

# Security Ranger

## Installation Guide



## Federal Communications Commission (FCC) / IC Canada Compliance Statement

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. However, there is no guarantee that interference will not occur in any given installation. If this equipment does cause interference which can be determined by turning the equipment on and off, the interference may be reduced by:

- Increasing the separation between the equipment and the receiver
- Reorient or relocating the equipment antenna.

Only the recommended antennas listed in Appendix A should be used with this equipment and the output power should be set depending on the cable length in accordance with the PervasID Power tool. (see section on antenna connection)

This equipment complies with FCC/IC radiation exposure limits set forth for an uncontrolled environment and meets the FCC radio frequency (RF) Exposure Guidelines in Supplement C to OET65 and RSS-102 of the IC radio frequency (RF) Exposure rules. This equipment should be installed and operated so that the antennas are kept at least 40cm or more away from a person's body (excluding extremities: hands, wrists, feet and ankles).

## ETSI Compliance

The SRM 9380 (Master) and SRS 9380 (Slave) Readers make up the Security Ranger product (the Security Ranger) and have been certified to IEC 62368-1/EN 62368-1 and EN 301 489-1/EN 301 489-3.

**Warning:** Please read this manual in its entirety before operating the Readers, as personal injury or equipment damage may result from improper use. Under no circumstances should the Reader enclosures be opened.

**Caution:** An appropriate power supply unit (PSU) that meets the RFID DAS 9380 Reader PSU Specification must be used to power each Reader. Any other PSU could be dangerous and failure to ensure this could make the product unsafe.

**Caution:** Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

## Check List

The PervasID Security Ranger consists of two 8-port UHF DAS RFID Readers, an SRM 9380 (Master) and an SRS 9380 (Slave), each capable of feeding eight antennas. The Master allows tag information to be uploaded over its Ethernet interface to a server for processing, analysis and display. The real-time information of assets is thereby logged. The Security Ranger System consists of:

1. A PervasID SRM 9380 Reader with internet access
2. A PervasID SRS 9380 Reader with internet access
3. 2x +24 VDC external power supplies with AC cord
4. 16x Coaxial cables
5. 16x UHF RFID antennas
6. Brackets
7. Shielded Cat 5 Cable
8. Installation Manual

# Table of Contents

## Contents

List of Acronyms.....	5
1 Introduction .....	6
1.1 SECURITY RANGER .....	6
1.2 Requirements for Using SECURITY RANGER .....	6
2 Installing the SECURITY RANGER System .....	8
2.1 Installing and Connecting the Security Ranger .....	9
2.2 Compliance with ETSI Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields .....	12
3 Troubleshooting .....	13
References .....	14
Appendix .....	15

## List of Acronyms

CRC	Cyclic Redundancy Check
DAS	Distributed Antennas System
EIRP	Effective Isotropically Radiated Power
EPC	Electronic Product Code
ERP	Effective Radiated Power
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
ISO	International Organisation for Standardisation
RF	Radio Frequency
RFID	Radio Frequency Identification
RSSI	Received Signal Strength
Rx	Receiver
Tx	Transmitter
UHF	Ultra High Frequency

# 1 Introduction

This manual provides detailed instructions for installing, connecting, configuring and operating the Security Ranger.

The intended audience for this manual is the operator installing and operating the Security Ranger. It is presumed that the operator has a good knowledge of RF propagation, exposure limits, radio interference, RFID, the EPC Gen2 spec, software, hardware systems integration and network connectivity.

## 1.1 Security Ranger

The Security Ranger is a fixed UHF RFID Reader and allows sensitive detection of RFID tags, including rapid identification of tags on the “outside” of a portal.

The Security Ranger system consists of a centralised Master Reader unit and a Slave Reader, both connected to antennas using coax cables. The antennas on the outside of the portal should be connected to the Master Reader and the antennas on the inside of the portal should be connected to the Slave unit. Antennas should typically not be separated by more than that detailed in the design specification supplied by PervasID.

The Security Ranger units are equipped with an Ethernet interface allowing tag information to be uploaded to a server for processing, analysis and display.

## 1.2 Requirements for using Security Ranger

### IT Interface Requirements

TCP/IP network equipment is required to connect to the Readers. The PervasID server is on IP address 192.168.2.20 and requires port 9998 to be open. NTP is also required for the Reader internal clock.

### Power Requirements

An external universal AC to DC power supply, a suitable +24VDC amp power supply is provided with each Reader. This must be fed by an AC single phase supply of 100-240V.

### Antenna Requirements

The Security Ranger is equipped with sixteen independent TX/RX antenna ports.

Operators must use the recommended antennas by PervasID and further details can be found on page 18. The transmit power must be adjusted according to the cable length and antenna gain to ensure 2W ERP limit (ETSI) and 4W ERP limit (FCC).

It is the installers responsibility to ensure that the combination of the configured reader output power, cables losses and antenna gain used do not exceed local regulations. PervasID provide a spreadsheet tool to help calculate the power settings of the reader which should be used to achieve the maximum allowed output power for various antenna and cable combinations. If you require a copy of this document please email [techsupport@pervasid.com](mailto:techsupport@pervasid.com)

All sixteen antenna ports may be used in order to maximise the coverage area. However, should the operators wish to operate with fewer antennas, then the unused ports MUST be terminated with a 50 ohms load (terminator) or damage to the unit will result.

## 2 Installing the Security Ranger System

The following figures (Figures 2 and 3) illustrate the I/O ports, including antenna ports, located on the Security Ranger. Antenna ports and LED status indicators are located on the front panel of the Reader, Ethernet and USB interfaces are located on the back panel of the Reader. An illuminated Green light on **Power** indicates that the Reader is on. An illuminated Green LED light on any RF port (ie. RF 1 – RF 8) means that that port is active. An illuminated Green light on **Read** implies that the Reader is successfully detecting tags whilst an illuminated Green light on **CRC** implies that there is a CRC error over a tag read.

Under normal operation, the LEDs of the active ports will flicker indicating activity on the ports and the read LED will flicker as tags are read while the reader is reading.

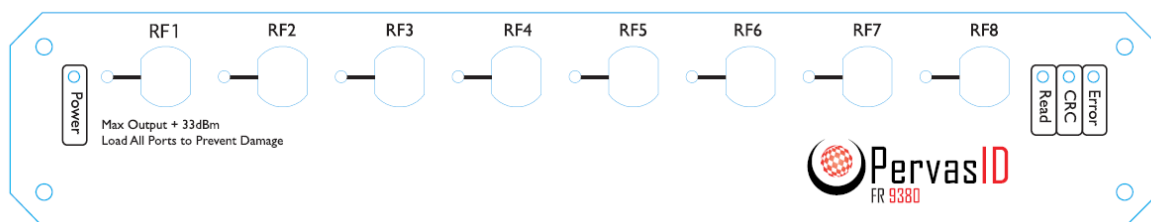


Figure 2: DAS RFID Antenna Ports and Status LEDs

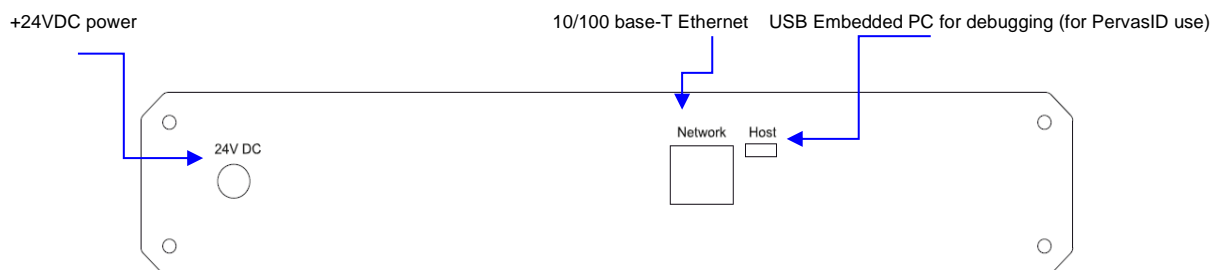


Figure 3: FR Port Connections

The USB Embedded PC interface labelled **Host** on Figure 3 gives access to the embedded WinCE PC and may be used to configure the reader IP address. Please contact PervasID should you require access to this interface.

**Warning: Do not run a Reader with the micro USB cable connected to a laptop**



## 2.1 Installing and Connecting the Security Ranger

The primary installation and connection steps for the Security Ranger system are:

### 1. Position the Reader appropriately and mount the Readers in a stable location

Choose an appropriate location for the Readers with the feet down. You should always keep the units away from extreme temperatures and sources of electromagnetic interference as this may degrade performance and lifetime of the Readers.

**Caution** It should be noted that heat is generated when the Readers are actively running, and care should be taken to ensure appropriate ventilation. Other instruments or items should not be placed on top of the Readers (please install feet down).

**Caution** This equipment is not suitable for use in locations where children are likely to be present.

### 2. Connect the antennas to the RF ports on the Readers

Each RF port should be connected to a recommended RFID antenna or ceiling tile port.

**Warning:** The Readers will be seriously damaged if any of the ports are not connected to an antenna or terminated with a 50-ohm load before operating it.

The following steps need to be taken in order to install the antennas reliably:

- 1) Select the antenna locations. The recommended antenna arrangement is detailed in the design specification supplied by PervasID. The antennas should also be positioned:
  - Away from metallic objects which appear in their field of view,
  - Away from sources of interference (such as compact florescent lights)
  - With a separation between antennas greater than 0.25m.
  - Away from locations where persons are likely be within 40cm of the radiating face of the antenna for periods exceeding 6 minutes.
- 2) The antennas should be securely mounted in accordance to local Health and Safety Regulatory Compliance and with the instructions supplied with the antenna brackets.

- 3) Attach the antenna cables to the antenna ports on the Readers as detailed in the design specification supplied by PervasID. The cable connectors should be as tight as can comfortably be achieved by hand, but under no circumstances should tools be used to tighten. A note should be made of the cable type and length connected to each antenna port.

### **3. Connect the Master Reader to the Slave Reader**

You should connect the Master Reader to the Slave Reader using the sync cable provided. The sync connections ports are located on the rear panel of each Reader.

### **4. Connect power to the Readers**

You should connect the 24VDC external universal power supplies into a suitable power outlet.

Once you have successfully connected, the Power and Status LEDs on the Readers should indicate that the Readers are on. The connection and activity LEDs on the Ethernet should indicate a network connection.

### **5. Connect the Readers to the network**

You are now ready to connect the installed Security Ranger to your network.

You should connect the Readers directly to your Ethernet network using a shielded cable. Once the Readers are powered, they will communicate with a hosted server.

Make sure that there is no firewall in place which might prevent the Readers communicating with the server. You must be able to communicate with the server (192.168.2.20) over the assigned port (default port 9998) and NTP on port 123. The reader is configured by default to DHCP but can subsequently be given a static address.

### **6. Connecting to the Ranger GUI**

Follow the instructions provided for the installation and connection of the Ranger Server and GUI. When the Readers are correctly connected they will appear in the Ranger GUI display.

### **7. Selecting and configuring the setting on the Readers**

The output power of each port should be configured according to the desired output power, cable length and antenna in-use. The PervasID cable calculator spreadsheet tool can be used to determine the power setting which should be used. Other settings

as required by your application can also be configured. This can be obtained by contacting [techsupport@pervasid.com](mailto:techsupport@pervasid.com) .

Reader settings are configured through the Ranger GUI once connection has been confirmed. A suitable settings file will be supplied by PervasID for your application. All the Readers which have been connected to your installation (including those previously connected) will be displayed.

## **8. Test the Reader installation by reading tags**

You can confirm that connections and functionality are correct by reading tags. Using the Ranger GUI software interface, you can quickly verify Reader operation by running an inventory operation.

## 2.2 Compliance with ETSI Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields

European Council Recommendation 1999/519/EC details basic restrictions and reference levels on human exposure to electromagnetic fields as advised by the ICNIRP and states that adherence to these recommended restrictions and reference levels should provide a high level of protection as regards the established health effects that may result from exposure to such fields.

By the very nature of the Security Ranger system design and installation for correct operation, users should not find themselves within close proximity of the antennas. EN 62311:2008 is the applicable Harmonised Standard for EM fields generated by this Security Ranger system and all installations comply with this standard and the recommendations, and are safe when antennas are installed such that:

**(a) A minimum antenna separation of 0.25m is maintained**

**and**

**(b) An individual can be no nearer than 40cm from an antenna for a period of 6 minutes at any one time.**

These guidelines are based on the Maximum Permissible Exposure (MPE) Calculation Report generated by UL. Please get in touch with [techsupport@pervasid.com](mailto:techsupport@pervasid.com) should you wish you see the report.

**Warning:** We strongly recommend that users must follow above guidelines. Under no circumstances should the Security Ranger be installed and operated outside these specifications.

### 3 Troubleshooting

If you experience a problem with Security Ranger, this brief section presents a few suggestions to correct the issue.

Error	Cause	Resolution
No illuminated Green LED light is observed	Power is not supplied to the Reader	Check the power connection to the Reader
Power LED is on but no other LED lights are on during an inventory operation	The reader is not correctly configured.	Check the reader parameters.
No Ethernet Connection	The Network settings are incorrect/ firewalled out	Check the ip/port/dhcp network setting via CERHOST, Check lights on the Readers Ethernet Socket- Check with the Network Administrator.

If you are still unable to determine the cause, you may want to contact PervasID directly. Please send an e-mail to [techsupport@pervasid.com](mailto:techsupport@pervasid.com) in the first instance.

## References

- [1] Specification for RFID Air Interface,  
[https://www.gs1.org/sites/default/files/docs/epc/uhfc1g2\\_1\\_0\\_9-standard-20050126.pdf](https://www.gs1.org/sites/default/files/docs/epc/uhfc1g2_1_0_9-standard-20050126.pdf)
- [2] [https://www.gs1.org/docs/epc/uhf\\_regulations.pdf](https://www.gs1.org/docs/epc/uhf_regulations.pdf)
- [3] Safely Technical Justification Document for Electromagnetic Fields generated by PervasID “FR 9000”, Maximum Permissible Exposure (MPE) Calculation Report, Sulis Consultants Limited, April 2013.

## Appendix

### Recommended Antennas

- Callidus RFID 240x240 panel antenna
  - EU (ETSI) version, LHCP, white: 18-361.TE UW
  - EU (ETSI) version, LHCP, black: 18-361.TE UB
  - US (FCC) version, LHCP, white: 18-361.TU SW
  - US (FCC) version, LHCP, black: 18-361.TU SB