

Customer Information Notice: CIN162

Nanosonics® AuditPro™ IT & Security Customer Notice

Table of Contents

1	Customer Information Notice: CIN162.....	2
2	High Level System Overview.....	2
2.1	Data Flow	3
3	Networking and Connectivity	4
3.1	Connecting trophon2 devices.....	4
3.2	Connecting AuditPro handheld mobile scanning devices	5
3.3	Static IPs and DHCP address reservation	5
3.4	Networking and Connectivity Summary	6
4	Users and Access Controls	7
4.1	User access to the AuditPro Mobile Handheld Scanning Device.....	7
4.2	User access to the AuditPro Cloud Application.....	7
5	Security and Compliance.....	7
5.1	Security of the AuditPro Mobile scanning device	8
5.2	Security of trophon2	9
5.3	Security of the AuditPro cloud application.....	9
5.4	Encryption of customer data.....	10
5.5	Retention of Data	10
5.6	AuditPro Security FAQ	10
6	Appendix A – List of supporting documents	11
7	Appendix B - Whitelisting for internet access	12
8	Appendix C – Acronyms	13

1 Customer Information Notice: CIN162

This document explains the Nanosonics AuditPro system networking and security considerations in detail. It describes how the product interacts with the internet and hospital IT network, including the cyber security measures. This document should be viewed in combination with the associated MDS2 document to gain more knowledge about the system security overall. Supporting documents can be found in Appendix A, all acronyms and their definitions can be found in Appendix B.

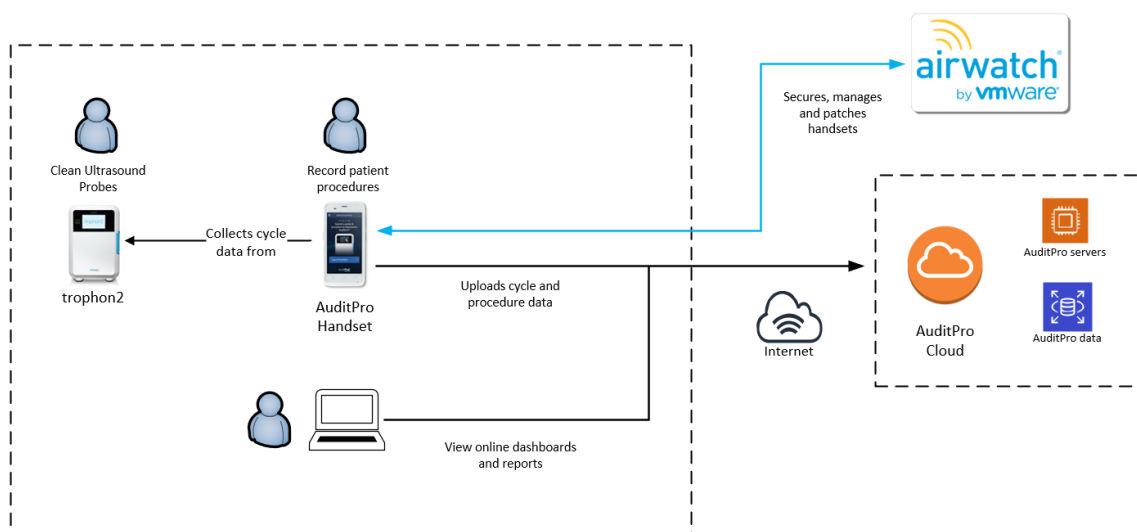
The instructions in this document are applicable to the following software versions:

- Nanosonics AuditPro Mobile Application 1.5
- Nanosonics AuditPro Cloud Application 1.5

2 High Level System Overview

AuditPro consists of three components: trophon^{®2}, the AuditPro handheld mobile scanning device and the AuditPro cloud application.

The following diagram shows a high-level overview of relationship between the components of the AuditPro system.



trophon2

The trophon2 device, manufactured by Nanosonics, performs high level disinfection of ultrasound probes. Operators reprocess ultrasound probes in trophon2 and the device logs these disinfection cycles in its internal database.

AuditPro Handheld Mobile Scanning Device (MSD)

The MSD is used to record information about ultrasound procedures at point of care. The AuditPro MSD also connects to trophon2, over your network and downloads cycle data from the trophon2's internal database. The AuditPro MSD then uploads both procedure data and cycle data to the AuditPro cloud.

The AuditPro MSD is a Honeywell EDA51HC Healthcare Grade device running Android. The MSDs are secured, managed and updated by Nanosonics through VMWare WorkspaceOne (Airwatch).

AuditPro Cloud

The AuditPro cloud stores data uploaded from the AuditPro MSD, and provides web based interfaces and dashboards for users to view reports and manage data.

The AuditPro cloud is hosted on AWS (Amazon Webservices) and managed by Nanosonics.

2.1 Data Flow

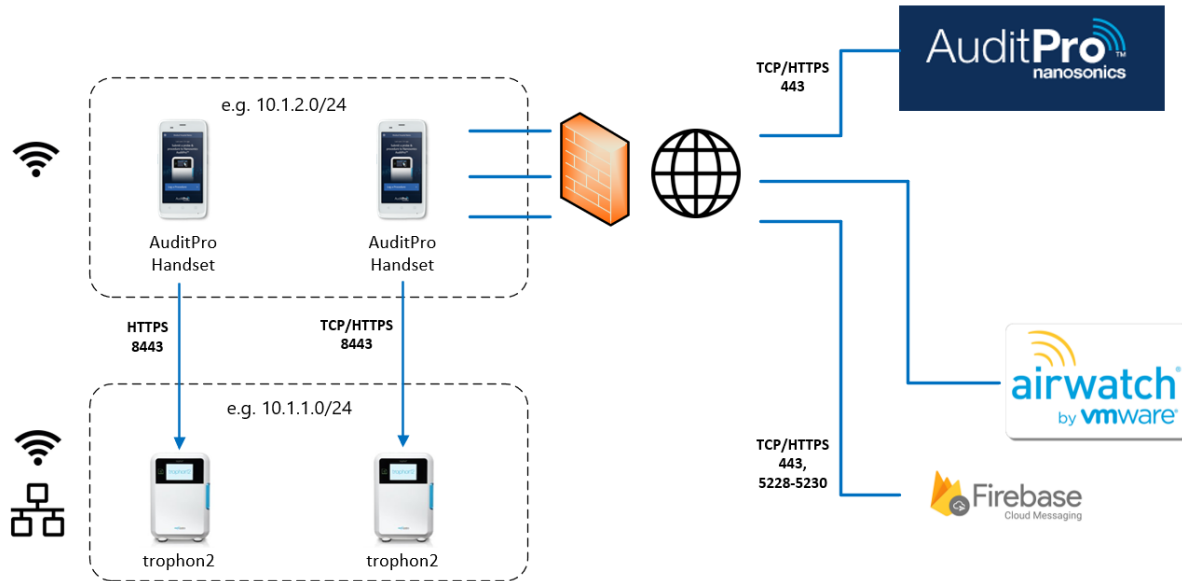
Source	Destination	
AuditPro MSD	trophon2	Calls the trophon2 API to download data
AuditPro MSD	AuditPro Cloud	Calls the AuditPro cloud to send cycle and procedure data
AuditPro MSD	Google Firebase FCM	Opens a connection to FCM to receive push notifications
VMWare WorkspaceONE (formerly AirWatch) MDM	AuditPro MSD *	Receives configuration updates, application updates and security patches
Firebase FCM	AuditPro MSD *	Sends push notifications

* although the data flow describes the AuditPro MSD as the destination of this traffic, the data is transmitted over a socket connection initiated by the AuditPro MSD. No connections are initiated outside your firewall requiring inbound firewall rule changes or tunneling.

3 Networking and Connectivity

Both trophon2 and the AuditPro handheld mobile scanning device (MSD) must be connected to the customer network.

The diagram below shows two trophon2 devices and two AuditPro MSDs running in an example network.



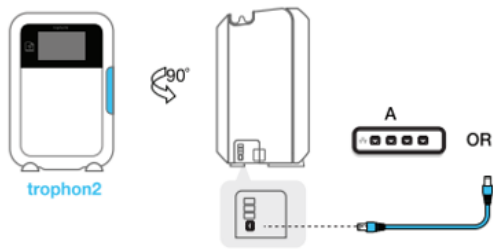
3.1 Connecting trophon2 devices

Each trophon2 device must be connected to your network so that it can be reached from the AuditPro MSD.

The AuditPro MSD connects to the trophon2 via **HTTPS** on port **8443** and addresses the trophon2 device by its IP address. When the trophon2 is connected to a different subnet or VLAN to the AuditPro MSD, routing rules may be required to allow the trophon2 device to be reachable by its IPV4 address from the AuditPro MSD.

There are three ways to connect a trophon2 device to your network.

Ethernet



trophon2 has an ethernet port and can be connected to your network using an RJ45 cable. The device can be configured, through its GUI, to use a static IP, or to use DHCP. If DHCP is used then the DHCP address must be reserved.

Wi-Fi dongle

trophon2 can be joined to your wireless network using a Wi-Fi dongle which connects to the devices USB-2.0 port. The device is configured to join your network by selecting the network SSID and entering the password through the trophon2's GUI. Wi-Fi details such as SSID and password are stored in the firmware of the trophon2. The device will obtain an IP address via DHCP and that IP address must be reserved for the trophon2.

3.2 Connecting AuditPro handheld mobile scanning devices

The AuditPro mobile scanning device (MSD) needs to be connected to a Wi-Fi network at your facility.

When the AuditPro MSD is connected to a different subnet or VLAN to the trophon2 devices – likely, if the trophon2 devices are connected to a wired network - then routing rules may be required to allow the trophon2 device to be reachable by its IPV4 address from the AuditPro MSD on your Wi-Fi network.

Additionally, the AuditPro MSD needs to be able to connect to the internet through an internet gateway. The AuditPro MSD communicates with the AuditPro cloud SaaS application as well as the VMWare Workspace One mobile device management system.

If your facility only allows outbound internet access to a whitelist of addresses, then please refer to Appendix B.

3.3 Static IPs and DHCP address reservation

The AuditPro mobile scanning device (MSD) connects to trophon2 using its IP address. This IP address is stored when the trophon2 and AuditPro MSD are first registered at your facility.

It is important that the IP address of the trophon2 devices do not frequently change, or the AuditPro MSDs will not be able to connect to them, which will cause delays and may lead to loss of data within the AuditPro system.



If trophon2 is connected to your network by ethernet then it can be configured to use a static IPV4 address, or to use DHCP. If DHCP is used, then the IPV4 address which is leased to

trophon2 should be reserved indefinitely in your DHCP server so that it does not change when the device sends DHCP lease renewal requests.

If trophon2 is connected to your network by Wi-Fi then it can only be configured to use DHCP. In this case, the IPV4 address which is leased to the trophon2 should be reserved in the DHCP server so that it does not change when the device sends DHCP lease renewal requests.

The AuditPro MSD does not require a static IP or reserved DHCP address and can obtain a new IP address each time it connects to your network.

3.4 Networking and Connectivity Summary

	trophon2	AuditPro MSD
		
Connection Type	Ethernet Wi-Fi via USB adapter Wi-Fi via wired access point	Wi-Fi
Requires outbound internet Access	No	Yes
Requires static IP or DHCP reservation	Yes	No
Requires inbound access from internet	No	No
Wi-Fi authentication modes	WPA / WPA2 PSK WPA2-Enterprise (SSID and password) 802.1x EAP	WPA / WPA2 PSK WPA2-Enterprise (SSID and password) 802.1x EAP

4 Users and Access Controls

4.1 User access to the AuditPro Mobile Handheld Scanning Device

The workflow for AuditPro means that the mobile scanning device is used by many different sonographers within a department and that the device is frequently picked up and put down. AuditPro does not require users of the handset to individually identify themselves by authenticating.

The handset screen automatically locks after 2 minutes and must be unlocked with a PIN. The PIN number is set at a device level and can be changed by the customer on a per-device basis.

4.2 User access to the AuditPro Cloud Application

The AuditPro cloud application requires users to be authenticated.

The AuditPro cloud application can be integrated with your own identity provider for single sign-on. AuditPro can be integrated with any OAUTH2 and OpenID Connect compatible identity provider including:

- ADFS 2016
- AzureAD
- Okta
- Auth0

We recommend SSO integration for customers with specific user management or MFA requirements.

For customers who have not integrated with their own identity provider, users authenticate to the AuditPro cloud application using their email address and a password. AuditPro has password complexity requirements for strong passwords, which must be changed every 90 days. Multi-factor authentication is also supported.

5 Security and Compliance

HIPAA & GDPR Compliance

Nanosonics AuditPro™ is designed to allow customers to meet the requirements of the following acts and regulations:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- General Data Protection Regulation (GDPR).

ISO27001 accredited

Nanosonics is an ISO27001 certified company with policies and procedures to ensure that:

- appropriate security controls are in place to protect customer data
- security risks are recorded and managed
- access to customer data is controlled
- security incidents are appropriately managed

Secure Application Development

The AuditPro system has been developed to security best practice and follows (“Open Web Application Security Project” (OWASP) standards.

Penetration Testing

The Nanosonics AuditPro System undergoes regular end-to-end Penetration Testing, performed by a third party, to confirm the system is compliant with the third party’s comprehensive security framework.

5.1 Security of the AuditPro Mobile scanning device

The AuditPro mobile scanning device runs the Android operating system in a locked-down configuration managed by Nanosonics. Management of the devices is centralized through our MDM (mobile device management) platform.

We use VMWare WorkspaceONE (formerly called AirWatch) as our MDM.

The following controls are in place to secure the mobile scanning device.

Restricted USB port – the MSD’s USB port is configured to allow charging only. File transfer and USB debugging features are disabled.

Bluetooth disabled – Bluetooth is disabled on the MSD and cannot be enabled by the end user

Restrictions on app installation – users cannot install additional apps either through the app market, or non-market means.

Compromise protection – monitoring software provided by VMWare detects if the device is compromised and enables Nanosonics to wipe compromised devices

Limited privileges – users of the MSD have restricted access to settings and are only able to perform basic tasks such as joining a WIFI network, setting the time, and changing the device PIN code.

Kiosk mode – the MSD runs in kiosk mode and automatically launches the AuditPro app. Users can only access the AuditPro app and relevant settings.

5.2 Security of trophon2

The trophon2 device has been developed in compliance with IEC 62304:2006+AMD1:2015. Medical device software - Software life cycle processes.

Trophon2 stores cleaning cycle data in its internal database and exposes this information through a web API.

This API is secured using mTLS. Connecting clients must provide a valid X.509 certificate to establish a connection and retrieve data from the API. These certificates are issued by Nanosonics and unique X.509 certificates are issued to each trophon2 and each AuditPro mobile scanning device.

5.3 Security of the AuditPro cloud application

The Nanosonics AuditPro cloud application is engineered to protect customer data.

The AuditPro cloud is run on an Amazon Web Services. Data collected as part of the Nanosonics AuditPro system is securely stored in multi-zone, HIPAA and GDPR compliant AWS server facilities in US East 1, North Virginia and US West 1, North California (DR).

Industry-best-practice measures are in place in the design of AuditPro to reduce security attack vectors:

Network Ingress: a managed firewall controls network ingress to the cloud hosting environment, restricting access to white-listed IPs and opening only necessary ports

Network Isolation: a tiered network design limits exposure to the internet with a DMZ for web load balancers and isolated private subnets for web application servers and databases.

Active Application Security: AuditPro uses CloudFlare as web application firewall (WAF) with a managed ruleset providing protection to the latest threats, in addition to providing Automatic DDoS mitigation and acting as a Content Delivery Network.

Cloud Security and Compliance Auditing: The AuditPro cloud environment is configured with monitoring in place to scan for compliance breaches of regulations such as HIPAA, PCI and FedRAMP.

Cloud Infrastructure Management and Support: an ISO 27001 certified company provides 24/7 maintenance and support of the AuditPro cloud environment. Processes have been put in place to maintain secure management and support of AuditPro infrastructure in AWS.

Additionally, AWS has certification for compliance with ISO/IEC 27001:2013, 27017:2015, 27018:2019, and ISO/IEC 9001:2015 and CSA STAR CCM v3.0.1.

AWS also supports additional security standards and compliance, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171.

5.4 Encryption of customer data

Data encryption is used end-to-end between trophon2 and the AuditPro cloud SaaS application.

An encrypted connection is made between the AuditPro MSD and trophon2 using mutual TLS (client certificate authentication).

The AuditPro MSD file system is encrypted at rest.

The transmission of data between the AuditPro MSD and the AuditPro cloud application is encrypted over HTTPS as is communication from users accessing the cloud portal.

Transport of data within the cloud application is encrypted and the database and file systems in the cloud application encrypt the data “at rest”.

5.5 Retention of Data

Data is retained by Nanosonics for a maximum of 4 years from the end of subscription but may be deleted at any time from end of subscription.

5.6 AuditPro Security FAQ

Does AuditPro capture PHI (Protected health information)

No, neither trophon2 nor AuditPro capture, store or transmit PHI.

Does AuditPro capture PII (Personally identifiable information / personal data)

Yes, AuditPro captures PII about trophon2 operators – their name OR Employee ID (as programmed by facility) as required to meet decontamination standards in most regions. The AuditPro cloud captures the name and email address of users.

No PII of patients is captured by AuditPro.

What operating systems are used in trophon2 and AuditPro system and how are they updated?

trophon2 runs *Yocto Linux*. Updates to the firmware are periodically made by our service team. If a critical security vulnerability is identified that requires upgrading of trophon2 firmware then our service team will arrange to perform this onsite or replace your trophon device.

The AuditPro MSD runs the Android operating system. Regular kernel patches are released by the device manufacturer and Nanosonics ensures that critical vulnerabilities are deployed over the air to AuditPro MSDs.

The AuditPro cloud runs a variety of operating systems including Windows Server and Linux. Nanosonics ensures that operating systems are regularly patched and security updates are applied.

Management of devices used to access the AuditPro cloud application such as laptops and computers are the responsibility of the facility.

Can we manage the mobile scanning device through our own MDM?

No, the AuditPro mobile scanning device is managed by Nanosonics through VMWare's WorkspaceONE (WS1) MDM platform. At this time, it is not possible to enrol the AuditPro mobile scanning device into a different MDM.

Do you, the vendor, need remote access to our network?

No, Nanosonics does not need remote access to your network to manage AuditPro.

Nanosonics support can perform remote assistance on the mobile handsets when arranged with the customer. This is done through an application installed on the mobile handset, and the handset's existing connection to the VMWare WorkspaceONE mobile device management system. No network ingress is required.

Do you support single sign-on? Can you authenticate our users with their existing credentials?

Yes, the AuditPro cloud application can be integrated with any OAUTH2 and OpenID Connect compatible identity provider including:

- ADFS 2016
- AzureAD
- Okta
- Auth0

6 Appendix A – List of supporting documents

The following supporting documents are available from Nanosonics on request.

1. CIN140: Nanosonics AuditPro IT Security MDS2 Document
2. CIN103: MDS2 Document for trophon2
3. L03075: Nanosonics AuditPro Quick Start Guide

7 Appendix B - Whitelisting for internet access

The AuditPro mobile scanning device requires access to the internet from your network. It needs to be able to contact the Nanosonics AuditPro cloud, VMWare WorkspaceONE (WS1) MDM, and Google services.

Because the list of IP addresses used by Google and VMWare are controlled by those respective third parties, and subject to change without notice, we advise customers that it is preferable to allow AuditPro unrestricted access to the internet through your internet gateway.

For customers who require whitelisting of all outbound internet traffic, Nanosonics can work with you to provide a list of IP addresses and DNS names for whitelisting.

8 Appendix C – Acronyms

Acronym	
AES	Advanced Encryption Standard
AWS	Amazon Web Services
CCM	Cloud Controls Matrix
CSA	Cloud Security Alliance
DDoS	Distributed Denial-of-service attack
DNS	Domain Name System
DSS	Data Security Standard
FedRAMP	The Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
GDPR	General Data Protection Regulation
HIPAA	Health Information Technology for Economic and Clinical Health Act
HITECH	Health Insurance Portability and Accountability Act
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
MDM	Mobile Device Management
MDS2	Manufacturer Disclosure Statement for Medical Device Security
mTLS	Mutual TLS (Transport Layer Security)
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PCI	Payment Card Industry
PoE	Power over Ethernet
QR code	Quick Response code
RFID	Radio-Frequency Identification
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security