Connex Central Station 1.8.7 Security White Paper

Baxter is committed to protecting the security of our products and the data privacy of our customers. We strive to maintain and improve the security of our devices throughout the product lifecycle, including:

- Security by Design
- Security risk management
- Secure coding
- Security scanning and testing
- Responsible vulnerability disclosure processes
- Vulnerability and threat monitoring
- Security patch management
- Incident response
- Information sharing

Baxter maintains continued vigilance for cybersecurity threats and vulnerabilities affecting our products and services. We are dedicated to ensuring that our customers receive information related to these threats, openness, and actions to maintain the integrity of our products and the protection of patient data. Baxter maintains a global Product Security program focused on designing security best practices into our products and keeping operations secure throughout our product's lifecycle to fulfill these commitments.

Effective security management is a shared responsibility. Our product literature and support teams provide recommended network settings and configurations to enable proper and secure connectivity. We advise customers to conduct a hazard analysis under ISO/IEC 80001 Application of Risk Management for IT-networks Incorporating Medical Devices before deployment to identify and remedy any interoperability issues.

If you would like to report a potential product-related privacy or security issue (incident, breach, or vulnerability), don't hesitate to get in touch with cybersecurityreports@hillrom.com or visit https://www.hillrom.com/en/responsible-disclosures/ for the latest information on known product vulnerabilities and information.

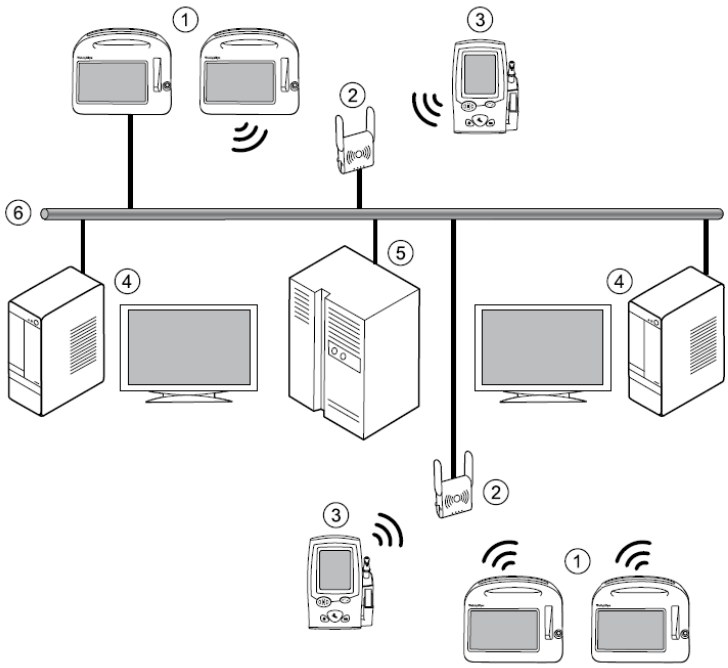
The purpose of this document is to detail how Baxter's security and privacy practices have been applied to the CONNEX CS product, what you should know about maintaining the security of this product, and how we can partner with you to ensure security throughout this product's lifecycle.

Contents

1 Product Description

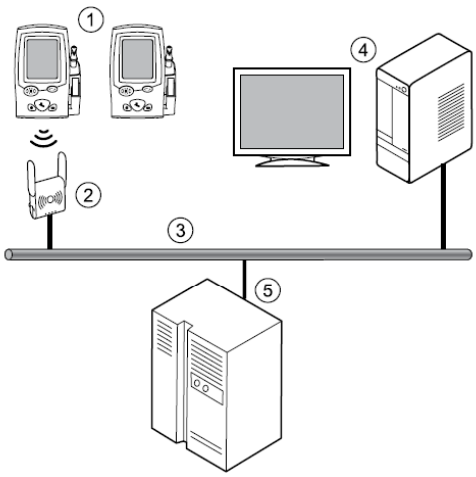
CONNEX CS is a software product that provides clinicians with a means to monitor the vital signs of several patients simultaneously by running on dedicated hardware, such as a computer workstation, and document the vital signs data in other hospital information systems, most notably the EMR. The monitoring station receives patient vital signs and alarm data from compatible patient monitors over a network, then displays the data and alarms, enunciated audibly and visually, acting as an ancillary alarm system.

Server-based system diagram



1. Wired or wireless monitors
2. Wireless access point
3. Wired or wireless episodic device
4. Central station
5. Central station server
6. Network

Server-only system diagram



1. Episodic devices (wired or wireless)
2. Access point
3. Network
4. Customer-provided PC running Connex viewer
5. Connex server

2 Hardware Specifications

CONNEX CS is a software-only product. Customers will need to provide hardware that meets or exceeds the specifications listed in the Connex CS Technical Specifications document provided by their sales representative.

3 Operating Systems

CONNEX CS Workstation runs on Microsoft Windows 10, and CONNEX CS Server runs on Windows Server 2012 R2/2016/2019 64-bit.

4 Third-party Software

The CONNEX CS product has its own Software Bill of Materials (SBOM) with all the software components. SBOM can be made available upon request after the completion of an NDA.

5 Network Ports and Services

CONNEX CS does not provide any network service.
CONNEX CS implements TCP/IP outbound network communication, where the traffic is restricted to:

- IP address of the machine running CONNEX CS service
  Port number at which CONNEX CS service is listening to, plus ports in the ephemeral range [1500-4000]. See table on the following page.

If desired, CONNEX CS application can be run in a network across separate VLANs. A list of required open ports is shown below. The ECS and CCS ports (unsecured or secured) may be disabled as needed by setting the port number to "0" in CS Connection Settings.

Port #	**Protocol**	**Service**	**Firewall:** Inside or Outside	**Application**
53	UDP, TCP	DNS for NRS	I	Optional DNS communication allows Vital sign devices to locate a CONNEX CS system on the network.
7711-7720	UDP	NRS	I	Network Rendezvous Service request/response, data from Vital Signs device to locate CONNEX CS application server
281, 7750	TCP	ECS	I	Episodic Connectivity Service, spot profile data from Vital Signs device. (7750 for secure episodic data connection)
291, 7751 51500-51501	UDP TCP	CCS	I	Continuous Connectivity Service, continuous profile patient data from Vital Signs device. (7751 for secure continuous data connection)
7731, 7732	TCP	Connex Client Services	I	Service interface for managing Patient data, configuration, user account management, and readings. Internal Welch Allyn applications use them.
7733	TCP	ECS	I	Connex ProView remote access to the Connex Server Database.
8001-8099	TCP	Corepoint	I	HL7 data between clients and Enterprise Gateway application.
51500	TCP	AGS	I	Alarm Gateway Service provides alarm messages to a 3rd party system in a data stream.
80 443 & 5938	TCP	TeamViewer Server	O	TeamViewer®
22	TCP	SecureLink Server	O	SecureLink® (On CSAS Server Only)
80 / 443	TCP	Axeda Server	O	Partner Connect agent
3011 & 3030	TCP	N/A	I	Partner Connect remote agent deployment utility
283, 16283 & 7721	TCP	Service Monitor	I	Service Monitor service, device health, and status data from Vital Signs device. (Port 16283 for secure service data connection) Port 7721 is used for CSM Device Upgrades.
1433 1434	TCP UDP	SQL Server	I	Allows Remote SQL Server connection
137-139	UDP	SQL Server	I	SQL file sharing, data and schema transfer port
Port number may vary*	TCP	SQL Server	I	A recommended fixed port on a new SQL instance allows inbound remote connection to the SQL instance.
5094	TCP	Connex License Activation	O	Connection to the Welch Allyn License server during initial setup or for license reactivation
1024-65535	UDP	Lamarr Radio, NRS	I	This is a source port range for UDP communications from NRS back to a Vitals device with a Lamarr radio.
30000-65535	UDP	Newmar Radio, NRS	I	This is a source port range for UDP communications from NRS back to a Vitals device with a Newmar radio.

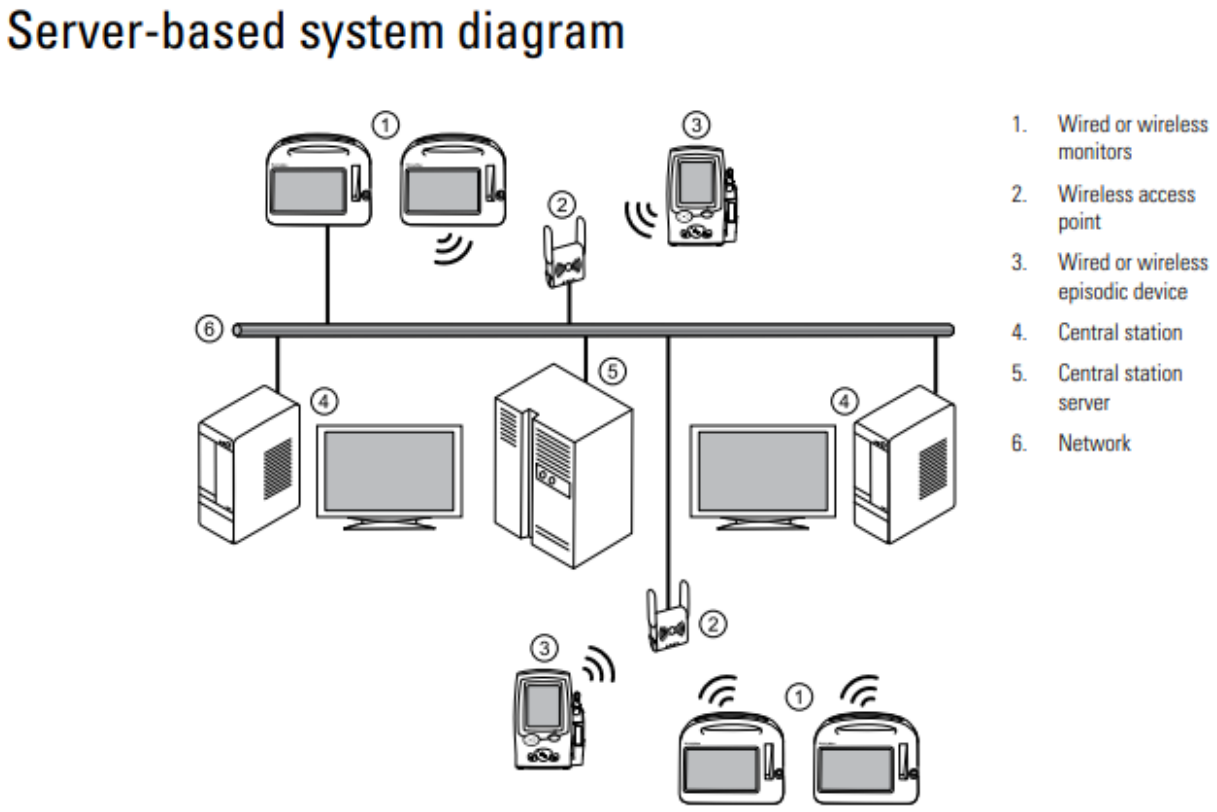
6 Sensitive Data Transmitted

The central station will provide the capability for tracking patient demographics and vitals, including but not limited to: NIBP, NIBP-derived pulse rate, temperature, SpO2, SpO2-derived heart rate, IPI, respiration rate, ECG snapshots, ECG-derived pulse rate, SpHB, and EtCO2.

7 Sensitive Data Stored

The central station will provide the capability for storing patient demographics and vitals, including but not limited to: NIBP, NIBP-derived pulse rate, temperature, SpO2, SpO2-derived heart rate, IPI, respiration rate, ECG snapshots, ECG-derived pulse rate, SpHB, and EtCO2.

8 Network and Data Flow Diagram



9 Malware Protection

CONNEX CS uses Certificate Authority and encryption. Anti-virus and malware software protecting the customer's server is the customer's responsibility.

10 Authentication Authorization

CONNEX CS has a service account intended for Baxter Technical Support Use, though the customer may own the password if they prefer. The product has role-based privilege sets. Users can be created and assign one or more roles. CONNEX CS provides Active Directory and/or Imprivata Confirm ID Medical Device Access authentication for clinicians accessing the vital signs monitors.

The Corepoint Integration Engine included with the product has its own set of users. In Corepoint, only one administrator is required to monitor and configure the application, although more can be created.

SQL Server logins are created for access to the database. Some of these logins may be disabled depending on features being used.

11 Network Controls

N/A. CONNEX CS is software only. The customer controls network communication support.

12 Encryption

Continuous and episodic data connections support server authentication and encryption (TLS/DTLS 1.2) between the system and the vital signs monitors.

CONNEX CS can implement encryption at rest (using SQL Server TDE (Enterprise Edition 2012-2017, Standard Edition 2019). SQL Server Transparent Data Encryption (TDE) supports the following encryption algorithms: AES-128, AES-192, or AES-256.

The product also provides: encryption in transit, user authentication, audit review, and additional security measures.

13 Audit Logging

CONNEX CS provides a primary logging mechanism intended for troubleshooting purposes. It shall log information about the following network communication in a log file:

- Configuration changes
- Connection success or failure
- Device Power ON
- Device Shut Down

These logs are password protected and accessible only by authorized service personnel: they can be moved into a USB drive through CONNEX CS Service screen once the Administrator password has been entered.

14 Remote Connectivity

CONNEX CS does not support remote connectivity.

15 Service Handling

Please refer to the CONNEX CS Service Manual.

16 End-of-Life and End-of-Support

CONNEX CS End-of-Life or End-of-Support dates are not established.

17 Secure Coding Standards

For the development of CONNEX CS, Baxter uses internal practices based on guidelines published by Microsoft.

18 System Hardening Standards

CONNEX CS does not use system hardening standards.

19 Risk Summary

A Software Risk Assessment was completed on the CONNEX CS product. Risks were assessed based on threat, impact, and vulnerability. Vulnerability scanning was completed on the product; no critical vulnerabilities were identified.

In addition, CONNEX CS is enrolled in Hill-Rom's Security Vulnerability Management Process, which routinely monitors our applications for vulnerabilities.

Customer responsibilities were identified in the risk assessment, specifically:

- Implementation of proper network protocols and malware protection

20 Disclaimer

The information contained in this Product Security White Paper is for reference purposes only. Nothing contained in this document or relayed verbally to any customer will be deemed to amend, modify or supersede the terms and conditions of any written agreement between such customer and Baxter or Baxter subsidiaries or affiliates (collectively, "Baxter"). Baxter does not make any promises or guarantees to customers that any of the methods or suggestions described in this Product Security White Paper will restore customers' systems, resolve any issues related to any malicious code or achieve any other stated or intended results. Customer exclusively assumes all risk of utilizing or not utilizing any guidance described in this Product Security White Paper.