Target CI الإصدار 1.5

دليل الأمن السيبراني

العربية

تاريخ التحديث: سبتمبر 2025

A Sonova Brand

المحتويات

1. مقدمة

توفر هذه الوثيقة معلومات فنية حول الأمان والخصوصية الخاصة بنظام برنامج Target CI v1.5 من شركة Advanced Bionics، والذي يُشار إليه فيما بعد باسم "برنامج التركيب". تم تصميم برنامج التركيب ليُستخدم من قِبل خبراء السمع المؤهلين (HCP) لتكوين (أي تركيب) أجهزة السمع للمرضى الذين تلقوا غرسات قوقعة صناعية من شركة Advanced Bionics.

تركز هذه الوثيقة تحديدًا على اعتبارات الأمن السيبراني والخصوصية المرتبطة باستخدام برنامج التركيب. وتتضمن تقييمًا لضوابط الأمان والخصوصية المدمجة حاليًا في البرنامج، بالإضافة إلى تلك التي يُتوقع تطبيقها وتكوينها ضمن بيئة تكنولوجيا المعلومات التي سيُستخدم فيها المنتج لغرضه المقصود.

لا تقدم هذه الوثيقة معلومات فنية تتعلق بالأمان والخصوصية حول:

- الإصدارات السابقة من برنامج تركيب AB
- برامج AB بخلاف Target CI v1.5
- مواقع AB الإلكترونية
- تطبيقات الهاتف المحمول من AB
- أجهزة AB السمعية

1.1 الاختصارات والتعريفات:

الاختصار	المصطلح
FSW	برنامج التركيب
HCP	خبير السمع
SaMD	البرنامج كجهاز طبي
AB	Advanced Bionics
IFU	إرشادات الاستخدام

2. موارد أخرى

2.1 دعم العملاء

للمقيمين داخل الولايات المتحدة وكندا، توفر شركة Advanced Bionics خطًا ساخنًا مجانيًا للدعم التقني (877-271-6727) حيث يتوفر دعم مهني مخصص من الاثنين إلى الجمعة، من الساعة 5:00 صباحًا إلى الساعة 5:00 مساءً بتوقيت المحيط الهادي.

بالنسبة للمقيمين خارج الولايات المتحدة وكندا، يتم توفير الدعم الفني إقليميًا. إذا كانت لديك أسئلة حول برنامج التركيب، أو الأجهزة المرتبطة به، أو أي مشكلات برمجية أخرى، فيرجى الاتصال بممثل شركة AB المحلي لديك.

2.2 AB Pro Portal

يمكن تنزيل برنامج التركيب والوثائق ذات الصلة من https://www.abproportal.com أو Sonova Web Client. يجب تسجيل الدخول إلى الحساب. قد لا يكون هذا المورد متاحًا في جميع الأسواق؛ اتصل بممثل AB الخاص بك للحصول على مزيد من المعلومات.

2.3 دليل التثبيت المتقدم

دليل التثبيت المتقدم لـ Target CI v1.5 متاح عند الطلب. يوفر الدليل معلومات فنية حول أداة تثبيت برنامج التركيب المناسب، بما في ذلك خيارات سطر الأوامر للتثبيت الصامت والآلي.

2.4 MDS2

يعد بيان الإفصاح الخاص بالشركة المُصنِعة لأمن الأجهزة الطبية (MDS2) نموذجًا قياسيًا في الصناعة يحتوي على إجابات تتعلق بالأمان والخصوصية حول برنامج التركيب الخاص بشركة AB. النموذج متاح عند الطلب.

2.5 إرشادات الاستخدام (IFU)

سيتم شحن IFU مع وسائط تثبيت البرنامج. بالنسبة لبعض الأسواق، تتوفر إرشادات استخدام إلكترونية للتنزيل على www.advancedbionics.com/ifu

قد تكون الأقسام التالية في إرشادات الاستخدام ذات صلة بمتخصصي تكنولوجيا المعلومات:

- وصف المنتج
- الحد الأدنى من متطلبات النظام وخصائص الأداء
- توجيهات لأمن تكنولوجيا المعلومات
- تعليمات التثبيت
- الدعم الفني

2.6 HIMSA

HIMSA هو بائع برامج تابع لجهة خارجية يقوم بإنتاج نظام Noah System 4، وهو نظام برمجي مصمم لمجال رعاية السمع حيث يوفر لخبراء السمع نظامًا غير معتمد على بائع محدد لأداء المهام المتعلقة بالعملاء.

يمكن تكوين برنامج التركيب بشكل اختياري لاستخدام Noah System 4 لتخزين البيانات بدلاً من قاعدة البيانات المحلية.

توفر صفحة الويب الخاصة بالأمان لشركة HIMSA إجابات عن الأسئلة الشائعة المتعلقة بأمن تكنولوجيا المعلومات حول نظام Noah System 4.

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

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

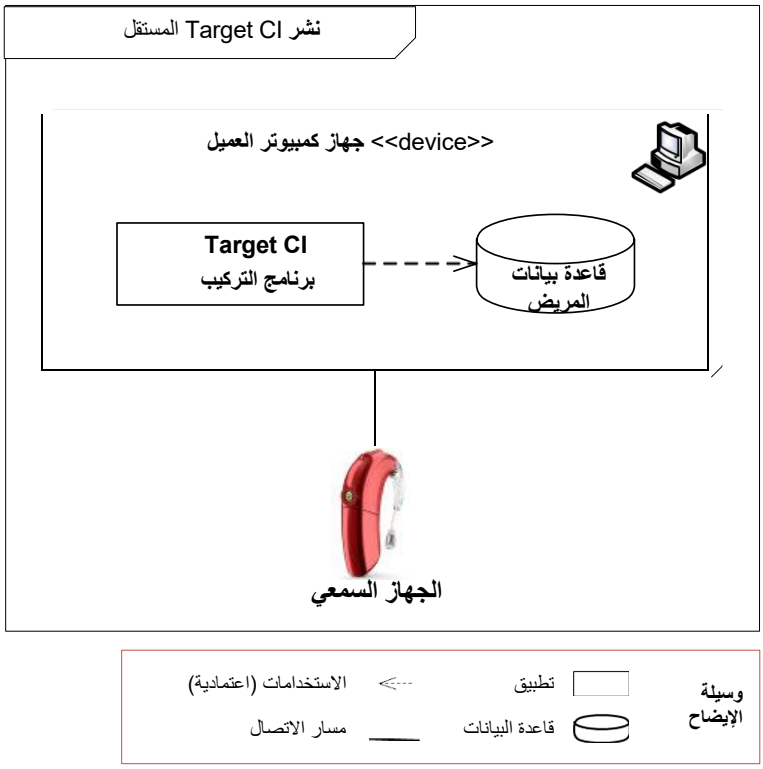
راجع قسم الأمان في مركز التعلم التابع لـ HIMSA للحصول على مزيد من المعلومات:
https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/

3. مخططات الشبكة والسياق

يوجد نموذجان مدعومان لنشر برنامج التركيب، وهو تطبيق عميل (SaMD) مُثبَّت على جهاز كمبيوتر يعمل بنظام التشغيل Microsoft Windows ومتوفر تجاريًا. لا يتضمن البرنامج أي أجهزة أو نظام تشغيل.

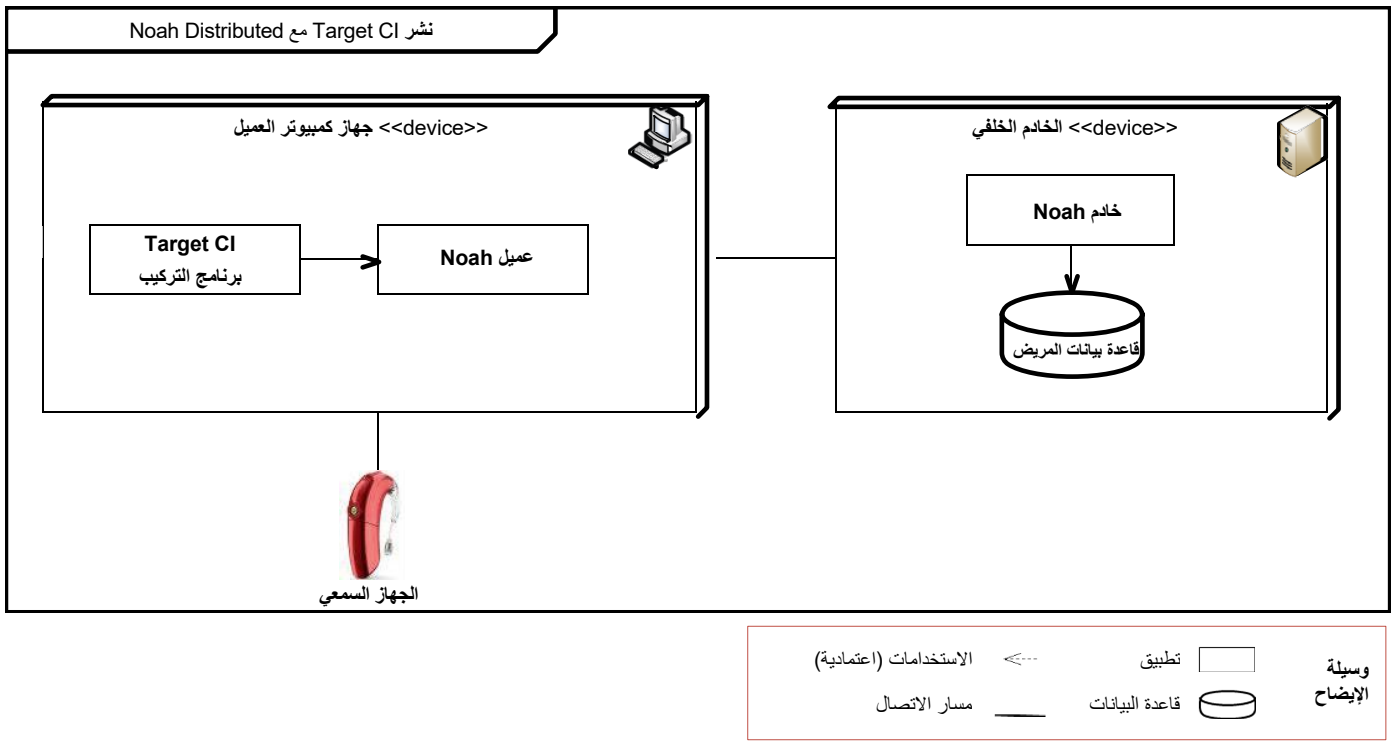
3.1 نموذج النشر 1: مستقل

في نموذج النشر المستقل، يتم نشر برنامج التركيب على جهاز كمبيوتر العميل. يتم تخزين قاعدة بيانات المريض على نفس جهاز الكمبيوتر وتثبيتها مع برنامج التركيب.



3.2 نموذج النشر 2: NOAH DISTRIBUTED

في نموذج النشر Noah Distributed، يتم نشر برنامج التركيب على جهاز كمبيوتر واحد أو أكثر من أجهزة العملاء. يتم نشر Noah، وهو نظام لإدارة المرضى تابع لجهة خارجية، على خادم داخلي يمكن الوصول إليه بواسطة أجهزة الكمبيوتر الخاصة بالعملاء. يتم تخزين قاعدة بيانات المرضى على خادم Noah ويمكن الوصول إليها عبر الشبكة بواسطة جهاز كمبيوتر عميل واحد أو أكثر.



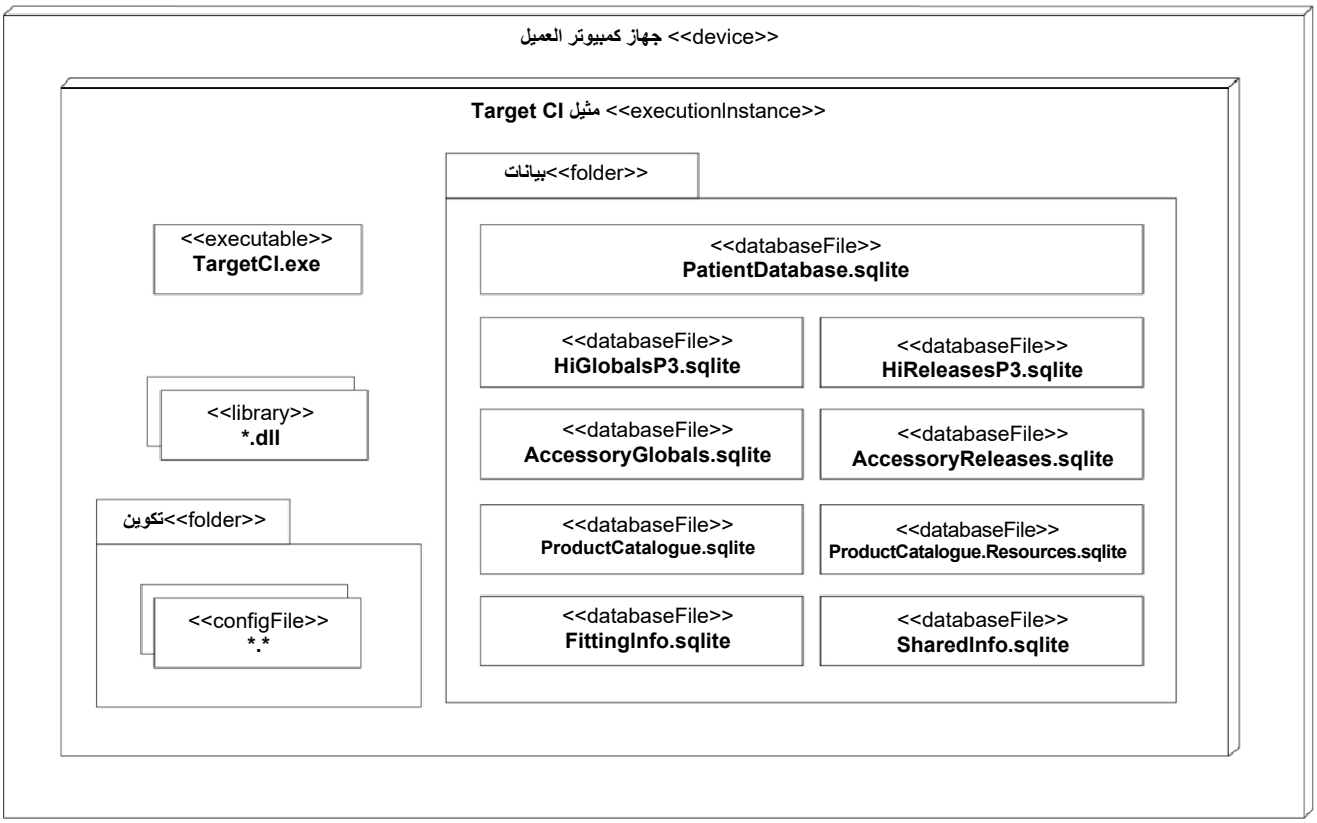
3.3 مكونات النشر

يتم تثبيت برنامج التركيب مع ملف قابل للتنفيذ ومجموعة من الملفات المرتبطة بما في ذلك ملفات DLL للمكونات وملفات التكوين وملفات قاعدة بيانات SQLite. يتم تثبيت ملفات التكوين في المجلد "%ProgramData%\ Advanced Bionics\Target CI\Target CI\Config" ويتم تثبيت ملفات قاعدة البيانات في المجلد "%ProgramData%\Advanced Bionics\Target CI\Target CI\Data". يحتوي مجلد البيانات على ملف قاعدة بيانات معاملات واحد والعديد من ملفات قاعدة بيانات المعلومات.

تخزن قاعدة بيانات المعاملات PatientDatabase.sqlite البيانات الديموغرافية وبيانات التركيب الخاصة بالمريض، ولن يتم تثبيتها إلا عند نشر برنامج التركيب في الوضع المستقل.

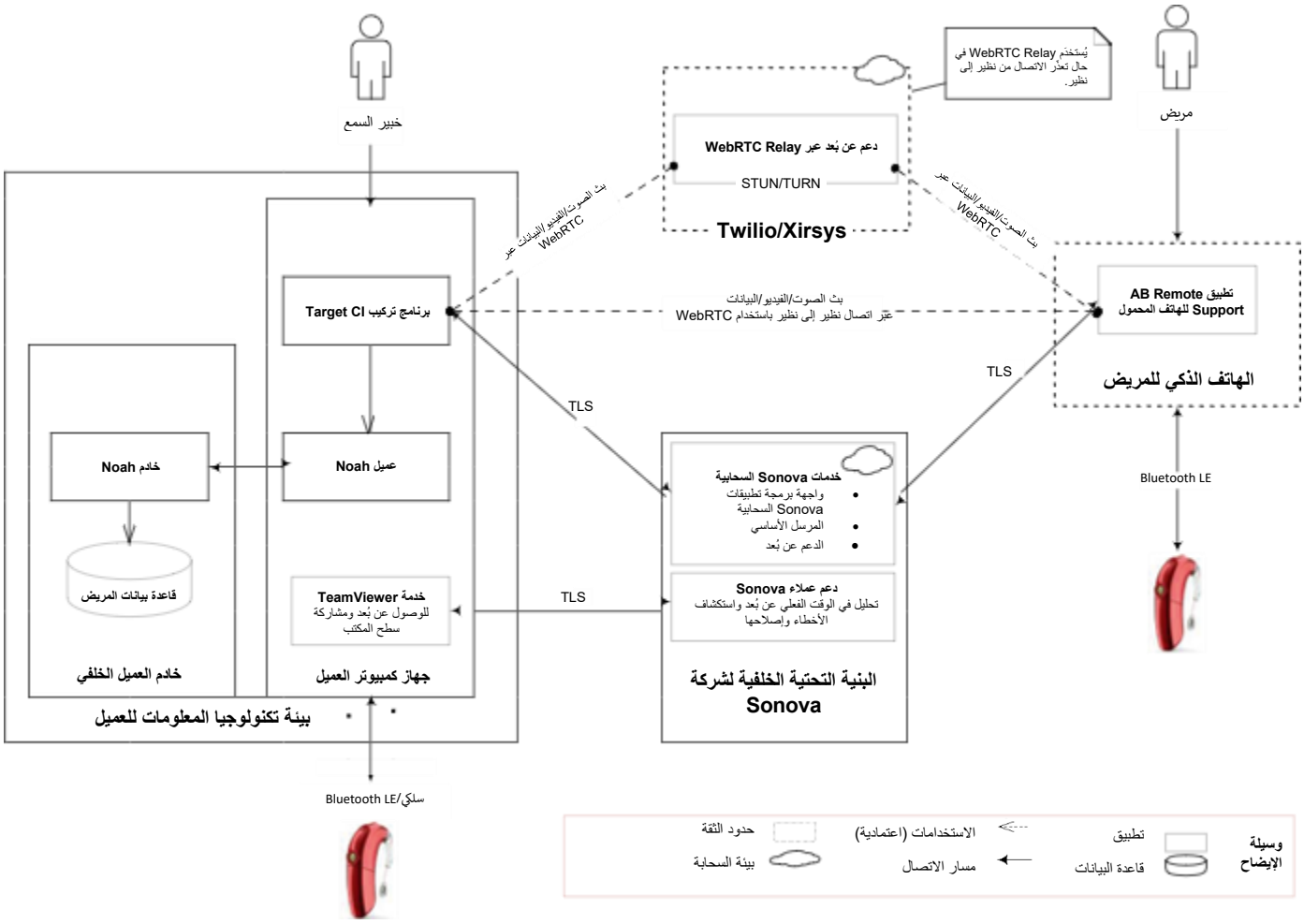
عند نشر برنامج التركيب كوحدة Noah، يوفر نظام Noah خدمات الاحتفاظ ببيانات المريض المطلوبة لبرنامج التركيب. تعد ملفات sqlite المتبقية جزءًا لا يتجزأ من برنامج التركيب، وهي مطلوبة في جميع نماذج النشر.

مكونات نشر برنامج Target CI



3.4 الترابطات بين الأنظمة

يوضح الرسم البياني والجدول أدناه الترابطات الأساسية للنظام. عادةً، يتم استخدام جزء فقط من الترابطات المتاحة.



المصدر / الوجهة	الخدمة	البروتوكول	المنفذ	الوصف
الأجهزة السمعية	اتصال جهاز السمع	اتصال سلكي / Bluetooth® منخفض الطاقة	لا ينطبق	يستخدم للتواصل مع الأجهزة السمعية للتحكم والتكوين وقراءة الحالة والبيانات
Noah	Noah 4 ModuleAPI	.NET Remoting	لا ينطبق	الواجهة الأساسية للوحدة المستخدمة للوصول إلى برنامج Noah (في نموذج نشر Noah distributed فقط)
خدمات Sonova السحابية	Sonova Cloud API، الموزع الأساسي، الدعم عن بُعد	REST،SOAP	443	يتم استخدام خدمات Sonova المستضافة في مركز بيانات Microsoft Azure من أجل: • جلب بيانات تكوين عميل برنامج التركيب من وحدة تخزين Sonova الخلفية • نقل بيانات التسجيل والتحليلات • إنشاء جلسات تركيب عن بُعد في الوقت الفعلي

المصدر / الوجهة	الخدمة	البروتوكول	المنفذ	الوصف
Twilio/Xirsys، تطبيق AB Remote Support للهاتف المحمول	الدعم عن بُعد	WebRTC	قائمة المنافذ المتاحة عند الطلب	تتم استضافة خدمات الاتصالات السحابية الخاصة بـ Twilio على منصات سحابية تابعة لجهات خارجية، وتحديدًا Amazon Web Services (AWS) وGoogle Cloud Platform (GCP). تُستخدم هذه الخدمات حصريًا بواسطة ميزة الدعم عن بُعد في برنامج التركيب، والتي تتيح إشارات WebRTC وعقد جلسات التركيب عن بُعد في الوقت الفعلي.
دعم عملاء AB	مشاركة سطح المكتب	بروتوكول ملكية TeamViewer	5938, 443, 80 راجع TeamViewerPorts	تُستخدَم لإجراء تحليل في الوقت الفعلي عن بُعد واستكشاف المشكلات التي تؤثر على عمليات تثبيت برنامج التركيب وإصلاحها. راجع القسم 6.6 الدعم عن بُعد للحصول على مزيد من المعلومات.

4. متطلبات النظام

نظام التشغيل	64-bit Windows 10 Pro/Enterprise
.NET Framework	الإصدار 4.8
وحدة المعالجة المركزية	Intel® Core™ i5 أو ما يعادله بأداء مماثل أو أفضل
ذاكرة الوصول العشوائي (RAM)	4 جيجابايت أو أكثر
مساحة القرص الصلب	3 جيجابايت أو أكثر
الحد الأدنى لمتطلبات العرض	• دقة 1280 × 1024 (أقصى تكبير 125%) • ألوان 24 بت
برامج تشغيل الأجهزة	• برنامج تشغيل Noahlink Wireless (يلزم وجود أحدث إصدار متوفر من HIMSA إذا كنت تستخدم واجهة برمجة Noahlink Wireless المتصلة عبر USB من جهة خارجية). • برنامج تشغيل CPI-3 (مطلوب إذا كنت تستخدم واجهة برمجة CPI-3 المتصلة عبر USB).
قاعدة البيانات	SQLite أو Noah System 4 (الإصدار 4.14 أو إصدار أحدث)
اتصال الإنترنت	مطلوب اتصال بالإنترنت للدعم عن بُعد وتسجيل التحليلات، راجع القسم 4.4 الترابطات بين الأنظمة؛ مطلوب الاتصال بالشبكة الداخلية عند استخدام نظام Noah 4 المتصل بالشبكة.
منافذ الشبكة	راجع القسم 3.4 الترابطات بين الأنظمة؛ راجع القسم 3. موارد أخرى — HIMSA للمنافذ التي يستخدمها نظام Noah 4.

5. التثبيت

5.1 المتطلبات

يجب أن يكون لديك حساب مسؤول لتثبيت برنامج التركيب. بمجرد تثبيت البرنامج، يمكن تشغيله دون الحاجة إلى أذونات إدارية أو عالية.

راجع القسم 8، سلامة البرنامج، للحصول على معلومات حول التحقق من سلامة البرنامج قبل التثبيت.

قبل التثبيت، يوصى مسؤولي النظام بالتأكد مما يلي:

• يجب أن يكون إصدار منتج برنامج التركيب الذي سيتم تثبيته هو الإصدار الأحدث المتاح.

• نظام التشغيل الأساسي مُحَدَّث.

5.2 أنواع أدوات التثبيت

تتوفر أداتان لتثبيت برنامج التركيب:

- أداة التثبيت القياسية
- أداة التثبيت الخاصة بمتخصصي تكنولوجيا المعلومات

أداة التثبيت الخاصة بمتخصصي تكنولوجيا المعلومات عبارة عن ملف MSI واحد وتستبعد المكونات الأساسية ولكنها تعادل أداة التثبيت القياسية.

تتضمن المكونات الأساسية الحزم القابلة لإعادة التوزيع Microsoft .NET Framework v4.8 وMicrosoft Visual Studio C++.

تدعم كلتا أداتي التثبيت سيناريوهات التثبيت المتقدمة، بما في ذلك التثبيت الصامت.

ينبغي استخدام أداة التثبيت الخاصة بمتخصصي تكنولوجيا المعلومات فقط إذا كانت مؤسستك تتطلب تثبيت المكونات الأساسية وإدارتها بواسطة مؤسستك وليس بواسطة أداة تثبيت برنامج التركيب. ينبغي استخدام أداة التثبيت القياسية في جميع الحالات الأخرى.

يمكن الحصول على أداة التثبيت الخاصة بمتخصصي تكنولوجيا المعلومات من الممثل الطبي لشركة AB. لا يمكن استخدام أداة التثبيت الخاصة بمتخصصي تكنولوجيا المعلومات لإصلاح أو إعادة تثبيت أو إلغاء تثبيت البرامج المُثَبَّتة بواسطة أداة التثبيت القياسية. لا يمكن استخدام أداة التثبيت القياسية لإصلاح أو إعادة تثبيت أو إلغاء تثبيت البرامج المُثَبَّتة بواسطة أداة التثبيت الخاصة بمتخصصي تكنولوجيا المعلومات.

6. ضوابط الأمن

برنامج التركيب هو تطبيق عميل يتم تثبيته على جهاز كمبيوتر تجاري يعمل بنظام التشغيل Microsoft Windows. يمكن تثبيت برنامج التركيب كتطبيق مستقل أو كوحدة Noah.

6.1 المصادقة – النشر المستقل

عندما يتم تثبيت برنامج التركيب كتطبيق مستقل، فإنه يعتمد على آليات التحكم في الوصول التي يوفرها نظام التشغيل المضيف. يمكن لموظفي تكنولوجيا المعلومات لدى العميل تكوين نظام التشغيل المضيف لإدارة المصادقة. لا يحتوي برنامج التركيب على أي ميزة تكاملية من هذا القبيل. توصي شركة Advanced Bionics بأن يقوم كل مستخدم بتسجيل الدخول إلى نظام التشغيل المضيف باستخدام حساب فريد لكل مستخدم.

6.2 المصادقة – نشر NOAH

عند تثبيت برنامج التركيب كوحدة Noah، يتم توفير التحكم في الوصول بواسطة نظام Noah System 4. راجع www.HIMSA.com للتعرف على عناصر التحكم في التدقيق المستخدمة بواسطة Noah System 4.

6.3 التفويض

لا يقيد برنامج التركيب الوصول إلى ميزاته بناءً على أدوار المستخدمين الفرديين. يدعم البرنامج وظيفة رئيسية واحدة وهي تركيب الأجهزة السمعية للمريض، ودور واحد للمختص بالتركيب. لا تنطبق عناصر التحكم في الوصول المستندة إلى الأدوار.

6.4 التدقيق – النشر المستقل

عندما يتم تثبيت برنامج التركيب كتطبيق مستقل، فإنه يعتمد على آليات التدقيق التي يوفرها نظام التشغيل المضيف. لا يحتوي برنامج التركيب على أي ميزة متكاملة من هذا القبيل. يمكن لموظفي تكنولوجيا المعلومات لدى العميل تكوين نظام التشغيل المضيف لتسجيل تشغيل/تنفيذ برنامج التركيب وعمليات تسجيل دخول المستخدمين. توصي شركة Advanced Bionics بأن يقوم كل مستخدم بتسجيل الدخول إلى نظام التشغيل المضيف باستخدام حساب فريد لكل مستخدم لتسهيل عملية التدقيق.

6.5 التدقيق – نشر NOAH

عند تثبيت برنامج التركيب كوحدة Noah، يتم توفير سجلات التدقيق بواسطة نظام Noah. راجع https://www.himsa.com/ للتعرف على عناصر التحكم في التدقيق المستخدم بواسطة Noah System 4.

6.6 الوصول عن بعد

تتيح ميزة مشاركة سطح المكتب إجراء التحليل عن بُعد في الوقت الفعلي واستكشاف المشكلات التي تؤثر على عمليات تثبيت برنامج التركيب وإصلاحها. تعتمد هذه الميزة على أداة TeamViewer QuickSupport التابعة لجهة خارجية (يتم تثبيتها افتراضيًا مع برنامج التركيب)، وتتيح لمتخصصي دعم عملاء AB الاتصال عن بُعد بجهاز كمبيوتر خبير السمع والتحكم الكامل في سطح المكتب، بما في ذلك الوصول إلى النظام الأساسي للتشغيل والملفات.

لإنشاء جلسة مشاركة سطح المكتب، يلزم تفاعل خبير السمع. يجب على خبير السمع أولًا تشغيل أداة TeamViewer QuickSupport (على سبيل المثال، من خلال برنامج التركيب Target CI) وإرسال بيانات اعتماد معرف TeamViewer الخاصة به إلى فريق دعم AB عبر قناة اتصال خارجية (مثل مكالمة هاتفية).

يتم عرض اسم عضو فريق دعم AB ومعرف TeamViewer الخاص به بشكل افتراضي على شاشة كمبيوتر خبير السمع أثناء كل جلسة مشاركة سطح المكتب النشطة.

يتم تأمين حركة مرور شبكة مشاركة سطح المكتب بالكامل وفقًا لمعايير بروتوكولات وخوارزميات التشفير أو بما يتجاوزها (تبادل مفاتيح RSA العامة/الخاصة وتشفير جلسة AES 256 بت).

يمكن إزالة TeamViewer QuickSupport يدويًا دون التأثير على وظائف Target FSW الأخرى. يدعم برنامج تثبيت Target FSW معلمة تثبيت عبر سطر الأوامر للسماح بتثبيت Target FSW عبر سطر الأوامر دون تضمين أداة TeamViewer QuickSupport.

7. حماية المعلومات

7.1 سياسة الخصوصية الخاصة بشركة ADVANCED BIONICS

يمكن تنزيل سياسة الخصوصية التي تصف كيفية قيام Advanced Bionics بجمع البيانات الشخصية ونقلها وتخزينها واستخدامها، من:
.AdvancedBionics.com/privacy

لا تستضيف شركة Advanced Bionics أو تخزن أو تنسخ احتياطيًا أي بيانات مخزّنة داخل برنامج التركيب أو قواعد بيانات Noah، ولا تتمتع بالوصول إليها، ما لم يتم إرسال البيانات صراحةً إلى شركة Advanced Bionics.

7.2 معايير معالجة المعلومات الفيدرالية (FIPS)

يتوافق Target CI v1.5 مع معايير التشفير FIPS 140-2.

7.3 الأمن أثناء النقل

يتم ضمان أمان الاتصالات وتمكينها في جميع اتصالات شبكة برنامج التركيب الداخلية والخارجية. باستثناء ميزة الدعم عن بُعد (التي تستخدم بروتوكول WebRTC) واتصال Bluetooth مع الأجهزة السمعية والملحقات، فإن جميع الاتصالات الأخرى محمية بواسطة بروتوكول أمان طبقة النقل (TLS)، الذي يضمن السرية والنزاهة والمصداقية.

TLS

يتوافق تكوين TLS مع أفضل الممارسات الحالية وتوصيات الأمان الموثقة في BCP 195 – توصيات للاستخدام الآمن لـ TLS وDTLS وBCP195 بما في ذلك:

- عدم دعم إصدارات SSL وTLS قبل 1.2
- عدم دعم مجموعات التشفير التي تستخدم خوارزميات التشفير التي توفر مستوى أمان أقل من 128 بت
- دعم امتدادات TLS الموصى بها لـ BCP 195
- عدم دعم الامتدادات غير الآمنة لـ BCP 195

DTLS

يعد التشفير ميزة إلزامية لـ WebRTC ويتم تطبيقه على جميع تدفقات الوسائط المرسلة عبر WebRTC. يعتمد بروتوكول التشفير المستخدَم على نوع القناة؛ حيث يتم تشفير بث البيانات باستخدام DTLS، بينما يتم تشفير بث الوسائط باستخدام بروتوكول النقل الآمن في الوقت الحقيقي (SRTP)، نظرًا لأنه خيار أخف وزنًا من DTLS.

يرجى الاطلاع على الرابط التالي لمزيد من المعلومات التفصيلية حول تكوين الأمان لخدمة الدعم عن بُعد عبر WebRTC:

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

BLE

يتم تشفير الاتصال اللاسلكي عبر تقنية Bluetooth منخفضة الطاقة للأجهزة السمعية والملحقات، وحماية سلامته بشكل افتراضي (باستثناء حالات استخدام التعريف والكشف). بالإضافة إلى ذلك، فإن مدة تفعيل وضع الاقتران عبر Bluetooth في جهاز السمع محدودة زمنيًا. يُرجى الرجوع إلى وثائق أجهزة السمع المتوفرة للحصول على وصف أكثر تفصيلاً حول أمان قناة الاتصال عبر Bluetooth.

7.4 الأمن أثناء التخزين

قاعدة بيانات المرضى - نموذج النشر المستقل

إذا تم تثبيت برنامج التركيب كتطبيق مستقل، فسيتم تخزين قاعدة بيانات المرضى محليًا في:
C:\ProgramData\Advanced Bionics\Target CI\Target CI\Data

لا يتم تشفير هذه السجلات بشكل افتراضي. يتم تخزين المعلومات الصحية المحمية (PHI) والمعلومات الشخصية القابلة للتعريف (PII) داخل قاعدة بيانات برنامج التركيب ولا يتم نقلها عبر الشبكة.

في بعض الولايات القضائية، قد تتطلب اللوائح تشفير جميع بيانات المرضى لتجنب المسؤولية المحتملة في حال فقدان البيانات أو سرقتها. قم بتمكين BitLocker أو أي تشفير كامل للقرص مكافئ (سواء على مستوى نظام التشغيل أو الأجهزة) لحماية البيانات من الوصول أو النسخ غير المصرح به أثناء تخزينها.

BitLocker هي ميزة مدمجة في نظام التشغيل Windows تقوم بتشفير محرك الأقراص بأكمله وتتطلب المصادقة للوصول إليه. تأكد دائمًا من مراجعة الإرشادات الرسمية لشركة Microsoft وسياسة أمان تكنولوجيا المعلومات لمؤسستك قبل تمكين BitLocker.

كيفية تمكين BitLocker

يجب أن تكون لديك امتيازات المسؤول لإدارة BitLocker.

1. ابحث عن "Manage BitLocker" (إدارة BitLocker)

   افتح قائمة Start (ابدأ)، واكتب Manage BitLocker (إدارة BitLocker)، ثم حدده من نتائج البحث.

2. حدد محرك النظام

   اختر محرك الأقراص الذي تم تثبيت Windows عليه لتكوين إعدادات التشفير.

3. اختر طريقة إلغاء القفل

   حدد أحد الخيارات التالية:

   - TPM only (TPM فقط)
   - TPM + PIN (TPM + رقم تعريف شخصي (PIN))
   - TPM + USB key (TPM + مفتاح USB)

   اتبع إرشادات Microsoft لأفضل الممارسات، وسياسة أمان تكنولوجيا المعلومات الخاصة بمؤسستك عند تحديد طريقة إلغاء القفل.

4. قم بإنشاء نسخة احتياطية من مفتاح الاسترداد

   قم بعمل نسخة احتياطية لمفتاح الاسترداد باستخدام طرق آمنة معتمدة من قبل المؤسسة. تشمل الخيارات الموصى بها ما يلي:

   - التخزين في Microsoft Entra ID (المعروف سابقًا باسم Azure AD) أو Active Directory للأجهزة المنضمة إلى المجال
   - الحفظ في موقع شبكة آمن وخاضع للتحكم في الوصول باستخدام التشفير وتسجيل التدقيق
   - استخدام حل الضمان الرئيسي المُدار المعتمد من قِبل مؤسستك

تجنب حفظ المفتاح على محركات الأقراص المحلية أو أجهزة USB أو طباعته ما لم يُسمح بذلك صراحةً بواسطة السياسة. يجب حماية مفاتيح الاسترداد بنفس درجة الصرامة التي تُحمى بها بيانات الاعتماد الحساسة الأخرى، ويجب تغييرها فورًا إذا تم كشفها.

5. بدء التشفير

اختر:

- محرك الأقراص بالكامل – يوصى به لمعظم سيناريوهات المؤسسات. يقوم بتشفير جميع القطاعات، بما في ذلك المساحة غير المستخدمة، لمنع استبقاء البيانات.

قاعدة بيانات المرضى – وحدة نشر Noah Distributed

عندما يتم تثبيت برنامج التركيب كوحدة Noah، يتم تخزين معلومات التعريف الشخصية (PII) داخل قاعدة بيانات المرضى التي يستضيفها Noah. قد توجد قاعدة بيانات المرضى التي يستضيفها Noah على جهاز آخر. يتم الاحتفاظ ببيانات التعريف الشخصية وبيانات المريض الأخرى بواسطة برنامج Noah، كما يضمن نظام Noah تشفير بيانات المريض في حالة السكون. قد يقوم برنامج التركيب بإرسال أو استقبال معلومات التعريف الشخصية عبر اتصال شبكي سلكي أو لاسلكي عند تكوين قاعدة بيانات Noah للوصول إلى الشبكة.

ستكون معلومات التعريف الشخصية (PII) المخزنة في قاعدة بيانات Noah المتصلة بالشبكة مرئية لمستخدمي أجهزة كمبيوتر شخصية مختلفة لديهم أذونات الوصول إلى نفس قاعدة البيانات المتصلة بالشبكة. يمكن أيضًا تكوين قاعدة بيانات Noah للوصول غير الشبكي وتثبيتها على نفس الكمبيوتر الشخصي مثل برنامج التركيب.

يمنع Noah برنامج التركيب من الوصول إلى قاعدة بيانات سجلات المرضى. عندما يفتح المستخدم ملف مريض في برنامج التركيب عبر Noah Client، يكون برنامج التركيب قادرًا فقط على القراءة من سجل المريض المفتوح حاليًا والكتابة إليه، ولا يمكنه الوصول إلى سجلات المرضى الأخرى في قاعدة بيانات Noah.

راجع القسم www.HIMSA.com لمعرفة معايير التشفير المستخدمة بواسطة Noah System 4.

ملفات تصدير RMA

يتيح برنامج التركيب إمكانية تصدير معلومات العميل إلى ملف. يمكن إرسال ملف RMA إلى Advanced Bionics لحل مشكلات RMA أو مشكلات الدعم ذات الصلة.

يتم تشفير ملف RMA بطريقة غير متماثلة باستخدام RSA وبطول مفتاح يبلغ 512 بت. لا يحتوي برنامج التركيب على أي وسيلة لفك تشفير ملف RMA.

ملفات التصدير مجهولة الهوية

يتيح برنامج التركيب تصدير معلومات العميل إلى ملف مجهول الهوية خاص بالعميل. يتم استبدال معلومات التعريف الشخصية الخاصة بالعميل، مثل تاريخ الميلاد والاسم بقيَم عامة. الملف غير مشفر ويمكن استيراده إلى نفس المثيل أو إلى مثيل مختلف من برنامج التركيب.

ملفات التصدير القياسية

يتيح برنامج التجهيز تصدير معلومات العميل إلى ملف تصدير قياسي. يستخدم الملف تنسيقًا ثنائيًا خاصًا ولا يتم تشفيره. يمكن استيراد الملف إلى نفس المثيل أو إلى مثيل مختلف من برنامج التركيب. عند استخدام هذه الميزة، يجب على مستخدمي برنامج التركيب التأكد من التعامل مع ملفات التصدير القياسية وفقًا لسياسات تكنولوجيا المعلومات المحلية الخاصة بهم لإدارة معلومات التعريف الشخصية غير المشفرة.

الجهاز السمعي

يقوم برنامج التركيب بتخزين معلومات العميل على الجهاز السمعي الخاص بالعميل. لا يتم تخزين معلومات التعريف الشخصية مثل اسم العميل وتاريخ ميلاده على الجهاز السمعي. يتم تخزين المعلومات الأخرى غير المتعلقة بمعلومات التعريف الشخصية باستخدام تشفير PBKDF2 بمفتاح 128 بت.

قد يرسل/يستقبل برنامج التركيب معلومات التعريف غير الشخصية للعميل إلى/من جهاز سمعي عبر جهاز سلكي خاص (مثل CPI-3)، أو تطبيق AB Remote Support للهاتف المحمول، أو جهاز Noahlink Wireless لاسلكي. يتصل جهاز Noahlink اللاسلكي بالجهاز السمعي باستخدام تقنية Bluetooth Low Energy (BLE) عبر قناة BLE قياسية مشفرة بـ AES 128 بت.

8. سلامة البرمجيات

8.1 التحقق من وسائط التثبيت التي تم تنزيلها

من الممكن تنزيل وسائط تثبيت برنامج التركيب Target CI في بعض المناطق من Pro Portal الخاصة بشركة Advanced Bionics أو Sonova Web Client. يمكن التحقق من وسائط التثبيت التي تم تنزيلها باستخدام أي أداة تجزئة موثوقة من نوع SHA-256.

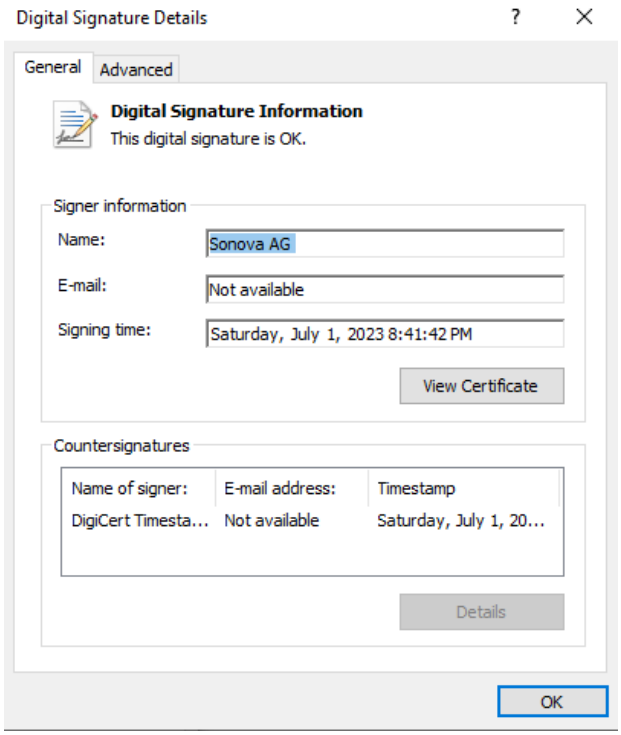
تجزئة SHA256 لملف التثبيت المضغوط القياسي (zip) هي:
A42B8F41A5A4111D1CDF67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

تجزئة SHA256 لملف التثبيت المضغوط (zip) الخاص بمتخصصي تكنولوجيا المعلومات:
DDAD362CC3213EFEA702D9F4A61740B34EDF794FE997811B6B2C908CE754B25F

8.2 التحقق اليدوي من برنامج التركيب قبل التثبيت

يمكن للمستخدمين تنفيذ الخطوات التالية للتحقق من سلامة وأصالة برنامج التركيب قبل التثبيت:

1. افتح Windows Explorer وانتقل إلى المجلد الجذر لوسائط تثبيت برنامج التركيب. إذا كانت وسائط التثبيت عبارة عن محرك أقراص محمول (USB)، فقم بإدخاله في منفذ USB وانتقل إلى المجلد الجذر الخاص به. إذا كانت وسائط التثبيت الخاصة بك عبارة عن ملف مضغوط (zip)، فقم بفك ضغطه إلى مجلد وانتقل إلى هذا المجلد.
2. انقر بزر الماوس الأيمن على SonovaVerify.exe وحدد Properties (خصائص) من قائمة السياق.
3. حدد علامة التبويب Digital Signatures (التوقيعات الرقمية).
4. انقر نقرًا مزدوجًا فوق توقيع "Sonova AG" SHA256.
5. تحقق من صحة عناصر التوقيع. وتحقق بصفة خاصةً من ظهور الرسالة "The digital signature is OK." (التوقيع الرقمي صحيح) بالقرب من الأعلى، وأن اسم الموقّع ووقت التوقيع يتطابقان مع الصورة التالية:



1. أغلق مربعات الحوار المنبثقة وانقر نقرًا مزدوجًا فوق SonovaVerify.exe.
2. تأكد من عرض "NO ERRORS DETECTED" (لم يتم اكتشاف أي أخطاء) كما هو موضح في الصورة التالية:

تُظهر الصورة أن SonovaVerify قام بالتحقق من صحة التوقيعات الرقمية لجميع الملفات الموجودة على وسائط التثبيت، بما في ذلك برنامج التثبيت. يتحقق ذلك من عدم تعرض وسائط التثبيت للعبث أو التلف أو المساس بها بأي شكل آخر. سيعرض SonovaVerify تحذيرات أو رسائل خطأ إذا كانت الملفات أو المجلدات مفقودة، أو تمت إضافة ملفات أو مجلدات غير متوقعة إلى وسائط التثبيت.

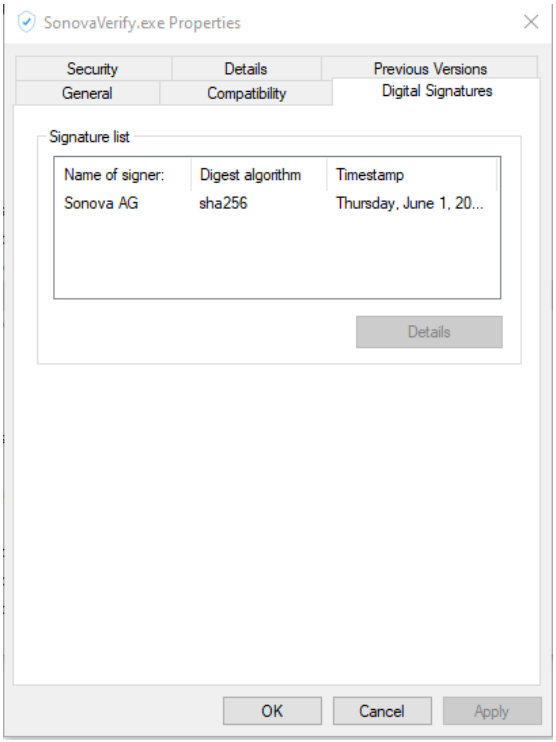
8.3 التحقق التلقائي من سلامة برنامج التركيب المُثبَّت

يتم دمج SonovaVerify مع برنامج التركيب ويتم تشغيله في كل مرة يتم فيها تشغيل التطبيق للتحقق من سلامة ملفات برنامج التركيب. يتم توقيع ملفات البرنامج رقميًا باستخدام ممارسات وشهادات قياسية في الصناعة صادرة عن هيئة تصديق موثوقة. يقوم البرنامج بإشعار المستخدم عبر رسائل تحذيرية إذا تم المساس بسلامة أي من الملفات البرمجية.

8.4 التحقق اليدوي من سلامة برنامج التركيب المثبّت

يمكن للمستخدمين تنفيذ الخطوات التالية للتحقق من سلامة وأصالة برنامج التركيب المثبَّت في أي وقت دون الحاجة إلى تشغيله:

1. افتح مستعرض Windows Explorer وانتقل إلى المجلد التنفيذي لبرنامج التركيب، والذي يوجد عادةً في: C:\Program Files (x86)\Advanced Bionics\Target CI\
2. انقر بزر الماوس الأيمن على SonovaVerify.exe وحدد Properties (خصائص) من قائمة السياق.
3. حدد علامة التبويب Digital Signatures (التوقيعات الرقمية).
4. انقر نقرًا مزدوجًا فوق توقيع "Sonova AG" SHA256.
5. تأكد من صحة عناصر التوقيع، وخاصةً من ظهور الرسالة "The digital signature is OK." (التوقيع الرقمي صحيح) بالقرب من الأعلى، وأن اسم الموقّع ووقت التوقيع يتطابقان مع الصورة التالية:



1. أغلق مربعات الحوار المنبثقة وانقر نقرًا مزدوجًا فوق SonovaVerify.exe.
2. تأكد من عرض "NO ERRORS DETECTED" (لم يتم اكتشاف أي أخطاء) كما هو موضح في الصورة التالية:

تُظهر الصورة أن SonovaVerify قد تحقق من صحة التوقيعات الرقمية لجميع ملفات البرنامج المثبّتة. يثبت هذا أن برنامج التركيب لم يتم العبث به أو إتلافه أو المساس به بأي شكل آخر. سيعرض SonovaVerify تحذيرات أو رسائل خطأ إذا كانت بعض الملفات أو المجلدات مفقودة، أو تمت إضافة ملفات أو مجلدات غير متوقعة إلى مجلد ملفات البرنامج.

9. لا يتم دعم التحديثات التلقائية والتحديثات البرمجية.

10. إدارة البيانات

10.1 قواعد البيانات

يستخدم برنامج التركيب قاعدة بيانات معاملات لتخزين بيانات المرضى، بالإضافة إلى مجموعة من قواعد بيانات المعلومات التي توفر تكوينات البيانات الوصفية المطلوبة للتطبيق.

راجع القسم 3. مخططات الشبكة والسياق - مكونات النشر للحصول على قائمة مفصلة بجميع قواعد البيانات التي تم نشرها بواسطة برنامج التركيب.

عندما يتم تثبيت برنامج التركيب كتطبيق مستقل، تكون قاعدة بيانات المرضى داخلية ضمن برنامج التركيب. تُخزَّن قاعدة بيانات المرضى الموجودة في الملف PatientDatabase.sqlite على نفس الجهاز المُثَبَّت عليه برنامج التركيب، وتوفّر مساحة تخزين لبيانات المرضى. لإنشاء نسخة احتياطية من بيانات التطبيق عند نشر Target CI كتطبيق مستقل، قم بإنشاء نسخة احتياطية من المجلد بالكامل الموجود في %ProgramData%\Advanced Bionics\Target CI\Target CI\Data. يجب حماية النسخ الاحتياطية للبيانات ليس فقط من الفقدان، بل أيضًا من السرقة. عند تثبيت برنامج التركيب كوحدة Noah، يتم تخزين بيانات المريض في قاعدة البيانات التي يوفرها نظام Noah. من الممكن تكوين قاعدة بيانات Noah للوصول إلى الشبكة. يمكن أيضًا تكوين قاعدة بيانات Noah للوصول غير الشبكي وتثبيتها على نفس الكمبيوتر الشخصي مثل برنامج التركيب. قم بتكوين تشفير قاعدة بيانات Noah لحماية البيانات (راجع وثائق HIMSA).

في وضع نشر Noah distributed، راجع الرابط التالي للحصول على إرشادات حول النسخ الاحتياطي واستعادة قاعدة بيانات مرضى Noah:

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 نقل البيانات

يتيح برنامج التركيب للمستخدمين نقل سجلات المرضى من برنامج التركيب السابق لشركة AB، SoundWave 3.2. يجب أن تكون سجلات المرضى قابلة للوصول من تثبيت SoundWave 3.2 الموجود على نفس الكمبيوتر المُثَبَّت عليه Target CI حتى يمكن نقلها.

10.3 تكوينات أجهزة السمع

يتيح برنامج التركيب إمكانية تصدير واستيراد تكوينات الجهاز وإعداداته.

10.4 التخلص من البيانات

يمكن العثور على تعليمات التخلص من البيانات في إرشادات الاستخدام (IFU) أو على الموقع التالي الخاص بنشر Noah:
https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/

11. بيئة الأمن – المسؤولية المشتركة

تم تصميم برنامج التركيب للاستخدام المقصود حيث تعتبر إدارة مخاطر الأمن السيبراني مسؤولية مشتركة بين أصحاب المصلحة في منظومة رعاية السمع بأكملها، والتي تشمل - على سبيل المثال لا الحصر- مستخدمي أجهزة السمع، والآباء أو الأوصياء القانونيين للأطفال الذين يستخدمون أجهزة السمع، وخبراء السمع، ومسؤولي تكنولوجيا المعلومات، ومرافق ومقدّمي رعاية السمع، وبائعي أجهزة السمع ومعدات البرمجة.

فيما يلي قائمة بأفضل توصيات الممارسات الشائعة وضوابط الأمان لبيئة التركيب حيث سيتم استخدام برنامج التركيب:

مستوى نظام التشغيل

- تطبيق عناصر التحكم في الوصول على مستوى نظام التشغيل، على سبيل المثال:
  - احذف حسابات الضيوف
  - فعِّل تسجيل دخول المستخدم في نظام Windows
  - حافظ على قائمة من المشغلين المعتمدين للتحكم في الوصول إلى النظام
  - قم بتعيين المستخدمين والأدوار المخصصة
  - قم بتطبيق متطلبات كلمات المرور القوية والحفاظ على سرية بيانات الاعتماد
- قم بتطبيق ضوابط التدقيق على مستوى نظام التشغيل
- حافظ على تحديث نظام التشغيل.
- احرص على تحديث إصدار برنامج التركيب المثبّت.
- قم بتمكين الحماية المحدثة من البرامج الضارة ومكافحة الفيروسات.
- قم بتمكين القائمة البيضاء للتطبيقات

حماية البيانات

- قم بتشفير بيانات المريض باستخدام أدوات أو عناصر تحكم تابعة لجهات خارجية على مستوى نظام التشغيل، على سبيل المثال، باستخدام تشفير محرك الأقراص (على سبيل المثال، Microsoft BitLocker المجاني) لحماية جميع البيانات. في عمليات نشر Noah، يُنصَح باستخدام تشفير قاعدة بيانات Noah.
- ينبغي تأمين الوسائط الخارجية التي تحتوي على البيانات المصدرة من برنامج التركيب بما في ذلك التقارير والسجلات. عندما لا تُستخدم بعد الآن، ينبغي مسح البيانات و/أو الوسائط أو حذفها بأمان.
- استخدم وسائط تخزين USB المزودة بوظيفة أمان مدمجة، مثل محركات أقراص USB المشفرة مع لوحة مفاتيح مدمجة.
- تأكد من الحفاظ على أمان بياناتك دائمًا:
  - عند نقل البيانات عبر قنوات غير آمنة، قم بإرسال بيانات مجهولة المصدر أو تشفيرها.
  - يجب حماية النسخ الاحتياطية للبيانات ليس فقط من الفقدان، بل أيضًا من السرقة.
  - قم بإزالة كافة البيانات من وسيط البيانات التي لم تعد تستخدم أو التي يجب التخلص منها.
- يجب على المستخدمين استخدام الإجراءات والأدوات المعتمدة للإزالة الآمنة للبيانات المخزنة على الوسائط القابلة للإزالة، وفقًا للوائح والمبادئ التوجيهية المعمول بها للتعامل مع معلومات المريض / معلومات التعريف الشخصية (PII) / المعلومات الصحية المحمية (PHI)

البنية التحتية لتكنولوجيا المعلومات

قم بتشغيل برنامج التركيب في بيئة شبكة آمنة محمية من الاختراق غير المصرح به. هناك العديد من التقنيات الفعالة لعزل وحماية أنظمة المعلومات الطبية، بما في ذلك تنفيذ حماية جدار الحماية، والمناطق منزوعة السلاح (الشبكة الفرعية المحلية (DMZs))، وشبكات المنطقة المحلية الافتراضية (VLANs) والجيوب الشبكية. حافظ على اتصال نشط بالشبكة لتلقي تحديثات نظام التشغيل.

المستوى المادي

- يجب تأمين محطة العمل التي تم تثبيت برنامج التركيب عليها ماديًا بطريقة تمنع وصول المستخدمين غير المصرح لهم إليها.
- تأكد من عدم قيام أي أفراد غير مصرح لهم بالعبث بالنظام.
- يجب التحكم في الوصول إلى الطابعات المتصلة بمحطة العمل.
- يجب وضع شاشة محطة العمل التي تم تثبيت برنامج التركيب عليها بطريقة تقيّد إمكانية رؤية محتوى الشاشة على المستخدم فقط.

المستوى التنظيمي

- يُسمح فقط للموظفين المدربين مهنيًا والمؤهلين بالكامل بتشغيل النظام. قبل السماح لأي شخص بتشغيل النظام، يجب التأكد من أنه قرأ تعليمات التشغيل المزودة مع برنامج التركيب وأنه يفهمها فهمًا كاملًا.
- إذا لاحظت أي نشاط مشبوه في حسابات برنامج التركيب أو أي عملية غير متوقعة، فاتصل بشركة Advanced Bionics. راجع القسم 2.1 للمزيد من المعلومات.

لمزيد من المعلومات حول المسؤولية المشتركة، وللحصول على قائمة أكثر تفصيلًا بتوصيات أفضل الممارسات وضوابط الأمان لبيئة التركيب التي سيتم فيها استخدام برنامج التركيب وتطبيقها على مستويات مختلفة، يُرجى الرجوع إلى:

- ورقة EHIMA البيضاء بعنوان "أفضل الممارسات للتركيب الآمن لأجهزة السمع" EHIMAWhitePaper

12. عملية التصنيع وتطوير البرمجيات

يتم أخذ الأمن السيبراني في الاعتبار طوال عملية تطوير البرمجيات بأكملها. تم تطوير برنامج التركيب وفقًا للمعيارين IEC 62304 و IEC 82304.

يتم فحص برنامج التركيب للكشف عن الفيروسات والبرامج الضارة كجزء من عملية التصنيع.

يتم تقييم الثغرات الأمنية في مكونات الجهات الخارجية المُدرجة في قاعدة بيانات الثغرات الأمنية الوطنية (NVD) التابعة للمعهد الوطني للمعايير والتكنولوجيا، وتُعالَج أثناء عملية التطوير، وتُراقَب بعد طرح برنامج التركيب في السوق.

13. مكونات البرنامج وقائمة المواد

يتضمن برنامج التركيب عددًا من مكونات البرمجيات التجارية الجاهزة.

يوضح الجدول التالي جميع مكونات SOUP (البرمجيات ذات المنشأ غير المعروف) الموزعة مع برنامج التركيب.

عنصر SOUP	وصف الوظيفة	الشركة المُصنِعة	الإصدار
ciAD Hearing Loss Simulator	مكتبة لمحاكاة فقدان السمع لمشغل الوسائط	ciAD (Jurg Haubold)	1.0.0.1
CredentialManagement	حزمة إدارة بيانات الاعتماد، وهي غلاف لواجهة برمجة تطبيقات إدارة بيانات الاعتماد في نظام التشغيل Windows	iLya Lozovyy	1.0.2
CSharpAnalytics	تُستخدم مع خدمة Google Analytics	Attack Pattern	1.6.1
Dapper	ORM	Sam Saffron,Marc Gravell,Nick Craver	2.0.78
Destructurama.Attributed	تُستخدَم بواسطة Nephele libraries.	Serilog Contributors	3.0
DirectShow 2005	يسمح بالوصول إلى وظيفة DirectShow الخاصة بـ Microsoft من داخل تطبيقات .NET.	Microsoft	2.0
DSL4	DSL 4 Fitting formula library	المركز الوطني لعلم السمع، كندا	4.2
DSL5	DSL 5 Fitting formula library	المركز الوطني لعلم السمع، كندا	5.0.34
GNOtometrics.Aurical	GNOtometrics.Aurical معاد تعبئتها لصالح Sonova	GNOtometrics	2.0.1.9
IceLink	تُستخدم لتكامل مؤتمرات الصوت/ الفيديو عبر WebRTC	FM (Frozen Mountain)	3.8.0.22151
IdentityModel	مكتبة عميل OpenID Connect و OAuth 2.0 تُستخدم في مكوّن Kona.CommonServices.Authentication لمصادقة OAuth 2.	Dominick Baier, Brock Allen	5.0.1
IMCInterfaces	مكتبة واجهة الاتصال بين الوحدات النمطية الخاصة بـ Noah	HIMSA II K/S	4.4.0.2266
LibGit2Sharp	تُستخدم بواسطة مكتبات Sonova للتواصل مع Git	مساهمو LibGit2Sharp	0.26.1
Mapster	تُستخدم لتعيين الكائنات داخل الكود	chaowlert,eric_swann	7.2.0.0

عنصر SOUP	وصف الوظيفة	الشركة المُصنِعة	الإصدار
MathNet.Numerics	تُستخدم لخوارزميات التركيب (مسار الإشارة، ومطابقة الهدف، وغيرها)	كريستوف روغ، ماركوس كودا، يورغن فان غايل والمساهمون	4.11.0
Microsoft.Bcl.AsyncInterfaces	توفر الواجهات IAsyncEnumerable<T> و IAsyncDisposable وأنواع المساعدة لـ .NET Standard 2.0	Microsoft	5.0.0
Microsoft.CodeAnalysis.Common	يتم استخدامه ضمن المكتبات التابعة لـ Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9
Microsoft.CodeAnalysis.CSharp	يتم استخدامه ضمن المكتبات التابعة لـ Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	3.9
Microsoft.Identity.Client	مكتبة MSAL لـ .NET هي جزء من منصة هوية Microsoft للمطورين (المعروفة سابقًا باسم Azure AD) الإصدار 2.0. تتيح لك الحصول على رموز أمان لاستدعاء واجهات برمجة التطبيقات المحمية. تستخدم معيار الصناعة OAuth2 وOpenID Connect.	Microsoft	4.38.0.0
Microsoft.Identity.Client.Extensions.Msal	ذاكرة تخزين مؤقتة آمنة عبر الأنظمة الأساسية لتطبيقات العميل العامة MSAL.	Microsoft	2.19.3.0
Microsoft.IdentityModel.JsonWebTokens	تتضمن أنواعًا توفر الدعم لإنشاء رموز JSON Web Tokens وتسلسلها والتحقق من صحتها. تُستخدم بواسطة المكونات التي تتواصل مع خدمات الواجهة الخلفية التي تستخدم رموز JSON Web للمصادقة.	Microsoft	6.8.0
Microsoft.IdentityModel.Logging	اعتمادية Microsoft.IdentityModel.Tokens	Microsoft	6.8.0
Microsoft.IdentityModel.Tokens	اعتمادية برمجيات SOUP Microsoft.IdentityModel.JsonWebTokens	Microsoft	6.8.0
Microsoft.Win32.TaskScheduler.dll	يستخدم لأداة النسخ الاحتياطي FSW (النسخ الاحتياطي التلقائي).	David Hall	2.5.11.0
Microsoft.Xaml.Behaviors.Wpf	XAML Behaviors هي وسيلة سهلة الاستخدام لإضافة تفاعلية شائعة وقابلة لإعادة الاستخدام إلى تطبيقات WPF باستخدام أقل قدر من الأكواد.	xamlexperiencesteam، Microsoft	1.0.1
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	11.0.61030.0
Microsoft Visual C++ 2017 Redistributable (x86)	Microsoft Visual C++ 2017 Redistributable	Microsoft	14.16.27024.1
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	يستخدم لضبط مستوى الصوت وتشغيل ملفات الصوت.	مفتوح المصدر	1.9
.NET Framework	.NET runtime framework.	Microsoft	4.8.3928.0
Newtonsoft.Json	يُستخدم لتسلسل وفك تسلسل JSON	James Newton-King	12.0.3
Nibelung	مكتبات تركيب NoahLink Wireless	GN ReSound	1.3.16.1

عنصر SOUP	وصف الوظيفة	الشركة المُصنِعة	الإصدار
Nlog	هذا أحد التبعيات الخاصة بـ HIMSA Nibelung.CPD (Noahlink Wirlesss)	كيم كريستنسن	4.4.0
NoahLink	برنامج تشغيل جهاز تركيب NoahLink	HIMSA	1.55.6.166
NoahLink Wireless	برنامج تشغيل جهاز التركيب NoahLink Wireless	HIMSA	2.0.0.68
Otometrics.HiPro2	مكتبات الاتصال HiPro	GNOtometrics	2.0.0.4
Otometrics.REMaccess	طبقة التجريد Otometrics فوق مكتبة واجهة الاتصال بين الوحدات في Noah	GN Otometrics	1.0.0.10
Pdfium.Net.SDK	مكتبة C# PDF لإنشاء وتحرير مستندات PDF في تطبيقات .Net	Patagames.com	4.54.2704.0
Polly	مكتبة تتيح للمطورين التعبير عن سياسات المرونة ومعالجة الأخطاء العابرة مثل إعادة المحاولة، وقاطع الدائرة، وعزل الحاجز، والعودة إلى الوضع الاحتياطي البديل بطريقة سلسة وآمنة الترابط	تطبيق vNext	7.2.1
Polly.Extensions.Http	مكتبة تحتوي على أساليب مساعدة محددة مسبقًا لتكوين سياسات Polly للتعامل مع الأخطاء العابرة الشائعة عند الاستدعاء عبر HttpClient.	تطبيق vNext	3.0
Polly.Contrib.WaitAndRetry	مكتبة لـ Polly تحتوي على طرق مساعدة لمجموعة متنوعة من استراتيجيات الانتظار وإعادة المحاولة.	Grant Dickinson، تطبيق vNext	1.1.1
Portable.BouncyCastle	هذا اعتماد على HIMSA Nibelung.CPD (Noahlink Wirlesss)	BouncyCastle.Crypto	1.8.10.0
protobuf-net.dll	إطار عمل للتسلسل يُستخدم لـ RC blob.	مفتوح المصدر	2.0.0.668
Serilog	مكون التسجيل المستخدَم لتطبيق Chinook بالكامل.	Serilog Contributors	2.10.0
Serilog.Enrichers.Thread	إثراء أحداث Serilog بخصائص من الخيط الحالي	Serilog Contributors	3.1
Serilog.Expressions	تصفية الأحداث في Serilog بناءً على التعبيرات	Serilog Contributors	2.0
Serilog.Sinks.Console	مستقبِل Serilog الذي يقوم بكتابة أحداث السجل إلى وحدة التحكم/الطرفية.	Serilog Contributors	4.0.0.0
Serilog.Sinks.Debug	مستقبِل Serilog الذي يقوم بكتابة أحداث السجل في نافذة إخراج التصحيح.	Serilog Contributors	2.0
Serilog.Sinks.File	اكتب أحداث Serilog إلى ملفات نصية بصيغة عادية أو JSON.	Serilog Contributors	4.1
Serilog.Sinks.Trace	مستقبِل التتبع التشخيصي لأحداث Serilog.	Serilog Contributors	2.1
Serilog.Settings.AppSettings	تكوين XML (تكوين النظام <appSettings>) دعم لـ Serilog.	Serilog Contributors	2.2.2
Security.Cryptography	امتدادات لواجهات برمجة التطبيقات الأمنية المضمنة مع إطار عمل .NET	Microsoft	1.7.2
SharpBITS API	SharpBITS.NET هو غلاف .NET wrapper لواجهة برمجة التطبيقات BITS API ويشمل أيضًا تطبيق واجهة مستخدم صغير لنظام Windows لتسهيل الوصول إلى عمليات التحميل عبر BITS.	perpetualKid	2.1.0.0
SharpZipLib	#ziplib (SharpZipLib)، المعروفة سابقًا باسم NzipLib) هي مكتبة Zip وGzip وTar وBzip2 مكتوبة بالكامل بلغة C# لمنصة .NET. توفر هذه المكتبة وظائف الضغط (مثل الضغط وفك الضغط وضغط التدفق وغيرها). نستخدمها في تطبيق تحديث البرامج الثابتة.	مفتوح المصدر	1.1.0.145

عنصر SOUP	وصف الوظيفة	الشركة المُصنِعة	الإصدار
Superpower	مكتبة مركّبة للمحللات اللغوية (Parser Combinator) بلغة C#	Superpower ،Datalust Sprache ،Contributors Contributors	2.3
SQLite.Interop	SQLite هي مكتبة برمجية توفر نظام إدارة قواعد البيانات العلائقية. تعني كلمة lite في SQLite خفة الوزن من حيث الإعداد وإدارة قاعدة البيانات والموارد المطلوبة. تتمتع SQLite بالميزات الملحوظة التالية: مستقلة ذاتيًا، بدون خادم، لا تحتاج لتكوين مسبق، وتدعم المعاملات. إنها قاعدة بيانات (SQLite 3.32.1) لتخزين معلومات عن المرضى (في الوضع المستقل)، وموارد كتالوج منتجاتنا والبيانات الوصفية الخاصة بالتركيب والملحقات والأجهزة السمعية.	فريق تطوير SQLite	1.0.113
System.Buffers	يوفر تجميع الموارد من أي نوع للتطبيقات الحساسة للأداء التي تقوم بتخصيص وإلغاء تخصيص الكائنات بشكل متكرر.	23rogramma,dotnetframework	4.5.1
System.Collections.Immutable	يتم استخدامه ضمن المكتبات التابعة لـ Sonova.HardwareAbstraction. Palio.Trafo	Microsoft	5.0
System.ComponentModel. Annotations	يوفر سمات تُستخدم لتعريف البيانات الوصفية للكائنات المستخدمة كمصادر بيانات.	23rogramma,dotnetframework	4.7
System.Configuration.Configuration Manager	يوفر أنواعًا تدعم استخدام ملفات التكوين.	Microsoft	5.0
System.Data.SQLite.Core	يتم استخدامه ضمن المكتبات التابعة لـ Sonova.HardwareAbstraction. Palio.Trafo	فريق تطوير SQLite	1.0.113.7
System.Drawing.Common	يوفر إمكانية الوصول إلى وظائف الرسومات في GDI+.	Microsoft	5.0.1
System.IdentityModel.Tokens.Jwt	يتضمن أنواعًا توفر دعمًا لإنشاء رموز JSON Web وتسلسلها والتحقق من صحتها. تُستخدم بواسطة المكونات التي تتواصل مع خدمات الواجهة الخلفية التي تستخدم رموز JSON Web للمصادقة.	Microsoft	6.8.0
System.IO.Abstractions	مجموعة من التجريدات للمساعدة في إمكانية اختبار التفاعلات مع نظام الملفات.	Tatham Oddie & friends	12.0.10
System.Numerics.Vectors	يوفر أنواعًا عددية معزَّزة بالأجهزة، ومناسبة لتطبيقات المعالجة والرسومات عالية الأداء.	24rogramma,dotn etframe work	4.5
System.Memory	يوفر أنواعًا لتمثيل وتجميع فعال لأجزاء الذاكرة المُدارة والمكدَّسة والأصلية وتسلسلاتها، إلى جانب العناصر الأساسية لتحليل النصوص المنسَّقة وتنسيقها بتشفير UTF-8 المخزّنة في تلك الأجزاء.	24rogramma,dotn etframe work	4.5.4
System.Reactive.Core	الامتدادات التفاعلية (Rx) لـ .NET	مؤسسة .NET	3.1.1
System.Reactive. Interfaces	الامتدادات التفاعلية (Rx) لـ .NET	مؤسسة .NET	3.1.1
System.Reactive.Linq	الامتدادات التفاعلية (Rx) لـ .NET	مؤسسة .NET	3.1.1
System.Reactive.PlatformServices	الامتدادات التفاعلية (Rx) لـ .NET	مؤسسة .NET	3.1.1
System.Reactive.Windows.Threading	الامتدادات التفاعلية (Rx) لـ .NET	مؤسسة .NET	3.1.1
System.Reflection.DispatchProxy	توفر فئة لإنشاء أنواع وكيل بشكل ديناميكي لتنفيذ واجهة محددة والاشتقاق من نوع DispatchProxy محدد. تُوجَّه استدعاءات الأساليب على المثيل الوكيل الذي تم إنشاؤه إلى نوع الأساس DispatchProxy.	Microsoft	4.7.1
System.Reflection.Metadata	توفر هذه الحزمة قارئ وكاتب بيانات وصفية .NET (ECMA-335) منخفض المستوى. إنها مُصمَّمة لتحقيق أداءٍ عالٍ، وتُعَدّ الخيار المثالي لبناء مكتبات على مستوى أعلى تهدف إلى توفير نموذج كائن خاص بها، مثل المترجمات.	Microsoft	5.0

عنصر SOUP	وصف الوظيفة	الشركة المُصنِعة	الإصدار
System.Runtime.CompilerServices.Unsafe	يوفر System.Runtime (وقت تشغيل النظام). فئة CompilerServices.Unsafe، التي توفر وظائف عامة ومنخفضة المستوى للتعامل مع المؤشرات.	24rogramma, dotnetframework	5.0
System.Security.AccessControl	توفر فئات أساسية تُمكّن من إدارة قوائم التحكم في الوصول والتدقيق على الكائنات القابلة للتأمين.	Microsoft	5.0
System.Security.Permissions	يوفر أنواعًا تدعم أمان الوصول إلى التعليمات البرمجية (CAS).	Microsoft	5.0
System.Security.Principal.Windows	توفر فئات لاسترجاع مستخدم Windows الحالي وللتفاعل مع مستخدمي Windows والمجموعات.	Microsoft	5.0
System.Text.Encoding.CodePages	يوفر دعمًا للترميزات المستندة إلى صفحات التعليمات البرمجية، بما في ذلك Windows-1252 وShift-JIS وGB2312.	Microsoft	5.0
System.Text.Encodings.Web	يوف أنواعًا لترميز السلاسل وتحريرها لاستخدامها في JavaScript ولغة ترميز النص التشعبي (HTML) ومحددات الموارد الموحدة (URL). إنه يعتمد على SOUP IdentityModel	24rogramma,dotnetframework	5.0
System.Text.Json	توفر أنواعًا عالية الأداء ومنخفضة في تخصيص الذاكرة تعمل على تسلسل الكائنات إلى نصوص بتنسيق JSON (JavaScript Object Notation) وإلغاء تسلسل نصوص JSON إلى كائنات، مع دعم مدمج لترميز UTF-8. كما يوفر أنواعًا تُستخدم لقراءة وكتابة نصوص JSON المشفّرة بتنسيق UTF-8، ولإنشاء نموذج كائن مستند في الذاكرة (DOM) يُستخدم للقراءة فقط، مما يتيح الوصول العشوائي إلى عناصر JSON ضمن عرض منظم للبيانات.	Microsoft	5.0.1
System.Threading.Tasks.Extensions	توفر أنواعًا إضافية تُبسّط عملية كتابة التعليمات البرمجية المتزامنة وغير المتزامنة.	25rogramma,dotnetframework	4.5.4
System.ValueTuple	يوفّر البُنى System.ValueTuple التي تُنفّذ الأنواع الأساسية للمجموعات في لغتَي C# وVisual Basic. يضيف دعمًا لمجموعات القيم، نظرًا لأنها متاحة فقط في الإصدارات الأحدث من .NET framework.	25rogramma,dotnetframework	4.5.0
Thrift	يستخدم لتعريف بروتوكول الاتصال remotelink	Apache	0.13.0.0
Unity	Unity Container (Unity) هو حاوية حقن تبعيات شاملة وقابلة للتوسّع.	مشروع Unity Container	5.8.13
WAP BT Dongle Driver	برنامج التشغيل WAP BT Dongle (دونجل التركيب)	iAnywhere Solutions	3.0.0.6095
WebSync	يُستخدم لدمج قناة بيانات التركيب	FM (Frozen Mountain)	4.9.32.0
Xps to Pdf render (NiXPS)	تحويل ملفات XPS إلى ملفات PDF برمجيًا؛ ويُستخدم في تقارير تطبيق التركيب.	NiXPS	2.6.7.0
مكتبات وقت التشغيل لـ MS-VisualC++ 7.1	مكتبات وقت التشغيل لـ Microsoft Visual C++	Microsoft	7.10.6030.0

14. المراجع

العنوان	الموقع الإلكترونى
إرشادات الاستخدام (إلكترونية)	https://ifu.advancedbionics.com/
سياسة الخصوصية العامة الخاصة بشركة Advanced Bionics	https://advancedbionics.com/privacy
HIMSA	https://www.himsa.com/
نظام Noah 4	https://www.himsa.com/products/all-about-noah-system-4/
نسخ البيانات احتياطيًا واستعادتها في قاعدة بيانات Noah الخاصة بك.	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/
تم الوصول إلى الحد الأقصى لسعة قاعدة بيانات نظام Noah.	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/noah-system-database-capacity-has-been-reached/
TeamViewer - قائمة المنافذ المستخدمة	https://community.teamviewer.com/English/kb/articles/4139-ports-used-by-teamviewer
BCP 195	https://www.rfc-editor.org/info/bcp195
وثائق أمان خادم LiveSwitch	https://developer.liveswitch.io/liveswitch-server/server/security.html
أفضل الممارسات للتركيب الآمن لأجهزة السمع - ورقة بيضاء من EHIMA	https://www.ehima.com/wp-content/uploads/2021/09/EHIMA Cybersecurity-FSW-Security-Whitepaper v1-Sep2021 .pdf

CE 0123

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

info.us@advancedbionics.com

EU REP Advanced Bionics GmbH
Feodor-Lynen-Strasse 35
D-30625 Hannover

info.switzerland@advancedbionics.com

لمزيد من المعلومات حول مواقع AB الأخرى، يُرجى زيارة
advancedbionics.com/contact

AB – A Sonova brand

يرجى الاتصال بمندوب AB المحلي للتأكد من موافقات الجهات التنظيمية وتوفر الأجهزة في منطقتك.

029-S396-21 Rev A 2025-09-15

ADVANCED BIONICS
POWERFUL CONNECTIONS