SONICU™
The Leader In Monitoring

Technical Overview

Wireless Meter

1. Sonicu Overview

Sonicu, a leader in wireless monitoring technology, offers an affordable scalable temperature and environmental monitoring platform built for regulatory compliance.

Sonicu collaborates with hundreds of organizations across the country, including many leading hospitals, manufacturing companies, universities, distribution, pharmaceutical, and research companies, that rely on Sonicu to safely store vaccines, drugs, food, and valuable research materials.

Sonicu offers a wide array of monitoring applications including temperature, humidity, pressure, sound, CO2 and custom IoT applications for organizations across a broad spectrum of industries.

Specific to the platform are wireless meters for temperature, humidity, air pressure, sound levels, and a host of other applications that transmit data via Wi-Fi, Ethernet, or Cellular to SoniCloud, our cloud-hosted monitoring platform.

SoniCloud is hosted on Amazon Web Services (AWS) US East, which is a FedRAMP-authorized system. AWS provides multi-regional failover, security controls and maintains continuous platform monitoring.

SoniCloud is a SaaS-based platform that requires no server or software maintenance.Sonicu periodically updates SoniCloud, allowing clients to benefit from the most recent system improvements.

2. Protected Health Information (PHI) and HIPAA Statement

Sonicu monitors and records environmental data such as the temperature of cold storage equipment, room temperature, humidity, sound, air pressure, etc. This is the only data that is transmitted to AWS.

No PHI or other HIPAA related information is transmitted by Sonicu devices.

3. System Access and User Credentialing

Clients access the SoniCloud platform by logging into the website at https://www.sonicumonitoring.com or via the mobile app.

This website can be accessed on desktops, laptops, IOS, and Android tablet and phone devices. Users log in with their own unique credentials and are limited to the sites and areas determined by the admin that are required for their job functions.

All user interaction happens within the sonicumonitoring.com domain and subdomains hosted with AWS.

Sonicu credentials users at two levels: **Admin and View**.

Clients may have as many users as needed at either level. Creating users is simple from within SoniCloud's user interface.

Admin level users can create, edit, and remove users as needed. Both Admin & View Users may choose to receive alarm notifications via text, email, phone calls, or a combination of these. All user notifications follow an audit trail for documentation and compliance.

Several reports, including VFC mandatory regulatory compliance reports and device summary reports, are available to users on-demand by logging into the system. Users can also elect to receive auto-generated reports via email at daily, weekly, or monthly intervals.

Sonicu's password policy system is configurable and includes the ability to force password minimum length as well as password complexity (requiring numbers, uppercase letters, lowercase letters, symbols, passwords cannot match previous passwords, etc.)

Sonicu also has a client-configurable password reset feature that requires passwords to be reset on a client-defined interval of days. All passwords in the Sonicu system are salted and stored encrypted (via the Blowfish encryption cipher) in the Sonicu database, ensuring that passwords are secure and cannot be easily decrypted in the unlikely event of a data breach.

All clients at the Enterprise 100 subscription level, or greater, have the ability to integrate their internal authentication structure with SoniCloud via SAML SSO.

Sonicu highly recommends that clients utilize this feature to ensure parity between client authentication requirements and SoniCloud authentication strategies.

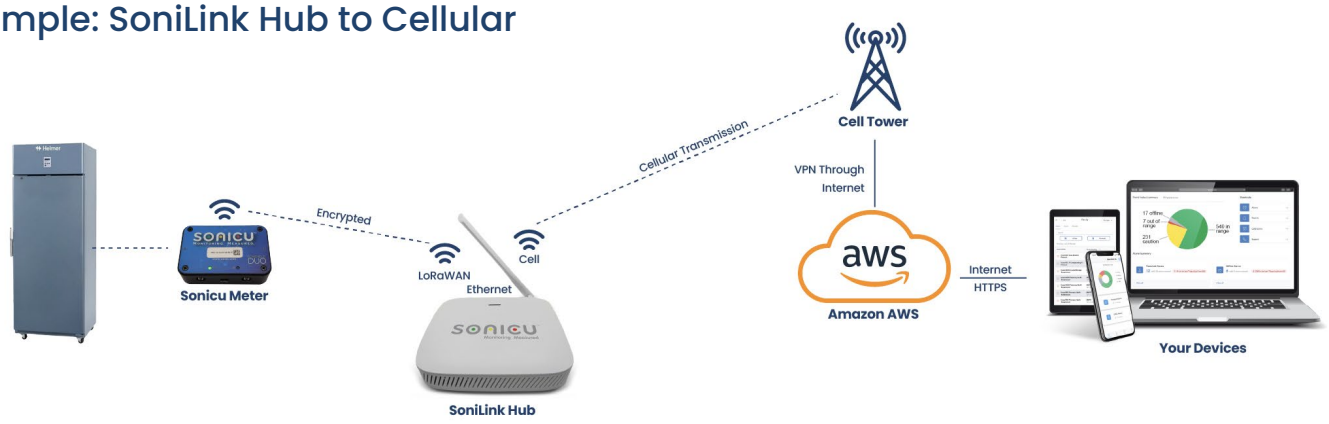
4. Data Transmission and Network Options

Sonicu offers several network options to best meet the client's security requirements, physical layout, and budget. The table below highlights the Sonicu data transmissions options.

		Network Placement	
		OFF Your Network	**ON Your Network**
Device Communication Method	Duo Meter to SoniLink Hub to Cloud	Example: SoniLink to Cellular (See Section 4.1)	Example: SoniLink to Ethernet (See Section 4.3)
			Example: SoniLink to Ethernet with Cellular Failover (See Section 4.3)
	Duo Meter to Cloud	Example: Directly to Cellular (See Section 4.2)	Example: Directly to WiFi (See Section 4.4)

4.1. Sensor to Cloud: OFF Your Network

Example: SoniLink Hub to Cellular



Sonicu's Duo meters sit in the client facility and never use the client's internal network. Sensor data is transmitted via Duo meters to a central cellular SoniLink Hub and then to Sonicu's AWS platform.

Using a LoRaWAN standard for low power, and wide-area (LPWA) networking, SoniLink is an ideal option for clients with one or many Duo meters in one area that shares a single cellular data plan via a hub.

The SoniLink Hub utilizes a cellular modem to send data to SoniCloud.

All traffic sent from the cellular modem is encrypted via a VPN and decrypted by Sonicu at AWS, ensuring data remains protected as it travels over the internet.

SoniLink LoRaWAN connectivity provides the longest-range wireless technology on the Sonicu platform and is ideal for customers wanting easy setup with reliable wireless technology.

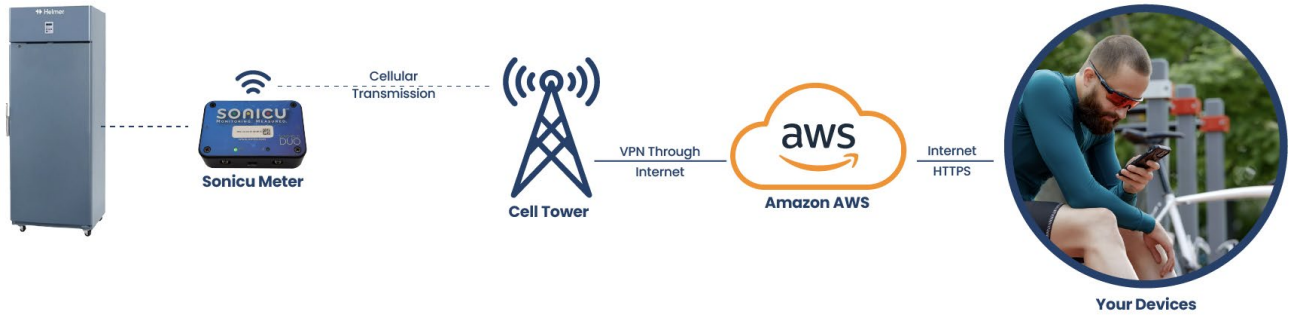
SoniLink has the additional benefit of supporting multiple SoniLink Hubs -- redundancy can be easily achieved by adding two or more SoniLink Hubs to the client's facility.

The SoniLink Hub uses a cellular modem to send data to SoniCloud.

All SoniLink traffic is encrypted using symmetric key AES-128 cryptography, ensuring that all traffic is secure between SoniLink and SoniCloud on AWS.

As the data is encrypted between the meter and SoniCloud, the SoniLink Hub cannot inspect the data and has no visibility into the data.

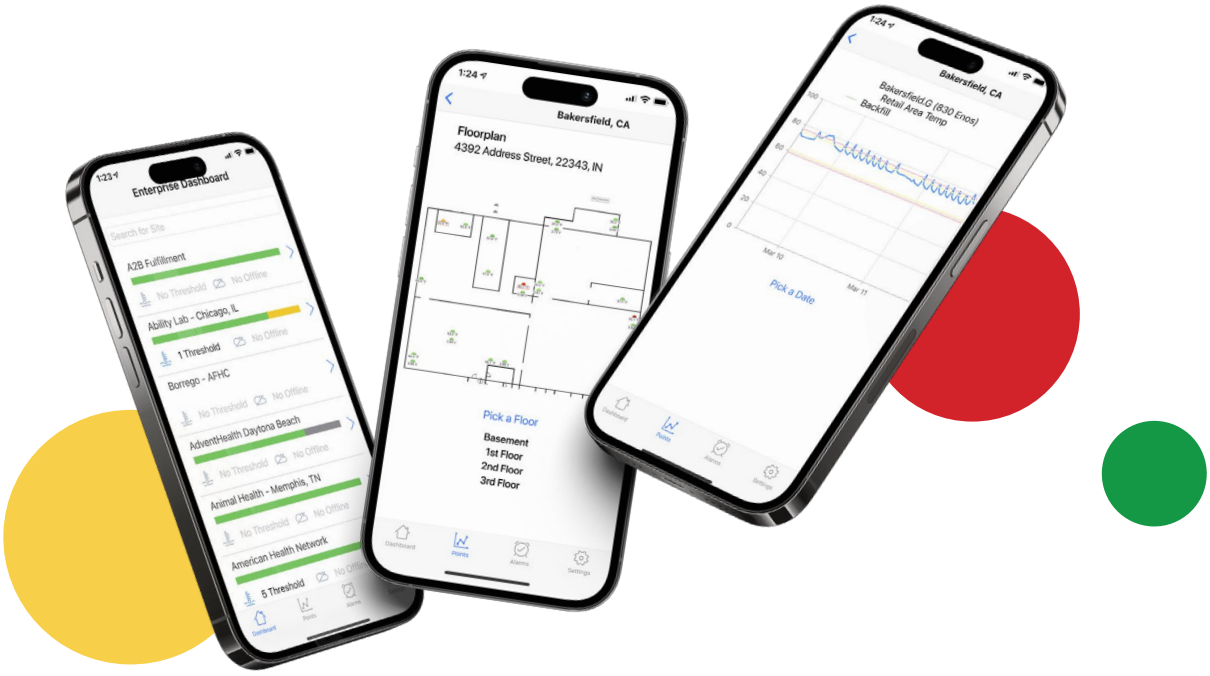
4.2. Sensor to Cloud: OFF Your Network Example: Cellular



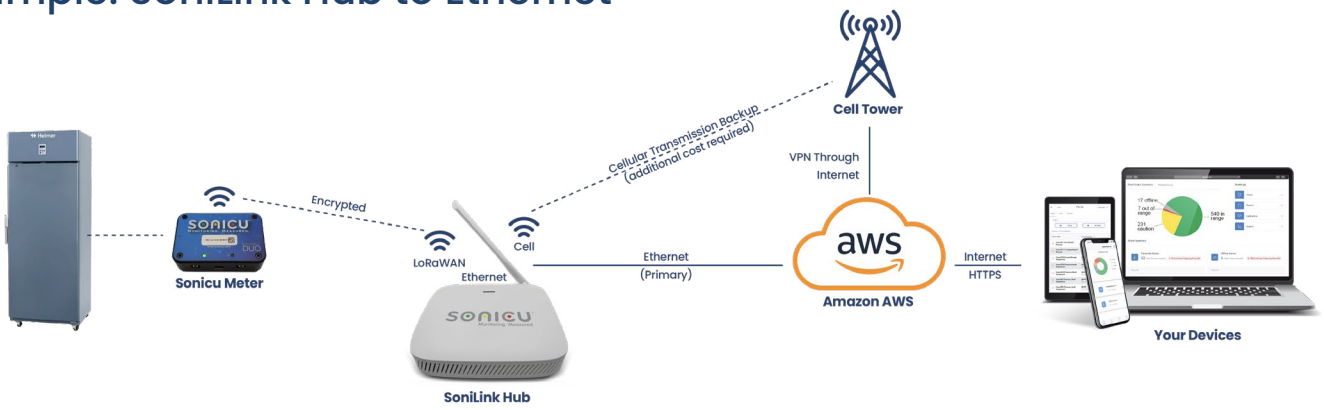
Most Sonicu Duo meters can serve both as the meter and a data gateway by using a cellular modem internal to the meter.

This is an ideal option for locations that have a small number of meters in each location and want to use a cellular transmission option.

Sonicu's Duo meters sit in the client facility and never use the client's internal network. All data sent from the cellular modem is encrypted over a VPN and decrypted by Sonicu at AWS, ensuring data remains protected as it travels over the internet.



4.3. Sensor to SoniLink Hub to Cloud: ON Your Network Example: SoniLink Hub to Ethernet



Data is transmitted via Duo meters using SoniLink Hubs that are connected via Ethernet. The hub uses the client network to send data to SoniCloud.

Using the LoRaWAN standard for low power, and wide-area (LPWA) networking, SoniLink wirelessly connects Sonicu sensors and meters to the cloud platform using a client's network via Ethernet. This is an ideal option for clients with many Duo meters in one area who want to use their network for data transmission.

SoniLink radios provide the longest-range wireless technology on the Sonicu platform and are perfect for customers wanting to ensure an easy setup with reliable wireless technology.

SoniLink has the additional benefit of supporting multiple SoniLink Hubs -- redundancy can be easily achieved by adding two or more SoniLink Hubs to the client's facility.

An Ethernet with cell failover option is available for customer applications with strict guidelines that cannot allow temporary service interruptions.

Additional data transmission information can be found in Section 4.5.

4.4. Sensor to Cloud: On Your Network Example: WiFi

Sonicu Duo meters can be equipped with Wi-Fi radios configured to communicate with the Client's WiFi network. This option allows the client to use an existing WiFi infrastructure to add meters anywhere the Wi-Fi network is accessible.

Additional data transmission information can be found in Section 4.5.

5. Network Transmission Options

Cellular

Sonicu maintains a VPN between Verizon and Amazon Web Services (AWS). A Cellular configuration offers additional advantages in that the system can be fully configured prior to shipping for simple implementation.

Sonicu is a Verizon Vertical Partner (VPP) and uses the Verizon 4G LTE network.

SoniLink

A long-range radio with chirp spread spectrum (CSS) and end-to-end encryption. Used when the client's internal Wi-Fi network cannot be used, the powerful radio allows for extremely long-distance communication.

SoniLink radios can transmit to multiple SoniLink Hubs, adding easy and reliable redundancy to the data transmission to SoniCloud. SoniLink utilizes the US902-928MHz band in North America.

WiFi

Standard 2.4 GHz WiFi with b/g/n network compatibility and WPA2 security as well as (802.1x) WPA2-Enterprise (PEAP-MSCHAPv2)

6. Network Requirements

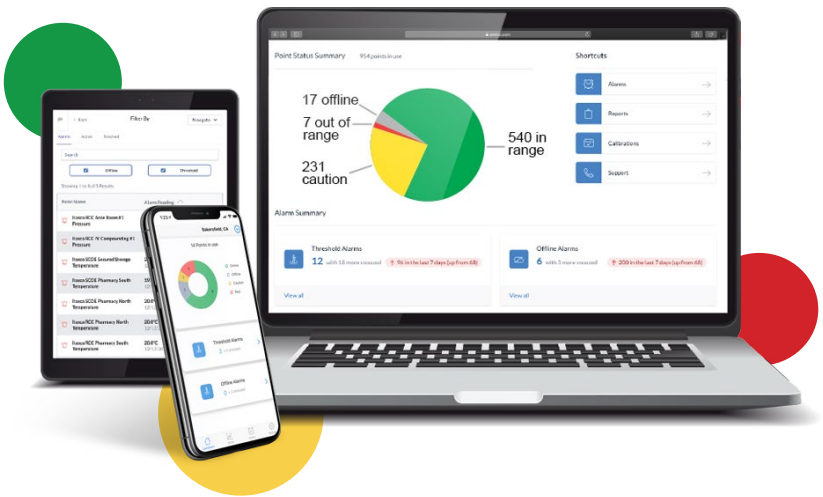
The following requirements pertain to ALL Sonicu data transmission options (Cellular, WiFi, Ethernet):

Sonicu's server will send Admin & View user emails from both @sonicu.com and @sonicumonitoring.com addresses. These web addresses should be added to the approved senders' list.

Web browsers communicate through Sonicu's SoniCloud monitoring site via www.sonicumonitoring.com. All web assets will come from this address.

Ethernet and WiFi network data transmission options require additional input from your IT department.

For these types of networks, Sonicu has a Network Questionnaire that clients complete on SoniCloud. The information below pertains to Sonicu devices that transmit on your network (WiFi or Ethernet).



Required port and connections for Duos and SoniLink Hubs

Wifi (Depends on Binary/HTTP/HTTPS) SoniShield Duos

80 dev1.sonicumonitoring.com (Binary)
443 hat1.sonicumonitoring.com (HTTPS)
80 hat1.sonicumonitoring.com (HTTP)

SoniLink (All ports and endpoints required) SoniLink Hubs

TCP 443 A27B5R0TVNCU3L.lns.lorawan.us-east-1.amazonaws.com TCP 443 A27B5R0TVNCU3L.cups.lorawan.us-east-1.amazonaws.com TCP 443 and 5798 ds.devicehq.com (Only for Cell Hubs)
UDP 123 time.nist.gov

Sonicu Network Defaults Editable Y/N Encryption WPA2 Y DHCP Auto Y Protocol Binary Y DNS 8.8.8.8 Y Authentication Passkey Only N

7. Data Storage Information

Sonicu is hosted on Amazon Web Services (AWS) for its security, redundancy, and scalability.

All Sonicu and client data is stored long-term with AWS. Below are some links related to AWS security.

Security - Overview of Amazon's security benefits, including redundancy.

Resources - List of white papers, articles, etc. regarding AWS security.

Fortune Article - Describes the physical security and requirements needed to access the servers.

Security Whitepaper- PDF detailing security benefits to clients.

FedRAMP - AWS information related to FedRAMP.

8. Device Security

To provide an extremely long battery life, Sonicu uses low-voltage microprocessors with minimal computing ability.

Sonicu's SoniShield devices feature an embedded microprocessor, a 32-bit microcontroller with less than 512KB RAM.

The extremely small technical capabilities of the microprocessor, combined with a custom firmware solution running on the device, reduces the potential of network attack.

Additional technical details can be provided upon request under an NDA.

9. Sonicu Cloud Infrastructure

Sonicu utilizes Amazon Web Services (AWS) technologies to provide reliable, scalable solutions for our clients.

Sonicu's internal AWS network credentials are based upon the principle of least privilege, ensuring that each service can only access what is required.

Sonicu uses the AWS Relational Database Service (RDS) to host its MySQL database in multiple regions with duplication and immediate failover to ensure high levels of quality.

Sonicu routinely patches its servers on a weekly basis, with any pressing industry-wide security threats (e.g., Heartbleed) being patched as soon as needed. Because the Sonicu platform is web-based, no patches need to be provided to the client directly.

10. FAQs

1. Does Sonicu store or transmit any Protected Health Information (PHI)?

Absolutely not. Sonicu monitors and records environmental data such as the temperature of cold storage equipment, room temperature, humidity, sound, air pressure, etc. This is the only data that is transmitted to AWS.

2. Can Sonicu meet our password access control requirements?

Yes! Sonicu has a large range of password control requirements that are configurable.

3. Does Sonicu reside on our local network?

Sonicu software, including the SoniCloud monitoring web interface, is located on AWS, not on the client's network.

Sonicu sensors, Duo meters, and gateways can, if chosen by the client, be located on the client's network; other options are available to separate Sonicu devices from a client's network if required.

4. Does Sonicu provide auditing capabilities?

Yes! Sonicu's SoniCloud software provides logs of important user actions, such as clearing alarms and changing alarm thresholds. These audit logs can be provided to the user as requested.

5. What software does the client need to use on the Sonicu platform?

The SoniCloud monitoring platform runs on any standard, current-generation web browser (Chrome, IE, Firefox, etc.) There is nothing else needed - no plug-ins, no additional software, nothing!

6. What data transmission options does Sonicu offer to ensure data security?

Sonicu provides encryption options over a cellular network (if the devices are located off the client's network) or offers a B2B IPSec VPN as required (if the devices are located on the client's network) for data transmission to AWS.

Sonicu requires HTTPS for all web connections.