ASPEN TECH
POLICY HUB

FREQUENTLY ASKED QUESTIONS

The Device Query Interface

Daniel Bardenstein

This document should be used by the Federal Drug Administration (FDA) to provide manufacturers and healthcare delivery organizations with an overview of Device Query Interfaces (DQIs). It addresses potential questions and concerns that may arise from new FDA guidelines.

What is active scanning?

Active scanning is a common way that cybersecurity teams effectively, accurately, quickly, and cheaply acquire a broad set of information about devices on their networks, including devices' identity, health, and vulnerabilities. Active scanning involves using automation to send large numbers of requests (i.e., questions or commands) to one or more devices to see how the device reacts. By examining how the device responds to each request, active scanning tools can make accurate and real-time inferences about a device's identity, function, health, and potential weaknesses.

Though active scanning is a common practice to secure "internet-of-things" (IoT) devices, healthcare cybersecurity professionals unfortunately are unable to leverage active scanning techniques on medical devices. As a result, it is difficult for hospitals and other healthcare facilities to secure these devices, leaving them – and their patients – more at risk of cyber attacks.

Why can't healthcare cybersecurity professionals use active scans on medical devices right now?

According to healthcare cybersecurity professionals, there are two main obstacles that prevent them from running active vulnerability scans on medical devices right now:

1. **Devices are too fragile**. Like an old computer that freezes up when it tries to run new, complex programs (such as a video game or photo editors), many medical devices lack the technical power to handle the deluge of requests generated by active scans. Making devices more powerful, such as by adding more processing power, memory, or storage, can be expensive for manufacturers.

2. **(Dis)incentives by manufacturers.** Some device manufacturers contractually prohibit the use of active scanning on their devices. Other manufacturers write in their contracts that running active scans voids the device warranty, eliminating any future customer support or software updates that device owners would otherwise receive. Manufacturers understandably do this to protect themselves from the risk of one of their devices malfunctioning and causing harm to patients, which requires notifying the FDA, who would likely investigate the incident and potentially issue a device recall. Recalls, in addition to brand damage and regulatory scrutiny, can be incredibly expensive for manufacturers, and thus disincentivize manufacturers from installing active scans.

Why is scanning medical devices important?

Active scanning is traditionally used to support several fundamental goals for cybersecurity teams tasked with defending their organization's networks and devices:

- **Asset discovery.** Without a safe, effective way to remotely scan devices, security teams have difficulty building and maintaining accurate inventories of their medical devices. Alternatives to active scanning are expensive, underdeveloped, and insufficient.

- **Vulnerability response.** When a new software vulnerability is discovered, security analysts have difficulty rapidly identifying potential impacts to their medical devices. The recent Apache Log4J vulnerability is a great example: both the Cybersecurity and Infrastructure Security Agency (CISA) and the FDA suggested that organizations should find any devices running Apache that may be susceptible to the dangerous Log4J vulnerability, which could allow cyber attackers to easily hack into and take over various devices. For this type of scenario, cybersecurity professionals outside of healthcare can use active scanning to find and identify devices running the Apache software; for medical devices, security teams must use less effective methods to achieve similar (but less accurate) results.

- **Legacy and end-of-life products.** Many medical devices are considered “legacy” or “end-of-life,” meaning that they are sufficiently old that the manufacturer no longer supports them and/or they are too outdated to integrate with modern digital protections. Since many of these devices are still useful to patients, such as twenty-year-old MRI machines, healthcare organizations can’t simply upgrade or replace these extra-vulnerable devices. Instead, they must closely monitor and protect them from potential threats. Active scanning is a valuable tool to create asset inventories of legacy devices and quickly identify potential vulnerabilities in them.

What is a Device Query Interface (DQI)?

A DQI is simply a feature or method in a medical device that allows device owners to safely query a device for important information without the risk of interrupting the device or causing a malfunction. This functionality essentially provides device owners an alternative way to get real-time information from a medical device without the need to run active scans, ensuring the continuous function of the device and patient safety.

As an analogy, a DQI is like a hotel concierge. If someone was trying to find information about guests staying at a hotel, active scanning would entail knocking on the door of every single room. A DQI acts like the concierge in the lobby, a single place that can provide a wide breadth of information about occupancy rate or where a certain guest is staying.

An Analogy: A Hotel Congierge

Active Scanning is like trying to identify every guest in a hotel by knocking on each door and seeing if anyone is inside.

The Device Query Interface (DQI) is like a hotel concierge, whom you can simply ask “How many guests are staying in the hotel tonight?” or “In what room is Jane Doe?”

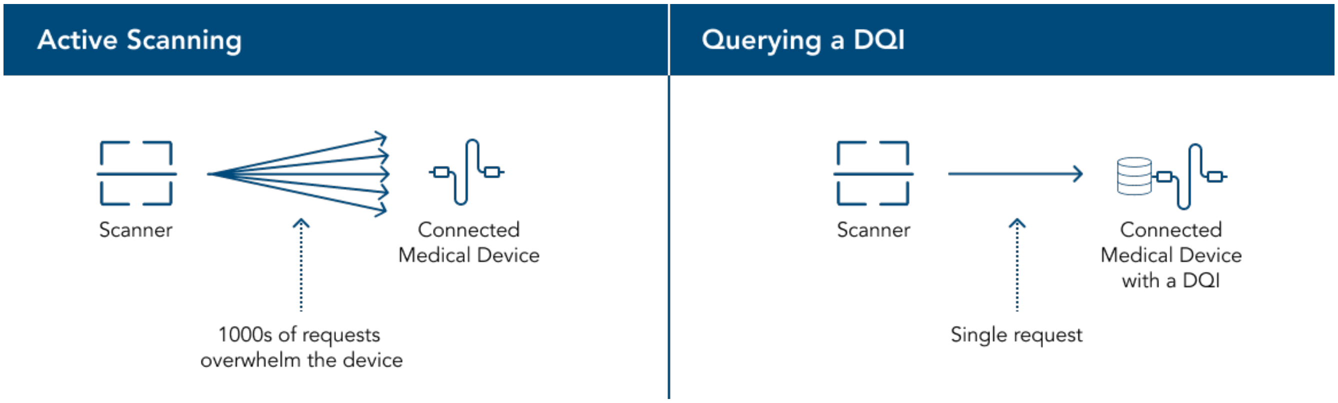
This functionality exists in connected devices in other industries, such as industrial control systems (ICS), where it’s very important that devices not be interrupted. In the ICS sector, some refer to this capability as “selective probing,” where device owners can selectively probe — i.e., make targeted requests for specific information — a connected device without risk of causing a device malfunction.

If this approach works for ICS devices, which can control power generation, manufacturing plants, and connected vehicles, it likely can be effective for medical devices.

How does a DQI work?

A DQI provides an interface in a device where a user can send requests in order to retrieve real-time information about a device, also known as selective probing. Whereas active scanning generates hundreds if not thousands of requests sent across a medical device, with a DQI device, owners can send individual queries to a device to get specific information. For example, a user could query a device's DQI for a list of software running on the device and the versions of each piece of software. The device would then aggregate that data (or have a prepared response ready to go) and return that data to the user. This exchange requires only two requests – the query and the response – which is easier for devices to handle than the barrage of requests from active scans.

DQIs would be able to provide important information to device owners to help them identify, diagnose, and monitor a device. This data might include device identifiers, health status, current configuration, and the names and versions of any software or firmware on the device.



Why is a DQI useful?

- **Building and maintaining an accurate asset inventory of medical devices.** Building and maintaining asset inventories is a fundamental mission for cybersecurity teams, allowing them to understand their organizations' 'digital footprint.' Devices with a DQI would make it easier for security analysts to safely and efficiently obtain real-time information about their medical devices, the health of those devices, and any potential software vulnerabilities in those devices. For example, a security analyst at a hospital could write a script that automatically queries each medical device every day at midnight (or another off-hour), to get the latest status of their medical devices, without risking adverse impact to patient care.

- **Rapidly identifying vulnerable medical devices**. After a new software vulnerability is disclosed by a security researcher or the device manufacturer, security teams at healthcare facilities can rapidly query the DQIs of their medical devices to see which devices are running vulnerable versions of the software. Once the set of impacted devices is identified, the security team can take additional preventative measures for those devices, such as patching, adding firewall rules, or isolating them from the rest of the network.

What are the benefits of a DQI for medical device manufacturers?

- **Better FDA compliance.** Following FDA guidance increases the likelihood that devices will receive FDA approval and avoids potential delays.
- **Reduce hacks, save lives, and protect the brand.** A hacked medical device can lead to patient harm or devastating breaches at healthcare facilities. This can also damage the manufacturers' brand and reputation with patients, customers, and the FDA. DQIs help customers better protect their devices against these scenarios.
- **Flexibility.** Because the DQI is a conceptual feature, manufacturers can decide how best to build a DQI for each of their devices.
- **Low cost.** DQIs are lightweight features that are very common across connected devices and don't require heavy research and development (R&D) investment.

What are the benefits of a DQI for healthcare delivery organizations (HDOs)?

- **Better asset inventories and visibility.** HDOs can more easily build and maintain accurate lists of devices in their environment and quickly identify problems.
- **Faster vulnerability response.** With DQI-enabled scans, HDOs can find and protect vulnerable devices faster from newly discovered vulnerabilities.
- **Better security and less risk.** With better asset inventories and faster vulnerability response, HDOs will be more secure and reduce the chance of a devastating cyber breach.

- **Increased patient protection.** More secure medical devices and HDOs means patients are better protected from direct or indirect harms caused by hacked medical devices.

How Can I Build a DQI?

Basic Components

At its core, a DQI consists of the following components:

1. A certain interface or endpoint that can receive requests.
2. A method for the device to aggregate data about itself. The data can be gathered either in real time when it receives a request, or, for commonly requested data, regularly gathered in advance and stored for even faster response times.
3. Returning data back to the user in an easily readable format.

Protocols

Manufacturers can select from established methods of communication protocols based on each device's specific requirements. Below is a list of some commonly used "internet-of-things" (IoT) communication protocols and some environments where they can be used:

- HTTP/HTTPS
- Message Queueing Telemetry Transport (MQTT)
- Constrained Application Protocol (CoAp)
- Windows Management Instrumentation (WMI)
- Simple Network Management Protocol (SNMP)
- Link Layer Discovery Protocol (LLDP)
- WebSocket
- Bluetooth

- Radio Frequencies

What security considerations should I keep in mind when building a DQI?

Manufacturers should also design their DQIs securely to prevent potential abuse. For example, an unauthorized cyber attacker may try to use the DQI to find hackable weaknesses in a device. Alternatively, flooding a device's DQI with queries (either intentionally or unintentionally) could cause the device to malfunction.

Manufacturers should conduct further "threat modeling" exercises to identify other potential threats and abuses of the DQI feature, and then design protections for each scenario. For example, to prevent the unauthorized hacker from finding weaknesses, the device could require DQIs to authenticate users, forcing users to prove their identity (such as with a username and password). Or to prevent malfunctions caused by flooding a device with requests (a "denial-of-service" attack), manufacturers can place limits on how many requests can be made to a DQI per minute or per hour.