

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 1 OF 21</b>

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

Baxter Healthcare 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 Healthcare 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, vulnerabilities, and actions to maintain the integrity of our products and the protection of patient data. In order to fulfill these commitments, Baxter Healthcare maintains a global Product Security program focused on designing security best practices into our products and maintaining secure operations throughout our product's lifecycle.

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 hazards analysis pursuant to ISO/IEC 80001 Application of Risk Management for IT-networks Incorporating Medical Devices prior to deployment in order 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), please contact [productsecurity@Baxter.com](mailto:productsecurity@Baxter.com) or visit <https://www.hillrom.com/en/responsible-disclosures/>.

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 2 OF 21</b>

## Contents

1	Product Description .....	3
2	Hardware Specifications .....	3
3	Operating Systems .....	4
4	Third-party Software .....	4
5	Network Ports and Services .....	5
6	Sensitive Data Transmitted.....	7
7	Sensitive Data Stored .....	7
8	Network and Data Flow Diagram .....	7
9	Malware Protection .....	9
10	Authentication Authorization .....	9
11	Network Controls .....	10
12	Recovery Controls .....	10
13	Encryption .....	11
	FIPS 140.....	11
	Transport Layer Security.....	11
	Data At Rest .....	11
14	Audit Logging .....	12
15	Remote Connectivity .....	13
	Infrastructure Access .....	13
	Electronic Medical Records Access .....	14
	Transport Layer Security (TLS).....	14
	Service Access .....	17
16	Service Handling .....	18
17	End-of-Life and End-of-Support.....	19
18	Secure Coding Standards.....	20
19	System Hardening Standards .....	20
20	Risk Summary .....	20
21	Third Party Certification .....	20
22	Disclaimer .....	20
23	References .....	21

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 3 OF 21</b>

## 1 Product Description



**Figure 1.** Clinician saving physiological data.

The Welch Allyn® Connex® Spot Monitor, Figure 1, is intended to be used by clinicians and medically qualified personnel for monitoring of noninvasive blood pressure, pulse rate, noninvasive functional oxygen saturation of arteriolar hemoglobin (SpO<sub>2</sub>), respiration rate, and body temperature in normal and axillary modes of neonatal, pediatric and adult patients. The most likely locations for patients to be monitored are general med/surg floors, general hospital and alternate care environments.

Connex Spot Monitor performs patient vitals monitoring using integrated sensors and optionally supports a set of Bluetooth wireless sensors. Connex Spot Monitor can be integrated into the facility host systems to securely exchange vital information using wired and wireless interfaces.

## 2 Hardware Specifications

The Connex Spot Monitor (CSM) is designed and built by Baxter as a self-contained medical device. The CSM architecture is based on the TI AM335x Sitara® ARMv8® processor. The CSM's primary user interface is the integrated touch screen and integrated audio system. The monitor includes the following integrated sensors:

- SureBP® blood pressure module,
- SureTemp® or Braun® thermometry module, and
- Optional Masimo®, Nellcor®, or Nonin® SpO<sub>2</sub> module.

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 4 OF 21</b>

The CSM also includes connectivity interfaces, including:

- Ethernet 802.3 100BASE-T interface,
- Optional 802.11 wireless module,
- Optional Bluetooth “Classic” and Low-Energy Module,
- USB 2.0 Host interfaces, and
- USB service interface.

The CSM optionally interfaces to the Accessory Power Management (APM) stand, which provides an additional external power supply. The CSM optionally operates with various USB devices, including scanners and RFID readers; and Bluetooth devices, such as weight scales.

### 3 Operating Systems

The Connex Spot Monitor (CSM) device software is based on Yocto® Linux®. The current release of CSM software, v1.54.xx, uses the Yocto v3.1.

### 4 Third-party Software

A summary of the 3<sup>rd</sup> party software used in the CSM system is shown in *Table 1*. If the complete Software Bill of Materials (SBOM) is required, contact your Baxter representative for access instructions.

*Table 1. Third Party Software in CSM*

Vendor and Name	Version	Usage
Busybox	1.31.1	Base OS tools
GNU LibC 6	2.30	GNU C library
LibCrypto	1.1.1L	Cryptographic function library
LibCURL 4	7.69.1	Download software updates
LibLDAP	2.4.2	Query active directory
Linux Kernel	5.4.106	Linux kernel and base operating system
OpenSSL	1.1.1L	Certificate management, TLS connections
SystemD	244.5	System management
Yocto	3.1	Build system and Board Support Package

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 5 OF 21</b>

## 5 Network Ports and Services

The Connex Spot Monitor (CSM) interoperates with a broad array of different protocols. Network access is broadly characterized into network configuration protocols (DHCP, DNS, and NTP) host system access (HL7, Connect CS), and Smart Care Remote Management.

When so configured, the CSM will accept incoming requests as shown in *Table 2*. Unless the CSM initiates a connection request, all incoming and forwarding traffic is denied or dropped. Likewise, the CSM will open outgoing connections to remote services using the port numbers shown in *Table 3*. Destination endpoints for outgoing traffic is customer configured.

*Table 2. Inbound Network Ports and Services*

Port	Protocol	Service Name	Description of Service	Encrypted	Open/Closed
53	UDP	Domain Name System (DNS)	Resolve host names to IP addresses.	No	Open
68	UDP	Dynamic Host Configuration Protocol (DHCP)	Configure IP addresses, lookup EMR information in extended record.	No	Open
5900	TCP	Remote Display	Read-Only screen sharing through VNC.	No	Default disabled / closed.
7711-7720	UDP	Network Rendezvous Service	Select central station for network alarms & nurse call.	No	Default disabled, configurable.

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 6 OF 21</b>

Table 3. Outbound Typical Ports and Services

Port	Protocol	Service Name	Description of Service	Encrypted
53	TCP/UDP	Domain Name Service	Resolve host names to IP addresses.	No
68	UDP	DHCP	Request configuration lease.	No
123	UDP	Network Time Protocol	Time synchronization.	No
281	TCP	Episodic/HL7	Host for sending episodic monitoring data.	No
7750				Yes
283	TCP	Service Monitor	Remote service management.	Yes
389	TCP	Active Directory	Clinician authentication.	Yes
443	TCP	Software Update	Download software upgrade files from designated source.	Yes
8001-8099	HL7	HL7 EMR	EMR Access over HL7	Yes

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 7 OF 21</b>

## 6 Sensitive Data Transmitted

The Connex Spot Monitor (CSM) is designed to securely transmit sensitive data, including personally identifiable information (PII) and personal health information (PHI). Personal information includes:

- Patient identifiers such as medical record number, name, and date of birth,
- Patient location including room and bed, and
- Patient vitals including:
  - data collected using device sensors,
  - manually entered vitals reading,
  - modifiers, and
  - custom scores.

Other sensitive data that is optionally transmitted during configuration includes Active Directory credentials, client device certificates and private keys, and radio certificates and private keys.

## 7 Sensitive Data Stored

The Connex Spot Monitor (CSM) stores sensitive data, including personally identifying information (PII) and personal health information (PHI). Personal information includes:

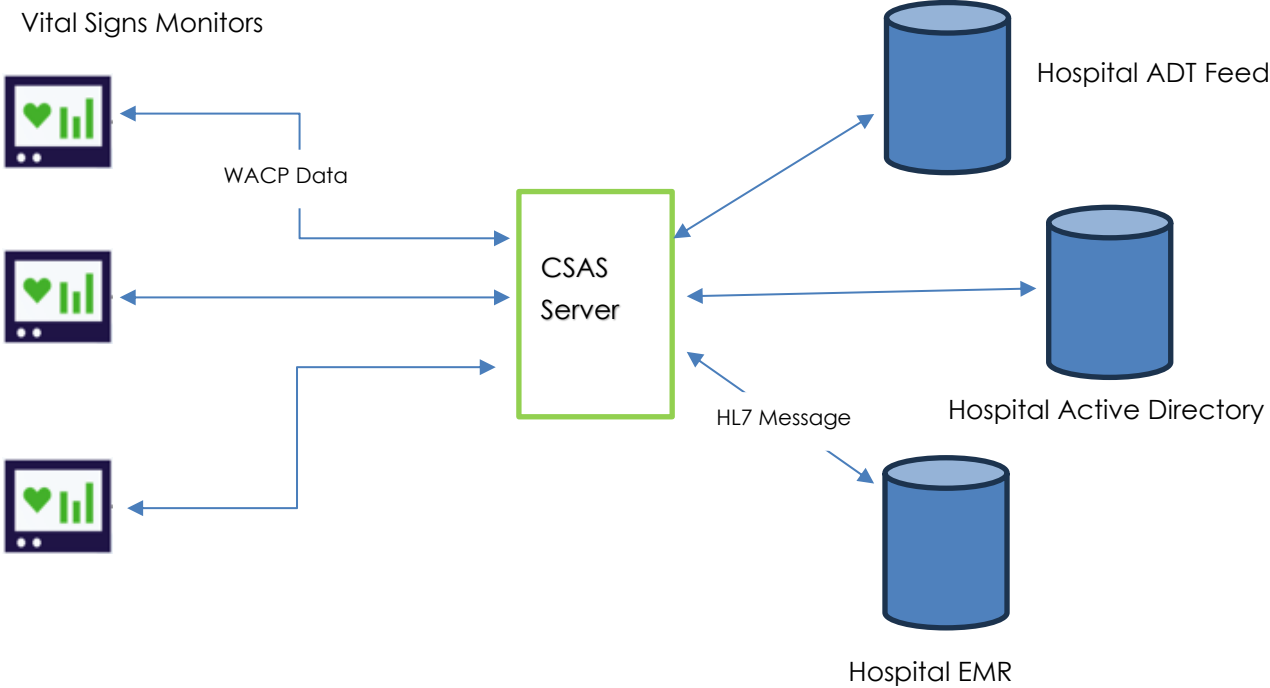
- Patient identifiers such as medical record number, name, and date of birth,
- Patient location includes room and bed,
- Patient vitals including:
  - data collected using device sensors,
  - manually entered vitals reading,
  - modifiers, and
  - custom scores.

Other sensitive data includes stored configuration values that optionally include Active Directory credentials, client device certificates and private keys, and radio certificates and private keys.

## 8 Network and Data Flow Diagram

Please refer to Figure 2 below for a high-level data flow diagram. Figure 3 depicts the intended workflow of the CSM.

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>	
			<b>ISSUE DATE: SEE STAMP</b>	
			<b>EFFECTIVE DATE: SEE STAMP</b>	
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 8 OF 21</b>	



**Figure 2.** High-level CSM Data Flow



<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 9 OF 21</b>



**Figure 3.** Intended CSM Workflow

## 9 Malware Protection

As an embedded device, the CSM does not have the ability to run additional, user-provided programs, and thus the traditional forms of malware protections do not apply. However, the CSM uses several important mitigations to make it more difficult to exploit any vulnerability in the software, including:

- Spectre mitigations (BPIALL workaround),
- Kernel Address Space Layout Randomization (KASLR),
- Linux Security Framework (LSF),
- Hardware Random Number Generator (HRNG).

## 10 Authentication Authorization

The CSM supports a flexible combination of authentication options, including:

- No clinician credentials required,
- Clinician enters identifier,
- Clinician identifiers must match EMR,
- Single-Sign-On with Active Directory®,
- RFID badge access with Imprivata®.

The CSM restricts access to non-clinical workflows, advanced settings, and configuration tools through an advanced settings password that is set by the facility.

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 10 OF 21</b>

By using Public Key Infrastructure (PKI), the CSM can authenticate to EMR and service end-points:

- server authentication against a set of configured certificate authorities,
- mutual authentication through client keys and server certificates.

The CSM also uses PKI to protect access to wireless networks, using certificates to:

- validate the Wi-Fi access points, and
- authenticate the CSM when joining to the network.

## 11 Network Controls

The wireless interfaces in the CSM are protected by internal Linux firewalls. The firewall is used to block unnecessary access to internal ports, as well as impose rate-limiting to harden the system against denial-of-service (DOS) attacks.

## 12 Recovery Controls

In the case of an anomalous event during upgrade, the CSM has backup capabilities for software and configuration files. The CSM has a software rollback feature that allows the last known successful installation to be restored. However, if software version 1.54.xx has been successfully loaded on the CSM, the software will not allow a rollback to an older version of software to keep users on a supported operating system. The software version rollback capabilities are outlined in Table 4.

*Table 4: Software Version Rollback Capabilities*

Base Software Version	Upgradable?	Downgradeable?
1.00.00 – 1.52.01	Yes	Yes, software can be downgraded to any previous version
1.54.00 or above	Yes	No, once upgraded to 1.54.00 or higher, software cannot be downgraded to a version lower than 1.54.00.

The instructions for the software rollback feature can be found in the Connex Spot Monitor Software Version 1.5X, Service Manual. In addition, if a new configuration file fails to be written on the device, the last known successful configuration is used on the next device reboot. As a backup mechanism, configuration files can be saved to a USB from the CSM device. More information on disaster recovery of the CSM device can be found in the Manufacturer Disclosure Statement for Medical Device Security – MDS2 for CSM software version 1.54.

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 11 OF 21</b>

## 13 Encryption

The CSM uses encryption to protect sensitive health information and device configuration data. To protect sensitive health information at rest, patient data is stored in an encrypted file within the device. To protect configuration data during transport and storage, the Welch Allyn Configuration Tool stores data in an encrypted bundle. The bundle is transported to the device, which extracts information from the encrypted bundle as needed.

### FIPS 140

When the wireless radio module operates in FIPS 140 mode, the module utilizes FIPS-approved encryption algorithms when associating with the facility's infrastructure. The module also uses FIPS-approved encryption algorithms to store configuration information including certificates and credentials.

### Transport Layer Security

When so configured, the CSM will use Transport Layer Security (TLS) to encrypt communications with remote hosts. The CSM uses TLS 1.3, the most recent version of the standard. TLS 1.3 will interoperate with older TLS 1.2 hosts. Following best practices, the CSM only supports a subset of the most secure ciphers (Please refer to *Table 5*). The CSM does not support TLS version 1.1 or prior.

*Table 5. Ciphers Supported by Transport Layer Security (TLS) in Connex Spot Monitor*

<b>TLS Version</b>	<b>Ciphers Supported by CSM</b>
TLS & DTLS 1.3	AES_256_GCM_SHA384, CHACHA20_POLY1305_SHA256, AES_128_GCM_SHA256, AES_128_CCM_8_SHA256, AES_128_CCM_SHA256
TLS & DTLS 1.2	TLS_ECDHE_RSA_AES256_GCM_SHA384, TLS_ECDHE_RSA_AES256_CBC_SHA384

### Data At Rest

The CSM protects data at rest using AES-256 encryption to ensure confidentiality of patient data stored internally. The CSM uses AES-256 to ensure confidentiality, integrity, and authenticity of configuration data when imported or exported.

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 12 OF 21</b>

## 14 Audit Logging

The CSM has a comprehensive device activity log which records important events, including auditable events to the device log files. Auditable events must be logged on the system side, as the device itself does not support the long-term storage required for audit logging. Logged events include the date and time stamp of the event. Each event includes the subsystem that generated the event, as well as a textual description of the event, including but not limited to:

Hardware and Operating System Auditing:

- hardware changes,
- system startup and shutdown,
- accessory connection attempts,
- time synchronizations,
- power and battery status changes,
- configuration file import or export.

User Interface Events:

- user selection that results in UI state change,
- clinicians log in / log out including entry method,
- patient entry, and
- creation of patient record.

Connectivity Events:

- changes to network configuration,
- changes to wired or wireless network connectivity,
  - wireless disconnects include last RSSI and AP MAC,
- wireless roaming events including AP MAC and RSSI values for APs,
- dynamic host configuration protocol (DHCP) events,
- rendezvous with host system, and
- USB and Bluetooth connections to PC.

Medical Functions:

- sensor readings,
- selection of automatic intervals program,
- physiological alarms, including who acknowledged or cleared the alarm,

Connected Workflows:

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 13 OF 21</b>

- match entered patient ID to host system,
- query patient records attempt from host system,
- match clinician id attempts with host system,
- verify single-sign-on attempts,
- attempts to send a saved patient record,

The software deidentifies any PHI prior to writing the data to the audit file. The CSM writes its audit logs to internal storage that is inaccessible to an end-user. The CSM will store up to 14 days of audit log history before automatically clearing the prior logs. Using the service interfaces, the facility can export the log files to a connected USB stick or via a secure remote connection to Smart Care Remote Management platform. More information on instructions for interpreting CSM log files can be found in the Connex Spot Monitor Software Version 1.5X, Service Manual.

More information about CSM audit controls can be found in the Manufacturer Disclosure Statement for Medical Device Security – MDS2 for CSM software version 1.54.

## 15 Remote Connectivity

While the CSM can operate entirely independently of network resources, the CSM can greatly enhance clinical and service workflows when operating in a connected environment. Through configuration, the facility can customize how the CSM operates with networked resources. Instructions on user-configurable network settings such as CA Root certificate configuration, Active Directory setup, instructions for restoring factory default settings, and instructions for changing the Advanced settings passcode can be found in the Connex Spot Monitor Software Version 1.5X, Service Manual.

### Infrastructure Access

The CSM supports several common enterprise network communications and configuration protocols as summarized in *Table 6*.

*Table 6. Network Infrastructure Protocols*

<b>Service / Protocol</b>	<b>Reason</b>
EAP & PEAP	Joining enterprise wireless network
Dynamic Host Configuration Protocol (DHCP)	Network configuration
Domain Name System (DNS)	IP Address resolution
Network Time Protocol (NTP)	Time synchronization

### **Wireless Ethernet (802.11)**

The optional wireless ethernet module supports communications over 802.11 a, b, g, and n. The

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 14 OF 21</b>

facility can selected Wi-Fi Protected Access (WPA2). The facility can configure PSK, Dynamic EAP-FAST, EAP-TLS, EAP-TTLS, PEAP-GTC1, PEAP MSCHAPv2, and PEAP-TLS. Based on the selected algorithm, the CSM will use pre-shared keys, stored authentication credentials, and/or device certificates to authenticate to the wireless infrastructure.

#### ***Dynamic Host Configuration Protocol (DHCP)***

The CSM can be configured to use static host configuration or the Dynamic Host Configuration Protocol (DHCP). The DHCP can be used on either the wired or wireless ethernet networks.

#### ***Domain Name System (DNS)***

When configured, the CSM will use the Domain Name System (DNS) to resolve host names into IP addresses.

### **Electronic Medical Records Access**


The CSM can be configured to interface to common Electronic Medical Record (EMR) systems directly using Health Level 7 (HL7) or through a gateway service such as Welch Allyn Connex CS. These services are summarized in *Table 7*.

#### **Transport Layer Security (TLS)**

*Table 7. Electronic Medical Records Access*

<b>Service / Protocol</b>	<b>Reason</b>
Health Level 7	Clinician & patient query, send saved readings.
Welch Allyn Connex CS	Clinician & patient query, send saved readings, and optionally time synchronization, Imprivata for badge and barcode scanning.
Active Directory (LDAP)	Clinician query and authentication.
Network Rendezvous Service (NRS)	Select a Connex CS instance.
Domain Name System (DNS)	Select a Connex CS instance using SRV records.
Dynamic Host Configuration (DHCP)	Select a Connex CS instance using vendor options.
USB and Bluetooth to PC	Send saved readings to connected PC.

Whether connecting to an HL7 or Connex CS remote system, the facility can configure the connection's security. The facility can configure whether to use an open channel or to enable TLS encryption. When enabling TLS encryption, the facility can configure the CSM to use server verification. In this mode, the CSM will verify that the server's certificates are authentically issued by a certificate authority (CA). The facility may choose to load their own root CA certificates or accept the provided CA certificates. The list of default CAs is available upon request.

	80031640	REVISION: A	BAXTER DHF: 90102328
			ISSUE DATE: SEE STAMP
			EFFECTIVE DATE: SEE STAMP
TITLE: Connex Spot Monitor SECURITY WHITE PAPER			PAGE 15 OF 21

For version 1.54.xx of the CSM software, the facility may also enable mutual authentication through use of client certificates. In this mode, when the CSM negotiates the TLS session, the CSM will use the configured client certificate when establishing the connection to the remote system. This allows the CSM to verify that the host is authentic and the host to verify that the CSM is authentic.

#### ***Health Level 7 (HL7)***

When configured to use HL7, the CSM will connect directly to the configured EMR using the HL7 protocol. Typically, these connections are made using TCP/IP over ports 8001 through 8099, although the facility can select additional ports.

#### ***Welch Allyn Connex CS***

When configured to use Connex CS, the CSM will connect to a Connex CS server that is maintained by the facility. Often, the Connex CS server operates as an integrator or front-end to another EMR system. The Connex CS service typically uses two different port numbers: 281 for an unencrypted connection, and 7750 for a TLS protected connection.

Facilities may have multiple Connex CS instances, and the hostname and port numbers may be different for each. In these cases, the facility can configure the CSM to use: static, DNS, DHCP, and NRS to select the proper Connex CS instance.

#### **Static Configuration**

Where the facility uses the static configuration, the single hostname (or IP address) and port number are stored in the CSM configuration file.

#### **DNS Configuration**

Where the facility uses the DNS method, the facility will configure the service identifier, and then the CSM will query the DNS system for a "SRV" record with the location and port of the Connex CS server.

#### **DHCP Configuration**

Where the facility uses the DHCP method, the facility will configure the service and port number in the vendor-specific option of the DHCP record. The CSM will extract the hostname and port number from the DHCP lease.

It is recommended that specific IP addresses are reserved for devices based on their MAC addresses in the DHCP server configuration to ensure consistent and conflict-free IP assignments. In addition, the following DHCP configurations are recommended:

- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are implemented on the device network to block abnormal DHCP traffic.

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 16 OF 21</b>

- DHCP rate limiting is implemented on the DHCP server to restrict the number of requests from a single source within a given amount of time.

### **NRS Configuration**

Where the facility configures the use of the Network Rendezvous Service (NRS), the CSM will use the hostname and port number contained in the NRS broadcast message. The Network Rendezvous Service is a network service that provides information about other available network services to allow a client to connect to and use these services. The CSM device uses NRS to find its assigned WACP server via network unicast. Because this service connection is unencrypted, it is recommended that customers use the DNS (Domain Name Service)/DHCP (Dynamic Host Configuration Protocol) and Host IP option instead of NRS. Customers can manually configure this service connection. It is also recommended customers employ TLS 1.2 encryption to ensure network configuration data is adequately protected. Client and server authentication controls are also in place to confirm the identities of clients and servers through certificate verification. The CSM can be configured to use the Connex CS as a proxy for an Imprivata® service. When the clinician uses an accessory barcode or RFID scanner for authentication, the CSM will use the Connex CS connection to verify the clinician using Imprivata.

### **Active Directory**

The facility can configure the CSM for Single-Sign-On (SSO) using Active Directory®. In this mode, when clinicians enter a username and password, the CSM will perform a query in Active Directory using the configured credentials to authenticate the clinician's entered name and password. As with EMR access, this connection can be protected by TLS and supports host certificate verification.

### **Point to Point USB and Bluetooth Connections**

The CSM can also laptop-connect via Bluetooth or tethered over USB to access a Connex CS server. In this mode, the CSM will only connect to the tethered device to send saved records. Access to both the Bluetooth and USB ports is initially enabled but can be disabled by the facility through configuration.



<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 17 OF 21</b>

## Service Access

The CSM supports several service interfaces, including: the Welch Allyn Service Monitor®, remote display capability, Smart Care Remote Management and software upgrade. Please refer to *Table 8* for a summary.

*Table 8. Service Access*

<b>Service</b>	<b>Reason</b>
Service Monitor	Remote management (includes device configuration, view of current device status, receipt of alarms). Acts as proxy to SCRM.
Remote Display (VNC)	Training and troubleshooting
Software Upgrade	Improve functions, fix bugs. Performed via SCRM and WAST
Smart Care Remote Management	Preventative maintenance, software updates. Connects to CSM via service monitor middleware.
Welch Allyn Service Tool	Calibration (if licensed), accuracy checks, software updates, service information download

The Service Monitor is an agent installed in the facility's network that acts as a proxy to the Welch Allyn Smart Care Remote Management® (SCRM) portal. The SCRM service allows the facility to perform service tasks such as device configuration and software upgrades, receive technical alarms, and view the current device status. When configured to use the service portal, the CSM will connect to the configured local Service Monitor agent to exchange information. The CSM will typically only connect to an intranet-based local Service Monitor. Starting with version 1.54.xx, this connection is protected using TLS.

## Remote Display

The CSM supports an optional remote display feature (VNC). When the facility enables this feature, a clinician can share the display of their CSM. The software will generate a one-time-password (OTP) that the facility's service personnel will need to use to access the display. The display is only available when enabled by the facility and initiated by the clinician. To protect the integrity of clinical workflow, the VNC server is restricted to remote viewing only. No remote interaction with the display controls is available to the remote viewer. When the clinician terminates the session, the remote display is also disabled.

VNC is for service use only. It is not intended for clinical use and is not encrypted. No PHI or PII should be shared across the VNC connection, and no patient information should be displayed on the device when the VNC connection is initiated. The VNC connection is temporary and can only be accessed via the Advanced menu.

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 18 OF 21</b>

### ***Smart Care Remote Management***

The CSM can be configured to operate with the *Smart Care Remote Management* cloud-based service. When so configured, the CSM will periodically connect to Service Monitor, a local service agent middleware to the Smart Care Remote Management platform. The CSM will send preventative maintenance information and product log files. Using the SCRM platform, customers command their fleet of CSM devices to update to a new version of software or apply new configuration files. The CSM does not communicate directly with the SCRM platform, but rather to a service agent that runs on the customers' network. Communications between the CSM, the local service agent, and the SCRM platform utilize TLS to encrypt the connection and to verify the authenticity of the remote hosts.

### ***Software Upgrade***

The CSM supports over-the-air (OTA) software upgrades using SCRM, as well as locally initiated software upgrades using the Welch Allyn Service Tool (WAST). In either case, a URL to the software upgrade files is sent to the CSM. When the CSM initiates a software upgrade, the CSM will open a TLS connection to the provided URL to retrieve the necessary files and perform a software upgrade. The facility can provide a URL that is within the facility's intranet or an external location. Further instructions on software upgrades are available in both the Connex Spot Monitor Software Version 1.5X, Service Manual and the Welch Allyn Service Tool, Installation and Configuration Guide.

### ***Welch Allyn Service Tool (WAST)***

WAST is a software application on a PC that interfaces with the device to perform software upgrades and download service information from the device. The WAST interface allows users to connect to, identify, and obtain information from the CSM, to verify and/or calibrate the device, to update/upgrade the device and configure the device.

## **16 Service Handling**

The CSM requires periodic maintenance including accuracy checks and calibration. The customer's technicians can perform many of these functions using existing tools such as the *Welch Allyn Service Tool* or the *Smart Care Remote Management* (see previous section). Routine maintenance or device failures may be carried out by Baxter or its subsidiaries. This work may be done on-site, or the device may be sent to the service center for repair. More information on securely decommissioning devices or safely sanitizing information from the CSM device when leaving customer control can be found in Connex Spot Software Version 1.5X, Instructions for Use.

### ***Customers' Technician / Service Access***

The customers' technicians can access the clinical user interface and, after entering a passphrase, access the advanced settings features of the user interface. Using this special

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 19 OF 21</b>

operation mode, the technician can export log files to a USB thumb drive, import encrypted configuration files, and device certificates. While in this mode, the technician has access to the same PHI / PII as a logged in clinician. Prior to service or access by a technician, the CSM should be cleared of all exams in the 'Review' tab. The CSM should not be in clinical use while service is performed.

The customer's technicians can also access a special service mode using a PC running the *Welch Allyn Configuration Tool*® application and a tethered USB connection. The technician can use this tool to upgrade the software, carry out accuracy checks, confirm device functionality, and if licensed, calibrate the device.

### ***Repair and Maintenance through Service Centers***

There are times when a CSM must be sent to a Service Center for repair. When this happens, a Return Material Authorization (RMA) is generated to track the CSM through the service center. The RMA process provides identification of the product and issue; and facilitates return of the device to the customer. Where possible, the customer is instructed to reset the advanced settings password to enable the service center's access to the device or perform a factory reset. Where this isn't possible, the CSM will be reset to factory settings to complete repair work. As a courtesy, the service center may reload a customer's configuration file back onto the device.

Baxter protects any PHI/PII stored on a device that is returned for service. Unless needed for investigational purposes, Baxter will not share/use/divulge any PHI/PII from any device returned for service. Further, all Baxter employees are trained and required to maintain compliance with HIPAA standards. In rare cases, such as investigations and with customer's knowledge and consent, access to stored data may be performed by Baxter engineers and/or Service Technicians.

## **17 End-of-Life and End-of-Support**

Baxter will support and maintain the CSM by releasing updated software as appropriate for features and or security patches. Baxter supports service on its products after the end of manufacture. There is no planned end of manufacture date for the CSM. Service timelines based on region are listed below:

- 5 years: US, Canada, Australia, LATAM (all except Colombia/ Brazil)
- 7 Years: EMEA (standard except Italy), APAC (all except ANZ/ Japan/ Thailand)
- 10 years: APAC – Japan & Thailand, LATAM – Colombia & Brazil, EMEA – Italy, EMEA (government tendered contracts)

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 20 OF 21</b>

## 18 Secure Coding Standards

The CSM is developed by Baxter using a variety of languages, including C, Python, and primarily C++. The software development lifecycle is compliant with IEC 62304. Additionally, Baxter standard operating procedures include static code analysis and expert code review. Static code analysis includes using up-to-date compilers that are capable of static code analysis, as well as the Fortify Static Code Analysis (SCA) tool. Expert code reviews are conducted by subject matter experts to ensure code quality and compliance to standards.

## 19 System Hardening Standards

The CSM is hardened according to the following industry standards:

- IEC 80001-2-2
- ISO IEC 27001
- ISO IEC 62304

Security requirements are incorporated into the product requirements based on the 19 IEC security capabilities from IEC 80001-2-2. These capabilities map directly to NIST SP 800-53. Other controls are considered based upon the output of the Security Risk Assessment (SRA).

## 20 Risk Summary

A security risk assessment was completed for the Connex Spot Monitor. Risks were assessed based on threats, impacts, and vulnerabilities. Vulnerability scanning was conducted by the Baxter security team and no findings were identified. A penetration test was also performed by a third party in which no high or critical risk items were identified. Reports can be made available upon request.

## 21 Third Party Certification

The CSM device does not have any third-party ancillary certifications.

## 22 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 customer that any of the methods or suggestions described in this Product Security White Paper will restore customer's systems, resolve any issues related to any

<b>Baxter</b>	<b>80031640</b>	<b>REVISION: A</b>	<b>BAXTER DHF: 90102328</b>
			<b>ISSUE DATE: SEE STAMP</b>
			<b>EFFECTIVE DATE: SEE STAMP</b>
<b>TITLE: Connex Spot Monitor SECURITY WHITE PAPER</b>			<b>PAGE 21 OF 21</b>

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.

## 23 References

The following documents are referenced in this White Paper:

- Connex Spot Monitor Software Version 1.5x, Service Manual
- Welch Allyn Service Tool, Installation and Configuration Guide
- Manufacturer Disclosure Statement for Medical Device Security – MDS2 – CSM SW 1.54 – For the MDS2 contact Hillrom Technical Support: <https://hillrom.com/en-us/about-us/locations/>
- Connex Spot Monitor Software Version 1.5X, Instructions for Use