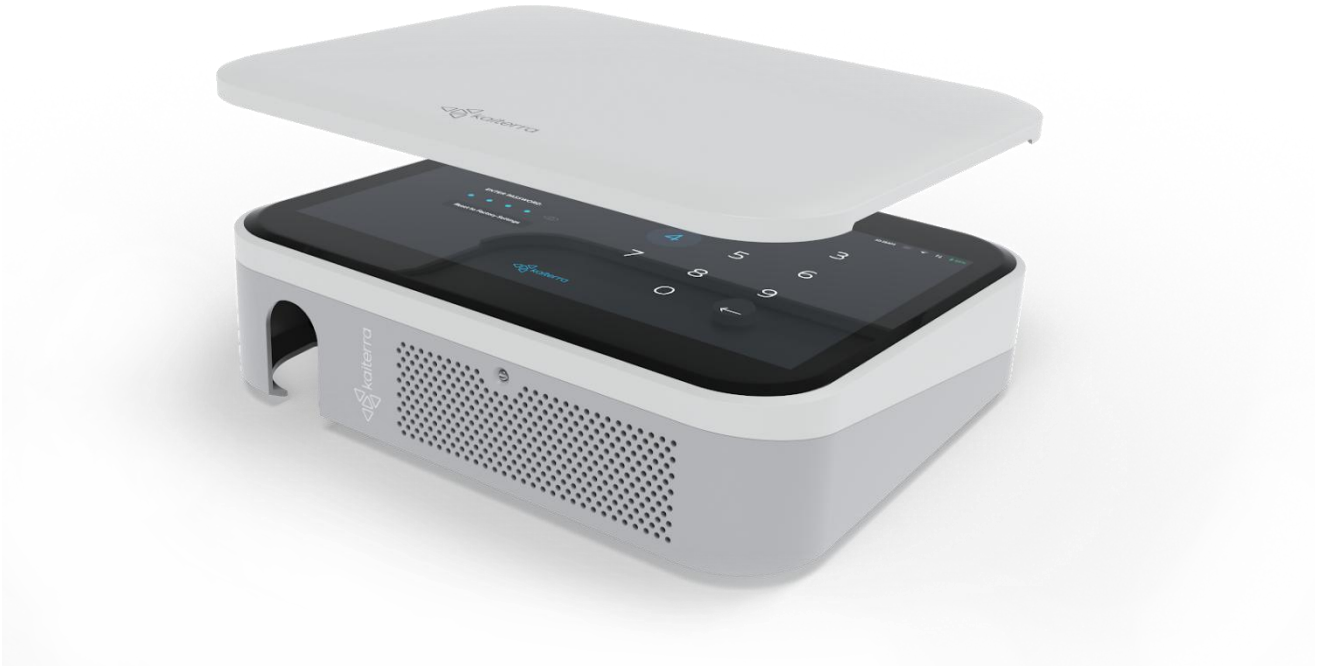

Kaiterra Sensedge OS Hardening Checklist

OCTOBER 2021

1.

Introduction

Hardening of the device through the following checklist is done to minimize exposure to threats and to mitigate possible risk.

Please complete each step of the checklist below.

Administrators may use the left-most column to mark each step when complete.

2.

How to use this checklist

Print the checklist and check off each item you complete to ensure that you cover the steps for securing your device.

3.

Device Details

Serial number *(Settings → Device Details)*	
Wi-Fi MAC address *(Settings → Wi-Fi)*	
Ethernet MAC address *(Settings → Ethernet)*	
Asset tag	
Administrator name	
Date	

4.

Checklist

Step (✔)	Actions
1. Disable Modbus *(Skip this step if you choose to use this method of communication)*	
	Navigate to the Settings menu Navigate to the Device Details tab Select “Connectivity” Select “Modbus” Ensure that Modbus is disabled
2. Disable BACnet *(Skip this step if you choose to use this method of communication)*	
	Navigate to the Settings menu Navigate to the Device Details tab Select “Connectivity” Select “BACnet” Ensure that BACnet is disabled
3. Disable Secondary MQTT *(Skip this step if you choose to use this method of communication)*	
	Navigate to the Settings menu Navigate to the Device Details tab Select “Connectivity” Select “MQTT” Ensure that the “MQTT Uri” field is blank
4. Disable Wi-Fi *(Skip this step if you choose to use this method of communication)*	
	Navigate to the Settings menu Navigate to the Wi-Fi tab Ensure that the Wi-Fi toggle is disabled

5. Enable PIN code	
	Navigate to the Settings menu Navigate to the General tab Select PIN code On the PIN code page, enable the PIN code a choose a 4-digit code On the PIN code selection choose “Always” *If the PIN code is forgotten, the device must be factory reset, and all historical data will be deleted. The device can only be factory reset if the serial number is input - ensure this number is kept safe.*
6. Enable Event Logging	
	This step should be followed if Syslog is used for event logging. Navigate to the Settings menu Navigate to the Device Details tab Select “Connectivity” Select “Syslog” Turn on the “Enabled” toggle Enter the correct details for your Syslog server Press the “Test” button to verify that the Syslog server receives the test log
7. Enable Auto Updates	
	This step may depend on internal policies for updates and patches. Enabling auto update will make the device automatically download and install patches and updates to the software, as they become available to the device. Navigate to the Settings menu Navigate to the General tab Enable “auto update”