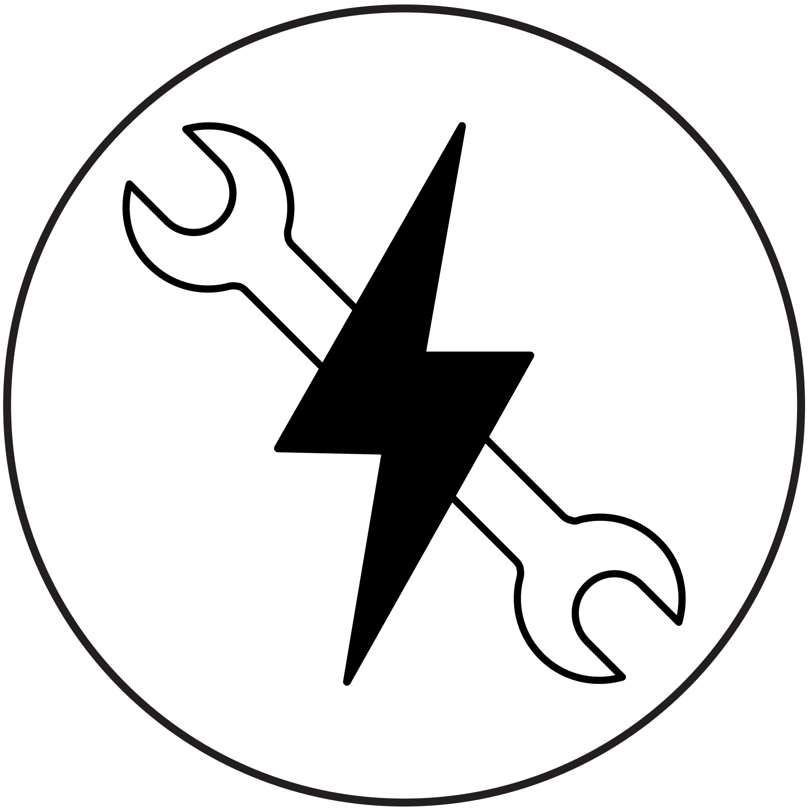
Configuration Guide

Pixii Home Cyber Security Information

Shaping the power of the future



Public

Document number: 16429, rev. 1.0
Author: Tomislav Fotak
Issue date: 14.10.2024

Table of Contents

Revision	Date	Comment
1.0	14.10.2024	Initial

1 Introduction

This document is intended for owners, aggregators, installers, and users of the Pixii Home systems and provides guidelines for securing your Pixii Home system when it is connected to the internet.
Battery Energy Storage System (BESS) units may be subject to various local regulations that govern their installation, operation, and maintenance, and this document does not replace such standards and requirements.

2 Threats and risks

Connecting an energy storage system to the internet can potentially introduce several risks, including:

- Cybersecurity threats: Internet-connected energy storage systems can be vulnerable to cyber-attacks that can compromise the security and safety of the system. For example, attackers can gain unauthorized access to the system, modify its settings, or even change the operation.
- Data breaches: Energy storage systems connected to the internet can also be vulnerable to data breaches, which can expose sensitive information about the system, its users, or the energy grid itself.
- Malware attacks: Internet-connected energy storage systems are at risk getting infected with malware, which can damage or disable the system, steal data, or use the system as part of a larger botnet.
- Remote control: An internet-connected energy storage system can potentially be controlled remotely, which could lead to malicious actions such as shutting down the system or causing it to discharge or charge when it was not intended to do so.
- Privacy risks: Energy storage systems connected to the internet may also collect data about their users, which could be used for nefarious purposes.

3 Mitigation

To mitigate the risks mentioned above, it is important to implement adequate cybersecurity measures, such as firewalls, encryption, and user authentication, as well as regular system updates.
The components in a typical installation are illustrated below. The separation between the Pixii system (left hand side) and the operator and owner systems (right hand side) is shown by the vertical line. The router is usually managed by the owner. Cloud-based systems such as orchestrations services are in the “Cloud”.

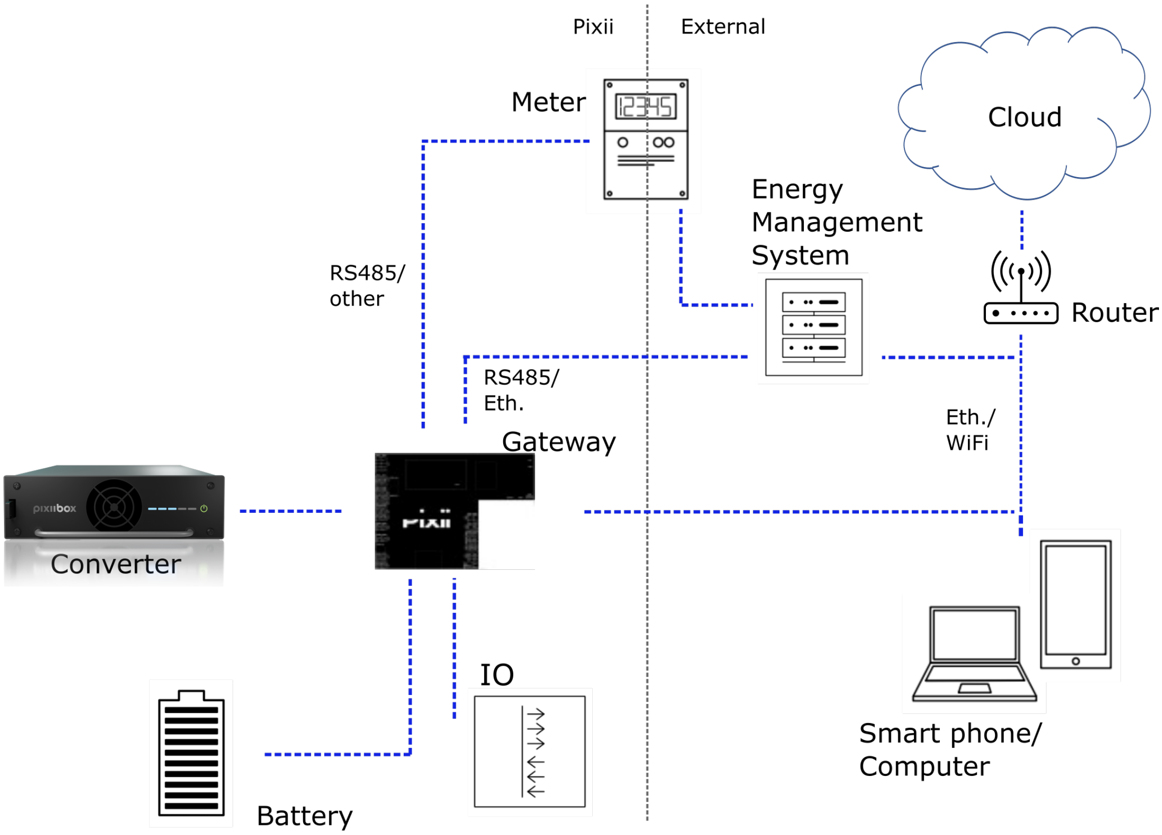


Figure 3.1 Components and connections in a Pixii Home system

3.1 Pixii PowerShaper settings

The Pixii PowerShaper has the following default settings from the factory to mitigate the factors listed in the chapter above:

- All incoming connection interfaces except the internal web servers are initially closed/disabled, and all power services are disabled.
- An internal firewall blocks all unused ports and services.
- The internal web server used for configuration only accepts HTTPS connections encrypted by TLS 1.2 or higher.
- All systems have unique passwords when delivered from the factory, which the user should change on commissioning.
- All connections (e.g., Modbus, Wi-Fi Access Point for local configuration, etc.) are disabled from factory, and the ones that will be used need to be actively enabled when configuring the system. The operator is responsible for closing these connections when not in use or required.
- The power services that will be used need to be enabled when configuring the system. The Pixii Gateway MQTT broker used on the local network only allows secure, encrypted connections and validation using keys/certificates unique to each Gateway.
- Only signed firmware/software update packages by Pixii are trusted for installation.
- All services used for connections with owner's/user's mobile application are protected from unauthorized incoming connections.
- All network traffic between Pixii Home unit and owner's/user's mobile application is additionally encrypted.
- There is no need to store any personally identifiable information to operate the system, unless the customer decides to use mobile application to connect to the Pixii Home.

3.2 Recommended actions for the operator/owner

Usually, the owner is responsible for the internet connection and local network, including the network equipment. The owner should set up the firewall on the router and monitor the network to ensure that the internet connection in and out of the system is secure, according to the applicable policies.

The owner can lock down as much as necessary. Any external (non-Pixii) cloud-based MQTT server for controlling the system (e.g. an orchestration platform) is operated by a third party, and they are responsible for determining the security features.

The Pixii Home software facilitates the use of the different common security options offered with the MQTT protocol.

The owner is responsible for restrictions regarding physical access to the system.

Below are some countermeasures and recommendations.

3.2.1 Securing the Internet router and local network resources

- Regularly check for firmware updates and install them promptly to keep the router up-to-date with the latest security patches and fixes.
- Change the default login credentials for the router and use strong, unique passwords. Avoid using common passwords or easily guessable phrases.
- Disable remote management of the router to prevent attackers from accessing the router's configuration settings from outside the network.
- Segregate the network into different subnets and assign separate VLANs for each user group to restrict access and prevent lateral movement in case of a breach.
- Configure firewalls on the router to block incoming traffic from suspicious IP addresses or to restrict traffic to specific ports and protocols that are not required. Do not use port forwarding.
- If remote access is required, enable VPN. Implement VPN connections to securely connect to the network from outside and prevent unauthorized access.
- Disable unnecessary services and features that are not required for the network's operation to reduce the attack surface.
- Monitor the network traffic and logs regularly to detect any anomalies or suspicious activities.
- Implement access controls to restrict access to sensitive data and resources only to authorized users and roles.
- Disable Wi-Fi if not required, e.g. if an owner/user does not want to use Pixii Home mobile application.

- If Wi-Fi access is required, use WPA3 or WPA2/3 encryption for Wi-Fi connections to prevent unauthorized access to the network. Avoid using WEP or WPA encryption methods as they are outdated and can be easily cracked.
  - » If owner/user wants to use mobile application to connect to Pixii Home and manage it, connect Pixii Home and mobile device running Pixii Home mobile application to the same subnet.

3.2.2 Securing mobile device

- Maintain physical control of a mobile device. Use original charging accessories or the ones from a trusted manufacturer. Avoid connecting mobile device to unknown removable media.
- Avoid jailbreaking or rooting a mobile device.
- Regularly check for operating system and mobile applications updates to keep up-to-date with latest security patches and fixes. It is advised to turn on automatic OS updates.
- Encrypt data on the mobile device if that option is available in the installed OS.
- Use strong passwords for accounts that are being used on mobile device, either as OS related account or account in some mobile application. Enable multi-factor authentication (MFA) where available.
- Lock a mobile device to an account that is being used on that device (e.g. enable ‘Find my iPhone’ in iOS). Newer versions of largest mobile operating systems do this by default.
- Keep mobile device locked and password/PIN/biometrics protected.
- Download applications and their updates only from trusted sources, such as official application stores.
- Avoid connecting mobile device to public or unprotected Wi-Fi networks, and connect only to trusted networks. Use a VPN to stay safe in situations where connection to unprotected network is required.
  - » Disable VPN only in cases when there is a connection to the same network as Pixii Home established and it is required to bind Pixii Home mobile application to a Pixii Home unit.
- Use password manager to store account passwords and to retrieve them when required by mobile applications.
- Grant only minimum set of required permissions to installed mobile applications. Do not grant a permission required by functionality that will not be actively used.

3.2.3 MQTT

MQTT (Message Queuing Telemetry Transport) is a lightweight messaging protocol often used in IoT applications for communicating with local and remote servers.
This chapter is intended mainly for aggregators working with Pixii Home system.
Below are some best practices for using MQTT securely:

- Use encryption to protect data in transit between the MQTT client and server. This can be achieved using Transport Layer Security (TLS) or Secure Sockets Layer (SSL) protocols.
- Use strong authentication mechanisms to prevent unauthorized access to the MQTT server. This can be done by using username/password authentication or client certificates.
- Use a secure connection between the MQTT client and server. This can be done using a Virtual Private Network (VPN), which provides an additional layer of security.
- Implement access controls on the MQTT server to restrict access to only authorized users and devices.
- Keep MQTT software and firmware updated to patch known vulnerabilities and improve security.
- Monitor MQTT communication for any unusual activity, such as unauthorized access or data tampering. This can be done using intrusion detection and prevention systems, or by analyzing MQTT communication logs.

4 Further information

Here are some online resources related to securing internet-connected energy storage systems:

- The National Institute of Standards and Technology (NIST) provides guidelines for securing internet-connected devices, including energy storage systems. Their website is https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/securing-data-devices-1
- The International Electrotechnical Commission (IEC) provides standards for cybersecurity in information technology (IT) and operational technology (OT) environments. See information for the standards and guidelines that are relevant for securing energy systems on https://www.iec.ch/cyber-security
- The Department of Energy (DOE) provides resources for securing energy systems, including cybersecurity guidelines and best practices. See https://www.energy.gov/cybersecurity
- Wikipedia has a long article covering many of the aspects of Computer security: https://en.wikipedia.org/wiki/Computer_security
- UC Berkley lists 10 secure computing tips: https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips
- The NSA has repository of advisories, info sheets, tech reports, and operational risk notices at https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/

Pixii