in the package.
	Authorized representative in the European Union	Indicates the authorized representative in the European Union.
	CE Mark	Indicates that a product has been assessed by the manufacturer and deemed to meet EU safety, health and environmental protection requirements. It is required for products manufactured anywhere in the world that are then marketed in the EU.
	Importer	Indicates the entity importing the medical device into the locale.
	Medical Device	Indicates the item is a medical device.

1.8 Storage and Handling

- Storage temperature range: -15°C – 45°C (5°F – 113°F)
- Storage relative humidity range: 5 – 95% RH (non-condensing)
- Storage pressure range: 30 kPa to 120 kPa
- Operating temperature range: 10°C – 40°C (50°F – 104°F)
- Operating humidity range: 5 – 95% RH (non-condensing)

- Operating range: 30 kPa to 120 kPa

1.9 Security Recommendations

There are steps you can take to help make the operating environment more secure.

- Do not connect the ANNE View Tablet to sensors outside of the system components.
- Do not connect the ANNE View Tablet to sensors with sensor IDs you do not recognize.
- Do not connect to unknown open wireless networks while operating the system. Avoid public/free Wi-Fi hotspots, and use only secure Wi-Fi networks.
- Always confirm the sensor ID displayed on the tablet with the one displayed on the system before use.
- Limit the information you enter into the ANNE View Tablet to only information required for use of the system.
- Use strong PINs and passwords.

1.10 Manufacturer Information

- If a replacement is needed for any component of ANNE View, contact your customer support representative.
- Contact your customer support representative for any of the following issues:
    - Assistance in setting up, using, or maintaining ANNE View
    - To report unexpected operation or events

Sibel Health Inc.
Address: 2017 N Mendell St. Unit 2SE, Chicago IL 60614, USA
Phone: (224) 251-8859
Website: www.sibelhealth.com

MDSS GmbH
Schiffgraben 41, Hannover 30175
Germany

Section 2. Tablet Setup & Battery Status

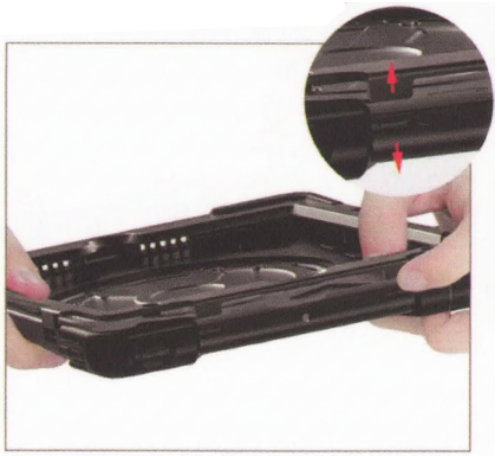
This section primarily covers the ANNE View application configuration of the tablets that have already been enrolled in a customer site.

2.1 Tablet Case Installation

Note: Your product may come with a case pre-installed.

The system includes a heavy duty rugged tablet case for ANNE View Tablet. Users can choose to install it or not depending on the scenario. To install the tablet case:

- Option 1: Refer to the instructions inside the tablet case package.
- Option 2: Contact your care location's IT support on-site.



Step 1
Open the four side clips to remove the front cover.

Step 2
From the top of the case peel the exterior silicone from the hard plastic back plate until the top half of the back plate is exposed.

Step 3

Install the tablet into the hard plastic back plate. Make sure the camera matches up with the corresponding cutout. Then reinstall the silicone cover, adjust the corner and the edge of the case, making sure it fitted correctly around all ports.camera and buttons.

Step 4

Replace the front cover onto the case starting at the sides and working your way around the case until all the clips holding the front cover have been clicked into place.

Step 5

(If using the VESA mounting feature) Use a screwdriver to tighten the screws one by one onto the bracket's back plate.

2.2 Open and Close the Tablet Stand

- **Open**: Open the stand and press it into the slot to secure the stand.

- **Close**: Pull the stand when not in use.

2.3 Turn On & Unlock Tablet

Step 1

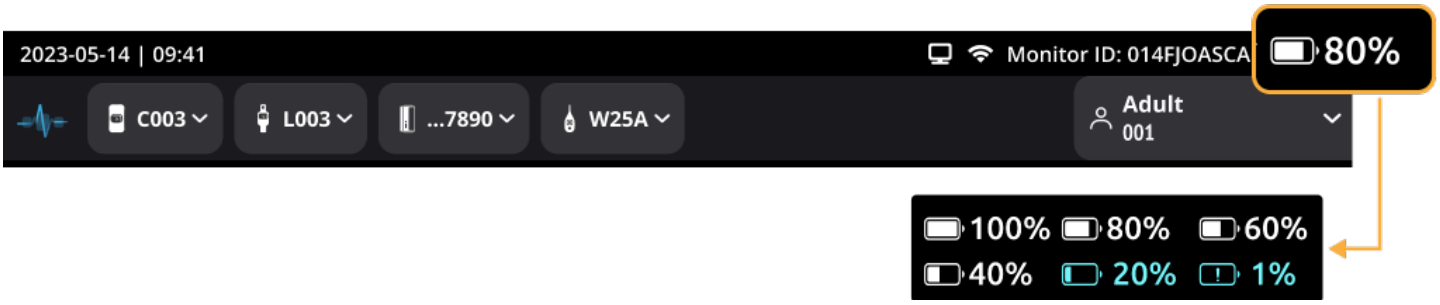
Turn on the tablet by long pressing using the power button.

Step 2

Press the home button and swipe up the screen to unlock.

2.4 Tablet Battery Status

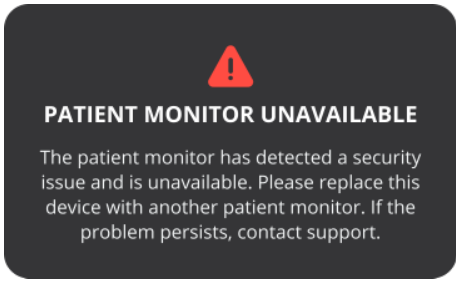
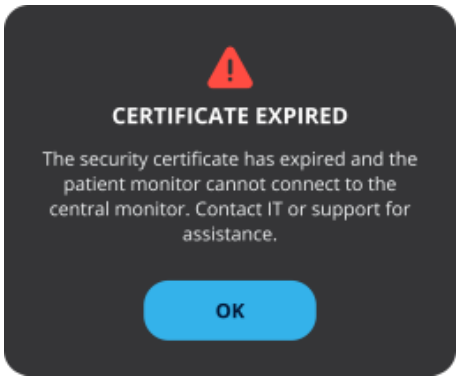
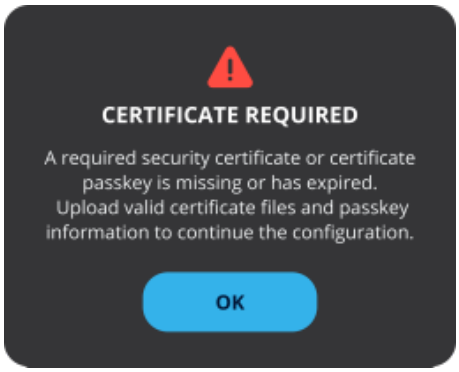
The tablet battery status is represented on the top bar to the left of the patient information. It shows the percentage of battery left for the tablet.



Charge with the tablet charger if needed.

2.5 ANNE View Error Handling

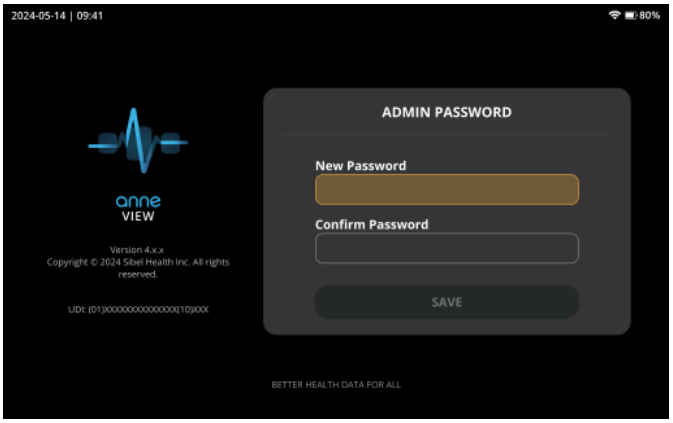
Table 3: ANNE View error handling

UI	Description	Solution
	The patient monitor has detected a security issue and is unavailable.	Please replace this device with another patient monitor. If the problem persists, contact support.
	The security certificate has expired and the patient monitor cannot connect to the central monitoring platform.	Contact IT or support for assistance.
	A required security certificate or certificate passkey is missing or has expired.	Upload valid certificate files and passkey information to continue the configuration.

Section 3. Initial Passwords

3.1 Admin User Password

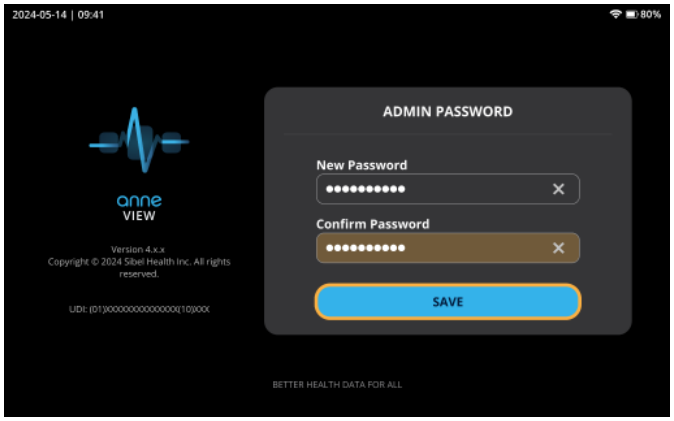
Step 1
Enter a new admin password to the first text field labeled with “New Password”.



Note: Admin password follows the criteria:

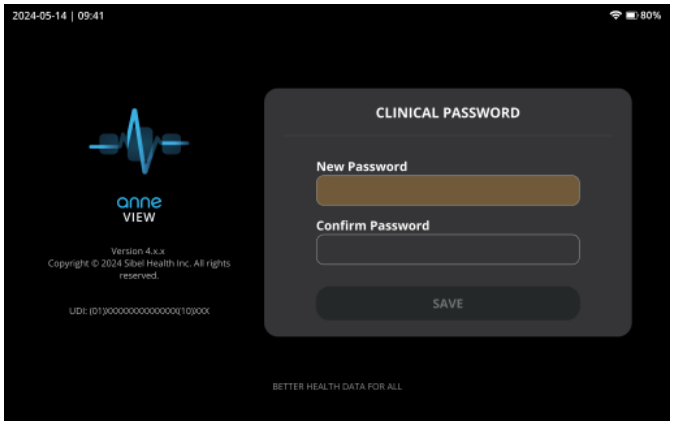
- 8 or more characters
- at least one uppercase letter
- at least one lowercase letter
- at least one number
- at least one special character

Step 2
Re-enter the admin password entered in Step 1 into the second text field labeled with “Confirm Password”.
After completing, select the “SAVE” button to go to the next step to set up the clinical password.



3.2 Clinical User Password

Step 1
Enter a new clinical password to the first text field labeled with “New Password”.

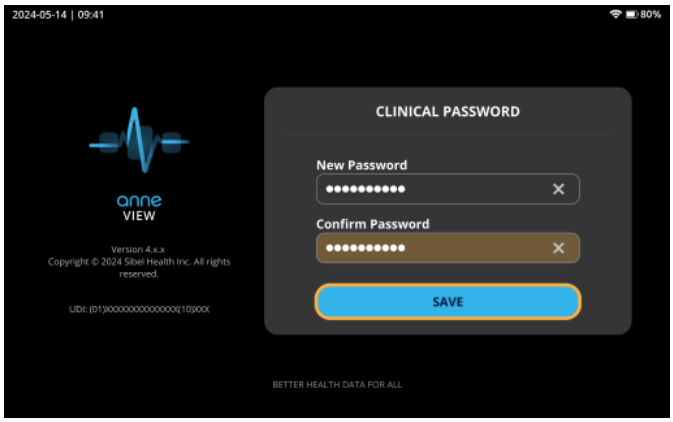


Note: Clinical password follows the criteria:

- 4 or more characters

Step 2

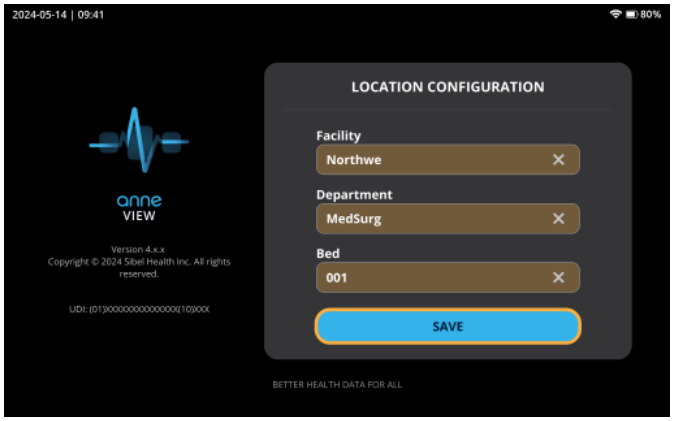
Re-enter the clinical password entered in Step 1 into the second text field labeled with “Confirm Password”. After completing, select the “SAVE” button to go to the next step to set up the clinical password.



3.3 Location Configuration

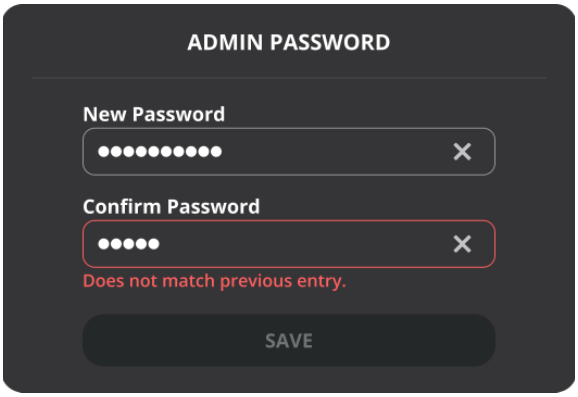
Enter all text fields including “Facility”, “Department”, and “Bed”. After completing, select the “SAVE” button.

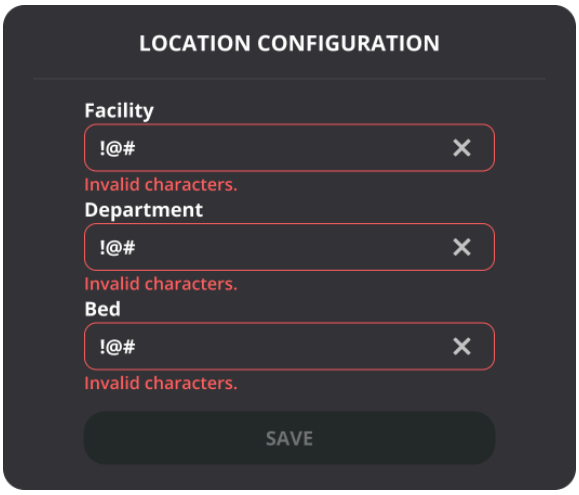
- Facility: Enter the hospital name.
- Department: Enter the care unit.
- Bed: Enter the bed label.



3.4 Error Handling

Table 4: Initial password errors

Setup step	UI	Description	Solution
Admin password, Clinical password		Password does not match the previous entry.	Try again by entering the same password as the previous entry.

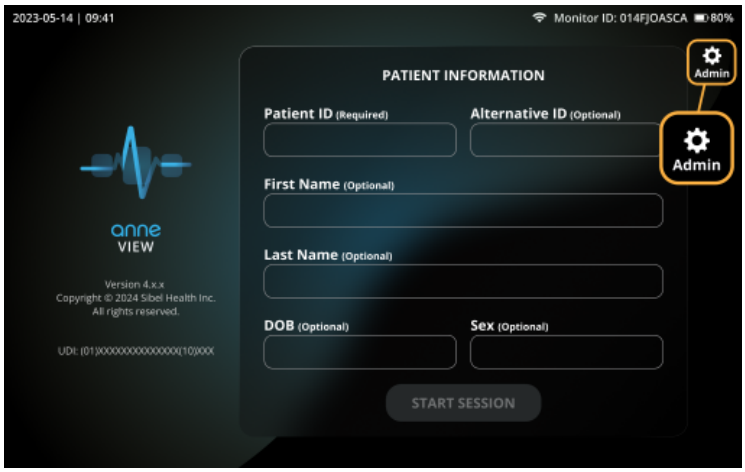
Setup step	UI	Description	Solution
Location Configuration		Invalid characters.	Try again by entering: 1. Maximum Length: Each field can have a maximum of 7 characters. 2. Allowed Characters: Characters permitted under RFC 3986 unreserved characters, except for the period (.), which must not be used.

Section 4. Admin Settings

4.1 Accessing Admin Settings

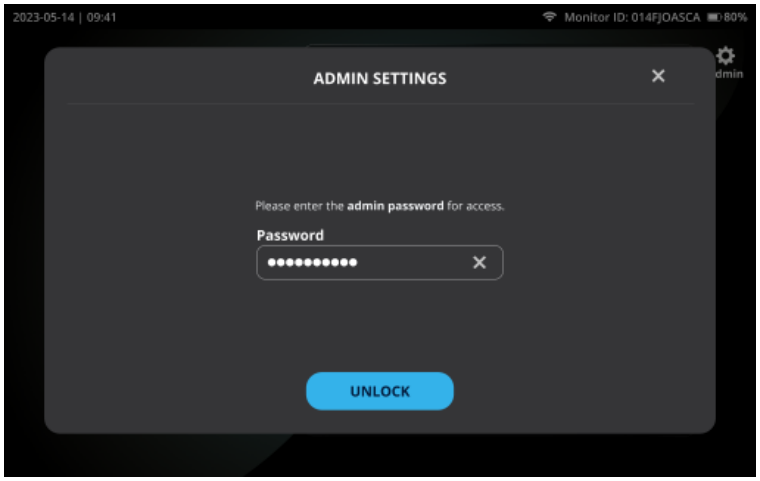
Step 1

Select the “Admin” button to access Admin settings when there is no ongoing monitoring session.



Step 2

Enter the admin password for access and select the “UNLOCK” button. After successful authentication, the Central Monitor Configuration page opens by default.



Note: Navigating away from a tab or exiting the Admin Settings with pending edits will trigger an "Unsaved Changes" popup.

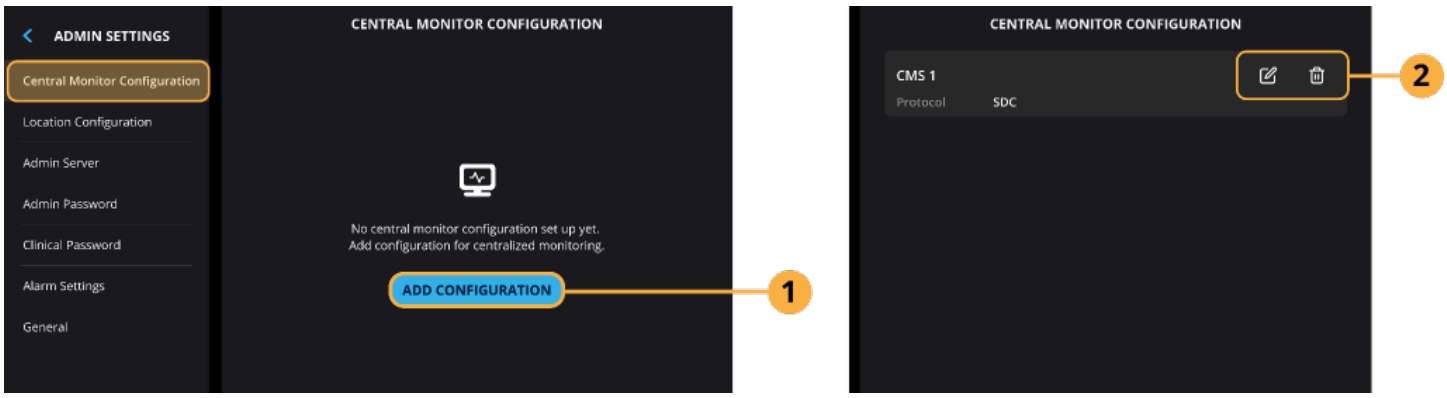
- Select DISCARD to ignore changes and leave the screen.
- Select BACK TO EDIT to remain on the screen.

4.2 Central Monitor Configuration

Note: Central Monitor Configuration applies to AVOP On Premises Configuration deployments where ANNE View communicates with on-site Sibel CMS and/or approved third-party systems using HL7 FHIR or IEEE 11073 SDC, according to the site architecture. AVSC Standalone Configuration does not support connectivity to the central monitor.

Step 1

Select the Central Monitor Configuration tab and select one of the following actions:

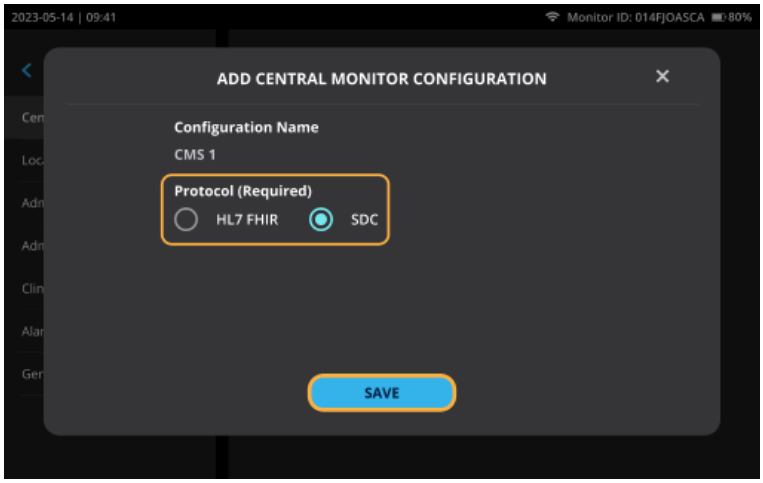


① Add(No central monitor configured): Select the ADD CONFIGURATION button.

② Modify/Delete: Select the / button.

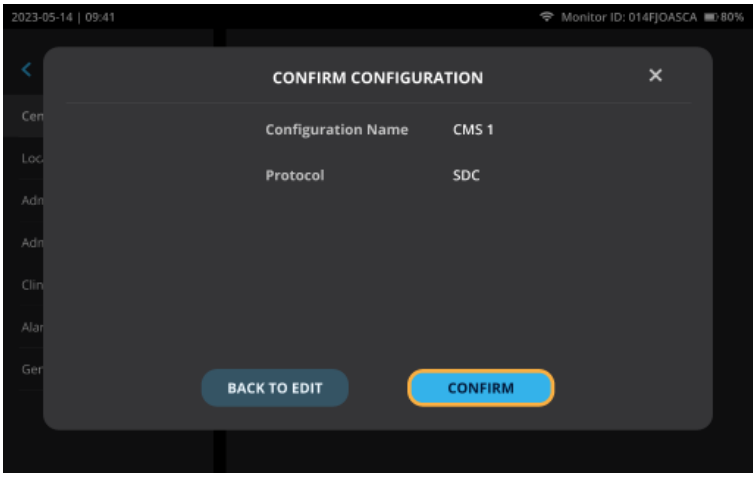
Step 2 (Add/Modify Only)

If you are adding or modifying a configuration, select SDC and tap the SAVE button.



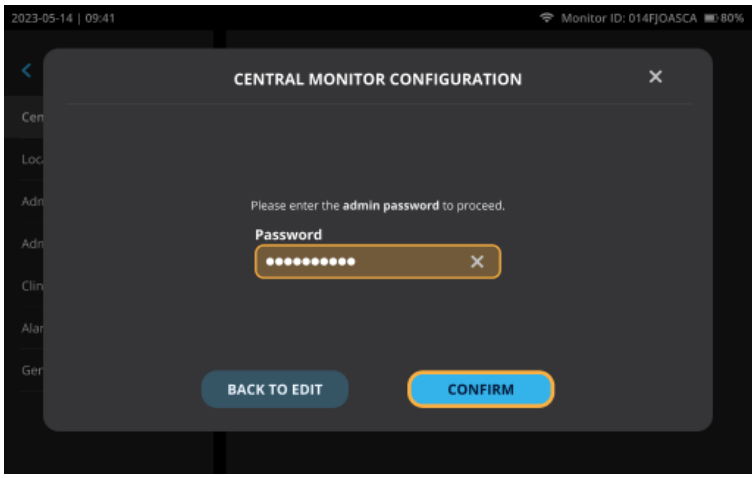
Step 3 (Add/Modify Only)

Confirm all entered details are accurate and select the “CONFIRM” button.



Step 4

Enter the admin password and select the “CONFIRM” button to proceed the action.



Step 5

View the saved configuration on the Central Monitor Configuration page.

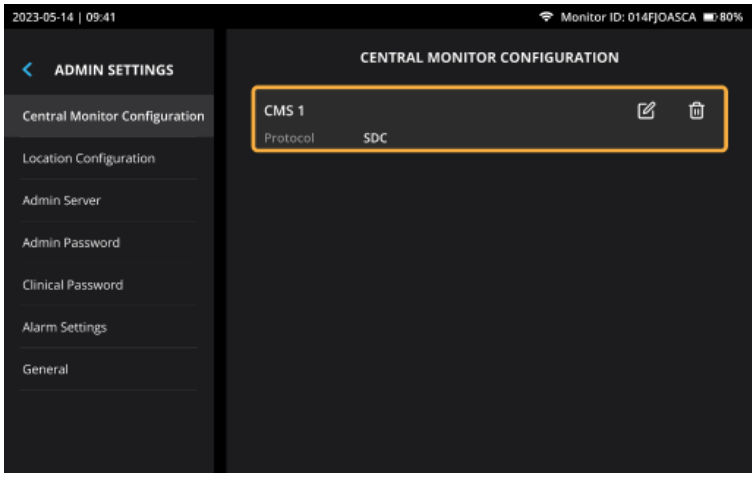


Table 5: Central monitor configuration parameters

Parameters	Description
Configuration Name	The Configuration Name is an auto-generated name for the Central Monitoring System.

Parameters	Description
Protocol	Central Monitoring System's protocol can be selected from these options: • HL7 FHIR • 11073 SDC
Host Address	Host Address is required to be provided for HL7 FHIR protocol only. Host Address is the Central Monitoring System's HTTPS host address to connect to through the application. E.g. https://test.io
Account ID	Account ID is required to be provided for HL7 FHIR protocol only. Account ID is a preassigned account number of the organization.

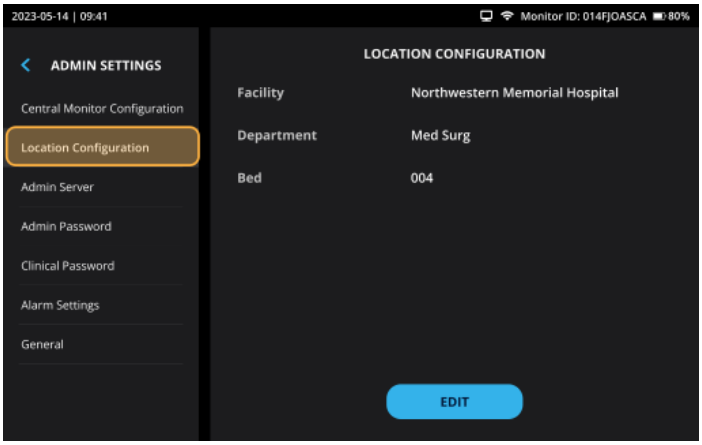
4.3 Location Configuration

Note: Location Configuration is used only for IEEE 11073 SDC communication. The configured Facility, Department, and Bed values are included as location context in IEEE 11073 SDC messages and are not displayed elsewhere in the ANNE View application.

4.3.1 Modify Configuration

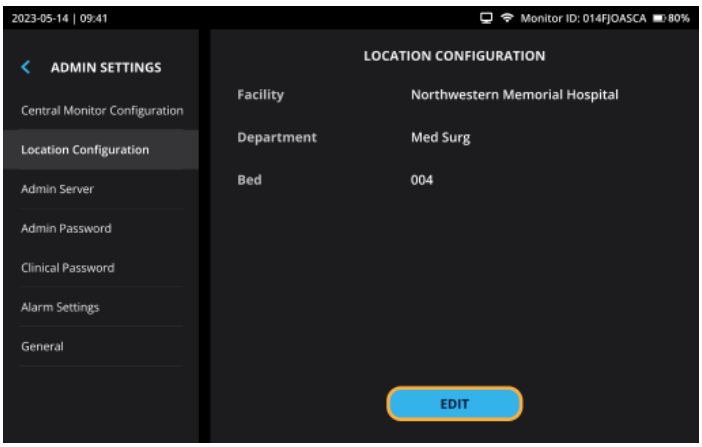
Step 1

Select the Location Configuration tab.



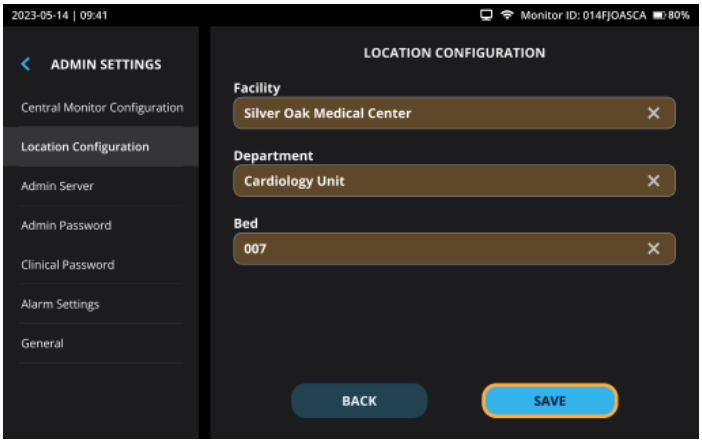
Step 2

Tap the "EDIT" button.



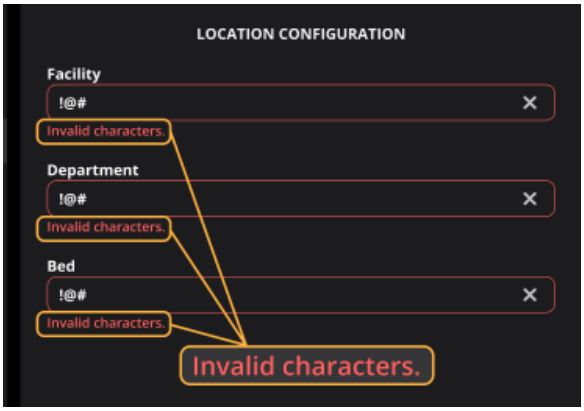
Step 3

Update fields (Facility, Department, Bed) and tap “SAVE” to apply updates.



4.3.2 Error Handling

Table 6: Central monitor configuration error handling

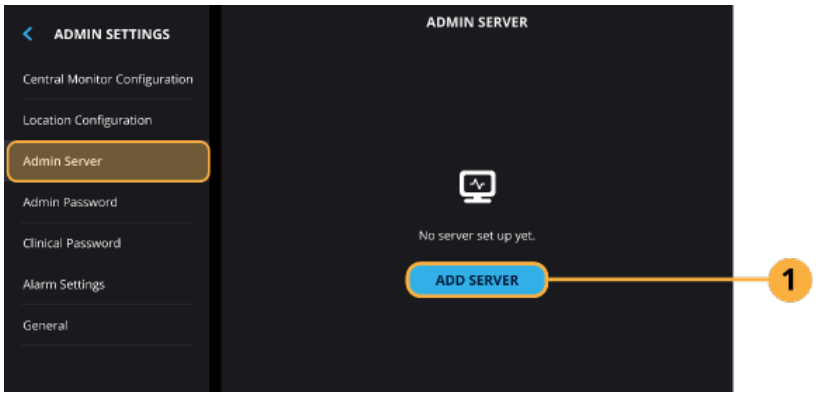
UI	Description	Solution
	Invalid characters.	Try again by entering: 1. Maximum Length: Each field can have a maximum of 7 characters. 2. Allowed Characters: Characters permitted under RFC 3986 unreserved characters, except for the period (.), which must not be used.

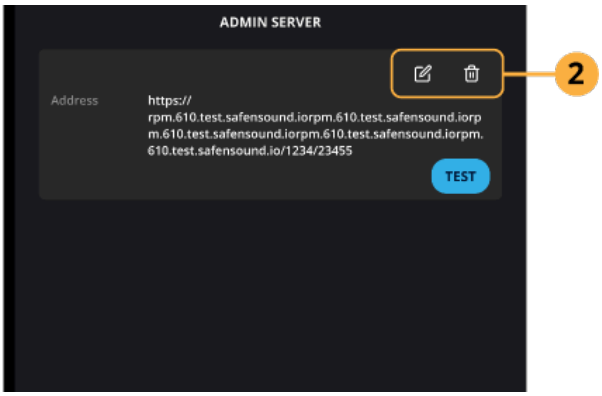
4.4 Admin Server

Note: Admin Server configuration applies to AVOP deployments where an approved Admin Server is part of the customer-site architecture. This section does not apply to AVSC, where the device is configured and managed by Sibel.

Step 1

Select the Admin Server tab and select one of the following actions:





① Add: Select the ADD SERVER button.

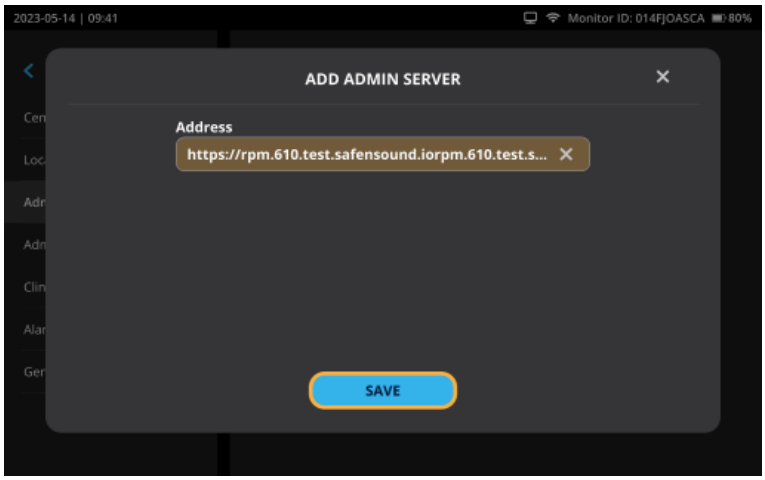
② Modify/Delete: Select the / button.

Step 2 (Add/Modify Only)

Enter or edit the address.

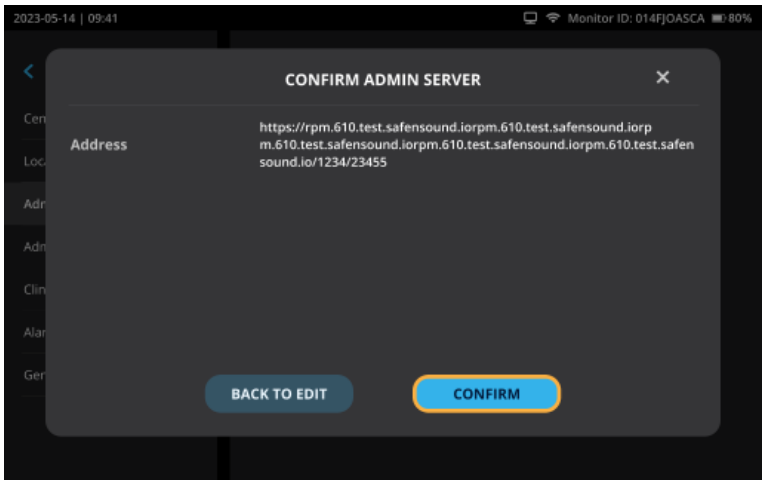
The Address is the Admin Server's HTTPS host used by the application to connect.
Example: https://api.<domain>

Select the "SAVE" button once all required parameters are entered.



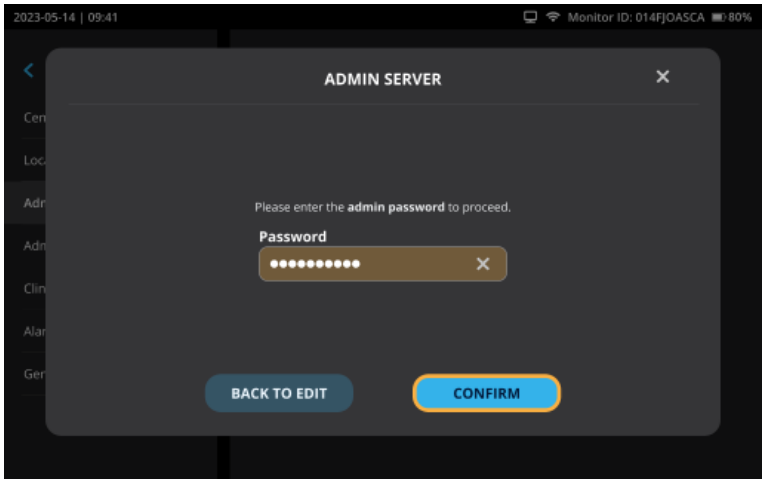
Step 3 (Add/Modify Only)

Confirm all entered details are accurate and select the "CONFIRM" button.



Step 4

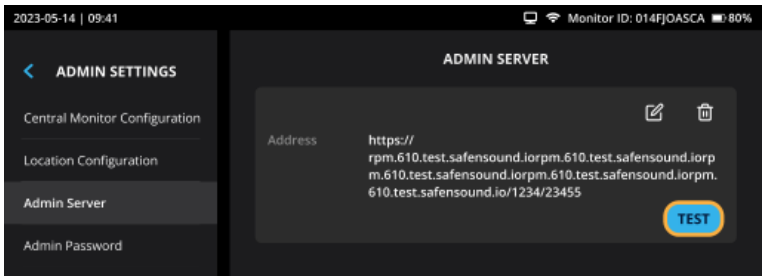
Enter the admin password and select the "CONFIRM" button to proceed the action.

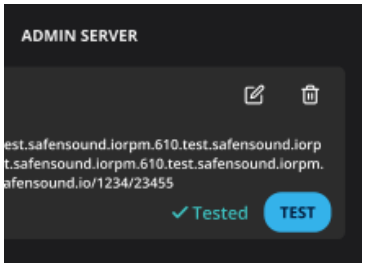


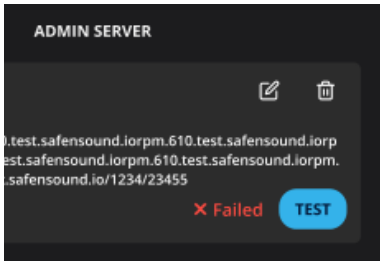
Step 5 (Add/Modify Only)

Once the address is added, tap the "TEST" button to verify.

- Success: Once the address is verified, you will be able to see the "Tested" success message.
- Failed: If the connection is unsuccessful, you will see a "Failed" message. This status will remain until another test is performed.





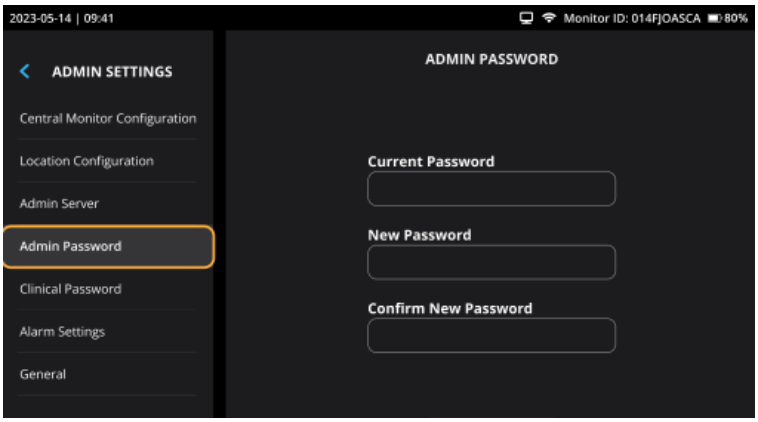


4.5 Password Management

4.5.1 Admin Password

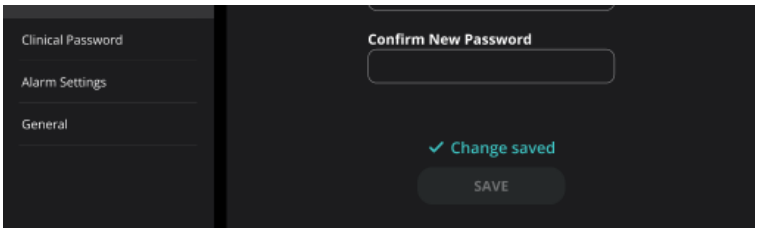
Step 1

Select the Admin Password tab.

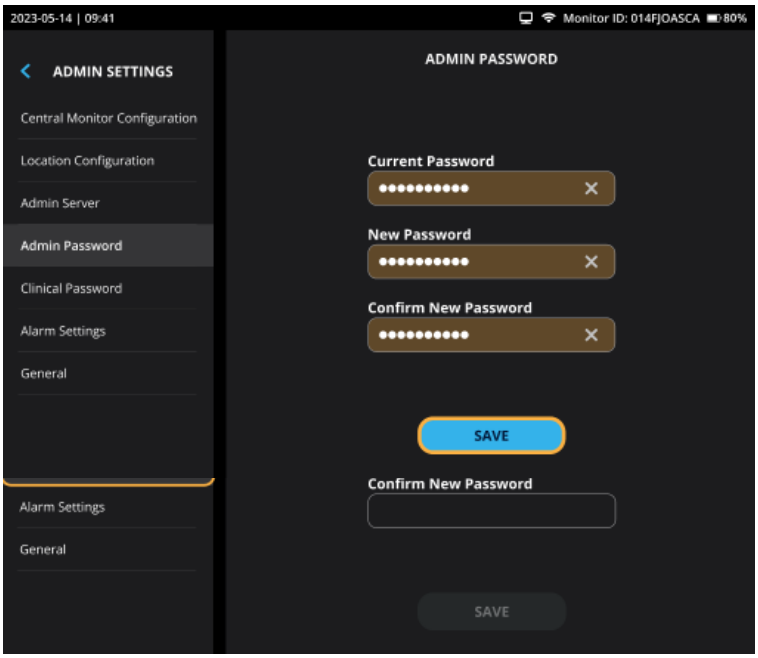


Step 2
Enter your current password and new password and select the “SAVE” button.

Note: Admin password follows the criteria:
- 8 or more characters
- at least one uppercase letter
- at least one lowercase letter
- at least one number
- at least one special character



Step 3
Once the new admin password is saved, you will be able to see the “Change saved” success message.

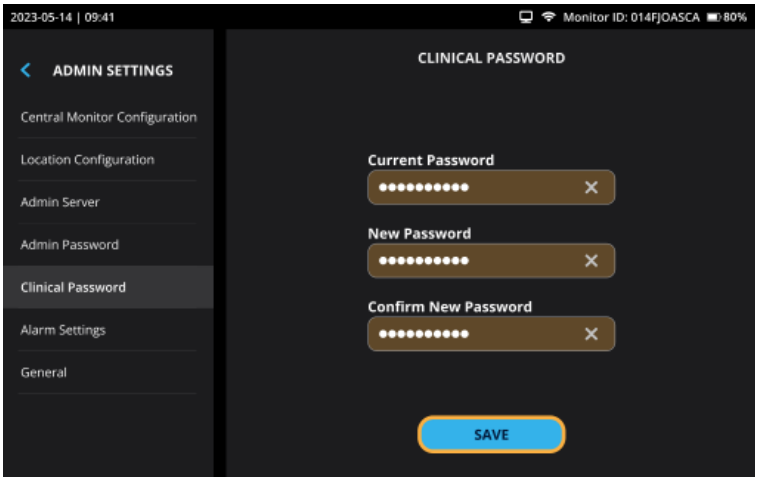


4.5.2 Clinical Password

Step 1
Select the Clinical Password tab.

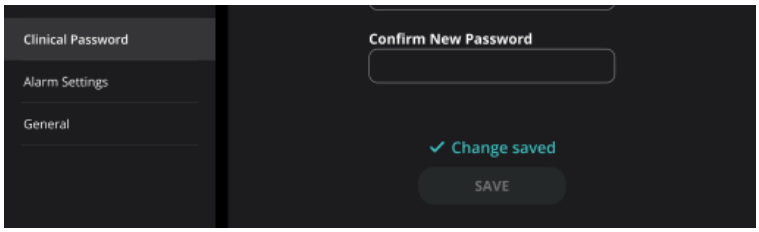
Step 2
Enter your current password and new password and select the “SAVE” button.

Note: Clinical password follows the criteria:
- 4 or more characters



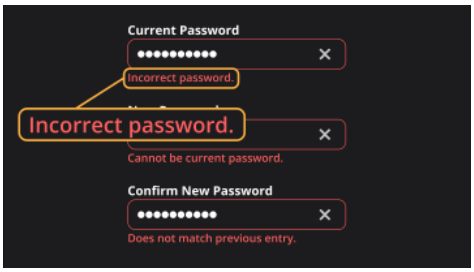
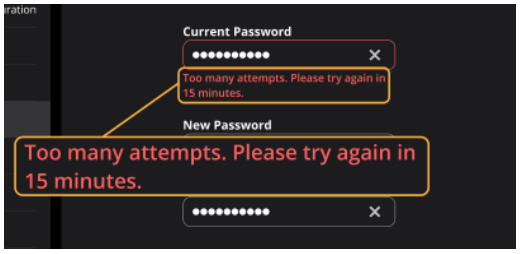
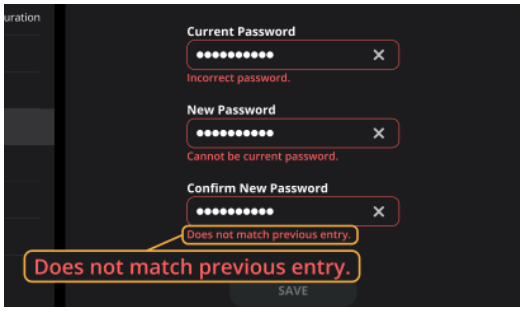
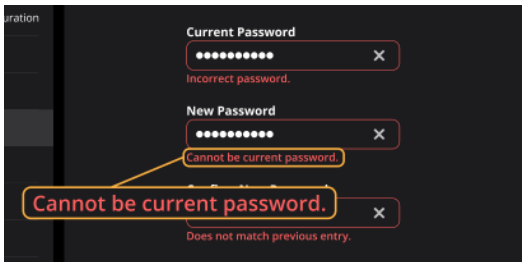
Step 3

Once the new clinical password is saved, you will be able to see the “Change saved” success message.



4.5.3 Error Handling

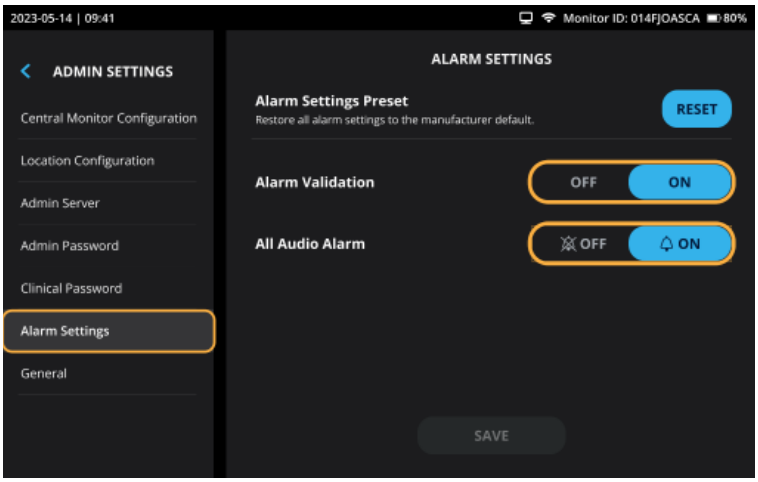
Table 7: Admin/clinical password error handling

UI	Description	Solution
	Incorrect password.	Please enter the correct password and try again.
	There were too many password attempts.	Please try again in 15 minutes.
	The re-entry of the new password does not match with the entry on the previous new admin password input field.	Please try again and enter the same password.
	The new password cannot be the same as the current one.	Please try again with a different password.

4.6 Alarm Settings

Step 1

Select the Alarm Settings tab. Manufacture default settings for “Alarm validation” and “All audio alarm” shall be ON.

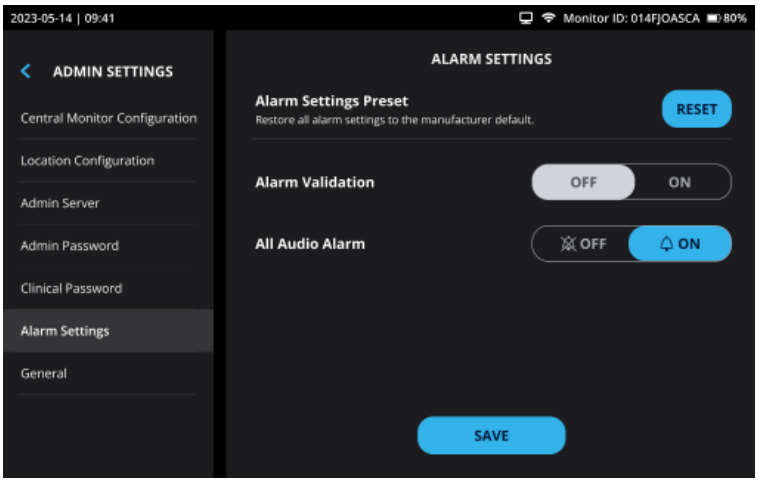


Note about alarm validation:

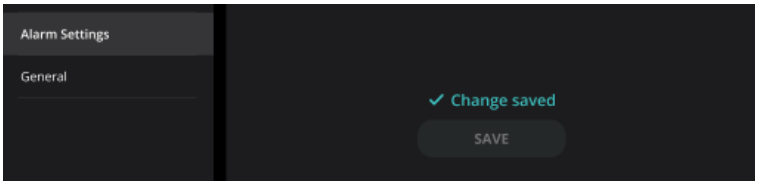
- When Alarm Validation is enabled, ANNE View confirms that an alarm limit has been violated for 95% of the time over a 15-minute validation period before annunciating an alarm. If there are enough invalid samples, the validation period may extend up to 22.5 minutes.
- Alarm validation applies to the following alarms:
  - High/Low Physiological alarms
  - Anne Chest: Lead off
  - Anne Limb: Poor skin contact
  - Anne Chest / Anne Limb: Invalid HR, RR, SpO2, PI, PR; Low signal
  - ANNE View Tablet: No Central, No Network
- Alarm validation does not apply to the following alarms:
  - Anne Chest / Anne Limb: Critical sensor battery, Low battery, Sensor failure, Sensor out of range
  - BP Monitor: Critical sensor battery, Low battery, Loose sleeve, movement detected, weak pulse, sensor failure
  - ANNE VIew Tablet: Low tablet battery

Step 2

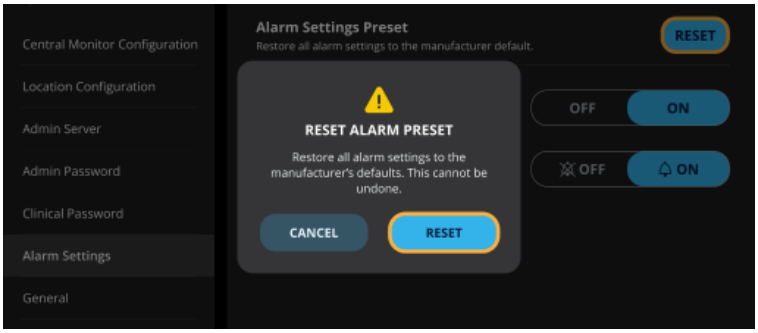
After switching any of the toggle, select the “SAVE” button.



Step 3
Once the new setting is saved, you will be able to see the “Change saved” success message.

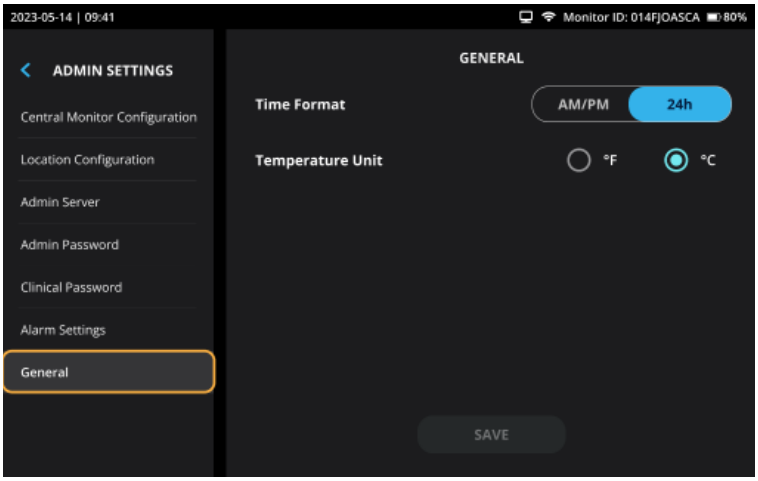


Step 4
When you select the RESET button, a confirmation popup will appear. Select “RESET” to apply the manufacturer’s default settings, or “CANCEL” to close the popup without making any changes.

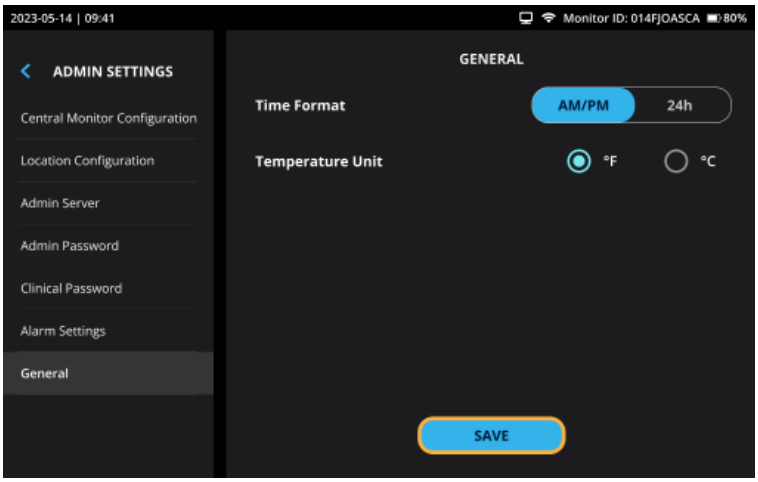


4.7 General

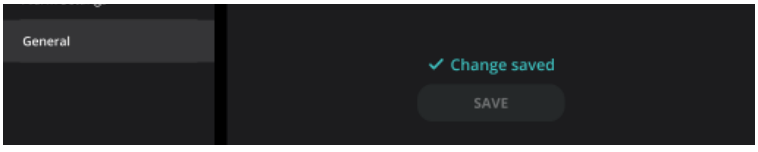
Step 1
Select the General tab.



Step 2
As long as one item changes in the list, the SAVE button will be available.



Step 3
Once the new changes are saved, you will be able to see the “Change saved” success message.



Section 5. ANNE View IT Administration and Lifecycle

5.1 Deployment Configurations

The ANNE View Patient Monitor supports two deployment configurations for IT integration, device management, and updates. In AVOP On Premises Configuration, the Patient Monitor may communicate with on-site Sibel CMS and/or approved third-party systems using supported interfaces such as HL7 FHIR or IEEE 11073 SDC, according to the approved deployment architecture. In AVOP, the hospital/owner-operator manages approved updates through the approved MDM solution, with Sibel Health support as needed. In AVSC Standalone Configuration, the Patient Monitor is configured, managed, and updated by Sibel Health before deployment or return, and does not depend on customer-site network connectivity, Sibel CMS, or third-party system connectivity for intended monitoring.

5.2 Central Monitoring Platform

By default, there is no central monitoring platform configured on the ANNE View application. IT administrators can add a central monitoring platform configuration by selecting protocols from either HL7 Fast Healthcare Interoperability Resources (FHIR) or IEEE 11073 Service-oriented device connectivity (SDC). The HL7 FHIR is a standard for exchanging healthcare information electronically. The ANNE View Tablet effectively employs WebSocket technology to transmit data conforming to the requirements outlined by the FHIR standard. The IEEE 11073 SDC standards provide a communication protocol for point-of-care medical devices, facilitating interoperability among devices and allowing them to communicate with each other seamlessly. The ANNE View Tablet can allow the request of unidirectional data with secured communication to transmit data as a service provider.

Note: The selection of the communication protocol should be based on the protocol that the receiving system executes.

5.3 ANNE View Maintenance

5.3.1 ANNE View Cybersecurity Considerations

Sibel Health has the following security considerations for the ANNE View installation in order to provide the highest level of security.

- The communication between the central monitoring platform and the ANNE View is encrypted using the X.509 certificates and that should be generated by a trusted certificate authority (CA) and managed by the organization. The management of the certificates encompasses the key generation, storage, backup, and revocation.
- Each deployed unit must have a unique child certificate of the organization's root or intermediate certificates in order to prevent the reveal of other devices' keys.
- Recommended certificate generation is to use 1 year expiration, using openssl with RSA:4096 encryption.
- In the potential case of a ANNE View Tablet certificate compromise, that certificate should be blacklisted and ANNE View Tablets from other units would not be impacted.
- All the stored PHI data is encrypted in the ANNE View using AES-256 encryption algorithm.

- ANNE View is strictly restricted for the device configurations such as customizing network configuration, non-market application installation, or hardware connection with unknown sources as both hardware and software are controlled by authorized MDM services.
- ANNE View protects the modification of cryptographic assets such as X.509 certificates by unauthorized users.
- ANNE View includes physical tamper protection such as hardware or firmware modifications by the manufacturer's security control.

5.3.2 ANNE View Security Patches

Explicit patches targeting discovered vulnerabilities are required and should be applied as soon as practical according to the applicable risk, customer change-control process, and Sibel Health instructions. These security-related patches do not include new functionality and are intended to secure the product from the identified vulnerability.

Upon completion and approval of a patch, Sibel Health will notify affected customers and provide the qualified release package and update instructions.

In AVOP On Premises Configuration, the hospital/owner-operator manages deployment of Sibel-approved security patches using the approved MDM solution, with Sibel Health support as needed.

In AVSC Standalone Configuration, Sibel Health manages the update process. AVSC devices are configured and updated by Sibel using the Sibel internal network before deployment or return to the customer.

5.3.3 ANNE View System Patches

The patchability rate for ANNE View updates follow a two-week sprint cycle and hot-fix process. Patch announcements will be communicated to clients via email and a distribution of the qualified release will be provided by Sibel Health following the Upgrade process in a subsequent section.

5.3.4 ANNE View Version Release

Full version releases of ANNE View will be generated based on Sibel Health internal software lifecycle management plan. The version release process will follow the proper testing phases (Verification and Validation) in order to produce a qualified release consisting of new functionality, remediations of anomalies from previous releases, as well as performance improvements.

5.3.5 ANNE View MDM Configurations

ANNE View MDM configuration depends on the deployed configuration.

In AVOP On Premises Configuration, the hospital/owner-operator manages the approved MDM configuration for deployed devices according to Sibel Health instructions. The MDM configuration supports approved application deployment, update management, kiosk mode, and recovery of the validated device configuration.

In AVSC Standalone Configuration, Sibel Health manages the MDM/kiosk configuration and update activities using the Sibel internal network before deployment or return to the customer.

Before returning an ANNE View Patient Monitor configured for standalone use to Sibel Health for configuration, update, service, or decommissioning, all active patient monitoring sessions shall be ended. Confirm that no patient monitoring session remains active before packaging, transfer, or shipment. This helps minimize the risk of PHI exposure during transport and service handling.

5.3.6 ANNE View Event Logging

Sibel Health logs will provide information relating to the health of the systems, as well as issues of the Anne View Application.

5.3.7 Device Event Handling

When anomalous conditions are detected, the system responds accordingly. For example, if continuous entering password attempts are identified, such as five consecutive password match failures, the system blocks further enter password attempts for 15 minutes.
All unknown entities without valid certificates are denied communication with the system.

5.4 ANNE View Decommissioning (EOL)

5.4.1 ANNE View Version Out of Support

ANNE View version will be supported up to two revisions backward, but once a revision is out of support clients will be instructed on the upgrade path to the latest version. Users who opt out of upgrades will no longer receive updates (Security nor Patches). Sibel Health will produce information relating to any known vulnerabilities to clients in order to inform them of the risks of not moving to the latest version.

5.4.2 ANNE View End of Life

When ANNE View runs into its End of Life scenario, Sibel Health will inform all clients of the date at which there will be no more support nor expectation of reliable use of the system. Sibel Health has created decommissioning documentation to safely remove the application from their installed location as well as options for data erasure.
See Section 5.4.3 of this IFU for ANNE View decommissioning steps.
Please note that sensitive information may be exposed if the system is incorrectly or incompletely decommissioned.

5.4.3 ANNE View Decommission

When ANNE View is to be decommissioned from use, the following steps must be taken to ensure all sensitive data and proprietary software are appropriately removed.

For AVSC Standalone Configuration, the hospital/owner-operator shall coordinate return with Sibel Health support or a Sibel Health field engineer before sending the Patient Monitor to Sibel Health for decommissioning. The following return preparation steps shall be completed by the hospital/owner-operator or with assistance from a Sibel Health field engineer, as applicable:

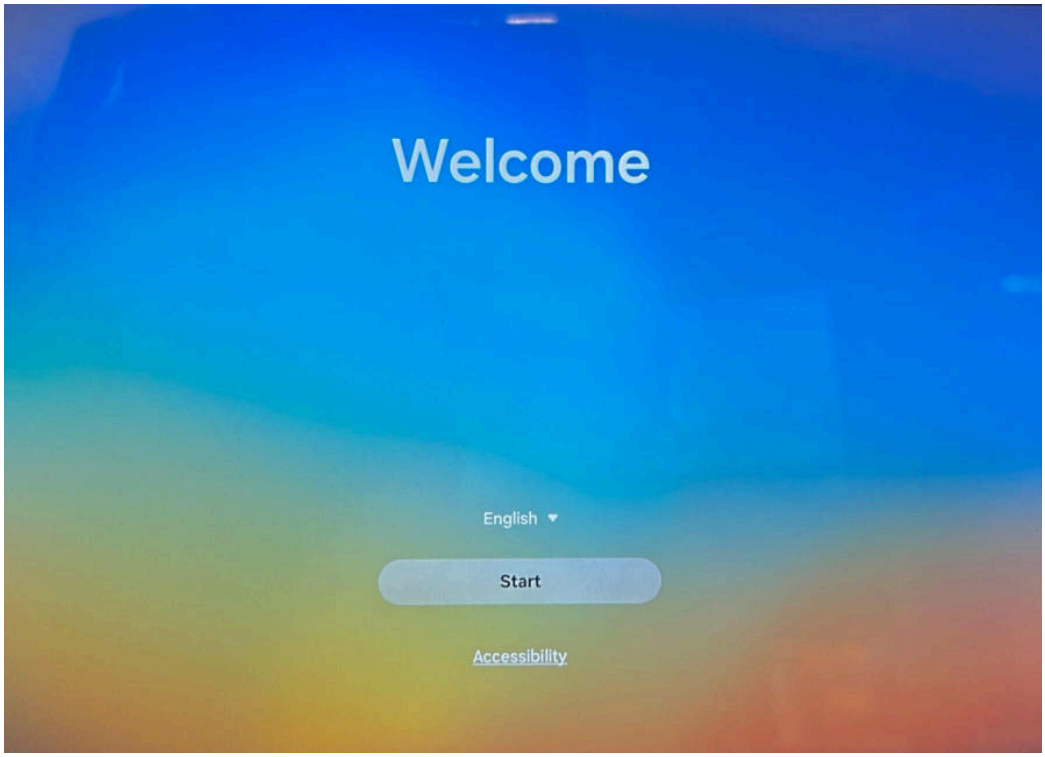
1) End all active patient monitoring sessions.
2) Confirm that no patient monitoring session remains active.
3) Remove the Patient Monitor from clinical use.
4) Package the Patient Monitor for return according to Sibel Health instructions.
5) Coordinate return shipment, transfer, or field engineer pickup with Sibel Health.

Sibel Health will perform decommissioning activities for returned standalone-configured Patient Monitors using the applicable internal process.

For AVOP On Premises Configuration deployments managed by the hospital/owner-operator, perform the following MDM decommissioning steps:

6) Enter into your Mobile Device Management (MDM) software
7) Select the correct ANNE View device to be decommissioned
8) Initiate a Factory Reset command (This will factory reset the device and wipe all information currently on the device as well as installed applications)
9) Remove the device from MDM Inventory after initiating the Factory Reset command to ensure the device does not reconnect to MDM.
10) Device will take some time to wipe and restart (please see screenshots below)
    a) Factory Resetting

b) Factory Reset Complete



Section 6. Vulnerability Disclosure

6.1 Sibel Health Vulnerability Disclosure Policy

As a provider of secure software, services, and research, the customer support representative takes security issues seriously and recognizes the importance of privacy, security, and community outreach. As such, the customer support representative is committed to addressing and reporting security issues. This policy outlines how to report vulnerabilities, what to expect in response, and how the customer support representative will handle them.

6.2 Reporting Security Issues

If you believe you have discovered a vulnerability in a product by the customer support representative or have a security concern you would like to report, please report it following these steps:

- **Email:** Send a detailed report to security@sibelhealth.com. If you feel the need, please use our PGP public key below to encrypt your communications with us.
    - Public PGP Key

```
None
-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEZt+KghYJKwYBBAHaRw8BAQdAi5TvQjkUR+3OeAwyRzck68CXwJB48cyT2agM
QDJlp4a0LEpvbmcgWW9vbiBMZWUgPGpvbmd5b29uLmxlZUBzaWJlbGhlYWx0aC5j
b20+iJMEExYKADsWIQSr1EgI/KSP5svTwCruWcLTCBvB8QUCZt+KggIbAwULCQgH
AgIiAgYVCgkICwIEFgIDAQIeBwIXgAAKCRDuWcLTCBvB8XQlAQDd4uf8JftUfefR
GLOC2nKNkyEvHTfxghCFrGTCl1GXLQEAmleqy8ZNKUqdb2dO0SvxnQtNqmFyNe1M
pklTAPJVfgi4OARm34qCEgorBgEEAZdVAQUBAQdAGM5w5lJozi/X8rJP6xmIvP5t
uJ8Xc0b/s6slT+ZfKRADAQgHiHgEGBYKACAWIQSr1EgI/KSP5svTwCruWcLTCBvB
8QUCZt+KggIbDAAKCRDuWcLTCBvB8Z9HAQCwDhcB8kCZQxxSyPLEon6mL+HB8leD
R49iMPOmdkyeDAD+Ku1Of1fUSP4e/ShmtcnjEF7d7RcA+NqbNAOLtWztIwg=
=F/DG
-----END PGP PUBLIC KEY BLOCK-----
```

- **Information to include:**
    - A detailed description of the vulnerability, including
        - Product or service name, URL, and affected versions.
        - Operating system of involved components.
        - Software configuration of the computer or device at the time of discovery.
        - Class or type of vulnerability (e.g., using a taxonomy like CWE).
        - Time and date of discovery.
    - Steps to reproduce the issue
        - Technical description of actions performed, order and result.
        - PoC code/Tools used to produce the vulnerable behavior.
    - Potential impact and severity estimate, If available.
    - Potential root cause, If available.

- Scope assessment, other products, components, services, or vendors thought to be affected, If available.
- Disclosure plans, specifically embargo and publication timelines, If available.

6.3 Our Commitment

When a vulnerability is reported to the customer support representative, we commit to:

- Acknowledgement of receipt of your report within 7 business days.
- Assess and verify the legitimacy of the vulnerability.
- Categorize the severity of the vulnerability based on potential impact.
- Develop a remediation plan based on severity and implement a fix.
- Provide an estimated timeline for remediation.
- Communicating progress throughout the remediation process through email
- Advisory communication with remediation following our internal vulnerability management procedure.
- Treating each report confidentially and not disclosing it to third parties without consent.
- Disclose vulnerabilities in release notes of updates.

Please note that not all issues will be in the scope of the customer support representative's vulnerability disclosure process, including:

- Reports of missing security headers that do not lead to significant impact or performance degradation.
- Outdated platform-specific issues.
- Social engineering attacks or physical vulnerabilities (e.g. office security).
- Issues with third-party services not managed by the customer support representative

6.4 Machine Readable SBOM

A machine-readable Software Bill of Materials (SBOM) listing all software components is available from Sibel Health upon request. Contact security@sibelhealth.com.