Klipspringer

Compliance with confidence

WATCHMANONE
SECURITY OVERVIEW

💻 www.klipspringer.com ✉ sales@klipspringer.com ☎ 01473 461800

Preface

This document aims to provide guidance on the D3 systems security status as a wireless system.

Table of Contents

Paper copies are valid only on the day they are printed. Contact the author if you are in any doubt about the accuracy of this document.

Klipspringer Limited, Foxtail House, Foxtail Road, Ransomes Europark, Ipswich IP3 9RX

www.klipspringer.com

Disclaimer: *The information provided in this document is provided "as is" without warranty of any kind. Klipspringer disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Klipspringer be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Klipspringer or its suppliers have been advised of the possibility of such damages.*

Document Lifetime

Klipspringer may occasionally update online documentation between releases of the related software. Consequently, if this document was not received recently, it may not contain the most up-to-date information. Please contact Klipspringer for the most current information.

Where to get help

Klipspringer support, product, and licensing information can be obtained as follows.

Product information - For documentation, release notes, software updates, or for information about Klipspringer products, licensing, and service, go to the Klipspringer website at: www.klipspringer.com

Technical support - For technical support email sales@klipspringer.com. Note that to open a service request, you must have a valid support agreement.

Your comments - Your suggestions will help us continue to improve the accuracy, organisation, and overall quality of the user publications. Please send your opinion of this document to: sales@klipspringer.com

If you have issues, comments, or questions about specific information or procedures, please include the title and, if available, the part number, the revision, the page numbers, and any other details that will help us locate the subject that you are addressing.

Revision History

This document has been revised by:

Revision Number	Revision Date	Summary of Changes	Author
v1	03/02/2022	Initial	J Dyer
v2	04/10/2022	Updated with MDP	J Dyer
v3	11/09/2023	MDP information updated	J Dyer

1. WM1 868Mhz System Overview

The WM1 family of monitoring systems comprise of a base station that communicates with paired wireless transmitters using a wireless protocol.

Each minute, the wireless transmitter wakes and takes a reading from the attached sensor, it then sends this data reading to the base station.

The base station is designed to be networked to provide email and audible alarm notifications in case of readings outside of the set parameters.

The base station front end is a standalone embedded system that connects directly to your business network with no need for any dedicated PC, server or specialised software installation. Data from the base station can be viewed directly via a standard web browser. The browser interface provides access to real time data, alarm notifications, full audit trails, analytical graphing tools and a report generator.

Base Station

Wireless Transmitter

2. System Security

The WM1 base station operates using bespoke embedded software that is permanently programmed into its flash memory. It does not use a conventional operating system such as Microsoft Windows or Linux. Instead, it runs on a minimal file system designed solely for recording sensor data. The D3 has no facility to download and run external code other than its own bespoke software.

The Rf transmitters communicate with the base station using a Su-1 Ghz bespoke embedded wireless protocol based on IEEE 802.15.4 MAC.

Data transferred between the sensor and the base station has 128-bit encryption. Data is sent in bespoke digital data packets that contain no identifiable system information.

The data sent wirelessly is hard coded and limited to very small packets of data containing sensor information. The wireless protocols contain no infrastructure to transmit anything other than our own sensor data.

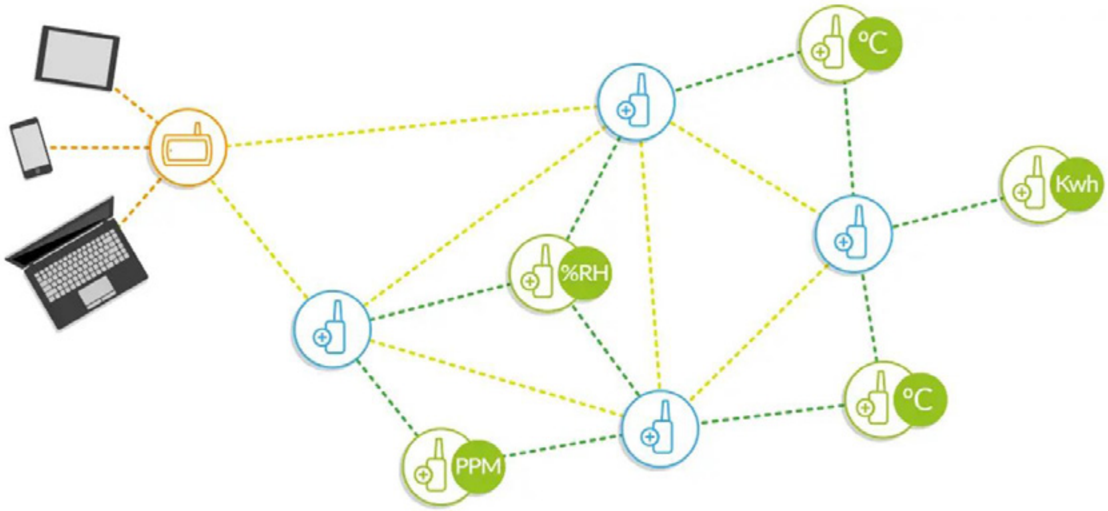
3. Wireless Network

3.1. Overview

The WM1 monitoring system uses a low power sensor network in order to read and transmit sensor data from remote locations to the WM1 base station for processing. The sensor network comprises of three distinct parts;

- ✓ Wireless Sensor transmitter
- ✓ Router
- ✓ Coordinator

The diagram below shows a typical network topology.



3.1.1. Coordinator – within base station (orange)

The coordinator is located physically within the base station and is used to offload all the network processing. The coordinator is the network manager and controls the network. The sensor data is sent to the coordinator and passed to the WM1 for processing.

3.1.2. Router/Repeaters (blue)

Routers are used to strengthen the network and forward messages from the wireless transmitters when they are not within radio distance of the base station. Routers are mains powered and can route the message between other routers – adapting to the local environment to find the best path back to the base station.

3.1.3. Wireless transmitter/sensor (green)

The wireless transmitters send the reading securely to the base station every minute. If they are not within distance of the base station, they can route the message though any local router.

4. My data portal (MDP)

MDP is disabled as default and must be activated on the base station by an administrator level user.

MDP is an option available on all WM1 systems **but is not required to be used** for the D3 system to operate or be accessed on a local network directly.

This option tends to be used where external access to the information is required and a secure connection is required to grant this access.

In a typical installation, the WM1 monitoring system will sit on the customer's local area network. A drawback of this is the user cannot access the unit remotely (outside of their network) without setting up either port forwarding or VPN's.

The primary requirement of My Data Portal (MDP) is to provide secure access to the monitoring system outside of their local network.

Its operation is very simple. It is a cloud application that acts as a reverse proxy to the back-end monitoring systems. The reverse proxy is an intermediate server (go-between) between the client's browser and WM1 monitoring system.

In normal operation the WM1 will initiate a secure persistent connection to MDP on Port443. Once connected and authenticated it switches the connection to a listening socket. The WM1 will then listen and respond to requests from MDP.

Each WM1 connected to MDP has a site ID/Key. MDP uses this site ID/Key to redirect the browser requests to the base station.

When the client's browser makes a secure connection to MDP, MDP displays a user login page.

For direct access only - after completing the user name, password and site id fields, the hash of this information is posted to the base station, the base station compares the hash sent against its own stored hash to enable access. No user names and passwords are stored on MDP.

For account access – a user account is created and the user generates a unique MDP username and password, this is hashed and stored on the MDP server, when a user logs in to the server the generated login hash is compared to the stored hash to enable access, the username and password are not stored on the MDP server.

Each base station creates a unique site key used for access by MDP. The site key can only be used for access over MDP. The site key is AES 128 encrypted. This site key is stored on MDP in its encrypted state. The site key is only sent once to authenticate after which a token system is used.

MDP essentially redirects TCP packets at a very low level to the base station. In addition, MDP server software only implements GET and POST commands.

5. Conclusion

The WM1 base station and attached wireless sensors are designed as a bespoke system for monitoring remote sensors. This inherently removes the risk of the system being “hacked” as there is simply no infrastructure for manipulating its core function.

Neither the base station nor the wireless transmitters contain any infrastructure that allows a third party to add code or use the system to access a connected network.

There is no capability to write third party code or applications to the base station, to add viruses, or access a connected network, in this regard the base station is more secure than a PC or PC driven device on the same network.