ANNE One
ADMIN IFU

Installation, Configuration, Service & Maintenance

support.sibelhealth.com

IFU P/N 443-00006G

Table of Contents

Section 1. Important Safety Information

1.1 Overview

This document is intended for qualified technical personnel responsible for configuration, maintenance, and servicing of the ANNE One system from the Admin Hub and its networked components. It does not describe clinical use or patient-facing operation.

Permitted service activities include:

- Installation and configuration of the system software and supporting infrastructure as described in this IFU and associated installation manuals, MA-00018 CMS Installation Instruction.
- System monitoring, log review, backup, restore, patching, and decommissioning activities explicitly described in this document.
- Network, server, and access control configuration consistent with the recommendations provided.

Prohibited actions include:

- Modification of software, firmware, system architecture, security controls, or configurations outside documented procedures.
- Use of undocumented interfaces, credentials, or backdoor access mechanisms.
- Servicing activities that could alter clinical functionality, data integrity, or regulatory compliance.

Manufacturer authorization required:

- Any deviation from documented installation, upgrade, patching, recovery, or cybersecurity procedures.
- Manual intervention at the database, container, or operating system level not explicitly described in this IFU or manufacturer-provided service documentation.

1.2 Glossary

Table 1: Glossary

Abbreviation	Definition
IFU	Instructions for use
RBAC	Role-Based Access Control
ADT	Admission-discharge-transfer
PM	ANNE View
BLE	Bluetooth Low Energy

EOL	End of Life
NFC	Near Field Communication
LED	Light-emitting diode
IP	Ingress Protection
IT	Information Technology
VM	Virtual Machine
TPM	Trusted Platform Modules

1.3 Symbols

Table 2: Symbols

Symbol	Title	Description
Rx ONLY	Prescription Use Only	Federal law restricts this device to sale by or on the order of a licensed healthcare practitioner
	Refer to instruction manual/booklet	To signify that the instruction manual/booklet must be read
	eIFU	Indicates the need for the user to consult the instructions for use or the electronic instructions for use.
QTY	Quantity Symbol	Indicates the number of units or pieces in the package.
EC REP	Authorized representative in the European Union	Indicates the authorized representative in the European Union.
CE 2460	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.

1.4 Manufacturer Information

- Contact your customer support representative for any of the following issues:
  - Assistance in setting up, using, or maintaining ANNE One
  - 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

EC REP

MDSS GmbH
Schiffgraben 41, Hannover 30175
Germany

Section 2. Product Specifications

2.1 Product Specifications

Table 3: CMS Server Specifications

	CMS (Server)
CPU	1 × 4-core CPU @ 2.4 GHz
RAM	16GiB
OS Disk	100 GB SSD (SCSI interface)
Data Disk	300 GB SSD (SCSI interface, ext4 format)
Network	100/1000 Mbps Ethernet
Other hardwares	Uninterruptible power supply
Operating System	Ubuntu 24.04 Noble Numbat
Supporting software	None

Table 4: CMS USB drive specifications

Make	iStorage
Model Number	IS-FL-DA3C-256-32
Storage Capacity	32GB
Interface	USB Type C with Type-A adapter
Data transfer rate	Read: 310MB/s Write: 246MB/s
Dimensions (mm)	Height: 80.10mm Width: 20.25mm Depth: 10.70mm
Weight	25g
Operating system compatibility	MS Windows, macOS, Linux, Chrome, Android, Thin Clients, Zero Clients, Embedded Systems, Citrix and VMware
Encryption keys	256-bit hardware encryption

2.2 Security Recommendations

The Target Server must be configured with the following security settings before CMS installation begins. These settings are verified during the pre-installation checklist.

Table 5: Target Server security configuration (MA-00020 Table 2-9)

Parameter	Required Value
Secure Boot	Enabled
TPM	Enabled (hardware passthrough or vTPM)
Disk Layout	LVM on OS disk
Disk Encryption	LUKS on OS disk
Disk Interface	SCSI (not VirtIO or NVMe)

2.2.1 SSH Access Security

The CMS installer connects from the Remote Machine to the Target Server over SSH. The following SSH security configuration is required:

- SSH key pair: RSA 4096-bit, generated on the Remote Machine.
- Private key permissions: restricted to the operator account only. The OpenSSH client refuses keys with open permissions.
- Public key authentication: enabled on the Target Server.
- Password authentication: disabled on the Target Server after public key deployment.

NOTE: The private key grants full SSH access to the Target Server. Do not email, share, or store it on unencrypted media.

2.2.2 TLS Certificate Requirements

The CMS requires a domain TLS certificate to encrypt HTTPS traffic between browsers, ANNE View Tablets, and the CMS. The customer IT administrator must provide the certificate files before installation.

Table 6: Required TLS certificate files (MA-00020 Table 2-10)

File	Format	Purpose
fullchain.pem	PEM	Certificate chain for the CMS

		domain
privkey.pem	PEM	Corresponding private key

Certificate requirements:

- Key algorithm: RSA 4096+ or ECDSA P-256+.
- Protocol: TLS 1.2+.
- Validity: 200 days recommended.
- SAN: must include all 6 CMS domain names; cms.<domain>, api.<domain>, cp.<domain>, dash.<domain>, hmdm.<domain>, mon.<domain>.
- Issuer: must be issued by a public certificate authority. Self-signed certificates are not supported.

NOTE: The fullchain.pem must contain the full chain from the leaf certificate through the issuing CA's intermediate certificate(s). ANNE View Tablets validate the chain against their built-in public CA trust store. A certificate issued by a private CA will fail validation and prevent tablets from connecting to the CMS.

2.2.3 SSL Interception Bypass

If the hospital network uses SSL interception (also known as TLS inspection or HTTPS inspection), configure a bypass rule for all CMS VLAN traffic. SSL interception replaces the server's TLS certificate, causing ANNE View Tablets to reject the connection.

2.3 Network Recommendations

The CMS and all devices (ANNE View Tablets, Remote Machine) must be on the same isolated VLAN. The customer IT administrator must configure the network infrastructure described in this section before installation begins.

Figure 1: CMS Cluster Network diagram

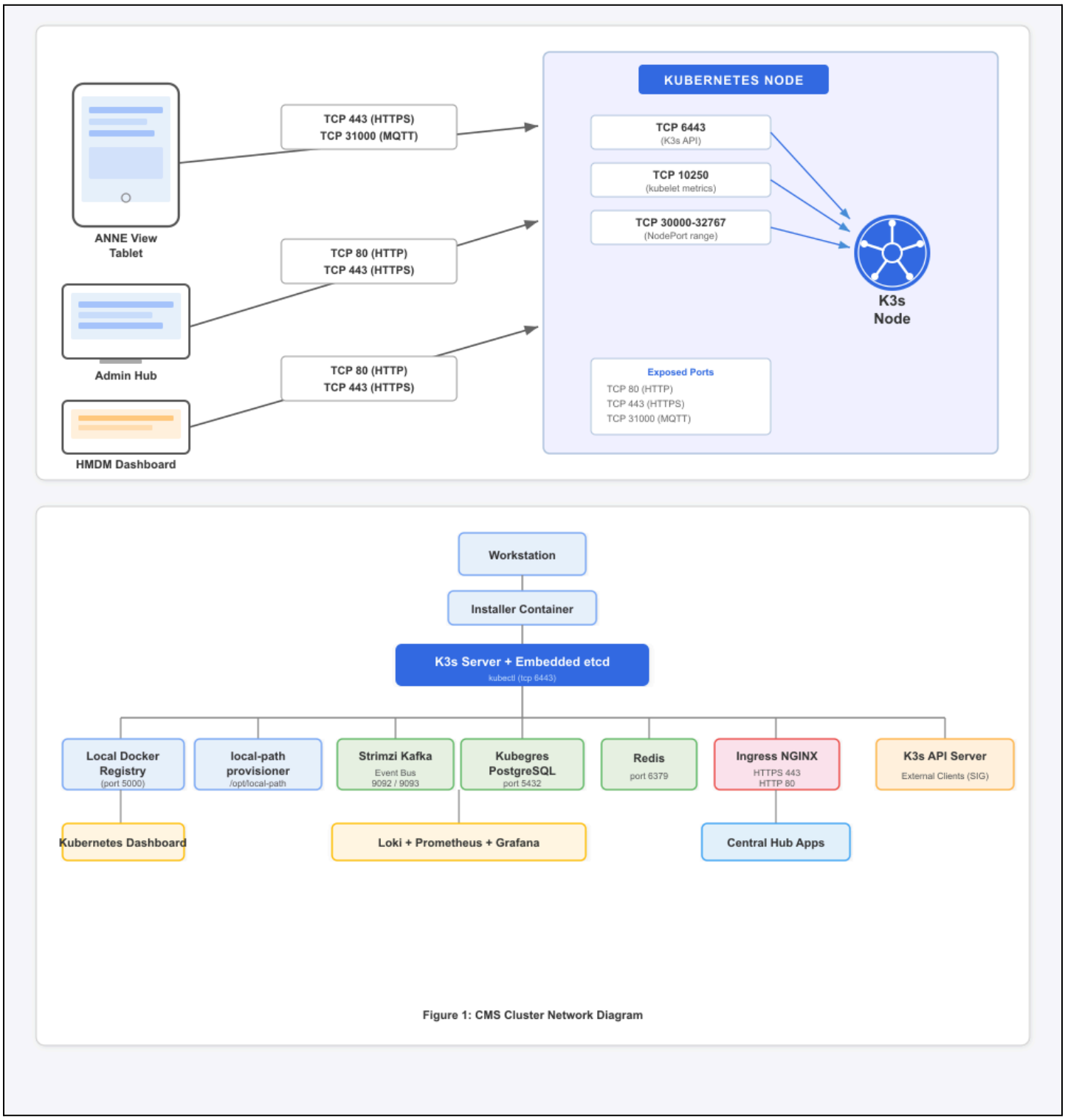


Figure 1: CMS Cluster Network Diagram

2.3.1 VLAN Design

The customer IT administrator must assign the following network parameters for the CMS VLAN:

Table 7: VLAN network design parameters

Parameter	Value	Notes
VLAN (LAN) ID	<assigned by IT>	e.g., 100
Subnet	<assigned by IT>	e.g., 10.10.100.0/24
Gateway	<first usable IP>	e.g., 10.10.100.1
Target Server IP	<static IP within subnet>	e.g., 10.10.100.10
Remote Machine IP	<DHCP or static within subnet>	Used during installation and ongoing maintenance
Tablet/Mobile IP	<DHCP or static within subnet>	Must resolve CMS hostname and access CMS (Wi-Fi interface)

2.3.2 Network Layer Requirements

The network between the Target Server and all other devices must meet the following requirements. If any requirement is not met, the CMS will not function correctly.

Table 8: Network requirements

Requirement	Details
IP addresses assigned to all devices	Every device on the VLAN must have an IP address (static or DHCP). During installation, only the Target Server and Remote Machine require assigned addresses. ANNE View Tablets are configured later during device onboarding.
IPv4 only	All CMS services bind to IPv4 only. Do not use IPv6-only addressing.
No SSL interception	If the hospital uses SSL interception, configure a bypass rule for all CMS VLAN traffic. SSL interception replaces the server's TLS certificate, causing ANNE View Tablets to reject the connection.

2.3.3 Service Ports

The Target Server exposes the following ports on the VLAN. All devices are on the same VLAN, so no firewall rules are required between them.

Table 9: Target Server service ports

Port	Protocol	Used by	Purpose
22	TCP	Remote Machine	SSH; installation and maintenance
80	TCP	Admin browsers	HTTP (redirects to HTTPS)
443	TCP	Admin browsers, ANNE View Tablets, Remote Machine	HTTPS; CMS web application, API, web portal
6443	TCP	Remote Machine	Kubernetes API; cluster management
31000	TCP	ANNE View Tablets	MQTT; Headwind MDM device management
123	UDP	ANNE View Tablets	NTP; time synchronization
53	UDP	ANNE View Tablets, Target Server	DNS; name resolution

2.3.4 DNS Configuration

The following DNS A records must point to the Target Server IP. Replace <domain> with the customer-chosen domain name for the CMS deployment:

Table 10: DNS A records

DNS Record	Target	Purpose
cp.<domain>	Target Server IP	Kubernetes API endpoint
cms.<domain>	Target Server IP	CMS web application
api.<domain>	Target Server IP	CMS API endpoint
dash.<domain>	Target Server IP	Kubernetes Dashboard
hmdm.<domain>	Target Server IP	Headwind MDM
mon.<domain>	Target Server IP	Grafana Dashboard
time.android.com	NTP Server IP	NTP time synchronization for ANNE View Tablets

The CMS operates on an isolated network without access to corporate or public DNS. The customer IT team must configure a local DNS server within the VLAN to serve the 7 A records above. The DNS server must meet the following requirements:

Table 11: DNS server requirements

Requirement	Details
A record support	Must serve static A records mapping hostnames to the Target Server IP and NTP server IP
Reachable by all devices	The Target Server, Remote Machine, ANNE View Tablets, and all admin workstations must be able to query the DNS server
Available on the CMS VLAN	The DNS server must be on the same VLAN or routable from it
No external dependency	Must not rely on internet connectivity or corporate DNS for the 6 CMS-related records
Default DNS server	Configured as the default DNS server for the network

2.3.5 NTP Time Synchronization

ANNE View Tablets synchronize their system clock with time.android.com by default. In an air-gapped network, the customer IT team must redirect this traffic to an internal NTP server. Accurate time synchronization is required for clinical record integrity, alarm log accuracy, and cross-system data correlation.

Table 12: NTP time synchronization requirements

Requirement	Details
NTP server	An NTP server must be reachable from the VLAN.
DNS override	The local DNS server must resolve time.android.com to the NTP server IP address.
UDP port 123	The VLAN firewall must allow UDP port 123 traffic between ANNE View Tablets and the NTP server.
Firewall rule order	Allow rules for NTP and DNS must appear above any Block or Drop rules in the firewall rule set.

Section 3. Administrator Dashboards and Service

3.1 Kubernetes Dashboard

3.1.1 Access

The Kubernetes Dashboard is available at https://dash.<domain>, where <domain> is the CMS domain name configured during installation.

Prerequisite: A DNS A record for dash.<domain> must resolve to the Target Server IP.

3.1.2 Authentication

To log in to the Kubernetes Dashboard:

1. Open https://dash.<domain> in a web browser.
2. Select the Token authentication method.
3. Enter the dashboard access token. Refer to the CMS Installation Guide for the location of credential files.

3.1.3 Dashboard Overview

The Kubernetes Dashboard displays the status of all CMS services running on the Target Server. Use this dashboard to:

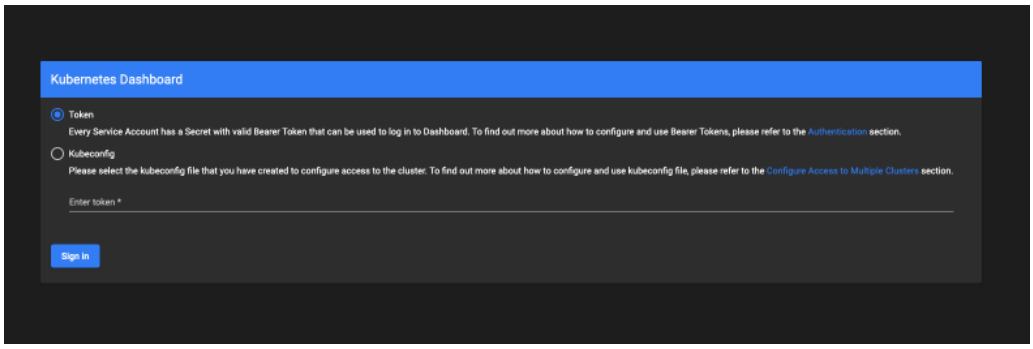
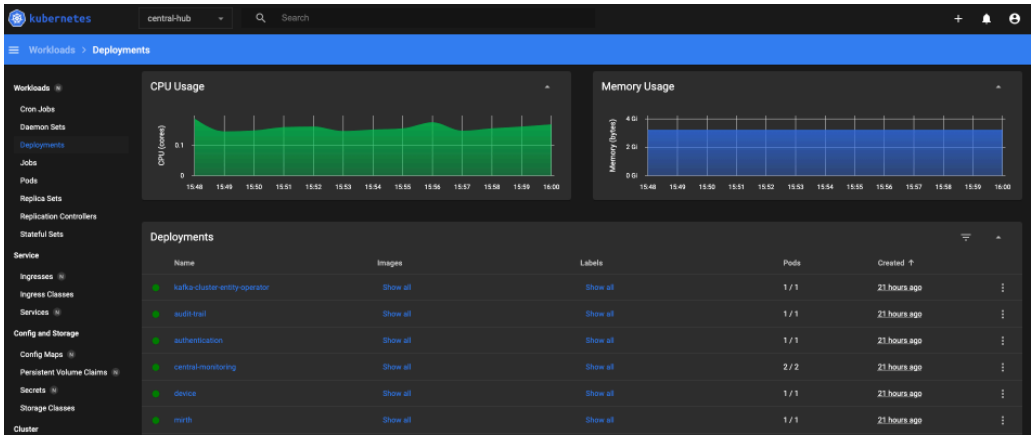
1. View the status of running pods and containers.
2. Monitor CPU, memory, and storage utilization per node.
3. View and export CMS service logs.
4. Check the status of deployments and replica sets.
5. Monitor namespace-level resource usage.
6. Set and adjust resource quotas.

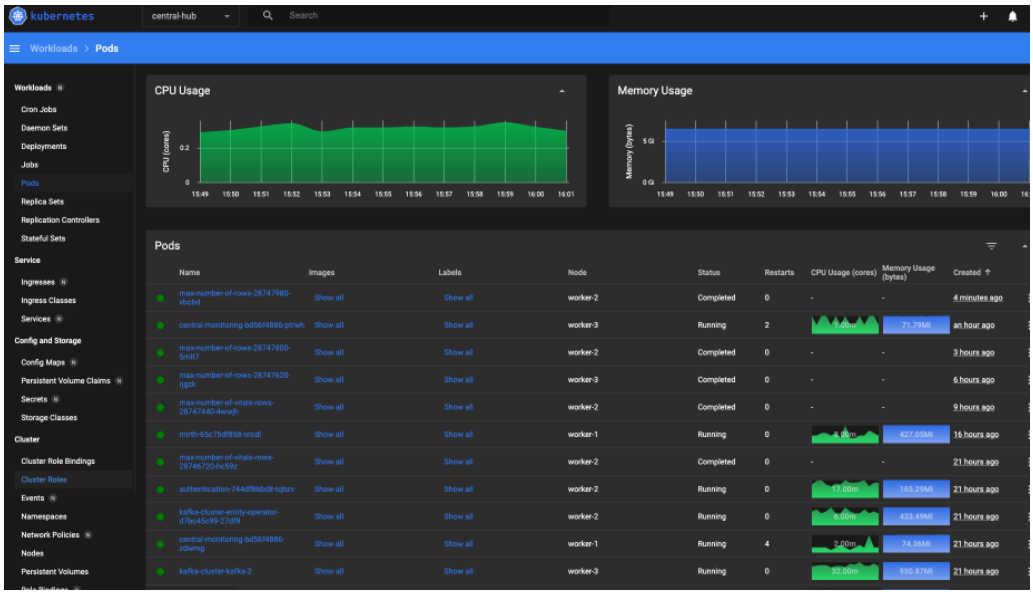
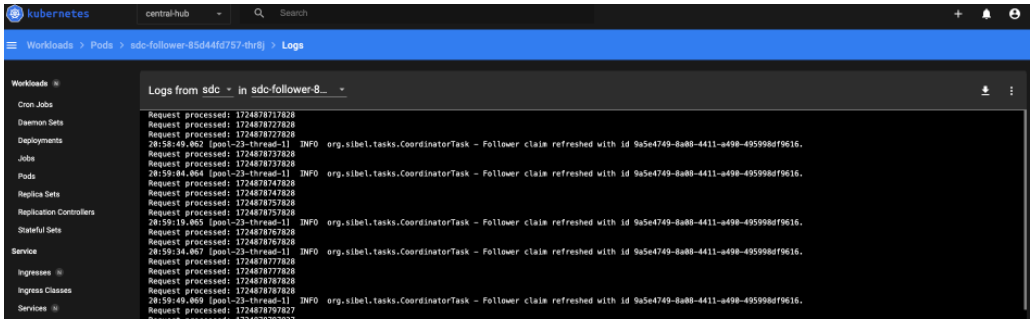
3.1.4 Monitoring Metrics

The following metrics are available in the Kubernetes Dashboard:

Table 13: Kubernetes monitoring metrics

K8s Dashboard	Image

Login	
Workload Status	
Deployments	

Running Pods	
Service Logs	

3.2 Grafana Dashboard

3.2.1 Access

The Grafana Dashboard is available at https://mon.<domain>, where <domain> is the CMS domain name configured during installation.

Prerequisite: A DNS A record for mon.<domain> must resolve to the Target Server IP.

3.2.2 Authentication

To log in to the Grafana Dashboard:

1. Open https://mon.<domain> in a web browser.
2. Enter the Grafana credentials. Refer to the CMS Installation Guide for the location of credential files.
3. Verify that the Grafana version displayed on the login screen matches the version specified.

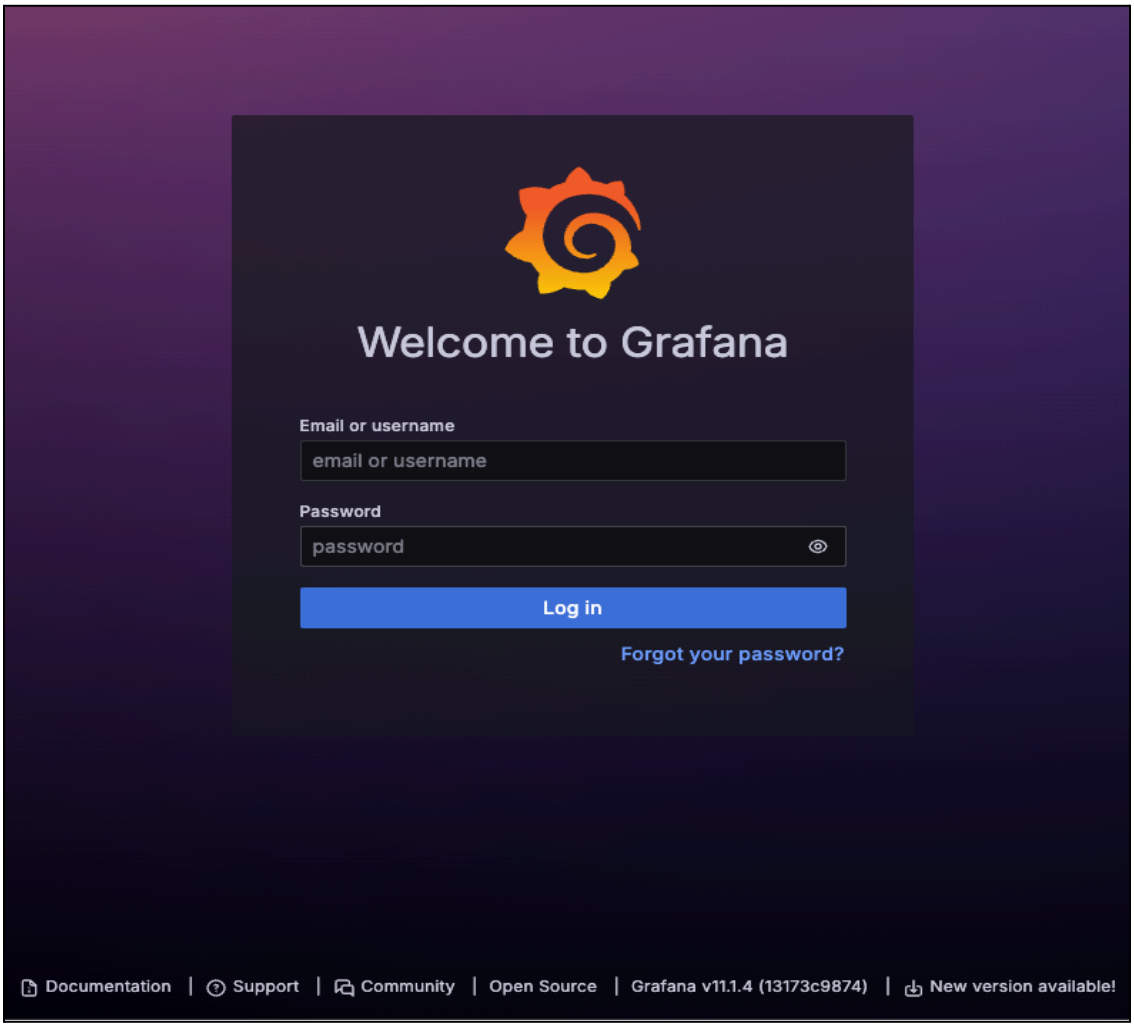


Figure 2: Grafana login screen

3.2.3 Dashboard Overview

The Grafana Dashboard provides monitoring and alerting for CMS services, infrastructure, and network activity. The CMS includes 20+ predefined dashboards. The default log retention period is 7 days.

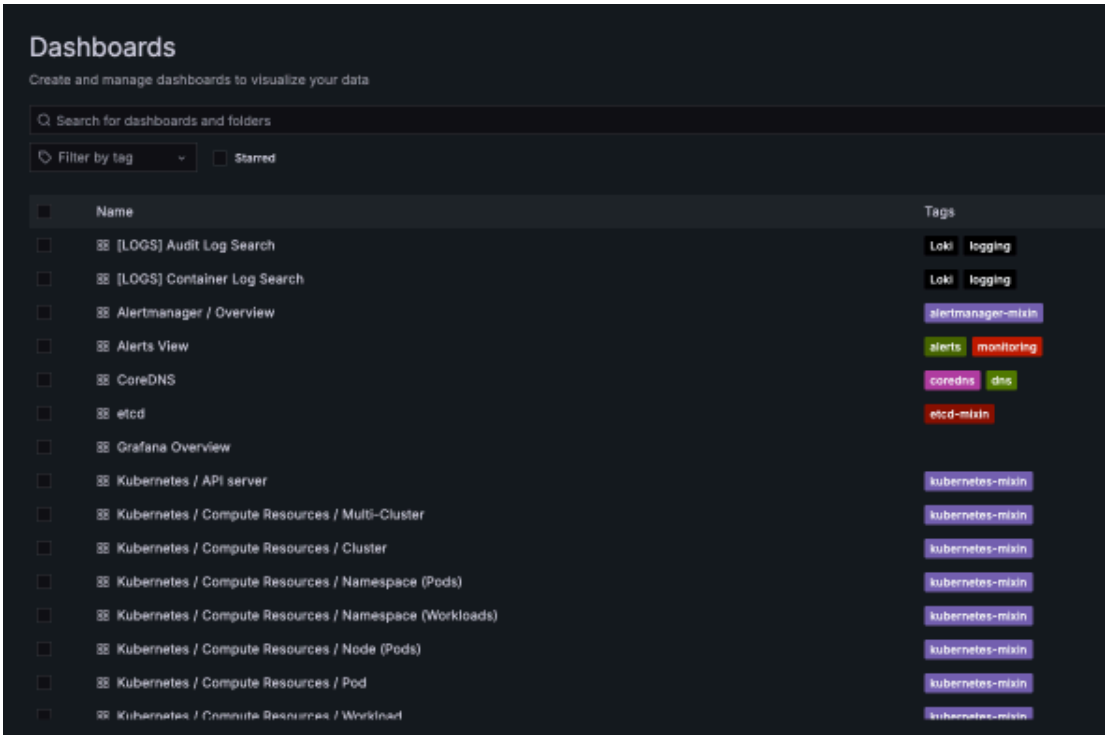
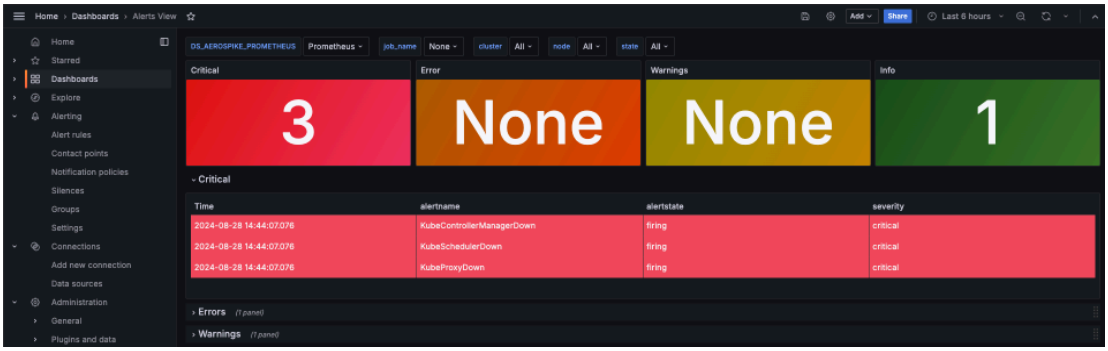
Use this dashboard to:

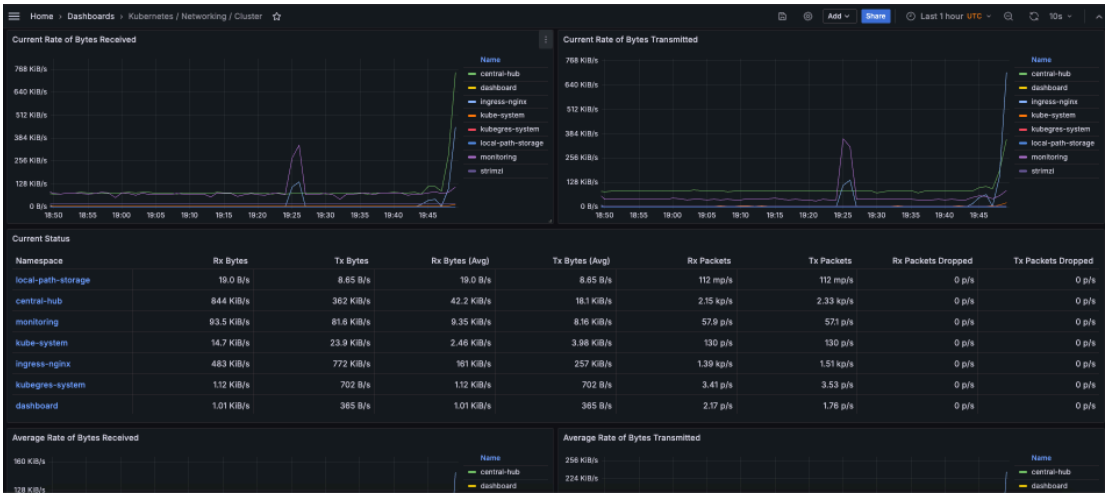
1. View predefined dashboards for CMS services, infrastructure, and network monitoring.
2. Create custom dashboards and alert rules.
3. Search container logs for troubleshooting.
4. Monitor CPU, memory, and disk usage across the cluster.
5. Monitor network traffic and workload distribution.
6. Review audit and proxy logs.
7. Manage user accounts and assign roles (Role-Based Access Control).
8. Integrate with an external Intrusion Detection System (IDS) or Security Information and Event Management (SIEM) solution.

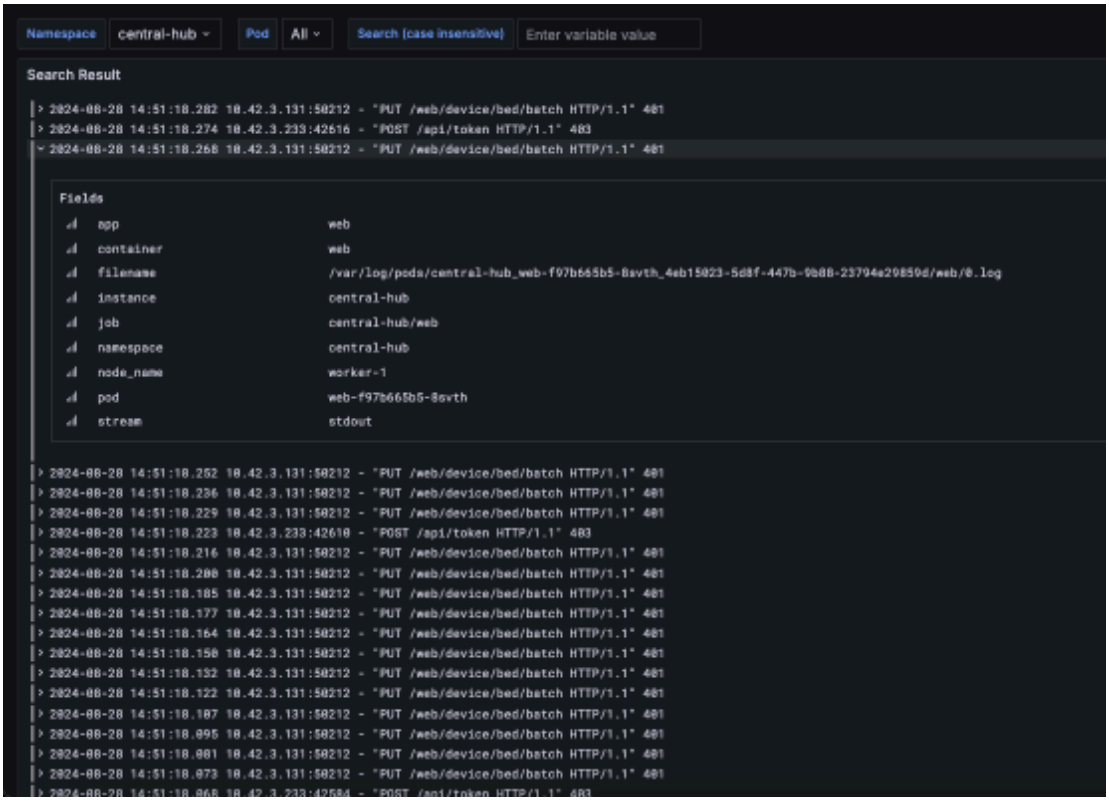
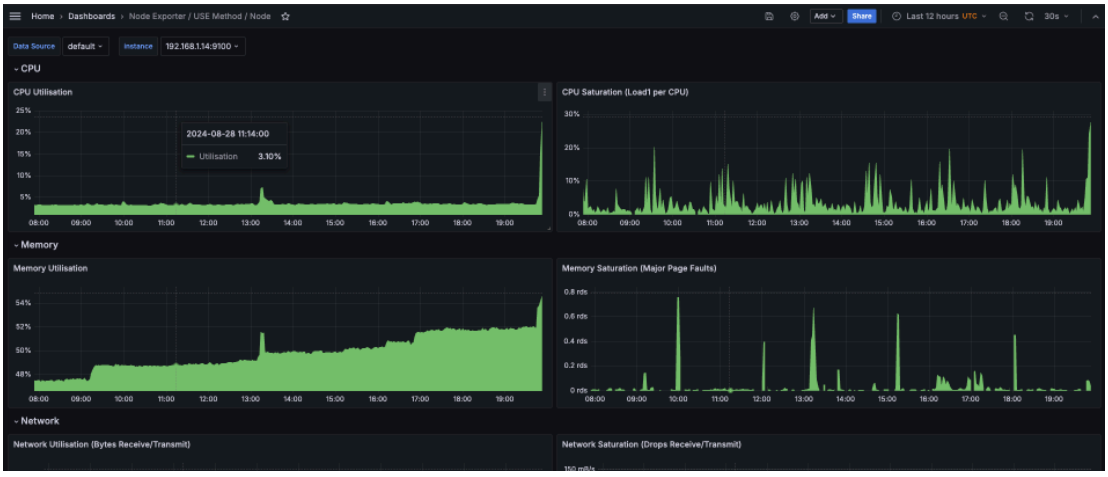
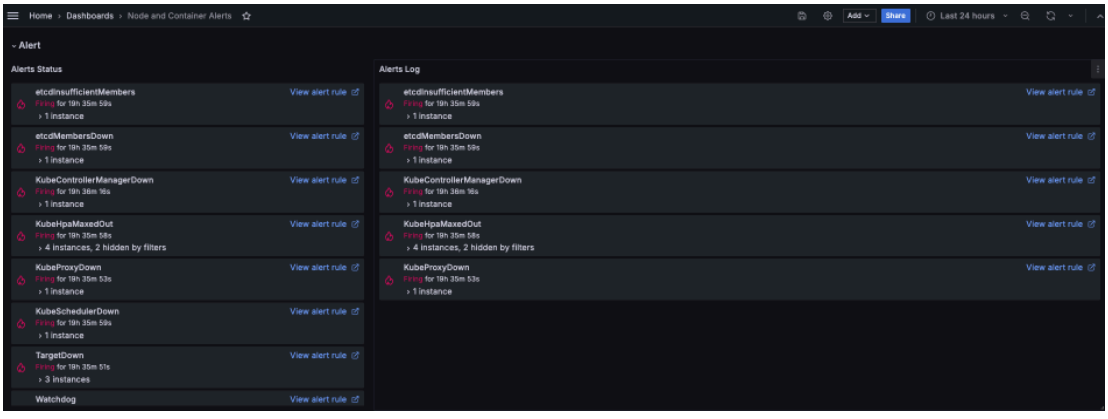
3.2.4 Monitoring Metrics

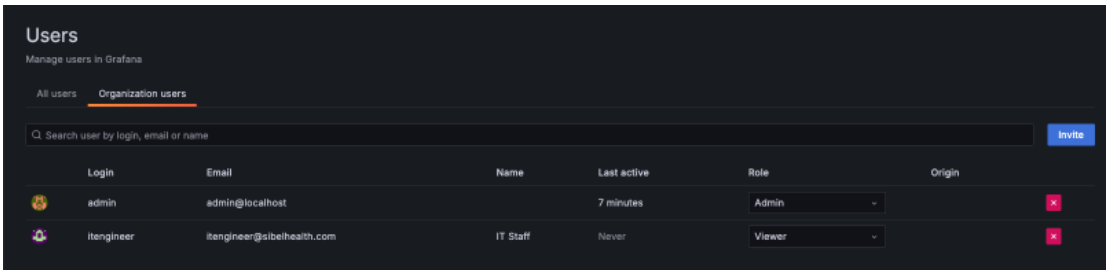
The following metrics and views are available in the Grafana Dashboard:

Table 14: Grafana monitoring metrics

Grafana	Image
Dashboard	
Alert View	

Cluster Resource	
Networking	

Container Logs	
VM Resource	
Node and Service Alerts	

User Creation and Management(RBAC)	

3.2.5 Log Storage

The CMS stores logs in two formats:

- Raw log format:
  - {Timestamp}-{Category}-{severity}-{service_timestamp}-{message}
- JSON log format (load balancer):
  - {"log": "{level} {service_timestamp} {caller} {message} {status} {error message}", "stream": "stderr", "time": "{timestamp}"}

Application logs are stored in /var/log/pods. System-level logs are stored in /var/lib/rancher/rke2/server/logs. Network-level logs from the load balancer are stored in /var/lib/docker/containers/.

The default log rotation configuration is:

- Maximum backup files: 10
- Maximum file size: 100 MB

3.2.6 Security Event Handling

The CMS monitors for the following security events and responds automatically:

Login lockout: After 5 consecutive failed login attempts, the system blocks further attempts for 15 minutes.

Certificate validation: Devices without valid certificates are denied communication with the CMS.

Network overload: If excessive network traffic affects CMS operations, the system pauses data streaming to dashboards and displays an error notification. Active monitoring sessions between sensors and ANNE View Tablets are not interrupted.

These events are logged and visible in the Grafana monitoring dashboards.

3.3 Local MDM Dashboard

3.3.1 Access

The Local MDM Dashboard (Headwind MDM) is available at https://hmdm.<domain>, where <domain> is the CMS domain name configured during installation.

Prerequisite: A DNS A record for hmdm.<domain> must resolve to the Target Server IP.

3.3.2 Authentication

To log in to the Local MDM Dashboard:

1. Open https://hmdm.<domain> in a web browser.
2. Enter the MDM credentials configured during CMS installation. Refer to the CMS Installation Guide for credential details.
3. On first login, the system prompts you to create a new password. Complete this step before proceeding.

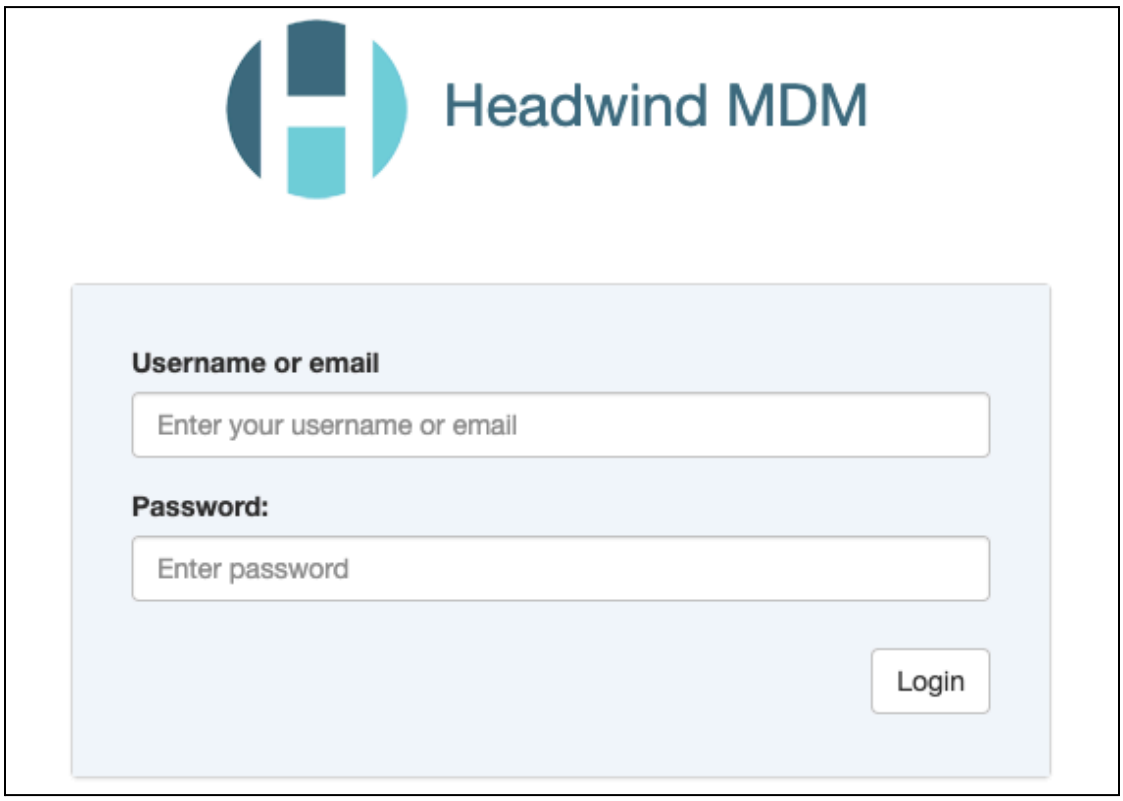


Figure 3: Local MDM dashboard login interface

3.3.3 License and Device Enrollment

A valid MDM license key is required to access the full functionality of the Local MDM Dashboard. The license key is provided by Sibel Health and must be applied after CMS installation is complete.

To enroll and configure ANNE View Tablets:

1. Open the Local MDM Dashboard.
2. Enroll each ANNE View Tablet using the configuration settings provided by Sibel Health.
3. Install the ANNE View application on each enrolled tablet.
4. Enable Kiosk Mode to restrict each tablet to the intended clinical application.

3.4 Admin Hub

3.4.1 Login

The Admin Hub is available at https://cms.<domain>, where <domain> is the CMS domain name configured during installation.

Prerequisite: A DNS A record for cms.<domain> must resolve to the Target Server IP.

To log in:

1. Open https://cms.<domain> in a web browser.
2. Enter the credentials configured during CMS installation. Refer to the CMS Installation Guide for credential details.

NOTE: The IT administrator configures the Admin Hub account and password during installation.

3.4.2 Error Handling

Table 15: Admin Hub login error handling

Error message	Root cause	Recommended user action
Server error. Please try again in a few minutes.	Server error of the system.	Try again later or check the service status. If the issue persists, contact Sibel Health support.
Incorrect password. Please try again.	User inputs wrong password.	Try again with the correct password.
Too many attempts. Please try again in 15 minutes.	User inputs the password failed for at least 5 times.	Try again after 15 mins. If you forgot the password, reset the password.

3.4.3 Sensor Lifetime Dashboard

The Sensor Lifetime Dashboard displays all devices registered in the CMS. The following information is shown for each device:

- Serial number
- Device type
- Device age
- Expiration status
- Last seen timestamp
- The following filters are available:
- Operation status
- Expiring within 7 days
- Recently added in last 24 hours

- Serial number or device type

NOTE: Device age and expiration status are not available for non-Sibel manufactured devices (ANNE View Tablets and OEM devices). In this section, "device" refers to both ANNE View Tablets and sensors.

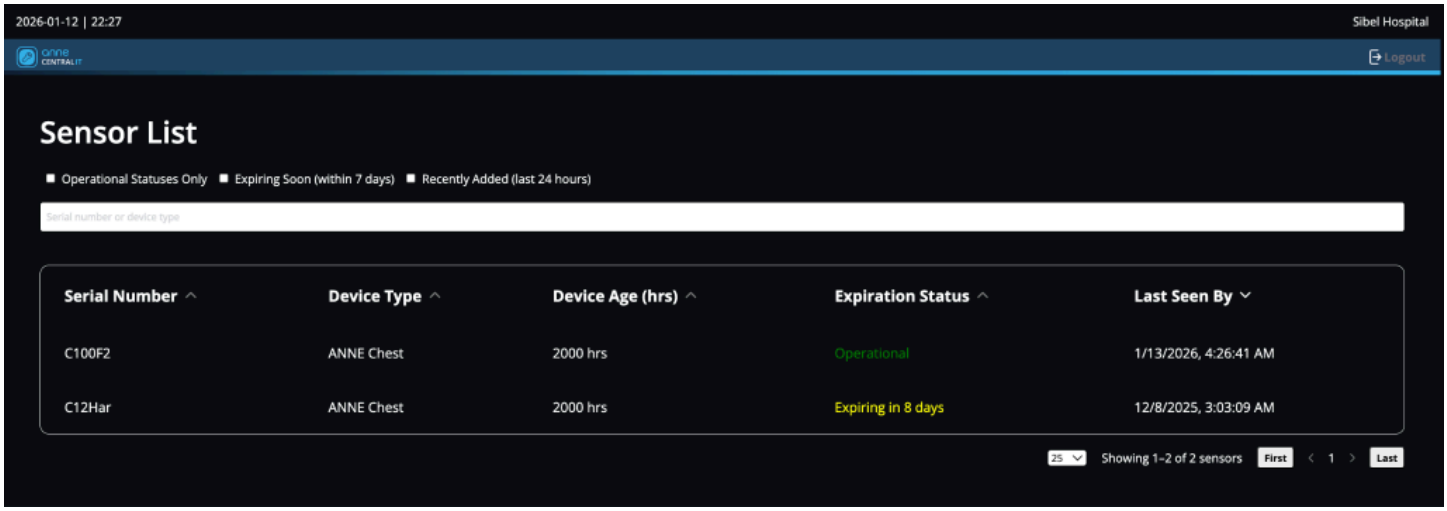


Figure 4: Sensor Lifetime dashboard

3.4.4 Logout

To log out, click the Logout button in the top-right corner of the Admin Hub.

NOTE: The system automatically logs out the user after 15 minutes of inactivity.

Section 4. CMS Maintenance

4.1 CMS Maintenance

4.1.1 CMS Cybersecurity Implementation

The CMS implements the following cybersecurity controls for authentication, data protection, and session management.

- Authentication between ANNE View and Target Server is using the X.509 certificate chain based on certificates and chain validation; only incoming requests from the ANNE View are validated by Target Server. Recommended certificate generation is to use 1 year expiration, using openssl with RSA:4096 encryption.
- No PHI data will be stored in the database of the CMS.
- JSON web token is used for secure data transmission between the CMS web portal and the backend gateway token is valid for 15 minutes and refresh token valid for 7 days.
- The CMS is not using a master key store to avoid the risk of brute force, insecure storage, and side-channel attacks.
- Sibel Health recommends that certificate validity periods range from a minimum of 6 months to a maximum of 1 year, ensuring a balance between security and operational efficiency.

4.1.2 CMS Security Patches

Explicit patches targeting discovered vulnerabilities are required patches and should be updated as soon as they are received. These security related patches will not include new functionality and should be standalone patches to be deployed to secure the product from the vulnerability.

Upon completion and approval of a patch, patch distribution will be provided by Sibel Health to the clients via secure and encrypted media.

CMS security patches can be applied by an IT Administrator with access to the CMS installation. The CMS security patches applicability steps are the same as CMS upgradation steps which is mentioned in MA-00018-C Section 5.

One can verify the latest version using K8s dashboard by checking the image version.

4.1.3 CMS Patches

The patchability rate for CMS updates follow a two-week sprint cycle and hot-fix process. Patch distribution will be provided by Sibel Health.

4.1.4 CMS Version Release

Full version releases of CMS will be generated based on Sibel Health internal development lifecycle. The version release process will follow the proper testing phases (Verification and Validation) in order to produce a release

consisting of new functionality, remediations of anomalies from previous releases, as well as performance improvements. Release distribution will be provided by Sibel Health.

4.1.5 CMS Backup and Recovery

The CMS automatically backs up the PostgreSQL database to the Target Server local filesystem. The backup uses a Kubernetes persistent volume claim (pg-backup-pvc) to store automated database dump files under /opt/local-path-provisioner/ on the Target Server.

Because the CMS runs as a single-node K3s cluster, all backup files reside on the Target Server itself. If the Target Server disk fails, both the database and its backups are lost.

4.1.5.1 Backup Verification

The IT administrator must verify that automated backups are functioning correctly. Connect to the Target Server via SSH to perform the following steps.

- Step 1: Verify the backup volume exists:

```
kubectl get pvc pg-backup-pvc -n central-hub
```

The output must show the PVC in Bound status.

- Step 2: Verify backup files are present and current:

```
ls -l /opt/local-path-provisioner/*pg-backup-pvc/*
```

Verify that recent backup files are present and that file timestamps are within the expected backup interval (within the last 24 hours for daily backups). If files are missing or stale, contact Sibel Health support.

4.1.5.2 Off-Site Backup

The local backups are stored on the same disk as the CMS. To protect against disk failure, copy backup files to a separate, secure storage location on a regular schedule.

NOTE: Copy backup files to off-site storage at least weekly. Store copies in an encrypted location that meets the organization's data protection requirements.

4.1.5.3 Service Recovery

CMS services run as Kubernetes pods on the Target Server. If a pod fails, the Kubernetes cluster automatically creates a replacement pod with its original configuration, restoring the service to full functionality.

If a manual recovery is required, an authenticated and authorized administrator can restore the cluster configuration from the backup.

4.1.6 CMS Event Logging

Sibel Health provides Audit trail logging and monitoring capabilities within its systems and subsystems. These logs and metrics will provide information relating to the health of the systems, performance measures of the systems, as well as anomalies or issues within the components of the systems. These events will be an administrative function and available in the Admin dashboard to check status, logs, metrics, and graphs.

Hospital IT Administrators need to regularly review the logs through a continuous monitoring standard operating procedure.

4.1.7 CMS Cryptography Control

Sibel Health shall manage the lifecycle of keys and certificates via appropriate cryptographic modules; these modules provide encryption, access control, and secure storage of sensitive data. All cryptographic assets will be managed and maintained by Sibel's Information Security Manager, conforming to the recommendation by NIST SP 800-131A, Transitioning the Use of Cryptographic Algorithms and Key Lengths and FIPS 140-3, Security requirements for Cryptographic Modules.

4.1.7.1 Cryptographic Assets Storage

Sibel Health stores and maintains cryptographic assets, keys and certificates, in secure vaults by utilizing advanced encryption algorithms in order to prevent unauthorized access and by ensuring the controlled access to authorized personnel only. The cryptographic module ensures the encrypted backup of stored assets to support the failover mechanism.

In a case where the control of cryptography assets are requested by clients due to their organizations' internal cybersecurity requirements, Sibel Health will inform clients of applying appropriate cryptographic modules following the cybersecurity best practice such as FIPS 140-3, Security requirements for Cryptographic Modules.

- FIPS 140-3 (FIPS 140-2 Section 4.7) describes requirements regarding cryptographic key management.

4.1.7.2 Cryptographic Assets Access Control

All Cryptographic assets shall be encrypted, and the access shall be strictly controlled through Role-Based Access Control (RBAC) policy by Sibel's designated IT/Security Manager; Sibel Health is following the access control policy recommended by FIPS 140-3.

Sibel Health will also provide recommendations to clients for designing their access control policy accordingly. The recommendation by Sibel Health will consider the roles and services:

- IT Administrator (Superuser)
- Serves as a superuser, governs the access control policy and manages the lifecycle of cryptographic assets.
- Healthcare Professionals (User)
- Serves as a user, access to the clinical passwords of CMS.

4.1.7.3 Cryptographic Assets Generation and Renewal (Rotation)

Cryptographic keys and certificates are generated prior to the deployment and during the deployment of CMS.

The keys and certificates that are required prior to the deployment are:

- Digital signature key pairs for both ANNE View and CMS software
- TLS/SSL Certificate chain for secure network communication within CMS
- Sibel's rootCA and IntermediateCA Certificate chain for secure authentication and communication between ANNE View and CMS

Upon client's request on its own cryptography management, Sibel Health will provide the client's IT administrator the following information:

- Cryptography algorithm and protocols
- Cryptography validity

When it comes close to the end of cryptography validity, Sibel Health will renew or rotate the keys and certificates according to NIST SP 800-57 Part1, Recommendation for Key Management, and NIST 1800-16B, Securing Web Transactions.

Sibel Health will track the validity of keys and certificates via the cryptographic module, which will be configured to notify Sibel Health's IT/Security Manager or Cybersecurity Engineer 30 days prior to the key rotation or certification renewal.

Client IT administrators are recommended to execute the key rotation of CMS software according to the cryptoperiod described in Table 16.

Table 16: Cryptoperiod and Certificate Validity Recommendation per Asset Type by NIST SP 800-57 Part1 and NIST SP 1800-16B

Asset Name	**Asset Type**	**Validity / Cryptoperiod**
Key		
Digital Signature	Private Signature Key	1 to 3 years
Digital Signature	Public Signature-Verification Key	Not specified, but follows Private key (1 to 3 years)
User Authentication	Private Authentication Key	1 to 2 years
User Authentication	Public Authentication Key	1 to 2 years
Postgres Encryption Key	Symmetric Data Encryption Keys	3 years
Password		
Postgres Auth Key	Password	1 year
Redis Auth Key		
Admin password		
Admin Dashboard Token		
Monitoring Dashboard Password		
Certificate		
TLS/SSL Certificate	Certificate	3 months
IntermediateCA Certificate		1 year
Sibel's Root CA		3 year

Maintaining secure communication and cryptography within the system requires timely renewal of certificates and key rotation. Certificates should be renewed and validated at least 30 days prior to expiration of the current certificate, and keys should be rotated according to the cryptoperiod. Sibel Health follows the NIST SP 1800-16B guide for renewal of certificates.

The following steps outline the process for renewing certificates and delivering to clients:

- Monitor Certificate Expiration: Sibel Health IT/Security Team checks the certificate expiration date via the cryptographic module on a monthly basis. Sibel Health shall require client IT administrators to timely check the certificate expiry in case of their own management of certificates.
- Generate Certificate Signing Request (CSR): Create a new CSR for the certificate renewal. Use existing private keys or generate new ones to obtain a new certificate.
- Submit CSR to Certificate Authority (CA): Submit the CSR to a trusted CA.
- Obtain New Certificate: Once the validation is complete, receive the new set of certificates.
- Delivery of New Certificate: Sibel Health IT/Security Team will share renewed certificates to client IT administrators via a secure channel.
- Install the Certificate: Install/Replace the new certificate in the CMS system.
- Restart Services: Restart the CMS services to apply the updated certificate.
- Verify System Functionality: Check the CMS system to ensure the new certificates are functioning properly.

Hospital IT administrators are required to execute the key rotation of CMS software. Sibel Health will notify clients when key rotation is due, based on the system installation timeline and using secure email communication.

Once the keys or certificates are successfully replaced or rotated to the system, the hospital IT Administrators should confirm the CMS system functionality and operation.

To ensure the proper functioning of CMS system:

- Admin dashboard IT Admin Validation: Hospital IT Administrators can verify Infrastructure functionality through the Admin Dashboard to ensure all services are operational. A monitoring tool which is installed to support event detection can also be used for validation.
- Admin dashboard Validation: Hospital IT Administrators can verify the basic functionality of the system by checking user authorization and ensuring that the system performs its intended function correctly.

4.1.7.4 Cryptographic Assets Revocation

In case of key/certificate compromise,

- key revocation
- Re-issuance
- reconfiguration

In any event of a key or certificate compromise detected or passed the expiry or cryptoperiod, Sibel Health's IT/Security team shall respond with immediate actions including key revocation, re-issuance, and reconfiguration of impacted systems, and also invoke clients to take immediate actions to mitigate security risks.

The process shall be followed described in Section 4.1.7.3, Cryptographic Assets Generation and Renewal (Rotation):

- Cryptography Generation
- Key Revocation
- Re-issuance of Cryptography
- Replacement
- Verification of operation

4.1.7.5 Cryptographic Assets Deletion/Destruction

For cryptographic keys or certificates that are no longer in use, Sibel Health's IT/Security Manager shall destroy unused cryptographic assets and irrecoverable deletion from the cryptographic module. This prevents any possibility of recovering or reconstructing the cryptographic keys or sensitive data. Sibel Health Follow the guidance in NIST SP 800-88, which provides standards for secure data sanitization.

Sibel Health's IT/Security Manager shall confirm that client IT administrators follow the same protocols to ensure zeroization of cryptographic assets.

4.1.7.6 Key Credential Rotation Procedures

The following procedures describe how to rotate database and service credentials on the CMS. All commands are executed on the Target Server via SSH.

PostgreSQL Password Rotation:

1. Connect to the PostgreSQL pod:

```
kubectl exec -it postgres-0 -n central-hub -- bash
```

2. Connect to the database:

```
PGPASSWORD=${POSTGRES_PASSWORD} psql -U postgres
```

3. Change the password:

```
ALTER USER postgres WITH PASSWORD '<new-password>';
```

4. Exit the database and the pod:

```
exit
```

```
exit
```

5. Update the Kubernetes secrets:

```
kubectl patch secret postgres-creds -n central-hub --patch='{"data":
{"superUserPassword": "'$(echo -n <new-password> | base64 -w0)'"}}'
```

```
kubectl patch secret postgres-creds -n central-hub --patch='{"data":
{"replicationUserPassword": "'$(echo -n '<new-password>' | base64 -w0)'"}}'
```

6. Update the credentials file:

```
echo "superUserPassword = <new-password>" > /tmp/creds/postgres.txt
```

```
echo "replicationUserPassword = <new-password>" >> /tmp/creds/postgres.txt
```

Redis Password Rotation:

Update the Redis Kubernetes secret and credentials file:

```
kubectl patch secret redis-creds -n central-hub --patch='{"data": {"REDIS_PASSWORD":
"'$(echo -n <new-password> | base64 -w0)'"}}'
```

```
echo "REDIS_PASSWORD = <new-password>" > /tmp/creds/redis.txt
```

Kafka User Rotation:

Regenerate the Kafka user credentials:

```
kubectl get ku kafka-user -n central-hub -oyaml | kubectl replace --force -f -
```

Restart CMS Services After Credential Rotation:

After rotating any credential, restart all CMS stateful sets and deployments to apply the changes:

```
sts=$(kubectl get statefulsets -n central-hub --no-headers | awk '{print $1}')
for s in $sts; do kubectl rollout restart sts $s -n central-hub; done
deploys=$(kubectl get deployments -n central-hub --no-headers | awk '{print $1}')
for d in $deploys; do kubectl rollout restart deploy $d -n central-hub; done
```

4.1.7.7 Certificate Replacement Procedures

The following procedures describe how to replace TLS certificates without a full CMS reinstallation. All steps are performed on the Remote Machine using the CMS installer.

Domain TLS Certificate Rotation:

Use this procedure when the HTTPS ingress certificate has expired or the CMS domain has changed:

1. Place the updated fullchain.pem and privkey.pem on the Remote Machine.
2. Launch cms_installer.exe and select Domain certificate rotation.
3. Browse and select the new fullchain.pem (LB Public Key) and privkey.pem (LB Private Key).
4. Confirm and run the rotation.
5. Verify HTTPS access at https://cms.<domain> after completion.

Device Authentication Certificate Rotation:

Use this procedure when Sibel Health delivers updated device authentication certificates. These certificates are provided by Sibel Health; do not generate them.

1. Copy the updated intermediateCA.crt and rootCA.crt to the Remote Machine.
2. Launch cms_installer.exe and select Cryptographic rotation.
3. Browse and select the new intermediateCA.crt (Intermediate certificate) and rootCA.crt (Root CA certificate).
4. Confirm and run the rotation.
5. Verify ANNE View Tablet connectivity after completion.

4.2 Central Monitoring System Decommissioning (EOL)

4.2.1 Central Monitoring System Version Out Of Support

Central Monitoring System versions 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.

4.2.2 Central Monitoring System End of Life

When the Central Monitoring System 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. This describes how to safely remove the application from their installed location as well as options for data erasure.

Before the removal of CMS the backup of the data in Postgres should be taken. The commands could be executed from the installation image OR from the local system which has connectivity with Kubernetes API.

Make sure that the **kubeconfig** file is in the known location and follow the steps below from the Target Server.

1. Create a storage volume in Kubernetes cluster to hold the final backup data.

```
cat <<EOF > pg-backup-final-pvc.yaml
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: pg-backup-final-pvc
  namespace: central-hub
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 5Gi
EOF

kubectl apply -f pg-backup-final-pvc.yaml
```

2. Create a pod with the following commands.

```
cat <<EOF > pgsql-shell-final-backup.yaml
---
apiVersion: v1
kind: Pod
metadata:
  name: pgsql-shell-final-backup
  namespace: central-hub
```

```
spec:
  containers:
  - args:
    - /bin/bash
    - -c
    - sleep infinity
    image: postgres:14.12
    name: pgsql-shell
    envFrom:
    - secretRef:
        name: postgres-creds
    env:
    - name: PGPASSWORD
      valueFrom:
        secretKeyRef:
          name: postgres-creds
          key: superUserPassword
    volumeMounts:
    - mountPath: /var/lib/backup
      name: pg-backup-final-pvc
  volumes:
  - name: pg-backup-final-pvc
    persistentVolumeClaim:
      claimName: pg-backup-final-pvc

EOF

kubectl apply -f pgsql-shell-final-backup.yaml
```

3. The command above will create a pod and one it is running, please execute the following.

```
k exec -it pgsql-shell-final-backup -n central-hub -- bash
pg_dumpall -h postgres -U postgres -c | gzip > /var/lib/backup/final-backup.gz

# upon completion of the command you can exit from the shell

exit
```

4. The backup stores on one of the worker nodes of the Kubernetes cluster. The particular worker node can be found like this.

```
kubectl get pvc pg-backup-final-pvc -o
jsonpath='{.metadata.annotations.volume\.kubernetes\.io/selected-node}' -n central-hub

example output:
worker-1
```

5. The backup can be copied from the Kubernetes worker node to another location (another server) if

required. To do that, connect via SSH to the worker node with the PVC for the backup (see output above).

```
# The backup file location can be found as:

user@worker1:/#
ls -l /opt/local-path-provisioner/*pg-backup-final-pvc/final-backup.gz

-rw-r--r-- 1 root root 243775582 Aug 16 18:26
/opt/local-path-provisioner/pvc-e67622f9-62ef-4d6d-b246-cc5374156990_central-hub_pg-back
up-final-pvc/backup.gz
```

The backups could be copied over from the worker node to the desired location.

Upon copying the backup file from the VM to the desired location the VMs dedicated for CMS can be removed.

- Below are generalized example steps to remove the VMs.
    1. Stop the VM
    2. Detect the Disk mounted with the VM
    3. Remove/Delete the disk - This will wipe all the data from the disk.
    4. Delete the VM

Section 5. Vulnerability Disclosure

5.1 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.

5.2 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

```
-----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.

5.3 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 Sibel'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

5.4 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.