Product 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, vulnerabilities, and actions to maintain the integrity of our products and the protection of patient data. In order to fulfill these commitments, Baxter 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.

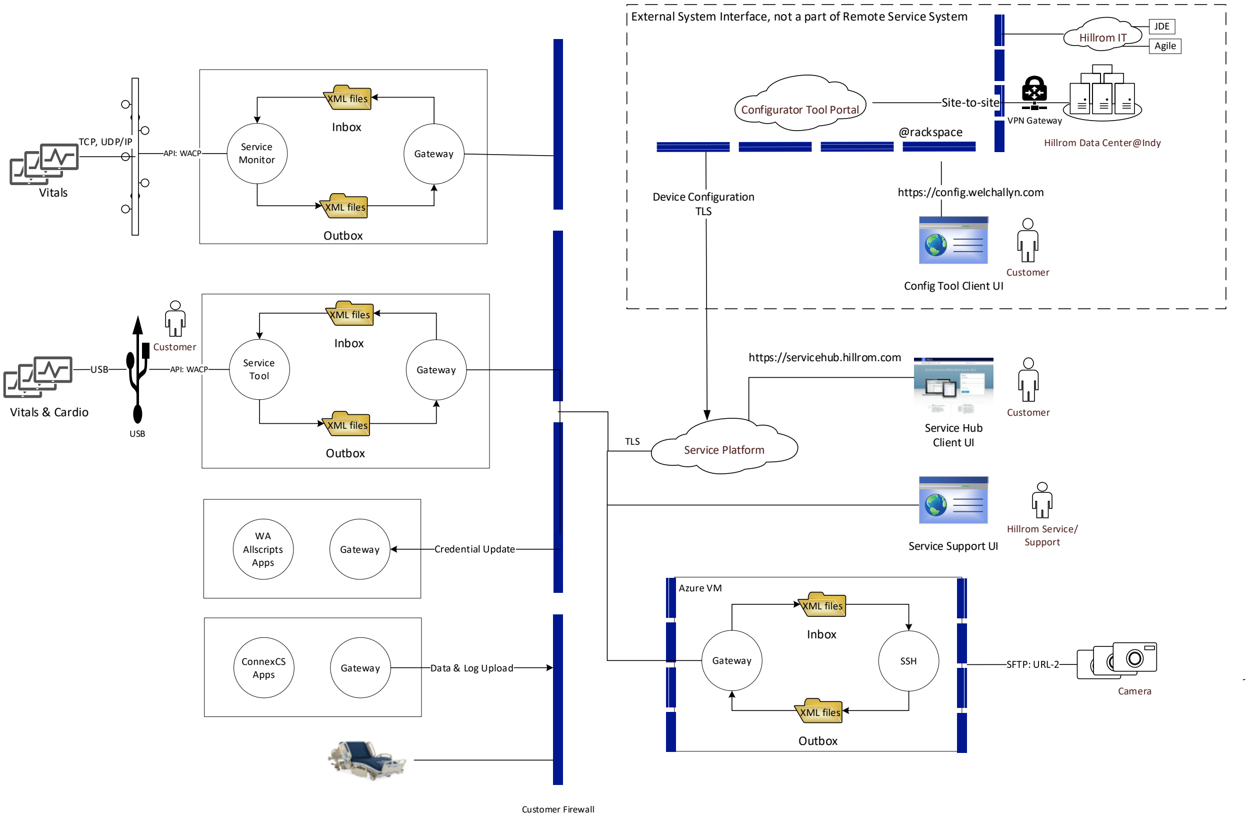
If you would like to report a potential product related privacy or security issue (incident, breach or vulnerability), please contact productsecurity@Baxter.com or visit https://www.Baxter.com/en/responsible-disclosures/

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

Contents

1 Product Description

The Remote Service platform provides Baxter service and support the ability to view and manage Baxter devices and applications remotely. The system also provides Baxter customers the benefit of viewing their own device health and preventive maintenance records, and the ability to manage their device updates remotely. Baxter SmartCare Remote Management is a Software tool for the remote service management of Connex devices, servers, and Central Stations. In addition, it also supports the vision devices and Baxter beds. The diagram below shows the system deployment landscape.



2 Hardware Specifications

Baxter SmartCare Remote Management is a Cloud based platform hosted on Software AG Cumulocity IoT Cloud which is a Software as a Service. The remote platform makes use of no hardware.

3 Operating Systems

Software AG cloud platform supports the following operating system:

- Windows Server 2012, 2016, and 2019
- Red Hat Linux Enterprise Server 7 and 8

Baxter SmartCare Remote Management agents currently supports the following operating systems:

- Windows 10 (32 and 64-bit)
- Windows Server 2012 R2 (64-bit)
- Windows Server 2016 (64-bit)
- Windows Server 2019 (64-bit)

4 Third-party Software

Vendor and Name	Version	Description
Keycloak	15.0.1	Keycloak is an OTS open-source Identity and Access Management solution. Its purpose is to link applications (i.e., SCRM, Cumulocity) with identity providers (i.e., Microsoft Azure AD, Google, …etc.), providing SSO for the application.

5 Network Ports and Services

Port	Protocol	Service Name	Description of Service	Encrypted	Open/Closed
443	TCP/HTTP(s)	Cumulocity IoT platform	Baxter SmartCare Remote Management setting at the top of Cumulocity IoT platform	Yes TLS 1.2	Open
8883	MQTT	Cumulocity IoT platform	Baxter SmartCare Remote Management setting at the top of Cumulocity IoT platform	Yes TLS 1.2	Open
7711	UDP	NRS port	NRS communication facilitate network unicasting over SmartCare Remote Management platform	No	Open
22	TCP(SFTP)	RV700 Fleet Management	RV700 Fleet Management communicates with SmartCare Remote Management	Yes TLS 1.2	Open
283 & 7721	TCP	Welch Allyn Service Monitor	Allow Welch Allyn Service Monitor communicates to a device (CSM, CVSM)	No	Open
Other Software AG Platform Ports					
5683, 5684, 5783, 5784	UDP	Software AG Platform Service Ports	Facilitate remote connectivity to Cumulocity	Yes DTLS	Open
80, 443, 1883, 8883, 9447, 31010, 8774	TCP	Software AG Platform Service Ports	Facilitate remote connectivity to Cumulocity	Yes TLS 1.2/1.3	Open

6 Sensitive Data Transmitted

Baxter SmartCare Remote Management does not transmit PHI.

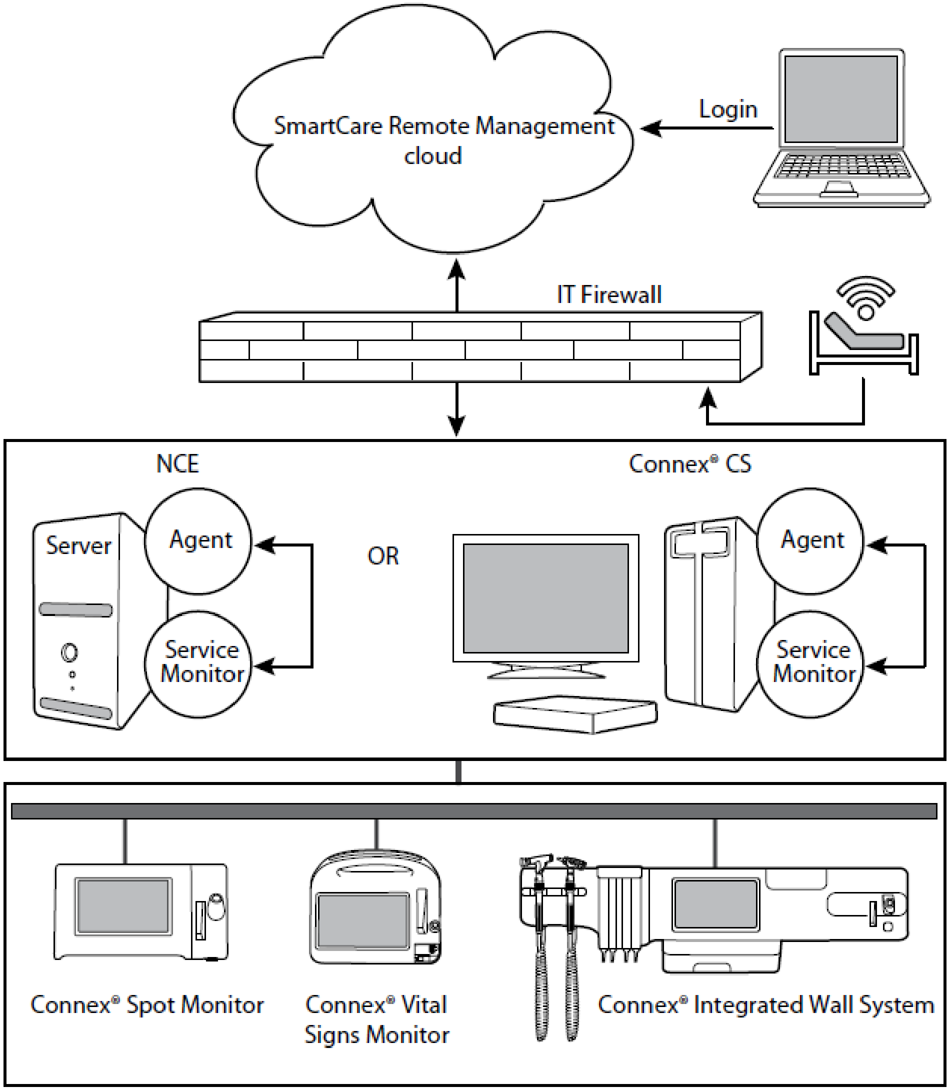
Baxter SmartCare Remote Management does transmit PII such as IP address and location information.

7 Sensitive Data Stored

Baxter SmartCare Remote Management does not store PHI.

Baxter SmartCare Remote Management does store PII such as IP address and location information.

8 Network and Data Flow Diagram



9 Malware Protection

Microsoft Azure cloud hosted application is ISO 27001:2013 Compliant (Information Security Management Systems) and SOC 2 type compliant (Data Security). Within the cloud infrastructure, all servers are equipped with protection tool “Trend Micro Deep Security” that provides antivirus protection, network intrusion detection and prevention, and integrity monitoring.

10 Authentication Authorization

The communication with Cumulocity will be done by HTTPS and Basic access authentication. Cumulocity platform provides Single-Sign-On capability. The feature can be enabled or disabled. The users whose accounts are created through the Cumulocity Portal are called local users. The SSO user accounts are created automatically upon successful user authentication by the external Identity service. SCRM is linked to the identity services through an identity broker, Keycloak.

The Remote Service Platform uses Keycloak v15.0.1., docker image hosted in Azure as an App Service. Identity services will be provided by Baxter Azure AD for internal Baxter users, and Microsoft Azure AD for SCRM customers. Customers must use Microsoft Azure AD as their identity provider to utilize SSO for SCRM.

11 Network Controls

Network Configuration

Application/service	Domain name, IP address, port	Protocol	Connection
	Port: 443		
Welch Allyn Service Monitor	283 7721	TCP TCP	Internal Internal
SmartCareRemote Management	https://smartcareremotemanagement.hillrom.com 52.224.38.138 Port: 443 MQTT Port: 8883	TCP (HTTPS)	Not applicable
RV700 Fleet Management Server	Production Service: **https://** service.retinavue.net Port:22	TCP (SFTP)	External
DCP	NRS port: 7711	UDP	Internal
File outbound types	.log,.zip, .txt, .csv	Not applicable	Not applicable
File inbound types	.tar.gz, .tar, .zip, .pim, .xml, *.txt, *.pdf, .waupdate, *.bas, *.json, .csv	Not applicable	Not applicable

Browser Information:

- Microsoft Edge: version 89 and higher
- Google Chrome: version 86 and higher
- Apple Safari: iOS 14 and higher

12 Encryption

Data is encrypted at rest and when traveling over network connections, including internal network with Transport Layer Security (TLS 1.2). Encryption keys are stored in Software AG Keystores and trust stores.

The communication with Cumulocity will be done by HTTPS and Basic access authentication. All passwords of agent and child device credentials are stored encrypted locally on filesystem or in platform.

The HTTP client used by the Gateway Agent supports the following ciphers. These ciphers are configured at the platform side.

- "TLS_DHE_RSA_WITH_AES_256_GCM_SHA384",
- "TLS_DHE_RSA_WITH_AES_128_GCM_SHA256",
- "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
- "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"

13 Audit Logging

Audit logging is managed by Software AG Audit API resource. The audit API resource returns URIs and URI templates to collections of audit records, so that they can be retrieved by criteria such as "all records from a particular user", or "all records from a particular application".

Audited information:

- Alarm modifications
- Operation modifications
- Two-factor authentication login attempts
- Smart rule modifications
- Complex Event Processing (CEP) module modifications
- User and group permissions modifications
- SSO and OAuth Internal logout and login attempts

14 Remote Connectivity

Remote connectivity to Cumulocity is done through TCP or UDP, depending on the application protocol being used. TCP has TLS 1.2/1.3 support, while UDP has DTLS. Open ports for each:

- UDP: 5683, 5684, 5783, 5784
- TCP: 80, 443, 1883, 8883, 9447, 31010, 8774

15 Service Handling

Baxter, IT assists with the creation of user groups that can create and support customer accounts. There is no PHI involved in any maintenance of SCRM.

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

Baxter will support and maintain the remote platform by consistently providing newer version with required features as per Business need until it is no longer supported by Baxter. At this point, there is no end-of-life support defined time length.

17 Secure Coding Standards

Software AG aligns with the framework and controls matrix of the CSA Security, Trust & Assurance Registry (STAR) program a provider assurance program of self-assessment, third-party audit and continuous monitoring. These assessments can be available to customers upon request. All products go through an automated source code security static analysis on a regular basis. The source or the binary security scanning is automated using the industry state of the art tools. Software AG Cumulocity IoT uses OWASP Top 10 and OpenSAMM security framework.

Baxter SmartCare Remote Management development team follows a “**C coding standard**”, a standard developed to minimized bugs in firmware by focusing on practical rules that keep bugs out, while also improving the maintainability and portability of embedded software.

18 System Hardening Standards

The Remote platform Hardening is performed according to CIS Benchmarks Level 1 profiles. The Level 1 profile is considered a base recommendation that can be implemented reasonably promptly and is designed not to have an extensive performance impact. The intent of the Level 1 profile benchmark is to lower the attack surface to Software AG while keeping machines usable and not hindering Software AG business functionality. Beside these, Baxter FLC security team conducts regular security vulnerability scanning and in addition a Static Application Security Testing (SAST) and penetration testing before any major release. Other system hardening standards are listed in the below table:

Name of Standard
IEC 80001-2-2
ISO IEC 27001
ISO IEC-62305

19 Risk Summary

A security risk assessment was completed on the remote platform. Risks were assessed based on threat, impact, and vulnerability. Vulnerability scanning were completed by Baxter FLC security team; no critical, high, and medium findings identified. In addition, penetration testing was completed by Software AG and no critical, high, medium findings were identified on the cloud platform. Software AG current penetration testing report is available for review and can be provided upon request.

20 Third Party Certification

Software AG aligns with the framework and controls matrix of the CSA Security, Trust & Assurance Registry (STAR) program a provider assurance program of self-assessment, third-party audit and continuous monitoring. CSA Security, Trust & Assurance Registry (STAR) program. The Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR) program is the industry's leading trust mark for cloud security.

The CSA Open Certification Framework (OCF) is a program for flexible, incremental and multi-layered CSP certifications according to the CSA's industry leading security guidance. The OCF/STAR program comprises a global cloud computing assurance framework with a scope of capabilities, flexibility of execution, and completeness of vision that far exceeds the risk and compliance objectives of other security audit and certification programs.

For all cloud hosted products, the Software AG RnD security team performs security penetration testing based on OWASP top 10 for each cloud release. We can presume how many releases happen in a yearly basis. But whenever there is a new release, Software AG performs security penetration testing on the cloud hosted product.

In addition, Cloud Security, Compliance, and certifications engages with an external security testing company to perform regular penetration test for standard Cloud services. Beside this, Baxter will also perform internal penetration testing on the application whenever a new software version is release as required by our Product Security SOP. The frequency can vary based on yearly project roadmap.

Physical access to data center or hosting facility is controlled and monitored by Software AG. Microsoft is responsible for all physical access controls to IaaS for Software AG Cloud Services. Microsoft takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the datacenter resources. Datacenters managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor.

21 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 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.