



SetPoint System IT Configuration Guide

Read all instructions, warnings and cautions carefully. Failure to follow them could lead to damage to the SetPoint System, cause it to malfunction, degrade its performance and/or result in harm.

Contact SetPoint Medical with any questions about the information contained in the SetPoint System IT Configuration Guide (Patient IFU). Copies of all SetPoint System Instructions for Use (IFUs) are available on the SetPoint Medical website. Any SetPoint System-related incident or problem, which is believed to represent a safety issue, should be reported to SetPoint Medical, Inc. immediately.

CONTACT INFORMATION:



SetPoint Medical, Inc.
25101 Rye Canyon Loop
Valencia, CA 91355-5004
United States

Tel: (661)-750-6140

Email: support@setpointmedical.com

www.setpointmedical.com



Caution: Federal law restricts this device to sale by or on the order of a physician.

SetPoint Medical is a registered trademark of SetPoint Medical, Inc.



Table of Contents

Introduction	3
Intended Audience	3
Purpose for Network Connectivity.....	3
Changing IT Configuration	3
Hazards of IT Misconfiguration	3
Network Configuration	4
Minimum Networking Requirements	4
Supported Network Configurations	4
Wireless Local Area Network Access.....	5
Cellular-Enabled iPad Internet Access.....	6
Cellular Internet Access via a Tethered Phone.....	7
TCP/IP Ports	7
Programmer Ports.....	7
Apple App Store Ports.....	8
Mobile Device Management Ports.....	8
Obtaining Updates	9
Recommended Security Enhancements	10
Network Encryption	10
Use Primary Credential Options	10
Multi-Factor Authentication for Users	10
Network Segregation, Firewalls, and Enterprise Hardening	11
Data Backups.....	12
Troubleshooting	13
Device Security Related Displays	13
Failed Network Configuration Displays.....	13
Programmer Security Related Displays	14
Security Forensics.....	15



Introduction

This guide provides requirements for network connectivity, descriptions of network operations, and details on network cybersecurity for use of the SetPoint System. On most Internet-connected networks, the Programmer will work without additional network connectivity configuration. This guide is intended for individuals evaluating compatibility of their networks for use with the SetPoint System or users who may be having trouble using the Programmer because of network connectivity issues.

Intended Audience

This guide assumes its audience to have general familiarity with networking and Information Technology (IT) concepts. Currently, this guide is not applicable to patients or surgeons, as there are no Internet connectivity requirements for at-home or surgical use.

Purpose for Network Connectivity

Internet connectivity is required by Programmer to operate. Programmer uses the Internet to connect with SetPoint Medical's Cloud Infrastructure. The SetPoint Medical Cloud Infrastructure provides software and firmware updates for devices, authenticates users and SetPoint Medical devices, digitally signs commands and requests, and more. Programmer cannot function without Internet access.

Changing IT Configuration

The connection of Programmer to an IT network that includes other equipment could result in previously unidentified risks to patients, operators or third parties. You should identify, analyze, evaluate, and control these risks. Changes to IT configuration should be evaluated against the recommendations of this guide. Changes to IT network configuration in ways that do not follow the recommendations of this guide may prevent Programmer from functioning. Changes to network encryption protocols may result in less secure network connections with Programmer.

Hazards of IT Misconfiguration

Misconfiguration of IT infrastructure may result in the inability to use Programmer, which, in turn, may lead to the following hazardous situations: Unexpected Stimulation, Temporary Painful Stimulation, and Temporary Loss of Therapy.



Network Configuration

Minimum Networking Requirements

The SetPoint System requires Internet access for use of the Programmer software. Home and surgical use environments have no Internet connectivity requirements. The following Quality of Service (QoS) parameters should be maintained to provide reliable, uninterrupted use of the Programmer software.

- **Latency:** DNS resolution latency to **setpointmedical.cloud** should be under 100 milliseconds. SSL Handshake latencies to **api.setpointmedical.cloud** and **identity.setpointmedical.cloud** should each be under 500 milliseconds. Higher latencies may result in disconnections when using Programmer.
- **Bandwidth:** A minimum bandwidth of 1 megabit/second, for both upload and download, is recommended for optimal use of Programmer. Lower bandwidths may work uninterrupted (if other requirements are met), but with a degraded experience for healthcare providers using Programmer.
- **Reliability:** Connections should be free of packet loss. Connections with packet loss may result in disconnections when using Programmer.
- **Interference Management:** If using a wireless network or cellular connection, the environment should be free of electromagnetic interference that may impact the wireless network connection.
- **Security:** All Internet connections should allow TLS 1.2+ connections that do not tamper with, or proxy, SSL certificates. Programmer will reject connections that cannot provide proper TLS 1.2+ connections. Wireless network connections should use modern security protocols (e.g., WPA2 or WPA3).
- **Coverage:** If using a wireless network or cellular network connection, comprehensive coverage should be included in all areas for the areas Programmer will be used. Failure to have wireless network coverage may result in disconnections when using Programmer.

Programmer transfers relatively small quantities of data, with a typical patient session transmitting a few hundred kilobytes of data. Some patient sessions (e.g., those that require firmware updates) typically transmit around a megabyte of data. Programmer is generally not of significant impact to metered connections such as cellular connections, but SetPoint Medical encourages users to consider bandwidth consumption and QoS needs.

Supported Network Configurations

Programmer requires Internet access and security negotiations using TLS 1.2+. Programmer has been demonstrated to work well on both wireless local area network connections (i.e., Wi-Fi) as well as cellular connection (both cellular connections on an iPad or cellular connections via a tethered phone).



Wireless Local Area Network Access

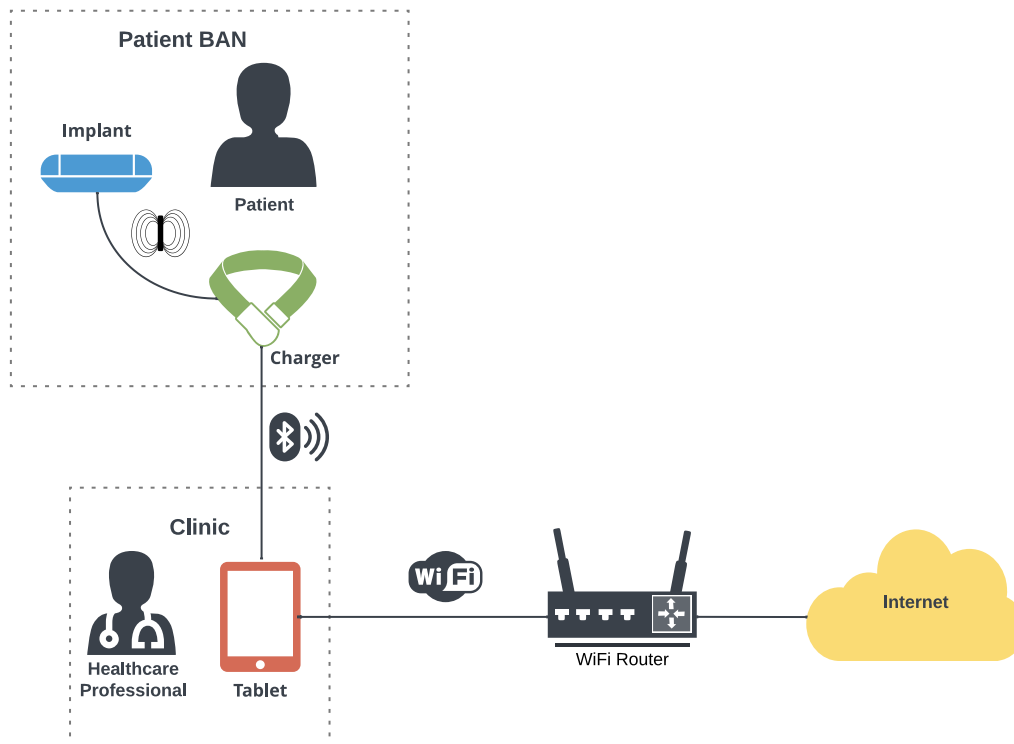


Figure 1 – Programmer to Wi-Fi Connectivity

The typical connectivity scenario for Programmer is connection to an Internet-connected Local Area Network via Wi-Fi. If a wired connection is required, Programmer does operate when Internet connectivity is obtained through an Apple-iPad compatible ethernet adapter. While Programmer leverages TLS 1.2+ to ensure that communications are secure even on open networks, it is still recommended that wireless networks use one of the protocols defined in the Network Configuration section of this document.



Cellular-Enabled iPad Internet Access

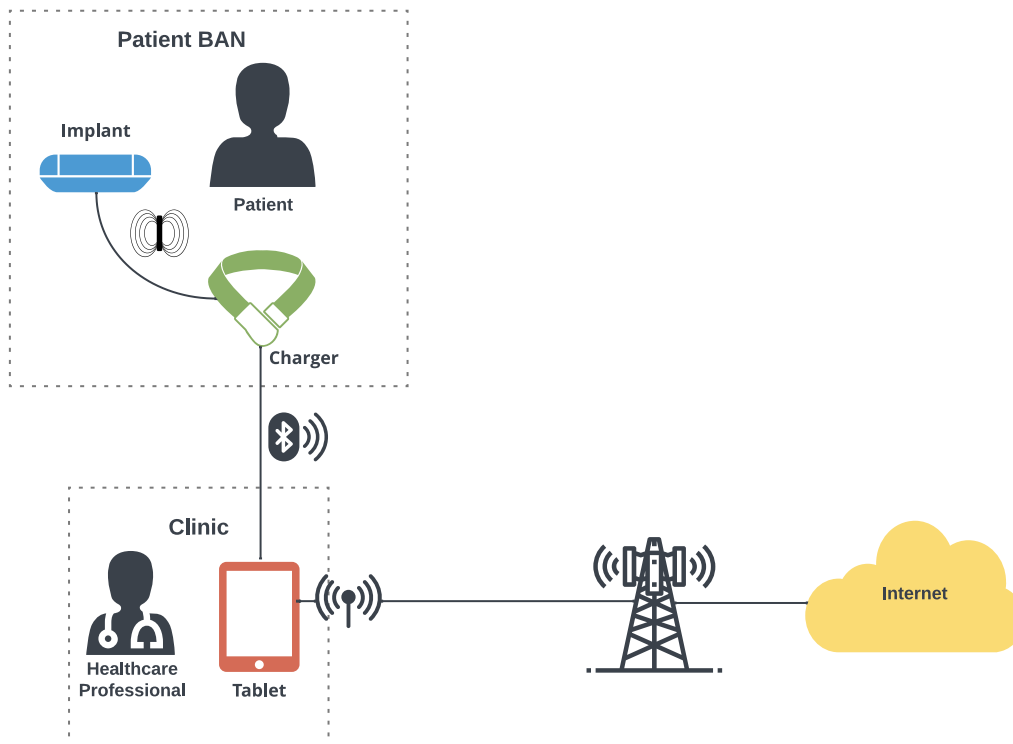


Figure 2 – Programmer Connectivity using Cellular Service

Apple iPads with Cellular capabilities and service may use the cellular connection with Programmer. In practice, most cellular connections in the United States can satisfy the Quality of Service requirements for the SetPoint System. However, some areas or buildings with poor coverage may provide inadequate responsiveness to use the SetPoint System. Depending on the terms of your service, cellular service charges may apply when using Programmer over a cellular connection.



Cellular Internet Access via a Tethered Phone

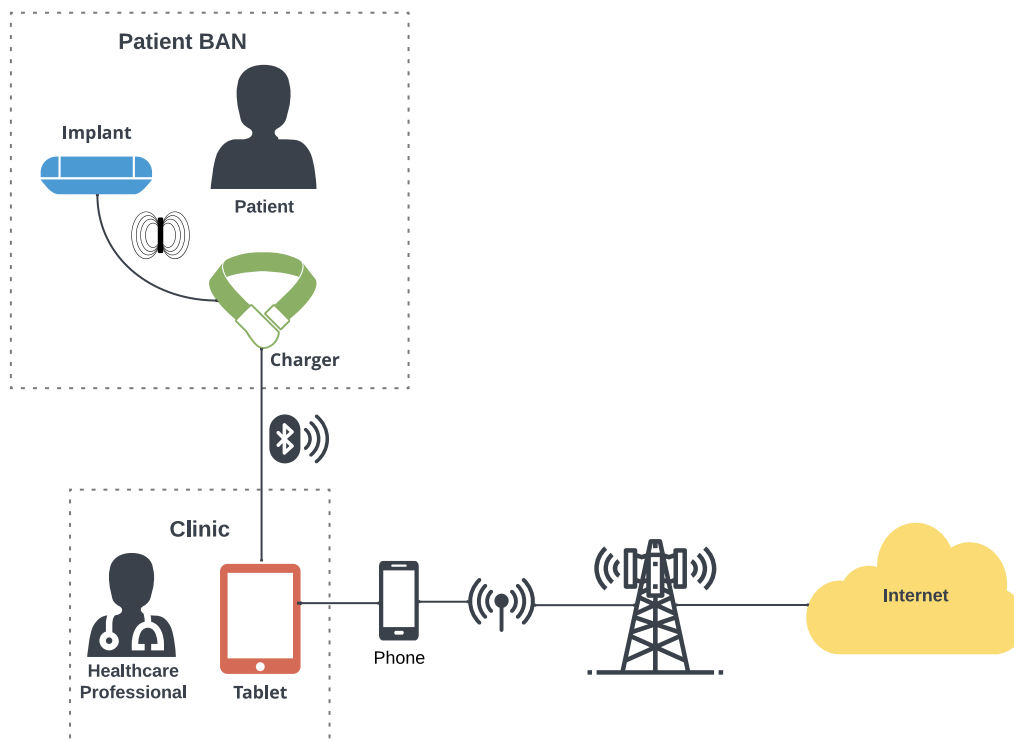


Figure 3 – Programmer Connectivity via Tethered Connection (i.e., “Mobile Hotspot”)

Programmer can operate on an iPad whose Internet access is achieved through a tethered connection (i.e., a “Personal Hotspot”) to a mobile phone. In this configuration, similar concerns about Quality of Service requirements and cellular service charges should be considered as when using a direct Wi-Fi or direct cellular Internet connection.

Additional Information:

- [Creating a Personal Hotspot from an iPhone or iPad](#)
- [Sharing a Mobile Connection by Hotspot or Tethering on Android](#)

TCP/IP Ports

Programmer Ports

The following are endpoints and ports that are used by the Programmer. If using a highly restrictive network configuration, these destinations need to be allowed in bi-directional communication:

Port	Endpoints	Traffic Direction	Description
80	*.setpointmedical.cloud	Incoming/ Outgoing	Used for Programmer core functionality including user authentication and therapy adjustment.
443	*.setpointmedical.com		

Table 1 - Device Names and Model Numbers



Apple App Store Ports

Updates to Programmer are deployed through Apple's App Store. Networks should be configured to allow updates deployed via Apple's App Store. Apple's own documentation should be consulted to know which ports and endpoints are used in Apple products. These may change over time.

Additional Information:

- [TCP and UDP Ports Used by Apple Products](#)
- [Instructions for Configuring Apple Products on Enterprise Networks](#)

Mobile Device Management Ports

Some iPads, particularly those that are part of clinical trial or study, may come pre-configured to run Programmer. These iPads are controlled through SetPoint Medical's Mobile Device Management (MDM) program. These iPads may need additional network configuration for proper functionality.

Additional Information:

- [List of Ports and Connections used by MDM Configured iPads](#)



Obtaining Updates

Programmer will alert users when an update to the software is required. The following message will be displayed if a software update must be performed:

“This version of Programmer is out-of-date and must be updated before signing in. Please contact SetPoint Medical for assistance.”



Figure 4 – Programmer’s Display when an Update is Required

Users should follow standard App Store update procedures to obtain their update to Programmer. If the iPad is controlled by SetPoint Medical’s MDM system, this message should not be seen and SetPoint Medical should be contacted.

Additional Information:

- [How to Manually Update Apps on Your Apple Device](#)

Firmware updates for the Charger and Implant are handled automatically by the Programmer software. Consult the SetPoint System Prescriber Instructions for Use.



Recommended Security Enhancements

This section contains optional, but recommended, procedures for enhancing or “hardening” the configuration of your network and the SetPoint System against cybersecurity threats. In the event a vulnerability was to be discovered, these security enhancements may provide additional mitigations that could ultimately prevent a vulnerability from being exploited.

Network Encryption

One of the following Wi-Fi security protocols is recommended whenever using Programmer over a Wi-Fi connection:

- **WPA2:** WPA2-PSK, WPA2-Personal, and WPA2-Enterprise are all acceptable variations of WPA2.
- **WPA3:** WPA3-SAE, WPA3-Personal, and WPA3-Enterprise are all acceptable variations of WPA3.

SetPoint Medical recommends that the following Wi-Fi security protocols are NOT used because of known and active vulnerabilities:

- **WEP**
- **WPA** (sometimes referred to as “WPA1”)

Use Primary Credential Options

The SetPoint System offers the use of both passwords and passkeys as primary authentication factors. Passkeys offer stronger security than passwords, and a passkey is highly recommended when it makes sense for users’ workflows (e.g., particularly in cases where users do not share a device and can take advantage of the iPad’s built-in biometric passkey authorization).

When choosing a password, the SetPoint System will offer the user a pre-generated passphrase instead of having users choose their own password. These passphrases have been designed to have brute-force resistant levels of entropy and are pre-screened to not be a part of any data breach. Users may still choose their own password, but all passwords will be pre-screened to ensure they are not part of any prior data breaches. This screening occurs when users sign in as well as when users change their password.

Multi-Factor Authentication for Users

SetPoint Medical recommends enabling multi-factor authentication (MFA) for all users. Programmer offers the ability to enable MFA from within the application (see the SetPoint System Prescriber Instructions for Use). It is advised that users choose authenticator applications that use Time-based One-Time Password (TOTP) over text message (SMS) authenticators. SMS authenticators are subject to a variety of attacks in the mobile phone system and are considered a weaker authenticator option.

Alternatively (or in addition to) the MFA options within Programmer, users that sign in with an alternative sign-in provider (e.g., “Sign in with Apple” or “Sign in with Microsoft”) are recommended to enable multifactor authentication on their account through the source platform. Both Apple and Microsoft offer extensive multi-factor authentication mechanisms.

Additional Information:

- [Apple: Two-factor Authentication for Apple ID](#)
- [Microsoft: Set Up Your Users with Multifactor Authentication](#)



Network Segregation, Firewalls, and Enterprise Hardening

No part of the SetPoint System accepts unsolicited TCP/IP traffic, and thus, network segregation techniques should not be required to ensure cybersecurity of the SetPoint System. Use of TLS 1.2+ ensures that communications should remain confidential and tamper-proof even in the presence of an adversary on the same network. Additionally, all TCP/IP traffic from the SetPoint System is only destined to the addresses defined above. It does not interact with other local network resources and should not present interoperability challenges with other equipment on the network.



Data Backups

IT personnel do not need to explicitly perform any procedures to backup or protect data on SetPoint Medical devices. Charger and Implant data is securely stored, and backed up, in SetPoint Medical's Cloud Infrastructure. Cybersecurity attacks to hospital or clinic networks (e.g., ransomware attacks) would not impact the data of the SetPoint System as it is stored securely on an external system.




Troubleshooting

Device Security Related Displays


Attempts to breach security on the SetPoint System are logged and securely transmitted to SetPoint Medical. Most of these will be blocked and invisible to the user, as no action will need to be taken. Should either the Implant or Charger encounter a security issue that is unrecoverable, an error state will be displayed on the Charger as indicated in the Charger LED Indications section of the SetPoint System Prescriber Instructions for Use.

Failed Network Configuration Displays

Issues in network connectivity will result in one of the two following error messages being displayed:

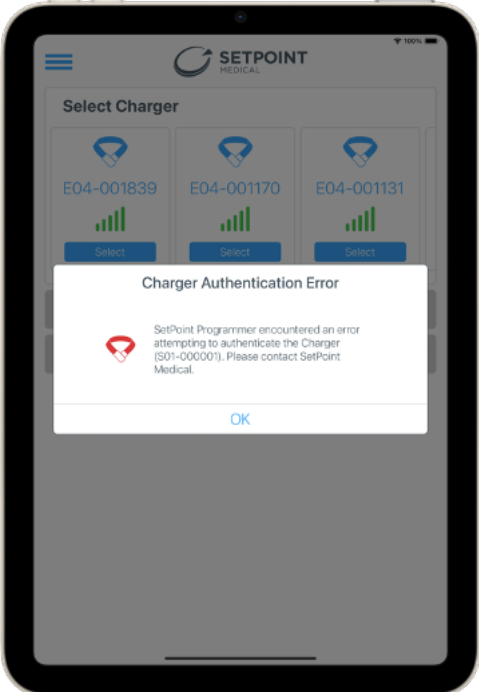
Error Display	Message
	<p>Programmer experienced an issue with connectivity. Check your network connection and contact SetPoint Medical if the issue persists.</p>



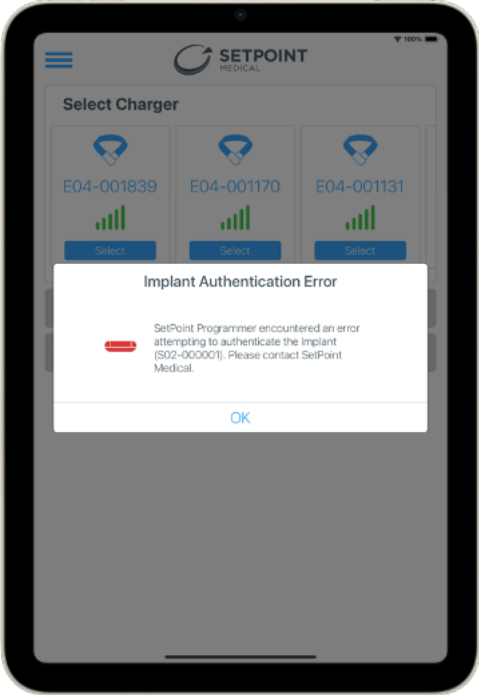
Error Display	Message
	<p>Network connection unavailable</p>

Programmer Security Related Displays

The following error messages may indicate a cybersecurity issue. If these messages are encountered, users should contact SetPoint Medical.

Error Display	Message
	<p>Programmer encountered an error attempting to authenticate the Charger (E04-XXXXXX). Please contact SetPoint Medical.</p>



Error Display	Message
	<p>Programmer encountered an error attempting to authenticate the Implant (M01-XXXXXX). Please contact SetPoint Medical.</p>

Security Forensics

SetPoint customers, including IT staff and administrators, do not need to monitor security forensics logs. Security logs of unusual device or account activity are automatically transmitted to SetPoint Medical. SetPoint Medical has post-market security monitoring procedures in place to watch for, and address, any cybersecurity threats. In the event an account appears compromised, SetPoint Medical may force a user to change their password or lock their account. SetPoint Medical support personnel will alert customers when suspicious security events or compromises are detected.