LANTRONIX®

Application Note:

Best Practices for IoT Device Security

Part Number APP-0041
Revision A May 2020

Intellectual Property

Contacts

Lantronix, Inc.
7535 Irvine Center Drive, Suite 100
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support
Online: www.lantronix.com/support

Sales Offices
For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about/contact

Disclaimer

All information contained herein is provided "AS IS." Lantronix undertakes no obligation to update the information in this publication. Lantronix does not make, and specifically disclaims, all warranties of any kind (express, implied or otherwise) regarding title, non-infringement, fitness, quality, accuracy, completeness, usefulness, suitability or performance of the information provided herein. Lantronix shall have no liability whatsoever to any user for any damages, losses and causes of action (whether in contract or in tort or otherwise) in connection with the user's access or usage of any of the information or content contained herein. The information and specifications contained in this document are subject to change without notice.

Revision History

Date	Rev.	Comments
May 2020	A	Initial document.

For the latest revision of this product document, please check our online documentation at www.lantronix.com/support/documentation.

Overview

This document describes Lantronix IoT device security best practices to protect against unauthorized access. Lantronix recommends using the guidelines below. These tips are not device-specific. Please see your device user guide for specific information on how to implement the suggestions.

Use a strong password

Change the factory default password, which could be called the Administrator, Telnet, or Web Manager password depending on the device. Use a strong password that is not easy to guess but is easy for you to remember. Include the following in your passwords:

- 8-12 characters
- Uppercase and lowercase letters
- Numbers
- At least one special character, such as @, #, ?, etc.

Disable unencrypted or unneeded protocols

Disable any protocols that don't have encryption if you don't use them. For example, Telnet, CLI Server, HTTP, and FTP should be disabled if available on your device and unneeded. Network discovery (UPnP and 77FE) protocols allow remote systems to discover or configure a device. Once device discovery is no longer needed, these protocols should be disabled as well.

Enable encryption and authentication

Enable encryption and authentication on protocols that support them, such as HTTPS. Use encryption for all Tunnel data, including SSH, SSL, and TCP AES. If the device has a wireless access point, enable WPA/WPA2 encryption.

Use signed firmware and scripts from authorized vendors

Keep your firmware up-to-date by installing the latest, digitally-signed firmware version to address any vulnerabilities. Only used scripts from authorized vendors on devices that support custom scripts. This feature is not available in all products.

Disable unused services

Disable any services that are not used, such as Bluetooth, BLE, or Wi-Fi.