

Target CI v1.6

CYBERSECURITY GUIDE

English

Updated: July 2026



Contents

1. INTRODUCTION	3
1.1 ABBREVIATIONS AND DEFINITIONS:.....	3
2. OTHER RESOURCES.....	4
2.1 CUSTOMER SUPPORT	4
2.2 AB PRO PORTAL	4
2.3 ADVANCED INSTALLATION GUIDE.....	4
2.4 TARGET CI FIREWALL CONFIGURATION	4
2.5 MDS2.....	4
2.6 INSTRUCTIONS FOR USE (IFU).....	5
2.7 HIMSA.....	5
3. NETWORK AND CONTEXT DIAGRAMS.....	6
3.1 DEPLOYMENT MODEL 1: STANDALONE.....	6
3.2 DEPLOYMENT MODEL 2: NOAH DISTRIBUTED.....	7
3.3 DEPLOYMENT ARTIFACTS.....	8
3.4 SYSTEM INTERCONNECTIONS	9
4. SYSTEM REQUIREMENTS	11
5. CYBERSECURITY IN PRODUCT LIFE CYCLE	12
5.1 DEPLOYMENT	12
5.2 INSTALLATION	12
5.3 CONFIGURATION AND OPERATION	13
5.4 REMOVAL AND DECOMMISSIONING	14
6. SECURITY CONTROLS.....	16
6.1 ACCESS CONTROLS	16
6.2 AUDIT LOGGING AND ACCOUNTABILITY CONTROLS	16
6.3 REMOTE ACCESS	17
7. INFORMATION PROTECTION.....	18
7.1 ADVANCED BIONICS PRIVACY POLICY	18
7.2 FEDERAL INFORMATION PROCESSING STANDARDS (FIPS)	18
7.3 PII/PHI PROCESSED BY THE PRODUCT	18
7.4 SECURITY IN TRANSIT	19
7.5 SECURITY AT REST	20
8. SOFTWARE INTEGRITY	23
8.1 VERIFICATION OF DOWNLOADED INSTALLATION MEDIA	23
8.2 MANUAL VERIFICATION OF FITTING SOFTWARE PRIOR TO INSTALLATION.....	24
8.3 AUTOMATIC VERIFICATION OF INSTALLED FITTING SOFTWARE INTEGRITY....	25
8.4 MANUAL VERIFICATION OF INSTALLED FITTING SOFTWARE INTEGRITY.....	26

9. SOFTWARE PATCHES AND UPDATES.....	28
10. DATA MANAGEMENT.....	28
10.1 DATABASES	28
10.2 DATA MIGRATION	28
10.3 HEARING DEVICE CONFIGURATIONS	28
10.4 DATA DISPOSAL.....	28
11. SECURITY ENVIRONMENT – SHARED RESPONSIBILITY.....	29
12. MANUFACTURING, SOFTWARE DEVELOPMENT, AND SECURITY MANAGEMENT	31
13. SOFTWARE COMPONENTS AND BILL OF MATERIALS	32
14. REFERENCES	49

1. INTRODUCTION

This document provides technical security and privacy information about the Target CI v1.6 software system from Advanced Bionics, hereinafter “fitting software.” The fitting software is designed for use by qualified hearing care professionals (HCP) to configure (i.e., fit) hearing devices for patients who have received cochlear implants from Advanced Bionics.

This document specifically focuses on the cybersecurity and privacy considerations that are relevant to the use of the fitting software. It includes an evaluation of the security and privacy controls that are currently integrated into the software, as well as those that are anticipated to be applied and configured within the IT environment where the product will be used for its intended purpose.

This document does not provide technical security and privacy information about:

- Previous versions of AB fitting software
- AB software other than Target CI v1.6
- AB websites
- AB mobile applications
- AB hearing devices

1.1 ABBREVIATIONS AND DEFINITIONS:

Acronym	Term
FSW	Fitting software
SaMD	Software as a Medical Device
Noah	A third-party patient management system from HIMSA used to store and manage patient demographics and fitting data
TeamViewer	A cross-platform remote access and desktop-sharing tool
SOUP	Software of Unknown Provenance
HCP	Hearing Care Professional
SaMD	Software as a Medical Device
AB	Advanced Bionics
Sonova	Advanced Bionics is a wholly owned subsidiary of Sonova and functions as an integral entity within the Sonova Group.
IFU	Instructions For Use
PHI	Protected Health Information
PII	Personally Identifiable Information
SBOM	Software Bill of Material

2. OTHER RESOURCES

2.1 CUSTOMER SUPPORT

For those located inside the United States and Canada, Advanced Bionics offers a toll-free technical hotline phone number (877-271-6727) where dedicated professional support is available Monday through Friday from 5:00am to 5:00pm Pacific Time.

For those located outside the US and Canada, technical support is provided regionally. If you have questions about the fitting software, related hardware, or other programming concerns, please contact your local AB representative.

2.2 AB PRO PORTAL

The fitting software and related documentation may be downloaded from <https://www.abproportal.com> or the Sonova Web Client. An account login is required. This resource may not be available in all markets; contact your AB representative for more information.

2.3 ADVANCED INSTALLATION GUIDE

The Target CI v1.6 Advanced Installation Guide is available upon request. The guide provides technical information about the fitting software installer, including command-line options for silent and automated installations.

2.4 TARGET CI FIREWALL CONFIGURATION

The Firewall Configuration document is available upon request. This document provides IT-focused guidance to ensure Target CI 1.6 works behind a corporate firewall, detailing the required HTTP/HTTPS access and the key hostnames. It covers WebRTC connectivity via Twilio and Xirsys, outlining TURN and peer-relaying ports and noting that many IPs are dynamic, so hostname-based rules should be used where possible.

2.5 MDS2

The Manufacturer Disclosure Statement for Medical Device Security (MDS2) is an industry-standard form containing security and privacy information about AB fitting software. This form is available upon request.

2.6 INSTRUCTIONS FOR USE (IFU)

The IFU will ship with the software installation media. For some markets, the electronic IFU is available for download at www.advancedbionics.com/ifu

The following sections in the IFU may be relevant to IT professionals:

- Product Description
- System Minimum Requirements & Performance Characteristics
- Guidelines for IT Security
- Operating Instructions
- Disposal and Hazardous Material
- Technical Support

2.7 HIMSA

The Hearing Instrument Manufacturer's Software Association (HIMSA) is a third-party software vendor that produces Noah System 4, a software system designed for the hearing care industry that provides hearing care professionals with a vendor-agnostic system for performing client-related tasks.

The fitting software may optionally be configured to use Noah System 4 for data storage rather than a local database.

HIMSA's security web page provides answers to common IT security questions about the Noah System 4.

<https://www.himsa.com/support/noah-enterprise-support/security-questionnaire-support/>

<https://www.himsa.com/support/noah-enterprise-support/security-considerations/>

See the Security section of the HIMSA Learning Center for additional security information:

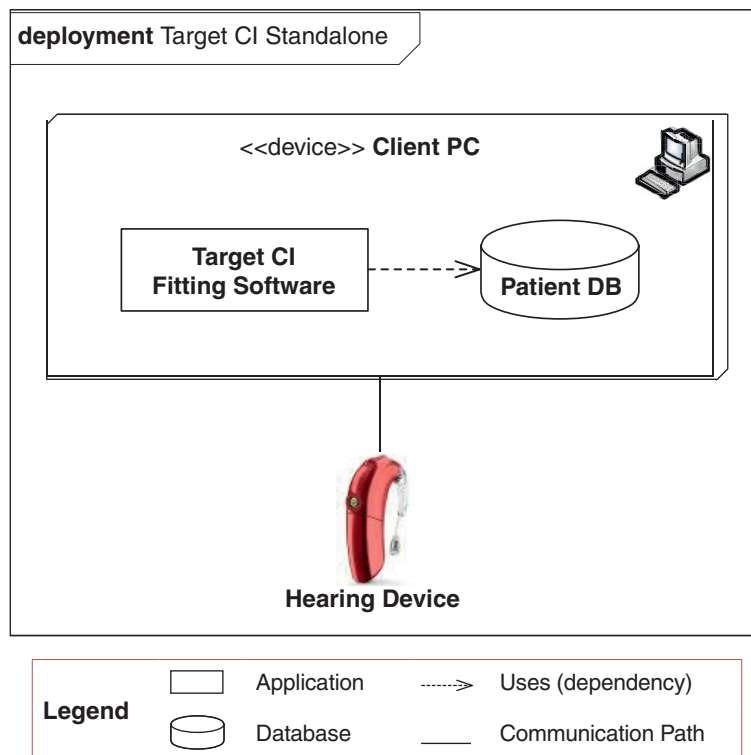
<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/>

3. NETWORK AND CONTEXT DIAGRAMS

There are two deployment models supported for the fitting software, which is a client application (SaMD) installed on a commercially available off-the-shelf Microsoft Windows PC. The software does not include any hardware or operating system.

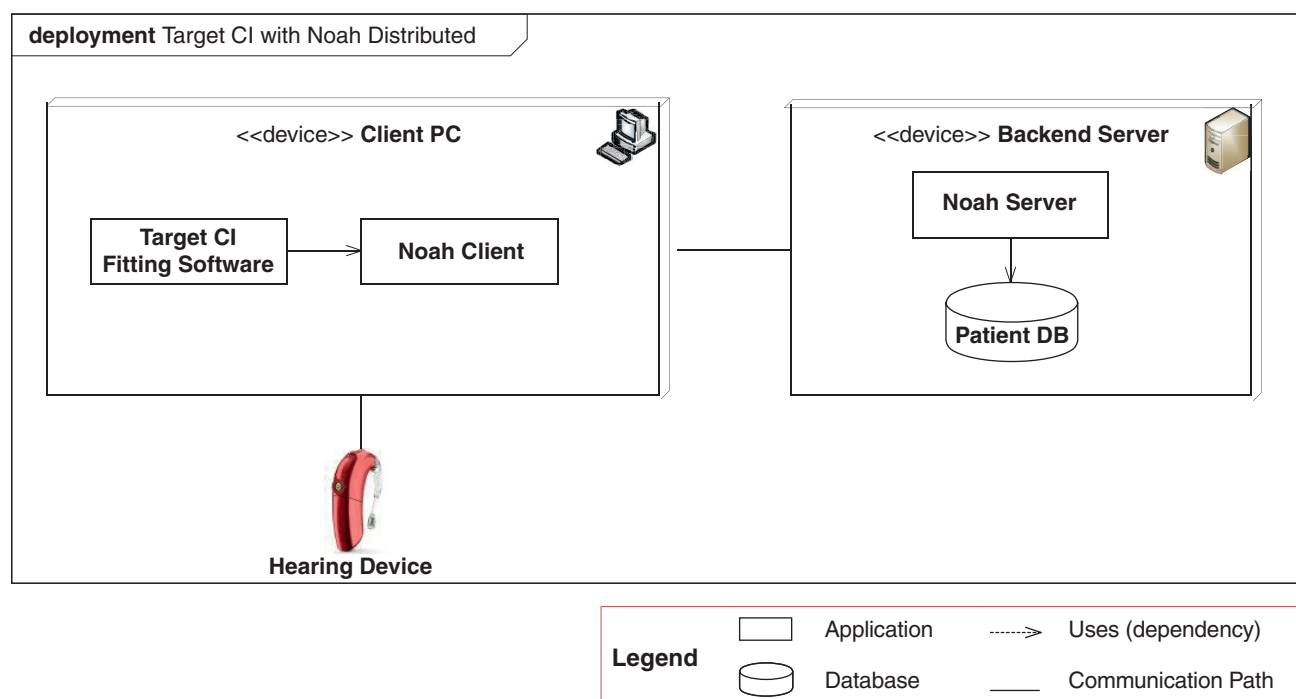
3.1 DEPLOYMENT MODEL 1: STANDALONE

In the standalone deployment model, the fitting software is deployed to a client PC. The patient database is stored on the same PC and installed together with the fitting software.



3.2 DEPLOYMENT MODEL 2: NOAH DISTRIBUTED

In the Noah Distributed deployment model, the fitting software is deployed to one or more client PCs with Noah installed. Noah, a third- party patient management system, is deployed to an internal server accessible to the client PCs. The patient database is stored on the Noah server and accessed over the network by one or more client PCs.

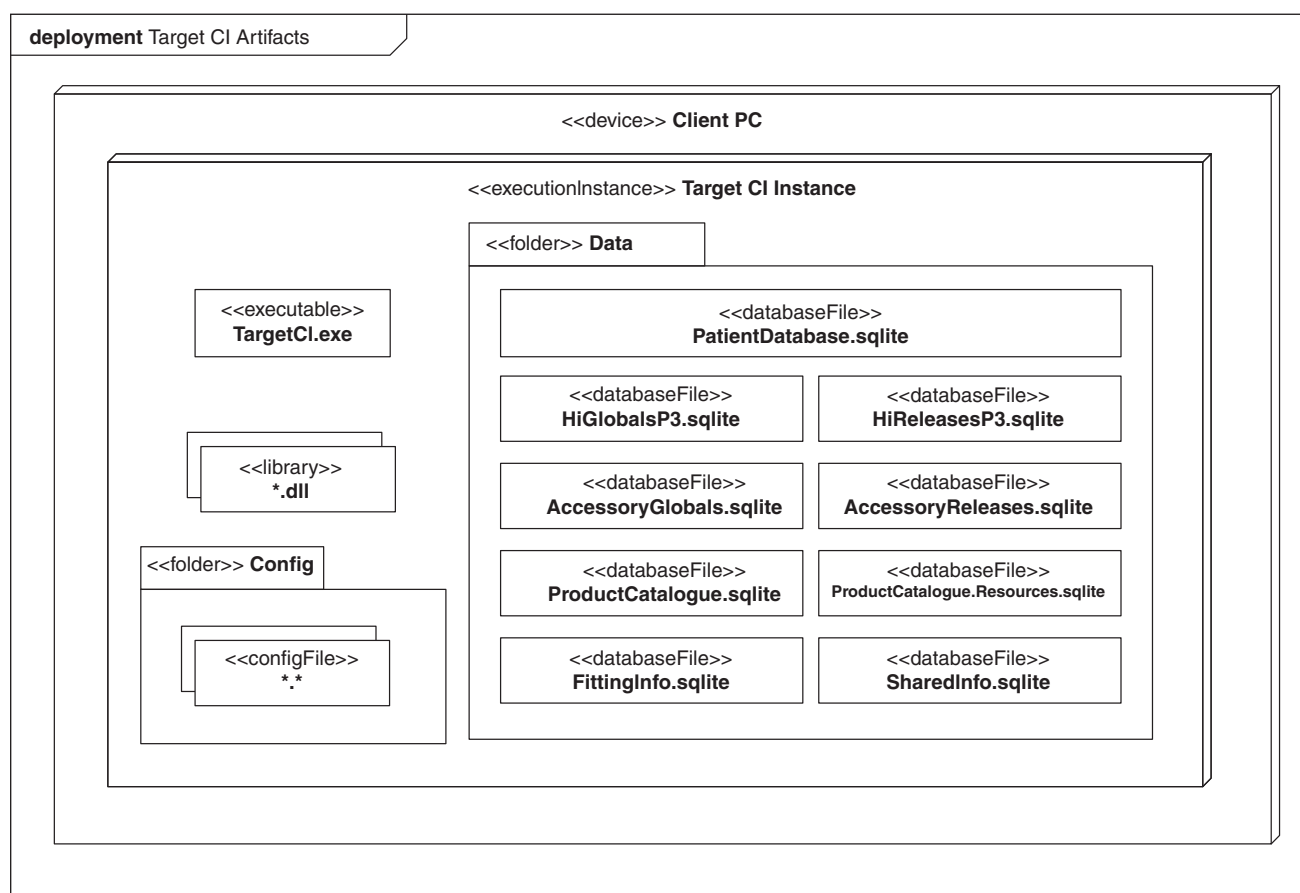


3.3 DEPLOYMENT ARTIFACTS

The fitting software installs with an executable file and a set of associated files including component DLLs, configuration files, and SQLite database files. The configuration files are installed in folder “%ProgramData%\Advanced Bionics\Target CI\Target CI\Config,” and database files are installed in folder “%ProgramData%\Advanced Bionics\Target CI\Target CI\Data.” The Data folder holds a single transactional database file and several info database files.

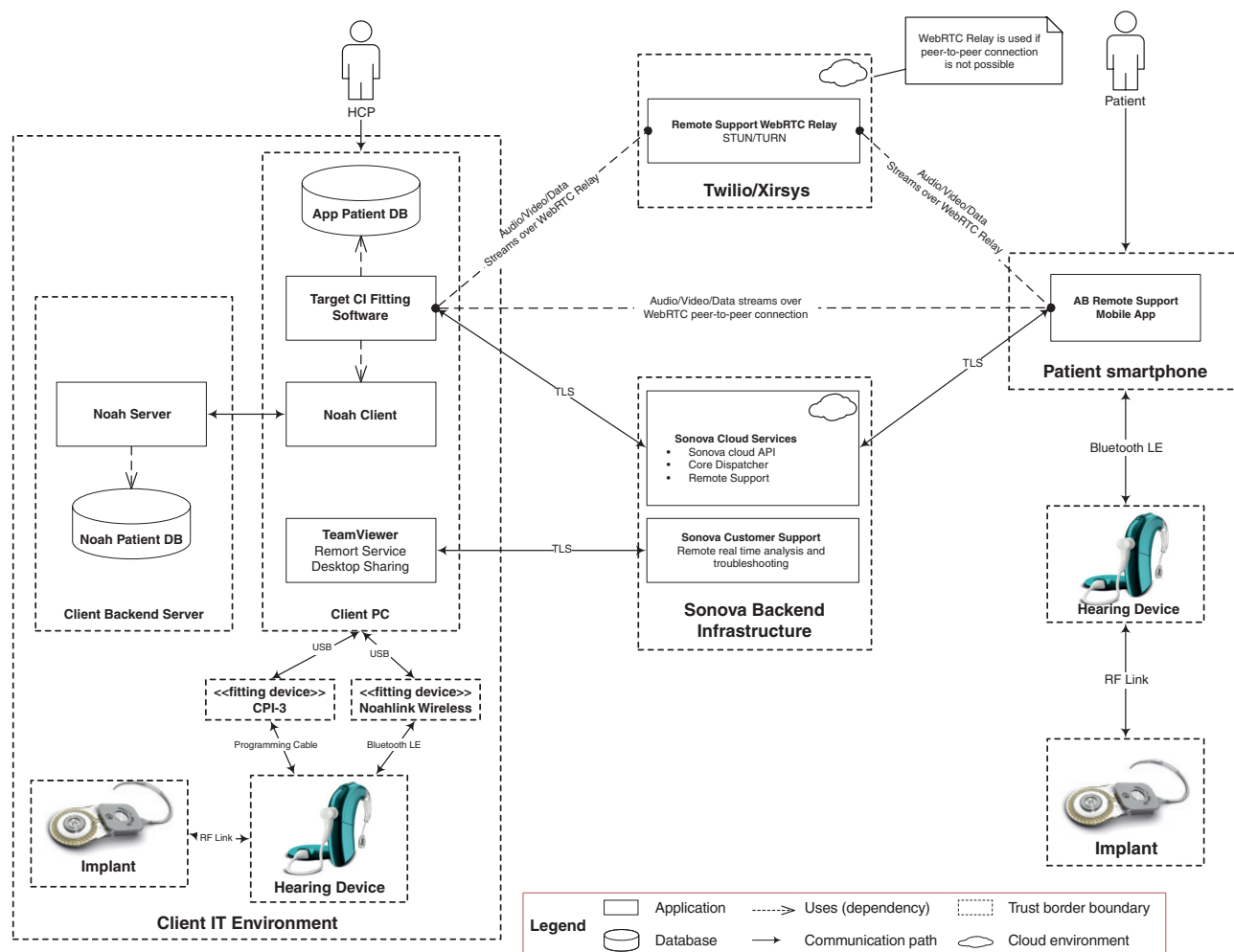
The transactional database, PatientDatabase.sqlite, stores the demographics and fitting data of the patient and will be installed only when the fitting software is deployed in standalone mode.

When the fitting software is deployed as a Noah module, the Noah system supplies the required patient data persistence services to the fitting software. The remaining sqlite files are integral to the fitting software and required for all deployment models.



3.4 SYSTEM INTERCONNECTIONS

The diagram and table below illustrate the primary system interconnections. Typically, only a portion of the available interconnections are utilized.



Source / Destination	Service	Protocol	Port	Description
Hearing device	Hearing device communication	Wired connection / Bluetooth® Low Energy	N/A	Used to communicate with hearing devices for control, configuration and status & data readout purposes
Noah	Noah 4 ModuleAPI	.NET Remoting	N/A	Primary interface for the module used to access the Noah software (in Noah distributed deployment model only)

Source / Destination	Service	Protocol	Port	Description
Sonova Cloud Services	Sonova Cloud API, Core dispatcher, Remote support	SOAP, REST	443	Sonova services hosted in a Microsoft Azure Data Center are used to: • fetch fitting software client configuration data from Sonova backend storage • transfer logging and analytics data • establish real time remote fitting
Twilio/Xirsys, AB Remote Support and AB Remote Support + Mobile Apps	Remote Support	WebRTC	Can be found in Target CI Firewall configuration document	Used by the remote support feature to perform WebRTC signaling and perform real time remote fitting sessions
AB Customer Support	Desktop sharing	TeamViewer proprietary protocol	5938, 443, 80 Refer to TeamViewerPorts	Used to perform remote real time analysis and troubleshooting of issues affecting fitting software installations. Refer to section 6.3 REMOTE ACCESS for more information.

4. SYSTEM REQUIREMENTS

Operating System	Windows 10,11, Pro/Enterprise
.NET Framework	Version 4.8
CPU	Intel® Core™ i5 or equivalent with equal or better performance
RAM	4GB or more
Hard Disk Space	3GB or more
Minimum Display Requirements	• 1280 x 1024 resolution (maximum scaling 125%) • 24-bit color
Device Drivers	• Noahlink Wireless driver (latest version available from HIMSA is required if using third-party USB-connected Noahlink Wireless programming interface). • CPI-3 driver (required if using a USB-connected CPI-3 programming interface).
Database	SQLite or Noah System 4 (version 4.16 or higher)
Internet Connection	Internet connection required for remote support and analytics logging, see section 3.4 System Interconnections; intranet required when using networked Noah System 4.
Network Ports	See section 3.4 System Interconnections; see section 2. Other Resources — HIMSA for ports used by Noah System 4.

5. CYBERSECURITY IN PRODUCT LIFE CYCLE

5.1 DEPLOYMENT

Approved Deployment Methods:

1. Download from the Sonova Web Client (SFTP) at <https://webclient.sonova.com>, or from AB Pro Portal at <https://www.abproportal.com>
2. Install from an official Advanced Bionics USB stick.

Before installation, verify the installer's digital signature, and scan the file with updated antivirus software. Refer to Section 8 for detailed integrity verification instructions. Apply standard healthcare IT security controls during deployment, including endpoint protection and network restrictions.

When using a USB stick:

- Use only official USB sticks provided by Advanced Bionics.
- Keep the USB physically secure and do not alter its contents.
- Scan the USB and installation environment with updated antivirus and application whitelisting.
- Advanced Bionics is not responsible for any unauthorized data stored on USB sticks containing the installation package.

5.2 INSTALLATION

An Administrator account is required to install the fitting software. Once the software is installed, it can be run without administrative or elevated permissions.

See section 8, Software Integrity, for information on verifying the integrity of the software prior to installation.

Prior to installation, system administrators are recommended to make sure that:

- the fitting software product version to be installed is the latest available.
- the underlying operating system is up-to-date.
- the integrity and authenticity of fitting software installer data is verified. See section 8 for information on validating the integrity of the software prior to installation

Two installers are available for installing the fitting software:

- Standard Installer
- IT Professional Installer

The IT Professional installer is a single MSI file and excludes prerequisite components but is otherwise equivalent to the Standard installer.

Prerequisite components include the Microsoft .NET Framework v4.8, and the Microsoft Visual C++ Redistributable packages.

Both installers support advanced installation scenarios, including silent installation.

The IT Professional Installer should only be used if your organization requires prerequisite components to be installed and managed by your organization and not by the fitting software installer. The Standard Installer should be used in all other cases.

The IT Professional Installer may be obtained from an AB clinical representative. The IT Professional installer cannot be used to repair, reinstall, or uninstall installations by the Standard installer. The Standard installer cannot be used to repair, reinstall, or uninstall installations by the IT Professional installer.

For advanced installation scenarios, follow the instructions in the Fitting Software Advanced Installation Guide (see Section 2.3). For standard installation scenarios, refer to Section 2.5 of this document, which includes a link to the Fitting Software Instructions for Use (IFU).

5.3 CONFIGURATION AND OPERATION

The fitting software supports a set of privacy & security controls and features. Some fitting software privacy & security capabilities are enabled by default, some are configurable at installation time and depend on the selected deployment model and others are configurable during normal usage through the application GUI.

Refer to:

- Section 6 for a list of security controls which improve the protection of the fitting software application system
- Section 7 for a list of security controls which improve the protection of data processed by the fitting software application

Additional privacy & security controls (which are not supported by the fitting software at application level) are expected to be enabled and configured by users (e.g., HCPs, system administrators, IT personnel) at OS level and/or at IT infrastructure level. Refer to Section 11 of this document for a detailed list of best practice recommendations and security controls for the fitting environment where the fitting software will be used.

Firewall

The fitting software is not provisioned with an internal firewall.

In case an external firewall is enabled (e.g. at OS level), its configuration might need to be updated in order to allow the required incoming and outgoing traffic (e.g. WebRTC audio/video/data streams during a Remote Support session). Refer to the fitting software Firewall Configuration document which contains the list of network addresses and ports used by the fitting software.

Proxy settings

The fitting software is provisioned with a local proxy. Through the fitting software GUI it is possible to change the settings of such proxy:

- No proxy
- Automatically detect proxy settings
- Manual proxy configuration. If this option is selected, the following settings are configurable:
 - Address
 - Port
 - Enable/Disable proxy authentication (username, password, domain)

5.4 REMOVAL AND DECOMMISSIONING

Refer to the fitting software IFU (Instructions for Use) document for detailed guidance on uninstalling the software.

The uninstallation program does not remove the categories of data listed in the following table. Unless otherwise stated in the “Notes” column of the table, such data needs to be manually removed from the systems by system administrators; e.g., by manually removing the files or by wiping the system disk used for data storage.

Data category	Default location	Notes
Application data	C:\ProgramData\ Advanced Bionics\Target CI\Target CI	Includes the following type of data: • Analytics data • Configuration data • Application logs • Temporary files
Personal data	C:\ProgramData\ Advanced Bionics\Target CI\Target CI\Data	Patient database (relevant for standalone deployment model only)
Remote access tool	C:\Program Files (x86)\Common Files\ Advanced Bionics\ TeamViewer	Used to perform real time analysis and troubleshooting of issues affecting fitting software including the ones during installation and uninstallation. Refer to section 6.3 for more information.

When you uninstall the fitting software from the computer/laptop that is slated for decommissioning or disposal, ensure that all sensitive data (e.g., PHI, PII) are wiped.

For Noah deployments refer, detailed instructions for data disposal for Noah deployments can be found at:

<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/>

External media containing data exported from fitting software including reports and logs should be secured. When no longer used, data should be securely erased and/or the media should be securely erased or destroyed.

Approved procedures and tools should be used for secure removal of data stored on removable media, according to applicable regulations and guidelines for handling patient information / personally identifiable information (PII) / protected health information (PHI).

6. SECURITY CONTROLS

The fitting software is a client application installed on a commercial Microsoft Windows off-the-shelf PC. The fitting software can be installed as standalone application or as a Noah module.

6.1 ACCESS CONTROLS

The fitting software does not restrict access to its features based on login requirements and roles of individual users. Role-based access controls are not supported.

Local user access

When the fitting software is installed as a standalone application, it depends on the access control mechanisms of the host operating system. Customer IT personnel may configure the host OS to manage user authentication and assign access rights or privileges. Each user is strongly recommended to log in with a unique, individual account.

Additional compensating controls are described in Section 11 of this document and in the Guidelines for IT Security section of the IFU.

When the fitting software is installed as a Noah module, access control is managed through Noah System 4.

For details on the access control features implemented by Noah System 4, refer to the documentation available at www.HIMSA.com.

Service access

On-site service support engineers can access the fitting software considering the access controls configured by the customer's IT personnel to manage authentication.

AB support engineers can gain access to the fitting software by using the Desktop Sharing feature supported by the fitting software. Refer to section 6.3 for detailed information about the security controls enabled for this feature.

6.2 AUDIT LOGGING AND ACCOUNTABILITY CONTROLS

The fitting software does not generate any additional audit logs or reports other than those provided by the underlying operating system.

Standalone deployment model

When the fitting software is installed as a standalone application, it relies on the audit mechanisms provided by the host operating system. The fitting software does not have any such integrated facility. The host operating system may be configured by the customer's IT personnel to log certain events like launches/executions of the fitting software. It is recommended that each user log into the host OS with a unique per-user account to facilitate auditing.

Noah Distributed deployment model

When the fitting software is installed as a Noah module, audit logging is handled by the Noah System (Noah Activity Log). For details on the audit controls available in Noah System 4, refer to the documentation provided at www.himsa.com

6.3 REMOTE ACCESS

The Desktop Sharing feature allows for remote real time analysis and troubleshooting of issues affecting fitting software installations. This feature is based on the TeamViewer QuickSupport 3rd-party tool (deployed by default together with fitting software) and allows AB customer support professionals to remotely connect to the HCP's computer and gain full desktop control of it, including access to the underlying operating and file system.

To establish a Desktop Sharing session, HCP interaction is required. HCP shall first execute the TeamViewer QuickSupport tool (e.g., through the Target CI fitting software) and communicate their TeamViewer ID credentials to the AB Support team through an out-of-band communication channel (e.g., phone call).

The AB support team member's name and their TeamViewer ID are by default displayed on the HCP's computer monitor during each active Desktop Sharing session.

All Desktop Sharing network traffic is secured using cryptographic protocols and algorithms considered secure by today's standards (RSA public/private key exchange and AES 256-bit session encryption).

The remote access tool can be manually removed without affecting other Target FSW functionalities. The Target FSW installation program supports a command line installation parameter to allow a Target FSW command line installation without including the remote access tool.

7. INFORMATION PROTECTION

7.1 ADVANCED BIONICS PRIVACY POLICY

The privacy policy describing how Advanced Bionics collects, transfers, stores, and uses personal data, can be downloaded from: AdvancedBionics.com/privacy.

Advanced Bionics does not host, store, backup, or have access to any data stored within the fitting software or Noah databases, unless the data is expressly sent to Advanced Bionics.

7.2 FEDERAL INFORMATION PROCESSING STANDARDS (FIPS)

Target CI v1.6 is compliant with FIPS 140-2 encryption standards.

7.3 PII/PHI PROCESSED BY THE PRODUCT

The fitting software processes patient personal and health information.

The patient information is either entered manually by the user of the fitting software, or it is received by the application through one or more of its data flows.

The following types of information are processed in the main data flows of the fitting software:

	Sonova cloud services (core dispatcher, remote support)	Hearing device	Mobile apps	Patient DB (local/Noah)	Remote access
Name				X	X(2)
Address				X	X(2)
Date of birth	X(1)		X	X	X(2)
Phone number				X	X(2)
Email address				X	X(2)
Medical record numbers				X	X(2)
Device identifiers & serial numbers	X(1)	X	X	X	X(2)
IP address	X(1)				
Audiograms, RECD, REUG	X(1)	X	X	X	X(2)
Fitting data		X	X	X	X(2)
Hearing device usage data	X(1)	X	X	X	
Fitting software usage data	X(1)				

(1) Pseudonymized prior of landing to Sonova datalake.

(2) During a real time desktop sharing session, AB customer support engineers gain full control of HCP's desktop including access to the underlying operating and file system and data stored in it. Refer to section 6.3 for more information.

For more detailed information about data collection and processing, contact your local support representative.

7.4 SECURITY IN TRANSIT

Communication security is ensured and enabled in all inbound and outbound fitting software network communications. Except for the Remote Support feature (which uses the WebRTC protocol) and Bluetooth communication with hearing devices & accessories, all other connections are protected by the Transport Layer Security (TLS) protocol which provides confidentiality, integrity, and authenticity.



TLS

TLS configuration is compliant to current best practices and security recommendations documented in BCP 195 – Recommendations for Secure Use of TLS and DTLS [8], including:

- Not supporting SSL and TLS versions prior to 1.2
- Not supporting cipher suites that use cryptographic algorithms offering less than 128 bits of security
- Supporting recommended TLS extensions of BCP 195
- Not supporting insecure extensions of BCP 195

DTLS

Encryption is a mandatory feature of WebRTC and is enforced on all media streams sent over WebRTC. The encryption protocol used depends on the channel type; data streams are encrypted using DTLS 1.2 and media streams are encrypted using Secure Real-time Transport Protocol (SRTP) used because it is a lighter-weight option than DTLS.

Refer to the following link for more detailed information about security configuration of Remote Support WebRTC:

<https://developer.liveswitch.io/liveswitch-server/server/security.html>

BLE

Bluetooth Low Energy wireless communication with hearing devices and accessories is encrypted and integrity protected by default (except for identification and detection use cases). In addition to that, the duration of the hearing device's Bluetooth pairing mode is limited in time. Refer to available hearing device documentation for more detailed description about security of Bluetooth communication channel.

7.5 SECURITY AT REST

Application data

Application data resides on the same machine, under the default directory:

C:\ProgramData\Advanced Bionics\Target CI\Target CI

The access right inherits from its parent folder and is limited to users logged on to the local system (built-in INTERACTIVE user group¹) during the installation of the software.

Authorized users have read and write access to the directory.

To reduce the risk of unauthorized access to the application data via the network, please ensure that none of the folders or files containing the data is shared on the network. The default locations of the application data are listed in 5.4.

¹ <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-special-identities-groups#interactive>

Patient database – Standalone Deployment model

When the fitting software is installed as a standalone application, the patient database resides on the same machine and patient data records are not encrypted at rest. PII is not transmitted over the network by the application.

Any user who can log onto the machine with the installed fitting software will have full access to all application data, including the patient database. Please consult section Data protection for guidance regarding recommended data protection measures.

In some jurisdictions, regulations may require encrypting all patient data to avoid potential liability in case of data loss or theft. Enable BitLocker or equivalent full-disk encryption (OS-level or hardware-based) to safeguard the data from unauthorized access or copying while the data is at rest.

BitLocker is a built-in Windows feature that encrypts the entire drive and requires authentication to access. Always consult Microsoft's official guidance and your organization's IT security policy before enabling BitLocker.

How to Enable BitLocker

Administrator privileges are required to manage BitLocker.

1. Search "Manage BitLocker"

Open the Start menu, type "Manage BitLocker," and select it from the search results.

2. Select the System Drive

Choose the drive where Windows is installed to configure encryption settings.

3. Choose an Unlock Method

Select one of the following options:

- TPM only
- TPM + PIN
- TPM + USB key

Follow Microsoft's best practice guidance and your organization's IT security policy when selecting the unlock method.

4. Back Up the Recovery Key

Back up the recovery key using secure, enterprise-approved methods. Recommended options include:

- Storing in Microsoft Entra ID (formerly Azure AD) or Active Directory for domain-joined devices
- Saving to a secure, access-controlled network location with encryption and audit logging
- Using a managed key escrow solution approved by your organization

Avoid saving the key to local drives, USBs, or printing it unless explicitly permitted by policy. Recovery keys must be protected with the same rigor as other sensitive credentials and rotated immediately if exposed.



5. Start Encryption

Choose:

- Entire drive – recommended for most enterprise scenarios. Encrypts all sectors, including unused space, to prevent data remanence.

Patient database – Noah Distributed Deployment module

When the fitting software is installed as a Noah module, PII is stored within the patient database hosted by Noah. The patient database hosted by Noah may reside on another machine. PII and other patient data is maintained by Noah software, and the encryption of the patient's data-at-rest is ensured by the Noah System. The fitting software may transmit/receive PII via a wired or wireless network connection when a Noah database is configured for network access.

PII stored on networked Noah database will be accessible to other users on different PCs that have permissions to the same networked database. The Noah database may also be configured for non-network access and installed on the same PC as the fitting software.

Noah prevents the fitting software from accessing the patient-record database. When a user opens a patient in the fitting software via the Noah Client, the fitting software is only able to read from and write to the currently opened patient record and is not able to access other patient records in the Noah database.

Refer to the following link for more information about encryption standards used by Noah System:

<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/patient-database-encryption/>

RMA Export Files

The fitting software allows client information to be exported to a file. The RMA file can be sent to Advanced Bionics to resolve RMA or related support issues.

The RMA file is asymmetrically RSA encrypted using a 2048-bit key length. The fitting software does not have any facility to decrypt an RMA file.

Anonymized Export Files

The fitting software allows client information to be exported to a client-anonymized file. The client's personally identifiable information, such as birthdate and name, are replaced with generic values. The file is not encrypted and can be imported into the same instance or a different instance of the fitting software.

Standard Export Files

The fitting software allows client information to be exported to a standard export file. The file uses a proprietary binary format and is not encrypted. The file can be imported into the same or a different instance of the fitting software. When using this feature, fitting software users must ensure that standard export files are handled according to their local IT policies for managing unencrypted PII.

Hearing Device

The fitting software stores client information on the client's hearing device. Personally identifiable information such as the client's name and birthdate are not stored on the hearing device. Other non-PII information is stored using PBKDF2 encryption with a 128-bit key.

The fitting software may transmit/receive non-PII client information to/from a hearing instrument via a proprietary wired device (i.e., CPI-3), AB Remote Support and AB Remote Support + mobile applications, or Noahlink Wireless device. The Noahlink Wireless device connects with the hearing device using Bluetooth Low Energy (BLE) via a standard BLE 128-bit AES encrypted channel.

8. SOFTWARE INTEGRITY

8.1 VERIFICATION OF DOWNLOADED INSTALLATION MEDIA

The Target CI fitting software installation media may be downloaded in some regions from Advanced Bionics' Pro Portal or Sonova Web Client. The downloaded installation media can be authenticated using any trusted SHA-256 hashing tool.

The SHA256 hash for the standard installation zip file is:

A42B8F41A5A4111D1CDF67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

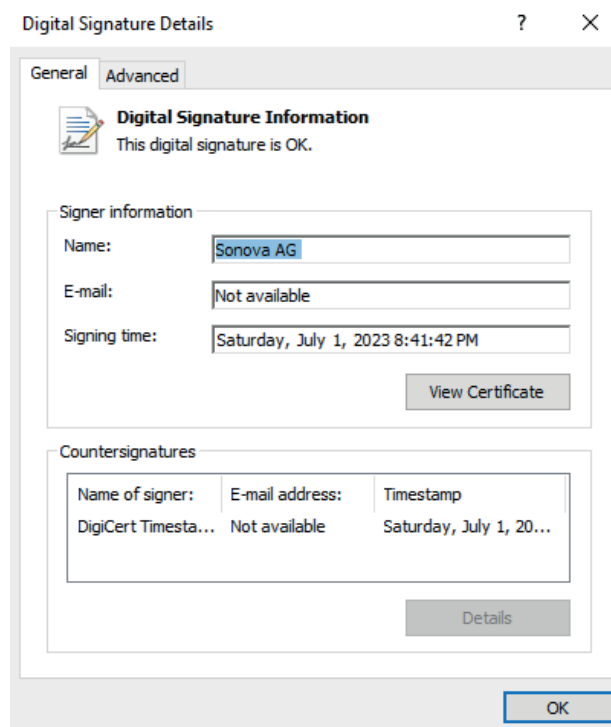
The SHA256 hash for the IT Professional installation zip file is:

DDAD362CC3213EFEA702D9F4A61740B34EDF794FE997811B6B2C908CE754B25F

8.2 MANUAL VERIFICATION OF FITTING SOFTWARE PRIOR TO INSTALLATION

Users may perform the following steps to verify the fitting software's integrity and authenticity prior to installation:

1. Open Windows Explorer and navigate to the root folder of the fitting software's installation media. If your installation media is a thumb drive, insert it into a USB port and navigate to its root. If your installation media is a zip file, unzip it to a folder and navigate to that folder.
2. Right click on SonovaVerify.exe and select Properties from the context menu.
3. Select the Digital Signatures tab.
4. Double click the SHA256 "Sonova AG" signature.
5. Verify the elements of the signature are valid. In particular, verify that the message "The digital signature is OK." appears near the top and that the signer's name and signing time match the following image:



6. Click the “View Certificate” button and the “Details” tab and verify that the value of the “Thumbprint” field matches this one: db88d10f0a1bfb12be6c3c46c516e507e14f2593
7. Close the popup dialogs and double click SonovaVerify.exe
8. Verify that “NO ERRORS DETECTED.” is displayed as shown in the following image:

```
SonovaVerify 0.0.4.0 Copyright 2019-2025 Sonova

Verifying: C:\Program Files (x86)\Advanced Bionics\Target CI\SonovaVerify.DAT
Target: C:\Program Files (x86)\Advanced Bionics\Target CI
Product: Target CI 1.5.11.0

FILES PROCESSED: 779

IGNORED FILES: 3
.\config\App.xml
.\data\
.\sonovaverify.dat

NO ERRORS DETECTED.
Press any key to continue . . .
```

The output “NO ERRORS DETECTED” corresponds to a successfully performed integrity and authenticity verification of the fitting software installation medium contents. This means that SonovaVerify.exe has authenticated and verified the integrity of all files and folders. This verifies that the contents of the fitting software installation media have not been tampered with, corrupted, or otherwise compromised.

SonovaVerify.exe will display warnings or error messages if files or folders are missing, or unexpected files or folders have been added to the installation media. In case warning or error messages are displayed, the integrity and authenticity verification of the fitting software installation media contents failed and it is recommended to:

- not proceed with installation
- not open or execute any file contained in the fitting software installation image report the issue to Advanced Bionics support (refer to Section 2.1)

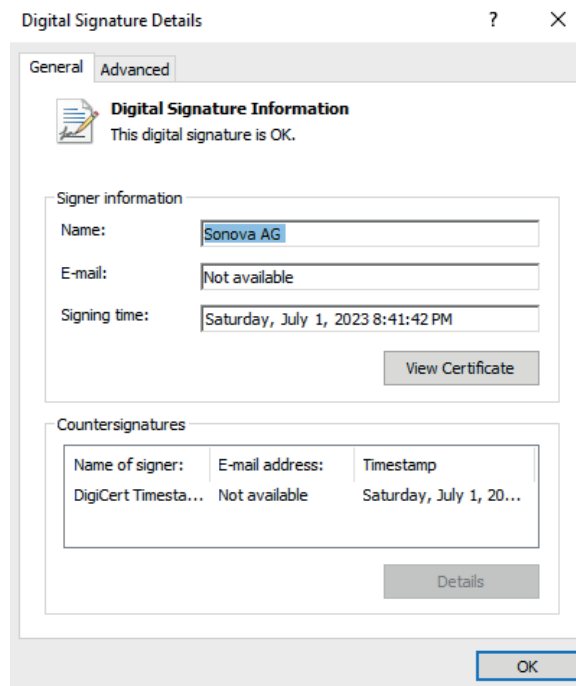
8.3 AUTOMATIC VERIFICATION OF INSTALLED FITTING SOFTWARE INTEGRITY

SonovaVerify is integrated with the fitting software and runs each time the application is launched to verify the integrity of the fitting software’s program files. Program files are digitally signed using industry-standard practices and certificates issued by a trusted certificate authority. The software notifies the user via warning messages if any program files are compromised.

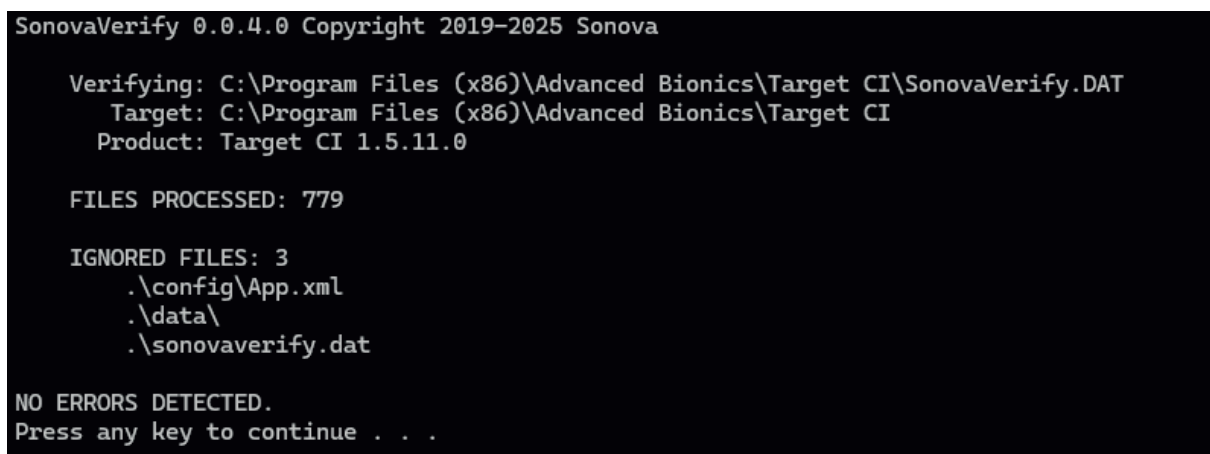
8.4 MANUAL VERIFICATION OF INSTALLED FITTING SOFTWARE INTEGRITY

Users may perform the following steps to verify the installed fitting software's integrity and authenticity at any time without the need to launch the fitting software:

1. Open Windows Explorer and navigate to the fitting software's executable folder, usually located in: C:\Program Files (x86)\Advanced Bionics\Target CI\
2. Right click on SonovaVerify.exe and select Properties from the context menu.
3. Select the Digital Signatures tab.
4. Double click the SHA256 "Sonova AG" signature.
5. Verify the elements of the signature are valid, in particular that the message "The digital signature is OK." appears near the top and that the signer's name and signing time match the following image:



6. Click the “View Certificate” button and the “Details” tab and verify that the value of the “Thumbprint” field matches this one: db88d10f0a1bfb12be6c3c46c516e507e14f2593
7. Close the popup dialogs and double click SonovaVerify.exe
8. Verify that “NO ERRORS DETECTED.” is displayed as shown in the following image:



```
SonovaVerify 0.0.4.0 Copyright 2019-2025 Sonova

Verifying: C:\Program Files (x86)\Advanced Bionics\Target CI\SonovaVerify.DAT
Target: C:\Program Files (x86)\Advanced Bionics\Target CI
Product: Target CI 1.5.11.0

FILES PROCESSED: 779

IGNORED FILES: 3
.\config\App.xml
.\data\
.\sonovaverify.dat

NO ERRORS DETECTED.
Press any key to continue . . .
```

The output “NO ERRORS DETECTED” corresponds to a successfully performed integrity and authenticity verification of the fitting software installation medium contents. This means that SonovaVerify.exe has authenticated and verified the integrity of all files and folders. This verifies that the contents of the fitting software installation media have not been tampered with, corrupted, or otherwise compromised.

SonovaVerify.exe will display warnings or error messages if files or folders are missing, or unexpected files or folders have been added to the installation media. In case warning or error messages are displayed, the integrity and authenticity verification of the fitting software installation media contents failed and it is recommended to:

- not proceed with installation
- not open or execute any file contained in the fitting software installation image report the issue to Advanced Bionics support (refer to Section 2.1)

9. SOFTWARE PATCHES AND UPDATES

Auto-updates are not supported. Refer to Section 12 for more information.

10. DATA MANAGEMENT

10.1 DATABASES

The fitting software uses a transactional database for storing patient data and a set of info databases that provide metadata configurations required by the application.

See Section 3. Network and Context Diagrams - Deployment Artifacts for a detailed list of all databases deployed by the fitting software.

When the fitting software is installed as a standalone application, the patient database is internal to the fitting software. The patient database, stored in file PatientDatabase.sqlite, resides on the same machine as the fitting software and provides the storage for patient data. To back up application data when Target CI is deployed as a standalone application, create a backup copy of the entire folder located at %ProgramData%\Advanced Bionics\Target CI\Target CI\Data. Protect data backups not only from data loss but also from theft. When the fitting software is installed as a Noah module, patient data is stored in the database provided by the Noah System. The Noah database may be configured for network access. The Noah database may also be configured for non-network access and installed on the same PC as the fitting software. Configure Noah database encryption to protect data (refer to HIMSA documentation).

For the Noah distributed deployment mode, refer to the following link for instructions about backup and restore of the Noah patient database:

<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/>

10.2 DATA MIGRATION

The fitting software allows users to migrate patient records from AB's previous fitting software, SoundWave 3.2. Patient records must be accessible from a SoundWave 3.2 installation on the same computer as Target CI in order to be migrated.

10.3 HEARING DEVICE CONFIGURATIONS

The fitting software provides for exporting and importing device configurations and settings.

10.4 DATA DISPOSAL

Refer to Section 5.4, Removal and Decommissioning, in this document and the Disposal and Hazardous Materials section of the IFU for guidance on data disposal. For Noah deployments, detailed instructions for deleting patient records are available at:

<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/>

11. SECURITY ENVIRONMENT – SHARED RESPONSIBILITY

The fitting software has been designed for an intended use in which cybersecurity risk management is considered a shared responsibility among stakeholders across the entire hearing care ecosystem which include, but are not limited to, hearing device users, parents or legal guardians of children who are hearing device users, HCPs, IT administrators, hearing care facilities and providers, vendors of hearing devices and programming equipment.

Here follows a list of best common practice recommendations and security controls for the fitting environment where the fitting software will be used:

OS level

- Apply access controls at OS level, e.g.:
 - Eliminate guest accounts
 - Activate the Windows user login
 - Maintain a list of authorized operators to control access to the system
 - Set Customized users and roles
 - Apply strong password requirements and keep credentials secret
 - Enable idle session timeout
- Apply audit controls at OS level
- Make sure the operating system is up to date
- Make sure the installed fitting software version is up to date
- Use adequate and up-to-date malware and antivirus protection
- Make sure to disable AutoRun and AutoPlay features
- Enable application whitelisting

Data protection

- Please ensure that none of the folders or files containing application data is shared on the network. The default locations of the application data are listed in the table in section 5.4. To check for network shares exposed by a computer, navigate to “Computer Management -> Shared Folders -> Shares” in Microsoft’s Computer Management tool or run PowerShell command `Get-WmiObject -class Win32_Share`.
- During installation the permission on the application data folder is set according to Section 6.1. Application data folders inherits access permissions from the parent folder. The permission management on the parent folder is the responsibility of the operator of the software.
- Encrypt patient data using 3rd party tools or controls at OS level by using drive encryption (e.g., the free Microsoft BitLocker) to protect all data. For Noah deployments, consider using the Noah database encryption.
- External media containing data exported from fitting software including reports and logs should be secured. When no longer used, the data should be securely erased and/or the media should be securely deleted.

- Use USB storage media with built in security functionality, like encrypted USB drives with integrated keypad.
- Always ensure data security by following these practices:
 - When transmitting data over unsecured channels, either anonymize or encrypt the data.
 - Protect data backups not only from data loss but also from theft.
 - Remove all data from data medium which are no longer used or will be disposed.
- Approved procedures and tools should be applied by users for secure removal of data stored on removable media, according to applicable regulations and guidelines for handling patient information / personally identifiable information (PII) / protected health information (PHI)

IT infrastructure

Operate fitting software in a secure network environment protected from unauthorized intrusion. There are many effective techniques for isolating and protecting medical information systems, including implementing firewall protection, demilitarized zones (DMZs), Virtual Local Area Networks (VLANs) and network enclaves. Maintain an active network connection to receive operating system updates.

Physical level

- The workstation where fitting software is installed should be physically secured in a way that it is not accessible to nor may be tampered by unauthorized personnel.
- Access to printers connected to the workstation should be controlled.
- The monitor of the workstation where fitting software is installed should be placed in a way limiting the visibility of the screen content to the user only.

Organizational level

- Only professionally trained, fully qualified personnel are authorized to operate the system. Before authorizing anyone to operate the system, it should be verified that the person has read and fully understands the operating instructions provided with the fitting software.
- Only personnel authorized to maintain and operate the fitting software must be provisioned with accounts for the machine where the software is installed. The computer and domain accounts and the associated access rights should be periodically reviewed and disabled if the access to the machine is no longer needed.
- If you notice any suspicious activity on your fitting software accounts or any unexpected operation, contact Advanced Bionics. Refer to section 2.1 for more information.

For more information about shared responsibility and for a more detailed list of best practice recommendations and security controls for the fitting environment where the fitting software will be used to be applied at various levels refer to:

- the EHIMA Whitepaper “Best Practices for Secure Fitting of Hearing Devices,” [EHIMAWhitePaper](#)

12. MANUFACTURING, SOFTWARE DEVELOPMENT, AND SECURITY MANAGEMENT

Cybersecurity is considered throughout the entire software development process. The fitting software is developed in compliance with IEC 62304 and IEC 82304 standards.

The fitting software is scanned for viruses and malware as part of the manufacturing process.

Vulnerabilities in third-party components listed in NIST's National Vulnerability Database (NVD), are assessed, and mitigated during the development process and monitored once the fitting software has been released to the market.

Configuration management

AB internally develops, documents and maintains under configuration control the baseline configuration of each released fitting software version.

All third-party software components used by the fitting software application are identified and documented in the software bill of materials (SBOM). SBOM is used by AB in cybersecurity risk management to assess and monitor the exposure to cybersecurity threats and disclosed vulnerabilities by using up-to-date vulnerability scanning tools.

Security updates

AB is constantly monitoring for security vulnerabilities affecting fitting software. This includes vulnerabilities in the fitting software and in third-party components used by the fitting software application.

Announced vulnerabilities are assessed based on the fitting software's configuration and use.

When needed, security vulnerabilities may be fixed by a broader fitting software release that implements patches to specific software components within the software set.

Vulnerability disclosure

We are committed to vulnerability disclosure and to improving the security of our products and services.

Reporting of suspected vulnerabilities or security concerns related to our products or underlying software/infrastructure is encouraged.

Please read our vulnerability disclosure policy published at <https://www.sonova.com/en/coordinated-vulnerability-disclosure-policy> and follow the instructions to submit a report.

13. SOFTWARE COMPONENTS AND BILL OF MATERIALS

The fitting software incorporates certain commercial off-the-shelf software components.

The following table enumerates all SOUP (Software of Unknown Provenance) distributed with the fitting software.

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
AForge.NET	AForge.NET maths and media library, part of and required by IceLink and LiveSwitch.	AForge.NET	2.2.5.0
Amplifon. Programmer	Component of Amplifon's software suite	Amplifon	3.3.4.0
Amplifon. Programmer.Core	Component of Amplifon's software suite	Amplifon	1.0.4.0
AutoMapper	Automates object-to-object mapping	Jimmy Bogard	10.1.1.0
BenchmarkDotNet	library for benchmarking, providing tools to measure and compare the performance of code	BenchmarkDotNet Community	0.13.0.0
Castle.Core	A core library of the Castle Project, offering components like dynamic proxy generation and inversion of control containers for .NET applications.	Castle Project	4.4.1
Chessie	A functional error handling library for F#	Open Source	0.6.0.0
ciAD Hearingloss Simulator	Hearing loss simulator library for media player	ciAD (Jürg Haubold)	4.0.0.1
ClosedXML	Simplifies reading, manipulating, and writing Excel files without requiring Excel to be installed	ClosedXML Community	0.95.4.0
CommandLine Parser	Provides a clean and concise API for parsing command-line arguments	CommandLineParser Community	2.4.3
Common.Logging	A portable logging abstraction for .NET applications	Common.Logging Community	3.4.1.0
CommonService Locator	Provides a common interface for service location, allowing applications to decouple from specific IoC containers.	Microsoft	2.0.5.0

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
Credential Management	Credential Management package is a wrapper for the Windows Credential Management API	iLya Lozovyy	1.0.2
CSharpAnalytics	Used for Google Analytics.	Attack Pattern	1.6.1
Dapper	ORM	Sam Saffron,Marc Gravell,Nick Craver	2.0.78.45418
Deconstructurama. Attributed	Used by Nephele libraries.	Serilog Contributors	3.1.0.0
Developer Express Suite	A comprehensive suite of UI controls and libraries for .NET developers, offering tools for building feature-rich applications.	Developer Express Inc	20.2.10.0
DirectShow 2005	Allows access to Microsoft's DirectShow functionality from within .NET applications.	Microsoft	2.0
DSL4	DSL 4 Fitting formula library	National Centre for Audiology, Canada	4.2
DSL5	DSL 5 Fitting formula library	National Centre for Audiology, Canada	5.0.34
ExcelNumberFormat	Provides functionality for parsing and formatting Excel number formats	Open Source	1.1.0.0
FM.dll	Integral to their real-time communication frameworks like LiveSwitch and IceLink	FM (Frozen Mountain)	2.9.32
FSharp.Core	The core library for the F# programming language	Microsoft	6.0.322.10402
FTDI Chip	A driver package from Future Technology Devices International (FTDI) that facilitates communication between USB devices and software applications.	FTDI	3.02.07
GNOtometrics. Aurical	GNOtometrics.Aurical repacked for Sonova	Natus Medical Incorporated	2.0.1.9
SharedUtilities.dll	provides common utility functions and shared resources across Natus applications.	Natus Medical Incorporated	1.0.0.0
Hardware.Info	A component that gathers and provides detailed information about the hardware configuration of a system	Open Source	11.1.0.1

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
Himsa.NLWSMAPI.dll	A library associated with HIMSA's Noah software	HIMSA	2.0.3.0
natus.otometrics.hipro2	HiPro communication libraries	Natus Medical Incorporated	2.0.0.4
lced.dll	facilitates real-time communications by enabling audio, video, and data streaming	FM (Frozen Mountain)	1.12.0.0
IceLink	Used for WebRTC audio/video conference integration	FM (Frozen Mountain)	3.13.100.13250
icudt.dll	offers Unicode and globalization support for software applications	FM (Frozen Mountain)	54.1.0.0
IdentityModel	OpenID Connect & OAuth 2.0 client library used by the Kona.CommonServices. Authentication component for OAuth 2 authentication.	Dominick Baier,Brock Allen	6.2.0.0
IMCInterfaces	Noah Inter-Module Communication Interface Library	HIMSA II K/S	4.4.0.2266
iText 7	PDF library to create, modify, and inspect PDF documents programmatically.	iText Software	7.1.16.0
JetBrains.dotMemory	A memory profiling tool to detect memory leaks and optimize memory usage in .NET applications	JetBrains	111.0.0.0
JsonDiffPatch DotNet.dll	Provides functionalities to compare and patch JSON objects	Open Source	1.0.1.0
LibGit2Sharp	Used by libraries coming from Sonova to communicate with Git	LibGit2Sharp contributors	0.26.1.93
LiveSwitch	Used for WebRTC audio/video conference integration.	FM (Frozen Mountain)	1.18.5.32382
log4net.dll	logging framework for .NET	Apache	4.7.0.3189
Mapster	Used for mapping objects in code	chaowlert,eric_swann	7.2.0.0
Mapster.Core	Used for mapping objects in code	chaowlert,eric_swann	1.2.0.0
MathNet.Numerics	Used for fitting algorithms (signal path, target matcher etc)	Christoph Ruegg, Marcus Cuda, Jurgen Van Gael and contributors	4.11.0

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
Microsoft.Bcl.AsyncInterfaces	Provides the <code>IAsyncEnumerable<T></code> and <code>IAsyncDisposable</code> interfaces and helper types for .NET Standard 2.0.	Microsoft	6.0.21.52210
Microsoft.CodeAnalysis.Common	Used by the libraries coming from Sonova. HardwareAbstraction.Palio. Trafo	Microsoft	3.900.21.12420
Microsoft.CodeAnalysis.CSharp	Used by the libraries coming from Sonova. HardwareAbstraction.Palio. Trafo	Microsoft	3.900.21.12420
Microsoft.CSharp.dll	Provides compilation and code generation using C#	Microsoft	4.700.19.56404
Microsoft.Diagnostics.FastSerialization.dll	Used for efficient serialization and deserialization of diagnostic data	Microsoft	1.0.0.0
Microsoft.Diagnostics.NETCore.Client.dll	A managed library that allows interaction with the .NET Core runtime for various diagnostic tasks, such as tracing and requesting dumps.	Microsoft	0.2.4.27602
Microsoft.Diagnostics.Runtime.dll	provides APIs for inspecting live processes and crash dumps, enabling developers to build debugging and diagnostic tools.	Microsoft	2.0.4.26801
Microsoft.Diagnostics.Tracing.TraceEvent.dll	A library for parsing and processing Event Tracing for Windows (ETW) events	Microsoft	2.0.70
Microsoft.DotNet.PlatformAbstractions.dll	Provides APIs for accessing information about the .NET platform	Microsoft	3.100.620.31604
Microsoft.Extensions.DependencyInjection.Abstractions	Defines the abstractions for dependency injection in .NET applications	Microsoft	6.0.21.52210
Microsoft.Extensions.Logging	Facilitates structured logging in .NET applications.	Microsoft	6.0.21.52210
Microsoft.Extensions.Options	Supports the configuration of options in .NET applications	Microsoft	6.0.21.52210

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
Microsoft.Extensions.Primitives	Provides interfaces and classes for change tracking and cancellation tokens, aiding in the management of mutable data and resource cleanup.	Microsoft	6.0.21.52210
Microsoft.Identity.Client	The MSAL library for .NET is part of the Microsoft identity platform for developers (formerly named Azure AD) v2.0. It enables you to acquire security tokens to call protected APIs. It uses industry standard OAuth2 and OpenID Connect.	Microsoft	4.38.0.0
Microsoft.Identity.Client.Extensions.Msal	Secure cross-platform token cache for MSAL public client apps.	Microsoft	2.19.3.0
Microsoft.IdentityModel.JsonWebTokens	Includes types that provide support for creating, serializing and validating JSON Web Tokens. Used by components that communicate with back-end services that use JSON Web Tokens for authentication.	Microsoft	6.8.0.11012
Microsoft.IdentityModel.Logging	Dependency of Microsoft.IdentityModel.Tokens	Microsoft	6.8.0.11012
Microsoft.IdentityModel.Tokens	Dependency of the SOUP Microsoft.IdentityModel.JsonWebTokens	Microsoft	6.8.0.11012
Microsoft.ML.OnnxRuntime	An inference engine for running machine learning models in the ONNX (Open Neural Network Exchange) format	Microsoft	1.12.1
Microsoft.ML.OnnxRuntime.Managed	The managed .NET wrapper for the ONNX Runtime	Microsoft	1.12.1
Microsoft.Office.Interop.Excel.dll	Part of the Office Interop assemblies, this DLL enables .NET applications to interact with Microsoft Excel	Microsoft	14.0.4733.1000
Microsoft.VisualStudio.TextTemplating.10.0	Provides text templating capabilities within Visual Studio, allowing developers to generate code and other text-based artifacts using T4 templates.	Microsoft	10.0.40219.1

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
Microsoft.Win32.Registry.dll	Provides access to the Windows registry	Microsoft	5.0.20.51904
Microsoft.Win32.SystemEvents.dll	Supports system event handling in .NET applications	Microsoft	8.0.23.53103
Microsoft.Win32.TaskScheduler.dll	Used for FSW backup tool (automated backups).	David Hall	2.5.11.0
Microsoft.Xaml.Behaviors.Wpf	XAML Behaviors is an easy-to-use means of adding common and reusable interactivity to your WPF applications with minimal code.	xamlexperienceteam, Microsoft	1.0.1.0
Microsoft DIA SDK	Provides APIs for working with debugging information in PDB files	Microsoft	2.0.0.0
MS VC++ 2008 Redistributable	Microsoft Visual C++ 2008 Redistributable	Microsoft	9.0.30729.6161
Microsoft Visual C++ 2010 x86 Redistributable	Microsoft Visual C++ 2010 Redistributable	Microsoft	10.0.40219.325
Microsoft Visual C++ 2012 Redistributable	Microsoft Visual C++ 2012 Redistributable	Microsoft	11.0.51106.1
Microsoft Visual C++ 2017 Redistributable (x86)	Microsoft Visual C++ 2017 Redistributable	Microsoft	14.16.27024.1
Mono.Cecil	Used for inspecting, modifying, and creating .NET assemblies	Microsoft	0.11.3.0
Moq.dll	Open-source .NET library for creating mock objects during unit testing	Moq Community (Open Source)	4.16.1.0
MS-VisualC++ 7.1 runtime libraries	Microsoft Visual C++ runtime libraries	Microsoft	7.10.6030.0
NAL-NL1	NAL-NL1 Fitting formula library	Australian Hearing	1.1.0.0
NAL-NL2	NAL-NL2 Fitting formula library	Australian Hearing	2.0.11
NAudio.dll	Used to adjust volumes and play soundfiles.	Open Source	1.9.0.0
.NET Framework	.NET runtime framework	Microsoft	4.8.3928.0
Newtonsoft.Json	Used for JSON serialization and de-serialization.	James Newton-King	13.0.3.27908
Newtonsoft.Json.Schema.dll	A schema validation library for JSON data	James Newton-King	3.0.14.25421
Nibelung	NoahLink Wireless fitting libraries	HIMSA	1.3.16.1

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
Nibelung2.CPD	NoahLink Wireless fitting libraries	HIMSA	2.0.3.0
Nlog	This a dependency of the HIMSA Nibelung.CPD (Noahlink Wirless)	Kim Christensen	5.0.4.1331
Noahlink	Noahlink fitting device driver	HIMSA	1.55.6.166
Noahlink Wireless Driver	Noahlink Wireless fitting device driver	HIMSA	1.1.0.0
Noahlink Wireless Upgrader	Noahlink Wireless firmware Upgrader	HIMSA	3.1.0.82
ModuleAPI.dll (Noah System)	A component of HIMSA's Noah System, providing APIs for integrating and managing audiological data	HIMSA	4.13.0.5404
NiXPS SDK	Provides functionalities for handling XPS (XML Paper Specification) documents	NiXPS NV	2.6.0.0
NPOI	An open-source library that facilitates reading and writing Microsoft Office documents in .NET applications	NPOI communi	2.4.1.0
NuGet Package Manager	A tool for managing .NET libraries and packages	Microsoft	6.3.0.131
Nunit	A unit-testing framework for .NET applications	NUnit Project	3.12.0.0
ONNX Runtime	Engine for Open Neural Network Exchange (ONNX) models	Microsoft	1.12.20220803.2.7048164
Open XML SDK	Provides tools for working with Office Open XML documents	Microsoft	2.7.2
OSExtensions.dll	library offering extensions for operating system functionalities	Microsoft	1.0.0.0
Otometrics.REMaccess	Otometrics' abstraction Layer above the Noah Inter-Module Communication Interface Library	GN Otometrics	1.0.0.10

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
Paket.Core.dll	An open-source dependency manager for .NET and Mono projects	Paket Community (Open Source)	7.1.5.0
Patagames.Pdf	The C# PDF Library to Create and Edit PDF documents in .Net applications.	patagames.com	8.57.30.48
Patagames.Pdf. Wpf	The C# PDF Library to Create and Edit PDF documents in .Net applications.	Patagames.com	4.19.18.48
Polly	Library that allows developers to express resilience and transient fault handling policies such as Retry, Circuit Breaker, Bulkhead Isolation and Fallback in a fluent and thread-safe manner	App vNext	7.2.3.0
Portable. BouncyCastle	This a dependency of the HIMSA Nibelung.CPD (Noahlink Wirless)	The Legion of the Bouncy Castle Inc	1.8.15362.1
Portable. BouncyCastle. Crypto	This a dependency of the HIMSA Nibelung.CPD (Noahlink Wirless)	The Legion of the Bouncy Castle Inc	1.9.0.1
protobuf-net.dll	Serialization framework used for RC blob.	Open Source	2.3.2.0
Google.Protobuf	Google's official Protocol Buffers library for .NET, facilitating the serialization and deserialization of structured data.	Google Inc	3.19.3.0
Perfolizer.dll	An open-source library for performance analysis	Open Source	0.2.1.0
Rhino.Mocks.dll	A dynamic mock object framework for .NET	Rhino Mocks Community	3.6.0.0
Security. Cryptography. NetCore.dll	provides cryptographic functionalities for .NET Core applications	HardDev	1.0.1.0

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
Serilog	The logging component which is used for the whole Chinook application.	Serilog Contributors	3.0.1.0
Serilog.Enrichers.Thread	Enrich Serilog events with properties from the current thread	Serilog Contributors	3.1.0.0
Serilog.Extensions.Logging	Integrates Serilog with Microsoft's logging abstractions	Serilog Contributors	3.1.0.0
Serilog.Expressions	Expression-based event filtering for Serilog.	Serilog Contributors	2.0.0.0
Serilog.Sinks.Console	A Serilog sink that writes log events to the console/terminal.	Serilog Contributors	4.0.0.0
Serilog.Sinks.Debug	A Serilog sink that writes log events to the debug output window.	Serilog Contributors	2.0.0.0
Serilog.Sinks.File	Write Serilog events to text files in plain or JSON format.	Serilog Contributors	4.1.0.0
Serilog.Sinks.NUnit.dll	Integrates with NUnit, directing log events to NUnit's test output, aiding in test diagnostics.	Serilog Contributors	1.0.3.0
Serilog.Sinks.Trace	The diagnostic trace sink for Serilog.	Serilog Contributors	2.1.0.0
Serilog.Settings.AppSettings	XML configuration (System.Configuration <appSettings>) support for Serilog.	Serilog Contributors	2.2.2.0
Security.Cryptography.NetCore.dll	Extensions to the security APIs shipped with the .NET framework	Microsoft	1.0.1.0
SharpBITS API	SharpBITS.NET is a .NET wrapper of the BITS API and a little Windows UI application for easier access to BITS up- and downloads.	perpetualKid	2.1.0.0

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
SharpZipLib	#ziplib (SharpZipLib, formerly NzipLib) is a Zip, Gzip, Tar and Bzip2 library written entirely in C# for the .NET platform. This library provides compression functionality (zip, unzip, stream compression, etc.). We use it in the Firmware Update app.	Open Source	1.3.3.11
SharpDX	Used by LiveSwitch: SharpDX.Direct3D11, SharpDX.Direct2D1, SharpDX.Mathematics	Alexandre Mutel	4.0.1
SocketIOClient	Provides a client for Socket.IO, enabling real-time bidirectional event-based communication in .NET applications	HeroWong	2.2.4.0
Superpower	A parser combinator library for C#	Datalust, Superpower Contributors, Sprache Contributors	2.3.0.0
SQLite.Interop	SQLite 3.36.0 Native Interop Library. SQLite is the inprocess database used to store information about patient (in standalone mode), our product catalog and its resources and the metadata for fitting, accessories and His. SQLite is Public Domain.	SQLite Development Team	1.0.115
System.Buffers	Provides resource pooling of any type for performance-critical applications that allocate and deallocate objects frequently.	microsoft, dotnetframework	4.6.28619.01

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
System.Collections.Immutable	Used by the libraries coming from Sonova. HardwareAbstraction. Palio.Trafo	Microsoft	7.0.22.51805
System.ComponentModel.Annotations	Provides attributes that are used to define metadata for objects used as data sources.	microsoft, dotnetframework	4.6.26515.06
System.Configuration.ConfigurationManager	Provides types that support using configuration files.	Microsoft	5.0.20.51904
System.CodeDom.dll	Provides classes for generating and compiling source code into executable files or assemblies	Microsoft	8.0.23.53103
System.Data.SQLite	Used by the libraries coming from Sonova. HardwareAbstraction. Palio.Trafo	SQLite Development Team	1.0.115.0
System.Diagnostics.DiagnosticSource	A logging library that allows developers to track and monitor diagnostic data	Microsoft	6.0.21.52210
System.Diagnostics.PerformanceCounter	Provides APIs to interact with Windows performance counters	Microsoft	7.0.22.51805
System.Drawing.Common	Provides access to GDI+ graphics functionality.	Microsoft	8.0.324.11603
System.Formats.Asn1.dll	Supports the encoding and decoding of Abstract Syntax Notation One (ASN.1) data	Microsoft	6.0.21.52210

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
System.IdentityModel.Tokens.Jwt	Includes types that provide support for creating, serializing and validating JSON Web Tokens. Used by components that communicate with back-end services that use JSON Web Tokens for authentication.	Microsoft	6.8.0.11012
System.IO.Abstractions	A set of abstractions to help make file system interactions testable.	Tatham Oddie & friends	12.0.10.46693
System.IO.Hashing.dll	Provides hashing functionalities within .NET, including algorithms for computing checksums and cryptographic hashes.	Microsoft	6.0.222.6406
System.IO.Packaging.dll	Enables reading and writing of package files	Microsoft	6.0.21.52210
System.IO.Ports.dll	Provides classes for serial port communication, enabling .NET applications to interact with hardware connected via serial ports.	Microsoft	8.0.23.53103
System.Net.Http.WinHttpHandler.dll	A specialized HTTP handler for Windows	Microsoft	6.0.422.16404
System.Numerics.Vectors	Provides hardware-accelerated numeric types, suitable for high-performance processing and graphics applications.	microsoft, dotnetframework	4.6.26515.06

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
System.Memory	Provides types for efficient representation and pooling of managed, stack, and native memory segments and sequences of such segments, along with primitives to parse and format UTF-8 encoded text stored in those memory segments.	microsoft, dotnetframework	4.6.31308.01
System.Reactive.dll		Open Source	5.0.0.1
System.Reflection.DispatchProxy	Provides a class to dynamically create proxy types that implement a specified interface and derive from a specified DispatchProxy type. Method invocations on the generated proxyinstance are dispatched to that DispatchProxy base type.	Microsoft	4.700.20.21406
System.Reflection.Metadata	This packages provides a low-level .NET (ECMA-335) metadata reader and writer. It's geared for performance and is the ideal choice for building higher-level libraries that intend to provide their own object model, such as compilers.	Microsoft	5.0.20.51904
System.Reflection.TypeExtensions	Provides extension methods for the reflection API	Microsoft	4.700.19.56404
System.Runtime.CompilerServices.Unsafe	Provides the System.Runtime.CompilerServices.Unsafe class, which provides generic, low-level functionality for manipulating pointers.	microsoft, dotnetframework	6.0.21.52210

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
System.Security.AccessControl	Provides base classes that enable managing access and audit control lists on securable objects.	Microsoft	6.0.21.52210
System.Security.Permissions	Provides types supporting Code Access Security (CAS).	Microsoft	5.0.20.51904
System.Security.Principal.Windows	Provides classes for retrieving the current Windows user and for interacting with Windows users and groups.	Microsoft	5.0.20.51904
System.Security.Cryptography.Cng.dll	Provides cryptographic functionality using Cryptography Next Generation (CNG) APIs	Microsoft	5.0.20.51904
System.Security.Cryptography.Pkcs.dll	Offers classes for handling Public Key Cryptography Standards (PKCS), including signed and enveloped data	Microsoft	6.0.1923.31806
System.Security.Cryptography.ProtectedData.dll	Provides methods for protecting and unprotecting data, utilizing Windows Data Protection API (DPAPI) for secure data storage.	Microsoft	6.0.21.52210
System.Security.Cryptography.Xml.dll	Enables XML encryption and digital signatures, supporting secure XML data handling in .NET applications.	Microsoft	6.0.822.36306
System.ServiceModel.Http.dll	Provides HTTP-based communication functionality for Windows Communication Foundation (WCF) services	Microsoft	4.700.19.56502

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
System.ServiceModel.Primitives.dll	Contains fundamental classes for WCF services, including base classes and interfaces for service contracts and channels.	Microsoft	4.700.19.56502
System.Text.Encoding.CodePages	Provides support for code-page based encodings, including Windows-1252, Shift-JIS, and GB2312.	Microsoft	5.0.20.51904
System.Text.Encodings.Web	Provides types for encoding and escaping strings for use in JavaScript, HyperText Markup Language (HTML), and uniform resource locators (URL). Is a dependency of SOUP IdentityModel	microsoft, dotnetframework	6.0.21.52210
System.Text.Json	Provides high-performance and low-allocating types that serialize objects to JavaScript Object Notation (JSON) text and deserialize JSON text to objects, with UTF-8 support built-in. Also provides types to read and write JSON text encoded as UTF-8, and to create an in-memory document object model (DOM), that is read-only, for random access of the JSON elements within a structured view of the data.	Microsoft	6.0.222.6406
System.Threading.Tasks.Extensions	Provides additional types that simplify the work of writing concurrent and asynchronous code.	microsoft, dotnetframework	4.6.28619.01

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
System. Threading. Channels	Provides a set of synchronization data structures for passing data between producers and consumers, supporting high-performance parallel programming.	Microsoft	6.0.21.52210
System. ValueTuple	Provides the System.ValueTuple structs, which implement the underlying types for tuples in C# and Visual Basic. Adds value tuples support since they are only included in later .NET framework versions.	microsoft, dotnetframework	4.6.26515.06
TestStack.BDDfy. dll	A Behavior-Driven Development (BDD) framework for .NET	TestStack Community	4.3.2.0
Thrift	Used for remotelink protocol definition	Apache	0.13.0.0
Unity.Container	The Unity Container (Unity) is a full featured, extensible dependency injection container.	Unity Container Project	5.8.13.0
Unity. Configuration	The Unity Container (Unity) is a full featured, extensible dependency injection container.	Unity Container Project	5.2.5.0
Unity. Abstractions	The Unity Container (Unity) is a full featured, extensible dependency injection container.	Unity Container Project	3.3.1.0
Unity. Interception. Configuration	The Unity Container (Unity) is a full featured, extensible dependency injection container.	Unity Container Project	5.1.7.0
Unity. Interception	The Unity Container (Unity) is a full featured, extensible dependency injection container.	Unity Container Project	5.5.5.0

SOUP ITEM	FUNCTIONALITY DESCRIPTION	MANUFACTURER	VERSION
Unity. Registration ByConvention	The Unity Container (Unity) is a full featured, extensible dependency injection container.	Unity Container Project	2.1.9.0
Unity. ServiceLocation	The Unity Container (Unity) is a full featured, extensible dependency injection container.	Unity Container Project	2.1.2.0
WAP BT Dongle Driver	WAP BT Dongle Driver (Fitting Dongle)	iAnywhere Solutions	3.0.0.6095
WebSync	Used for integration of fitting data channel	FM (Frozen Mountain)	4.9.32.0
WPFHexaEditor.dll	A hexadecimal editor control for WPF applications	FM (Frozen Mountain)	2.1.6
WpfScreen Helper.dll	A utility library for WPF applications that provides screen and monitor information	FM (Frozen Mountain)	2.1.0.0
Xceed Extended WPF Toolkit	A collection of WPF controls and utilities that enhance WPF applications with additional UI components.	Xceed	3.5.0.0
xmlunit-core.dll	A library for testing and comparing XML output.	XMLUnit Community	2.9.0.205
Xps to Pdf render (NiXPS)	Convert programmatically xps files to pdf; used in fitting app reports.	NiXPS	2.6.7.0

14. REFERENCES

Title	Website
Instructions for Use (Electronic)	https://ifu.advancedbionics.com/
Advanced Bionics Global Privacy Policy	https://advancedbionics.com/privacy
HIMSA	https://www.himsa.com/
Noah System 4	https://www.himsa.com/products/all-about-noah-system-4/
Backing up and restoring the data in your Noah database	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/
Noah System Database Capacity has been Reached.	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/noah-system-database-capacity-has-been-reached/
TeamViewer - List of used ports	https://community.teamviewer.com/English/kb/articles/4139-ports-used-by-teamviewer
BCP 195	https://www.rfc-editor.org/info/bcp195
LiveSwitch Server Security Documentation	https://developer.liveswitch.io/liveswitch-server/server/security.html
Best Practices for Secure Fitting of Hearing Devices EHIMA whitepaper	https://www.ehima.com/wp-content/uploads/2021/09/EHIMA_Cybersecurity-FSW-Security-Whitepaper_v1-Sep2021.pdf

 Advanced Bionics LLC
28515 Westinghouse Place
Valencia, CA 91355, United States
T: +1.661.362.1400

info.us@advancedbionics.com

 Advanced Bionics
Logistic Services GmbH
Rheinmetallstraße 18A
99610 Sömmerda, Germany

info.switzerland@advancedbionics.com

For information on additional AB locations, please visit
advancedbionics.com/contact

AB – A Sonova brand

Please contact your local AB representative for regulatory approval and
availability in your region.

The Bluetooth® word mark and logos are registered trademarks owned by
Bluetooth SIG, Inc., and any use of such marks by Sonova AG is under license.



029-S398-02