

Connected Devices Knowledge Base

RFID Tag Performance

version 22, August 2024

Introduction	3
RFID Chip	4
RFID antenna.....	5
Use case	7
Production quality and verification	8
Tag measurement Nedap Retail.....	9

Introduction

When deploying RFID at a retailer, the performance of the used RFID tag is extremely important. If the performance is not adequate for the application it is used for, the project will not be a success.

The performance of the RFID tag is determined by four main factors:

1. RFID chip
2. RFID antenna
3. Use case
4. The production quality and verification

Together this will determine the two most important performance indicators:

- **Turn on power** (also called sensitivity): the amount of power that is needed to turn on the chip, received from the reader. The less power a chip needs to go on, the better it is (the longer reading distance you get).
- **Backscatter power**: the amount of power that is returned from the chip to the reader. The more power a chip returns, the better it is (the longer reading distance you get).

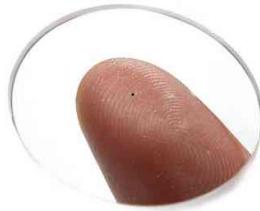
(i) In most setups the turn-on power is the main variable to determine the reading distance, as most readers are extremely sensitive.

(i) Most vendors specify above variables in their product sheet.

RFID Chip

The RFID chip is the component where the data is stored and that handles all the communication with the reader. It can be seen as a miniature computer, without any power supply: it is powered by the reader, over the air ('passive tag').

There are various vendors of RFID tag chips, all have their advantages and disadvantages.



RFID antenna

While the turn on power and backscatter power of the chip are important, they are not the only defining factor. A chip always comes with an antenna on the tag which determines the final turn on power and the back scatter power of the RFID tag.

The turn on power and backscatter power depend on the **frequency** the reader operates on. This means that for each region, a different turn on power and backscatter power are relevant. This is important for customers that operate around the globe. Not only the store locations are relevant, also the logistic hubs and production facilities should be taken into account here.

The vendors of the RFID tag are typically not the same as the vendors of the RFID chips. There are also many more vendors of tags, than there are of chips.

- ⓘ There is a strong trade-off between having an extremely good performance in one region, and a less good performance in other regions - and having average performance over all regions. The choice in this trade-off differs from vendor to vendor. Some make high-performance tags that only operate well in region 1, while others choose to make tags that work well in all regions, albeit with a bit lower performance.

- ⓘ In general the rule can be followed that the larger the antenna is, the better the turn on power and backscatter power are. However, this is no guarantee.

- ⓘ The design of the antenna also influences how well the RFID tag works in all orientations, and how well they work if there are a lot of RFID tags close together.



Use case

It is not said that a tag with low performance is unusable. Sometimes you just need a very small tag to do cycle counts on jewelry (and typically, smaller tags give lower performances). But, if you want to use this low-performing tag also for Electronic Article Surveillance (EAS) applications, it might not be a good fit.

Because the required performance depends so much on the use case, we always advise to test this, before deploying a solution.

An antenna is always designed to operate in a certain environment. This means that if the environment changes, the performance of the antenna might change as well. That's why we at Nedap Retail do not only look at the performance in free-space (the tag in open air), but also when the tag is applied to its final application. E.g. a paper swing ticket in between jeans, or on plastic packaging, or other use cases.



Manufacturers design the antennas for applications on specific products. It also means that when those tags are tested in free space environments they test less good than other tags, but in practice might work a lot better.

Production quality and verification

Making one tag that shows good performance is one thing, but making millions is another thing. Not only the performance should be good, it should also be consistent over a large batch. This is necessary to have predictable system performance down the chain.

The best suppliers not only have good production quality, but also strict quality control. They produce tags with turn-on power variations in the order of 1dB, which is pretty good.

Tag measurement Nedap Retail

At Nedap Retail we have the equipment to measure the turn-on power and backscatter power of RFID tags. We can advise on which tags to use in which applications. So, please contact us if you need any help

At Nedap Retail we always test more than one RFID tag, and preferably a larger batch to measure those variations.

So, in general, the performance of an RFID tag can be expressed in the following table:

Region	Turn On Power	Backscatter Power
Region 1
Region 2 and 3

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 22

Document Last modification date 21 August 2024

Document PDF Exported 2 October 2024 by Nedap Retail | Operations



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com



Connected Devices Knowledge Base

RFID GTIN Explained

version 42, February 2024

Introduction	3
GTIN.....	4
Contents of the GTIN	4
Serial number	5
Converting GTIN and serial to SGTIN	6
Examples.....	8
Encoding an SGTIN in a barcode	12

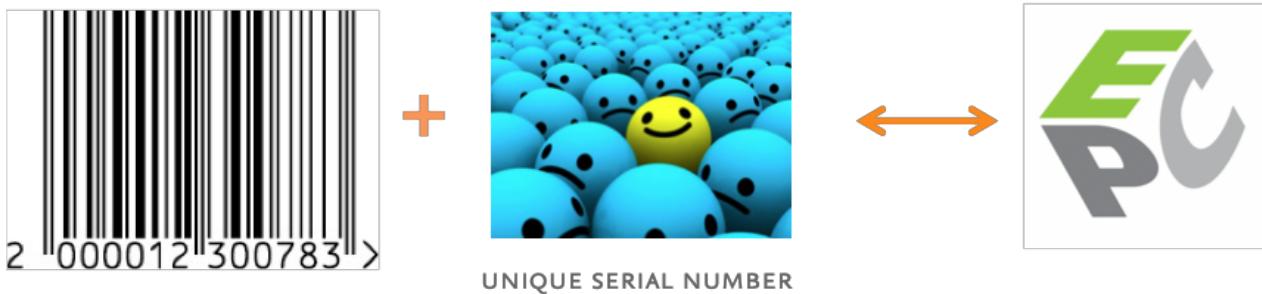
Introduction

When you put an EPC code in an RFID label to identify a unique product for retail operations, you have to use a SGTIN code. SGTIN stands for **S**erialized **G**lobal **T**rade **I**dentification **N**umber, and is part of the GS1 EPC global standards (<https://www.gs1.org/>). It is an evolution of the GTIN (Global Trade Identification Number), better known as the EAN or UPC code - familiar to most used barcodes in retail.



See also <https://www.gs1uk.org/standards-services/standards/standards-that-identify>

This application note details how to encode SGTINs from a barcode and decode to barcode plus serial number. This is handled by the iD Cloud app, but as the encoding can also be done in other process steps, it is good to have a better understanding on how this process works.



Generating an EPC from a GTIN (UPC or EAN) with a unique serial number

GTIN

The GTIN in an EPC is basically formed by taking either the EAN code (8 or 13 digits), or the UPC code (12 digits), and padding zeros in front until it reaches 14 digits.

Barcode	Example	GTIN
EAN8	87001235	00000087001235
EAN13	8701231234562	08701231234562
UPC	870123123456	00870123123456

There are very few rare exceptions to this, but those are omitted here. For more details please consult <http://www.gtin.info>.

Contents of the GTIN

A GTIN consists of three parts:

- Company prefix. Identifies the company that manufacturers the product, for example Nike.
- Item reference. Identifies the product, for example Air Max 2.
- Check digit. To make sure that the barcode is read correctly, a check digit is in place.

We take the GTIN **02000123007830** as an example (originating from EAN-13 code 200012300783):

0200012	300783	0
<company_prefix> <item_reference> <check_digit>		

The company prefix and item reference add up to length 12 but the length of each may vary. Typically, the company prefix is length 7 (may stretch to length 10), the item reference is length 5 (may shorten to length 2). GS1 licenses company prefixes which are guaranteed unique. The check digit is calculated following the GS1 EAN13 standard: http://www.gs1.org/barcodes/support/check_digit_calculator.



Based on the GTIN you can also find the related company details here: <https://gepir.gs1.org/index.php/search-by-gtin>

Serial number

The serial number should be unique for each GTIN that it belongs to. This is necessary to make sure that each product is identified uniquely, so duplicates should never exist.

- Self serialization (also called Multi-vendor Chip Serialization (MCS), preferred solution). This approach produces a serial number using a unique number put in place during chip production (stored in the TID memory of the chip).
- Iterating a serial number (increasing it every time you see a new item for this GTIN). This means that a central database needs to be maintained somewhere to ensure uniqueness of the serial number. This will typically only be used when a system integrator or single label supplier is involved in the RFID project.
- Random serial numbers. This approach generates a large random number which will minimize the risk of a serial number being generated twice for the same barcode. There is room for 38 bits, which means that there is a 1 in 2^{38} (1 in 274.877.906.944) chance of having a double serial number. This is good enough in most cases for closed-loop applications for small retailers, as the chance to win a lottery is much, much bigger.

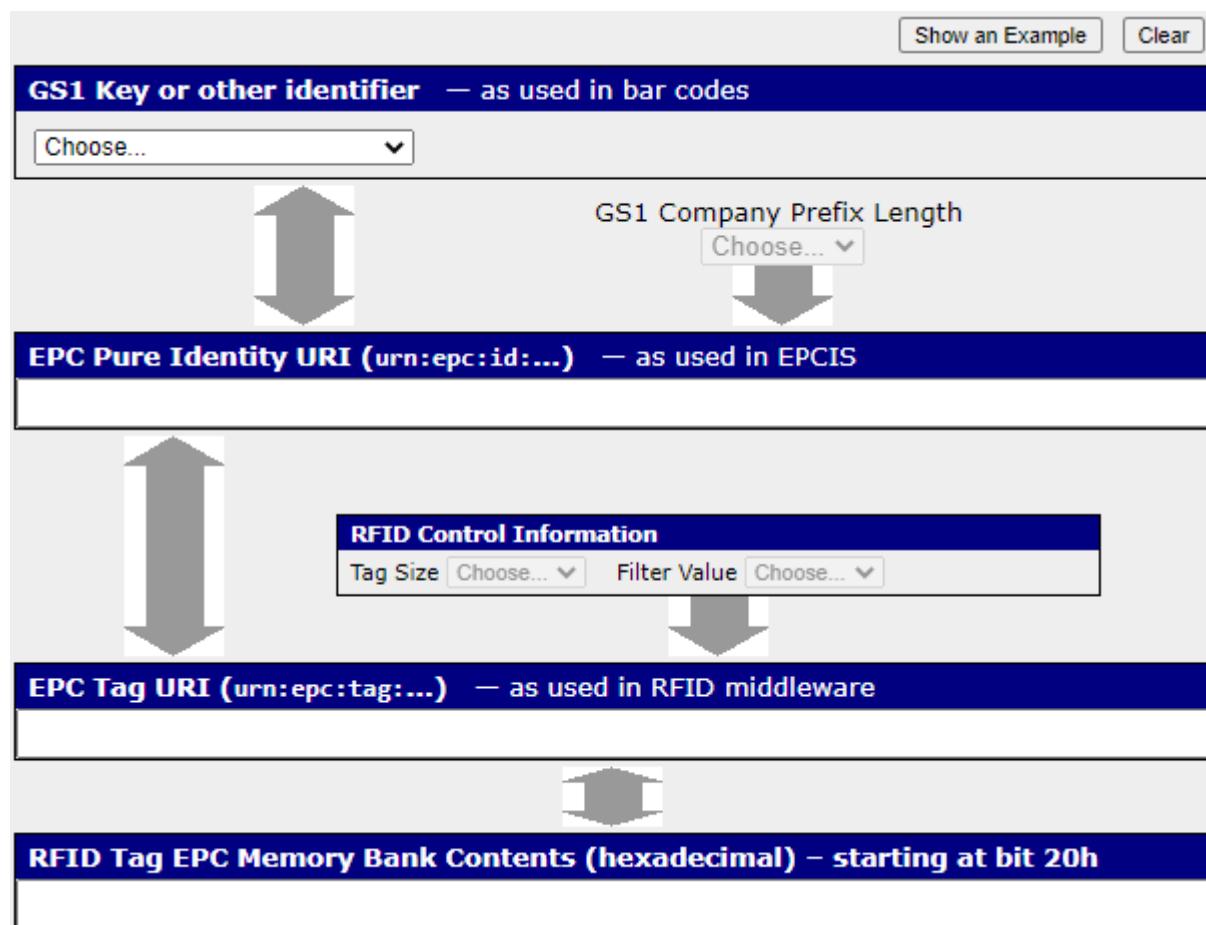
Converting GTIN and serial to SGTIN

When taking GTIN **02000123007830** and serial number **123456789012**, we generate an SGTIN **urn:epc:id:sgtin:2000012.030078.123456789012** with the EPC standard. See below an example using an online converter. There are many software libraries available to do this conversion and most label printing programs support this out of the box. The GS1 Tag Data Translation (TDT) standard describes how to represent the SGTIN as such a hexadecimal value. It is beyond the scope of this application note to explain the workings of TDT.

To convert the GTIN and serial number into an EPC code, you need to have the following additional information:

- GS1 Company Prefix Length: can be determined by knowing the company prefix.
- Tag size: this is typically 96 bits.
- Filter value: this should be set to 1: POS Item, as this is an item created for sale. Other options are: case, outer item, inner item, etc. - but those are not often used.

The result that is written to the RFID label (EPC memory) is 30347A13EC00C3DCBE991A14 in hexadecimal code. This identifies the fact that it is a SGTIN, the GTIN, serial number, etc.





GS1s online data translation tool: <https://www.gs1.org/services/epc-encoderdecoder>

Examples

So, to take this all into account, we are going to provide an example set-up. Let's say we have a retailer that sells four products:

- Shirt Blue, size M
- Shirt Blue, size L
- Shirt Red, size M
- Shirt Red, size L

As the retailer properly uses the GS1 EAN standard, those products will have the following EAN codes as example:

Name	Size	Picture	EAN
Shirt Blue	M		2000000000015
Shirt Blue	L		2000000000022
Shirt Red	M		2000000000039
Shirt Red	L		2000000000046

(i) The last character of the EAN is the check digit. The check digit doesn't contain any additional information and is calculated based on the other digits.

⚠ If the retailer uses the same EAN or UPC codes for physically different products, they are not following the standard, and might face challenges in migrating to RFID. Please contact support for more information.

These EANs cannot directly be used in an RFID set-up: we need to translate them to GTINs. We do this by adding a zero in front of the EAN.



If the retailer uses UPCs, those are 12 digits and 2 zeros need to be added to them.

Name	Size	Picture	EAN	GTIN
Shirt Blue	M		2000000000015	02000000000015
Shirt Blue	L		2000000000022	02000000000022
Shirt Red	M		0200000000039	02000000000039
Shirt Red	L		0200000000046	02000000000046

The next step is that we are going to assign serial numbers to those GTINs, to convert them into SGTINs - which we can use to encode in an RFID label. Let's assume that this retailer has two products on stock for each EAN. If we add the serial, we translate them to Pure Identity URIs. A Pure Identity URI is used to describe the GTIN and serial number in a way that has nothing to do with the physical representation (barcode or RFID label). We assume the GS1 Company Prefix length is 7.

Name	Size	Picture	GTIN	Serial	Pure Identity URI
Shirt Blue	M		02000000000015	1	urn:epc:id:sgtin:2000000.000001.1
Shirt Blue	M		02000000000015	2	urn:epc:id:sgtin:2000000.000001.2
Shirt Blue	L		02000000000022	1	urn:epc:id:sgtin:2000000.000002.1
Shirt Blue	L		02000000000022	2	urn:epc:id:sgtin:2000000.000002.2
Shirt Red	M		02000000000039	1	urn:epc:id:sgtin:2000000.000003.1
Shirt Red	M		02000000000039	2	urn:epc:id:sgtin:2000000.000003.2
Shirt Red	L		02000000000046	1	urn:epc:id:sgtin:2000000.000004.1
Shirt Red	L		02000000000046	2	urn:epc:id:sgtin:2000000.000004.2

As you can see, the numbering starts with '1' here. The serial number can be any arbitrary number, as long as it satisfies the requirement that in combination with the GTIN it is a unique number.



Please note that two different products (thus GTINs) can have the same serial number. Only the combination of GTIN plus serial number should be unique.

The last step is to translate the information above into something that can be encoded into an RFID label. When assuming that the RFID label is 96 bits and the filter value is 1 (POS item), we get the following results:

Name	Size	Picture	Pure Identity URI	Hexadecimal Value
Shirt Blue	M		urn:epc:id:sgtin:2000000.000001.1	30347A120000004000000001
Shirt Blue	M		urn:epc:id:sgtin:2000000.000001.2	30347A120000004000000002
Shirt Blue	L		urn:epc:id:sgtin:2000000.000002.1	30347A120000008000000001
Shirt Blue	L		urn:epc:id:sgtin:2000000.000002.2	30347A120000008000000002
Shirt Red	M		urn:epc:id:sgtin:2000000.000003.1	30347A12000000C000000001
Shirt Red	M		urn:epc:id:sgtin:2000000.000003.2	30347A12000000C000000002
Shirt Red	L		urn:epc:id:sgtin:2000000.000004.1	30347A120000010000000001
Shirt Red	L		urn:epc:id:sgtin:2000000.000004.2	30347A120000010000000002

Encoding an SGTIN in a barcode

Although it is not common, it is still possible to encode the full SGTIN in a barcode. This might be useful in cases where the RFID label is broken or missing. When you have the full SGTIN as barcode available on the label, this helps you to re-encode a new label. Another use case is for mobile checkout: there is no need to have an RFID reader present to still obtain the full SGTIN. The options are described in another document: “Representing an EPC in barcodes”.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 42

Document Last modification date 16 February 2024

Document PDF Exported 5 April 2024 **by** Nedap Retail | Operations



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands



nedap-retail.com

Connected Devices Knowledge Base

RFID EPC Standards

version 24, February 2024

Introduction	3
Air Interface Protocol.....	4
Inventory	4
Reading, writing and killing	4
Passwords and locking	5
Sessions and flags	5
Selecting labels	6
Tag Data Standard	7
EPC memory bank	7
TID memory bank	7
User memory bank	7
Reserved memory bank	8
EPC Information Services.....	9
Other standards.....	10

Introduction

Regarding RFID for our Nedap Retail products, we mean RFID according to the GS1 EPCglobal Gen 2 standard. EPC stands for Electronic Product Code. ISO also qualifies this standard as 18000-6C. GS1 is the international organization that handles barcode standards and hands out company prefixes for use in barcodes and EPCs.

The EPC standards not only describe how the reader communicates with labels (Air Interface Protocol) but also how data is encoded in the RFID label (Tag Data Standard), how data should be obtained from readers (Application Level Events), and how data is exchanged within multiple RFID systems (EPC Information Services).

A basic understanding of those standards is fundamental to understanding the inner workings of our products. However, Nedap Retail only uses standards that make life easier - standards that make things more complicated are not used.

The following standards are discussed in this document:

- Air interface protocol
- Tag Data Standard
- EPC Information Services

For more information on all the standards, please visit the EPCglobal website: <http://www.gs1.org/gsmp/kc/epcglobal>.

Air Interface Protocol

The Air Interface Protocol is the protocol that describes the communication between the RFID reader and the RFID labels. In this document, we will explain the general operation.

The Air Interface Protocol is a 'reader talks first' protocol, meaning the RFID reader will initiate communication with the labels. The reader first communicates with label 1, then with label 2, and so on (time-multiplexed).

Inventory

Doing an inventory is the basic building block for reading RFID labels. An inventory means that the reader will transmit a command, and all labels in the field will respond to that. In this command, the reader states several available time slots for replies from labels. This can be anywhere between 1 and 65536 time slots. The reader automatically determines the number of time slots.

If a label receives such a command, it chooses a random time slot in which the label will answer. If the reader has completed sending the Inventory command, it will continue asking, 'Is there a label in timeslot 1?'. There are now multiple possibilities:

- No label replies. It could be that when having 16 time slots and only eight labels, no label has thrown 1 for its time slot.
- One label replies.
- Multiple label replies, a so-called collision. In this case, typically, no labels will be read.

If there is one label in the time slot, the label will send out its EPC code, which the reader will receive. If the process has been completed successfully, the reader moves on to the next time slot. This will continue until all time slots in the original command have been done.

It might be that one or more labels were not read due to a collision. In that case, the reader will execute another inventory until all labels in the field have been read.

Reading, writing and killing

When you need to read specific memories from a label, write new codes to the label, or maybe even kill the label, a secondary step is added to the inventory process. When the label has returned its EPC code, the reader will reply with another command to execute a read, write, or kill command. The reader will move on to the next time slot when this command is completed.

(i) Please keep in mind that the write distance of a label could be much shorter than the distance that you can read a label. This has to do with the fact that writing consumes more energy than reading.

Passwords and locking

It is possible to secure specific areas of the label with a password. If enabled, you need a password to change the EPC code. It is impossible to protect reading the EPC or User memory with a password (more on User memory in the next chapter).

Besides having a password, it is possible to lock certain areas of the label for writing again: a so-called “permalock”. A permalock can not be reverted.

Sessions and flags

One might wonder how a label knows by which reader when it has been read. This is handled by so-called 'sessions' and 'flags'.

A label can have a flag 'A' or 'B'.

- When a reader first powers a label, the flag always starts at 'A.'
- If a label transmits its EPC to the reader during an inventory, and the reader acknowledges it, the flag is changed into 'B.'

In this way, the label will respond again once all labels are read in the field. The reader can define in its inventory command which flags it wants to read, either 'A' or 'B' (the target).

A typical reader can also switch automatically from A (moving all labels from 'A' to 'B') to B (moving all labels from 'B' to 'A'), and so on.

There are two ways a flag can change from 'B' to 'A':

- A reader reads with the target set on flag 'B'. After the EPC is received successfully by the reader, the flag is changed into 'A' again.
- After some time, the label automatically changes its flag from 'B' to 'A'. The exact behavior depends on the session that is used.

The reader can also select a 'session', which enable two possibilities:

- Having multiple readers inventorying the same tag population, as each session has its own flags. Then each reader can still make sure they read the complete population.
- The way a label changes its flag from 'B' to 'A' differs per session. This is summarized in the next table.

Session	Return To 'A' When In The Field	Return To 'A' When Not In The Field
0	Never	Directly
1	Between 500 ms and 5 seconds (typically one second)	Between 500 ms and 5 seconds (typically one second)
2	Never	After more than two seconds
3	Never	After more than two seconds

Selecting the right session and target is crucial for obtaining good read performance. Luckily, in all Nedap products, this is automatically taken care of.



Please note that the field in which a session persists can be much larger than the area in which a label is typically read. Sometimes this 'persistence' area could be 3-5 times as big as the typical reading area.

Selecting labels

Until now, we have assumed that all labels in the field (with the right flag) will always respond. This is not strictly necessarily the case.

Using select statements, it is possible only to have labels replying that comply with specific conditions. In this way, you can select, for example, the one label you need to write or kill or have only labels in the inventory belonging to a specific brand to optimize read performance.

The reader transmits a select statement before starting an inventory and includes the specific code to look for and the memory bank and address to look for it. It also states what to do if the label complies or not (e.g., only have labels respond that do not match or have only labels respond that do match).

Tag Data Standard

Now that we have a better understanding of how the communication between the RFID reader and label works, it is time to gain a better understanding of how data is stored in the RFID label.

Basically, there are always four types of memories inside an RFID label, which all have their own purpose and way of working:

- EPC memory bank: stores the EPC code and related information.
- TID memory bank: stores information on the used chip, and serial number.
- User memory bank: optional, can be used to freely store information.
- Reserved memory bank: contains the passwords for accessing and killing a label.

EPC memory bank

The EPC memory bank contains the most important information: the EPC code. This can be any string of characters, but preferably it is a code according to the EPC standards.

EPCglobal specifies multiple types of codes that can be put in the EPC memory; for retail, the SGTIN (Serialized Global Trade Identification Number) and SGLN (Serialized Global Location Number) are the most important.

The SGTIN is an evolution of the GTIN, better known as the EAN or UPC barcodes. Those barcodes contain a Company Prefix (identifying the company that produces a product, for example, 'Nike') and an Item Number (identifying the product, for example, 'Air Max 2 size 44 color green').

The SGTIN consists of the Company Prefix, the Item Number, and a new unique Serial Number. This Serial Number distinguishes one pair of 'Air Max 2 size 44 color green' from another, 'Air Max 2 size 44 color green', and is helpful for many applications.

The SGLN is the same: a Company Prefix with a Location Reference. This can be used to identify stores uniquely.

TID memory bank

In the TID memory bank the manufacturer of the chip (MDID), and the type of the chip (Model Number) is stored. Optionally, a unique serial number for the chip is added, that could be used for Multi-vendor Chip Serialization - a way to generate serial numbers for the EPC.

User memory bank

The User memory can be used to freely store information. This will typically not be used for fashion retail but can be used to store expiry dates, etc. etc.

Reserved memory bank

The reserved memory bank contains the passwords:

- Access passwords: to get read or write access to certain memory banks.
- Kill password: needed before you can “kill” the tag.

(i) It is not possible to kill a tag when it has no kill password. So, if you want to kill a tag that has no kill password, you first need to write the password and then send the kill command.

EPC Information Services

The EPC Information Services is a standard on exchanging high-level business data about EPCs. It is for example the protocol to obtain data from the !D Cloud app.

In general it answers the four questions What, Where, When and Why.

- What: EPC number, manufacturing data or transactional data
- Where: Location
- When: Event time or record time
- Why: Business process step, product state or current conditions.

For example: “the following products where received in store X at 9.00 this morning and are now ready for sale”.

Basically, each EPCIS event details the 'Why' in a business step (what happened) and a disposition (what is the current state). Some examples are:

- Business step: accepting receiving, holding, inspecting, storing, stocking, repackaging, packing, picking, loading, etc.
- Disposition:
sellable_not_accessible, sellable_accessible, non_sellable, non_sellable_expired, non_sellable召回ed, non_sellable_damaged, etc.

All possible business steps and dispositions are standardized in the Core Business Vocabulary (CBV) standard.

Other standards

There are some other standards defined by EPC global. Those are:

- Application level events (ALE)
- Low Level Reader Protocol (LLRP)
- Discovery Configuration and Initialization (DCI)
- Reader Management (RM)

At Nedap Retail we have chosen not to implement those standards, or use our own variation to those standards. The reasons vary but mostly those standards are either too complicated to be used, or too simple for what we want to achieve.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 24

Document Last modification date 16 February 2024

Document PDF Exported 5 April 2024 **by** Nedap Retail | Operations



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands



nedap-retail.com

Connected Devices Knowledge Base

RFID - Representing an EPC in barcodes

version 23, January 2024

Introduction	3
Sample information.....	4
Representation in barcodes.....	5
Summary	5
GS1-128 code (1D, laser)	5
GS1 DataMatrix (2D)	6
Used abbreviations	8

Introduction

This application note details how to encode an EPC in compatible barcodes. This enables the following:

- If an RFID label is broken, the specific EPC can be reprogrammed in a different label by using the barcode representation.
- If a POS has only a barcode scanner, it is still possible to deactivate a specific EPC for use with EAS applications.
- A smartphone app can show more information on a product and related products (e.g., stock information) without reading the RFID code.

The main GS1 document explaining this is called "RFID Barcode Interoperability GS1 Guideline", and you can find it here:

<http://www.gs1.org/BC-EPC-guidelines>

Sample information

The following pure-identity example is used:

urn:epc:id:sgtin:0614141.812345.6789

(of which the GTIN is **80614141123458**, the serial **6789**, and hexadecimal representation is **3034257bf7194e4000001a85** with a 96-bit tag)

Some tools that might help verification:

- Easy on-line tool for data translation: <https://www.gs1.org/services/epc-encoderdecoder>
- Barcode generator: <http://www.terryburton.co.uk/barcodewriter/generator/>

Representation in barcodes

When the EPC is encoded in a barcode, it all starts by forming a GS1 Element String. This is a combination of 'application identifiers' and the actual information. A full list can be found here: https://en.wikipedia.org/wiki/GS1-128#Full_list_of_Application_Identifiers. For the EPC, the following identifiers are relevant:

- (01) GTIN: The GTIN part of the EPC (length is 14)
- (21) Serial: The serial number part of the EPC (length is up to 20)

The resulting GS1 Element String is then:

(01)80614141123458(21)6789

Summary

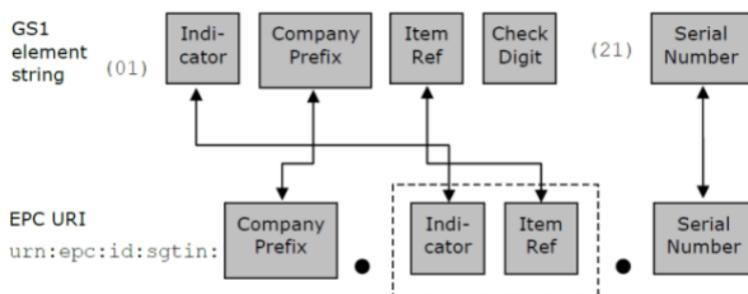
To summarize, see example below:

SGTIN EPC URI syntax:

urn:epc:id:sgtin:CompanyPrefix.ItemRefAndIndicator.SerialNumber

SGTIN EPC URI: urn:epc:id:sgtin:0614141.812345.6789

GTIN: (01)80614141123458(21)6789



GS1-128 code (1D, laser)

- Wikipedia: <http://en.wikipedia.org/wiki/GS1-128>
- GS1 Specification: http://www.gs1.org/docs/barcodes/GS1_General_Specifications.pdf

Example

(01)80614141123458(21)6789



GS1 DataMatrix (2D)

- Wikipedia: http://en.wikipedia.org/wiki/Data_Matrix
- GS1 Guideline: http://www.gs1.org/docs/barcodes/GS1_DataMatrix_Guideline.pdf

Example

(01)80614141123458(21)6789



Please note that the length of the serial number varies; thus, the size of the DataMatrix code can vary.

Used abbreviations

Standard terms may be abbreviated in this document. The following table shows the descriptions of the abbreviations used. RFID-specific abbreviations are highlighted.

Abbreviation	Description
API	Application Programming Interface - is a way for two or more apps to communicate with each other.
CC	Customer Counting
DM	Device Management
EAS	Electronic Article Surveillance
EPC (RFID)	The Electronic Product Code is one of the available formats for encoding identifiers on RFID tags. The EPC is a globally unique number that identifies a specific item in the supply chain.
External CC	External Customer Counting (e.g., Brickstream)
FRS	Fast Remote Service
GS1 (RFID)	(Global Standards 1) An international standards organization with member bodies in more than 100 countries worldwide. Nedap Retail follows the GS1 and RainRFID standards.
GTIN (RFID)	A Global Trade Item Number (GTIN) is a number that uniquely identifies a product. It can be found beneath the barcode of a product.
IO Box	Input/Output Electronics device
IR	Infra Red
MD	Metal Detection
RF	Radio Frequency
RFID	Radio Frequency Identification

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 23

Document Last modification date 31 January 2024

Document PDF Exported 31 January 2024 **by** Nedap Retail | Operations



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands



nedap-retail.com

Connected Devices Guideline

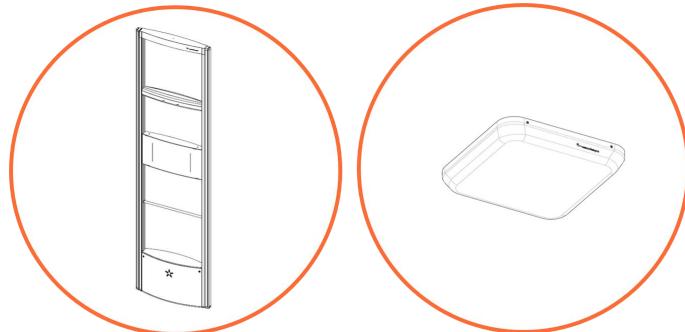
iSense RFID EAS Store prerequisites

version 12, April 2024



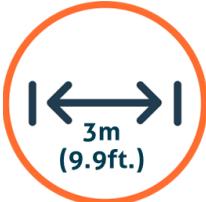
Store environment	4
Installation requirements.....	5

Prerequisites for a successful iSense RFID installation with Gates or iD Tops.



Gate and iD Top

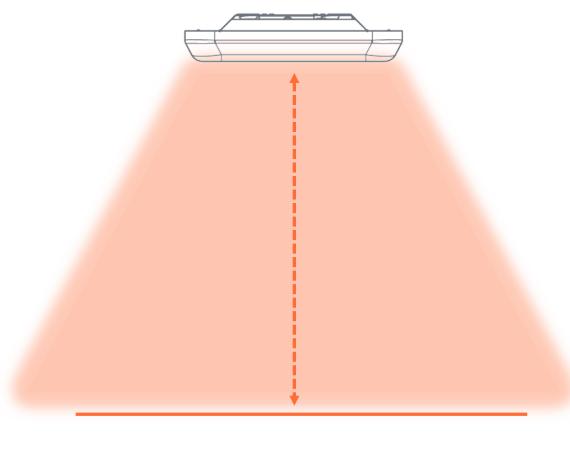
Store environment

What	Remarks
Label-free zone 	Have a label-free zone of: >1m (3.3ft) for Gates >1.5m (4.9ft) for Tops
Other RFID devices 	Keep distance from other RFID devices, >3m (9.9ft) is recommended
Metal objects 	
Tempered glass 	Metal objects, tempered glass, and mirrors reflect RFID signals. This might cause false alarms and or lousy detection. Try to avoid this close to the system
Mirrors 	

Installation requirements

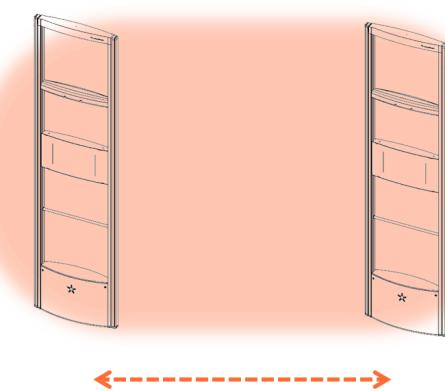
- Available network connection(s) (with internet connection)
- Available (always-on) power socket(s)
- Option to make cable conduits
- Distance and height:

Distance and height of the iD Tops

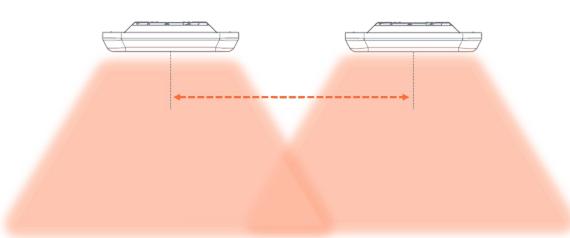


2.5m (8.2ft) recommended

Distance between Gates



2m (6.6ft) recommended



2.5m (8.2ft) recommended

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 12

Document Last modification date 5 April 2024

Document PDF Exported 5 April 2024 **by** Nedap Retail | Operations



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com



Connected Devices Guideline

iSense RFID Filtering and Beam Steering

version 24, February 2024

Introduction	3
Beam Steering	4
Disable Beam Steering	5
Beam Steering v1 / v2	6
Limitations	6
Filtering.....	7
Static Item Filter	7
Tag Muting	9
Chaos Filter	11
Advanced settings	11

Introduction

In general, there are many RFID labels near an iSense RFID system in, especially, smaller stores. As RFID signals can travel far into the store, this can result in degraded performance or false alarms for the iSense RFID system. Also people can walk close to the system with articles and labels.

The iSense firmware has advanced algorithms to make sure that the system still works well in busy retail environments which are further explained in this document:

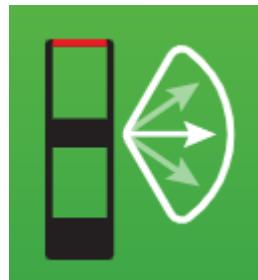
- Beam Steering
- Filtering
 - Static Item Filter
 - Tag Muting
 - Chaos Filter

Beam Steering

The principle of Beam Steering is based on a beam of the antenna which can be steered electronically in multiple directions. This means that we can say to the antenna 'look more to the left' or 'look more to the right'.

When using Beam Steering we can reduce the following issues:

- People walking along the system, but not under or through the system. Without Beam Steering this caused false alarms.
- Items that were only read due to reflections (e.g. people with metallic shopping carts or suitcases), causing false alarms.
- Merchandise stored outside of the store, taken into the store. Previously this caused alarms, now we are able to distinguish between outgoing and incoming labels.



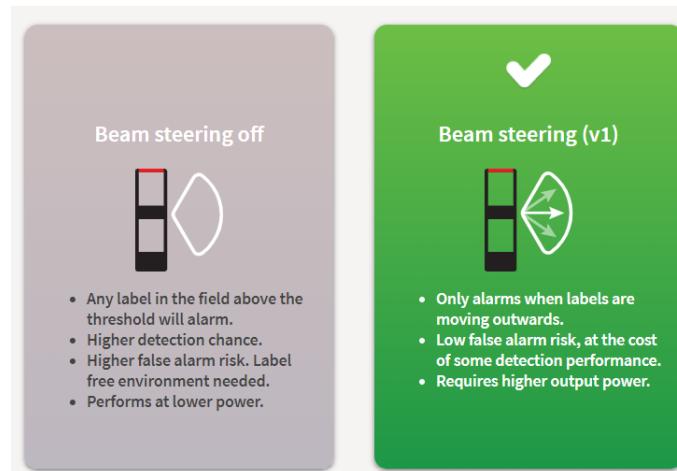
Disable Beam Steering

It is possible to disable Beam Steering, as in some cases it better matches customer expectations. When Beam Steering is turned off, there is no constant and fast switching in the antennas, and therefore the system is unable to determine the direction a label moves.

Turning off Beam Steering will detect more labels, because all beams work at the same time and do not have to switch between beams. It seems good that more labels are detected, but in fact there is also a down side, turning Beam Steering off also significantly increases the risk of false alarms. Without Beam Steering, labels that move within, or enter the store, are not filtered out.



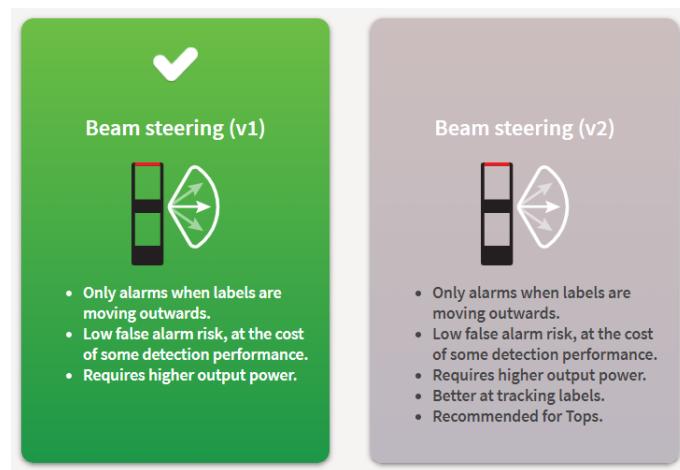
In general; use Beam Steering, only disable it in some special cases.



Beam Steering v1 / v2

In addition to disabling Beam Steering, it is also possible to change the Beam Steering version to find the optimal setting for the situation. Normally the default setting should be best:

- Version 1 is default for gates
- Version 2 is default for tops



Limitations

The maximum throughput of an RFID reader in practical circumstances is around 200 labels per second. If we want to know the direction of an RFID label, we need to read it multiple times. For example, first on beam 1, then on beam 2 and finally on beam 3. If this happens, we can assume that the label is moving in the direction of beam 3 (from beam 1). This would reduce the tag throughput to about 30 labels per second - at regular walking speed. This is also worsened by stray tags and other non-idealizing conditions. This is why Filtering is also important to solve this further.

Filtering

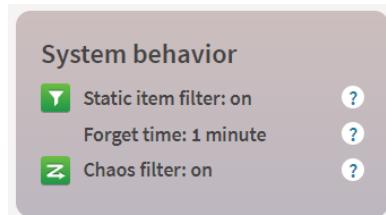
Without filtering, any RFID tag in the vicinity will communicate with the iSense system. In this way, the iSense system will quickly engage in communication with labels that are not relevant at the time and will significantly reduce performance for labels that really matter, namely labels that actually go outside the store.

There are 3 filtering options active in the iSense system:

- Static Item Filter
- Tag Muting
- Chaos Filter



The Filtering features are only enabled when using the EAS role with systems using Beam Steering.



Static Item Filter

The Static Item Filter is a software filter that ignores labels with a specific EPC after the following conditions have been met:

- The EPC has been observed for at least 4 minutes since first observed
- The EPC has been observed for at least 4 minutes with pauses of no longer than the forget time (default 1 minute)

If both are true, the label will be placed in the Static Item Filter, and will be ignored by the system.



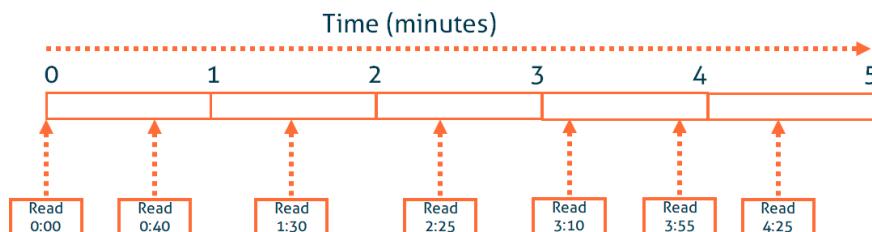
The label itself will still try to communicate and is not muted by the Static Item Filter.

This will happen in a zone close to the installed system. How close depends on the output power of the system and the local situation. In general this will be one to a few meters.

Example

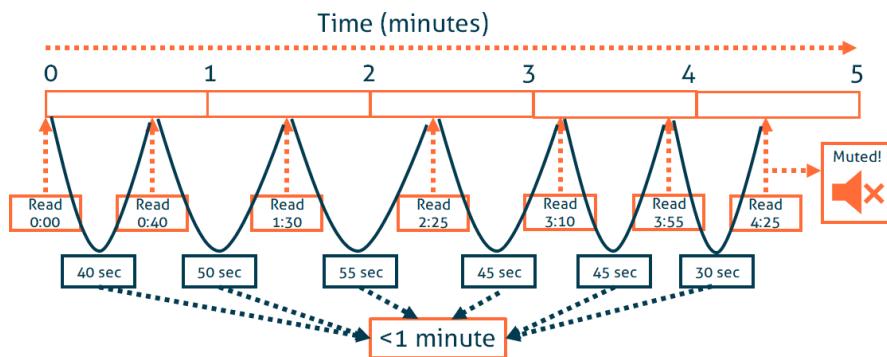
Let's take a look at an example:

A label is observed multiple times with a time span of 5 minutes. The forget time is 1 minute



The time between two consecutive readings is shorter than the set forget time (1 minute) and the total time is more than 4 minutes since it was first observed.

This means that both criteria are met, and so this label ends up in the Static Item Filter and is ignored



Remove from filter

A label is removed from the Static Item Filter if the label is not observed for longer than the forget time. In the example above this is 1 minute.

This can be done by moving the label further away from the system or by reducing the power of the system.



The labels that are used in the configuration on the calibration box are never muted, also not after the configuration is complete. So the calibration box can also be used to test the system after configuration.

Tag Muting

When a label enters the Static Item Filter, there are 2 options:

- Ignore the specific label. This means that the system will still communicate and process the label, but otherwise ignore it
- The other option is to have this specific label also stop communicating, in which case the system will no longer be affected by the communication with this label

For RFID EAS, the RFID reader has a maximum read throughput of approximately 30 label reads per second, depending on the exact configuration. This throughput is used to continuously monitor the status of these labels.

If many labels are placed close to the system, the reader may be 'too busy' with those labels. This affects system performance.

Tag Muting gives the reader more time to process labels that matter, without having to deal with labels that are static in the environment.

Remove Tag Muting

A label remains muted as long as it is powered by the RFID field. Remove the label from the field to unmute it again.



Please note that unmuted labels can still be filtered out by the Static Item Filter for the remaining forget time

Compatibility with other RFID systems

This feature allows cooperation with other RFID systems, even from other manufacturers. When the tag is temporarily muted, other readers are still able to read it. This means that muted tags can still be brought to the Point-of-Sale and read there, or included in a cycle count.

Technical implementation

The technical implementation is as follows:

- A tag is muted by asserting the Select (SL) flag of a tag.
- The reader only queries for tags that do not have the Select (SL) flag asserted.

A tag is unmuted when the persistence of the Select (SL) flag expires. The persistence for the Select (SL) flag is defined in the EPC Gen2 standard:

- Tag energized: indefinite.
- Tag not energized: larger than 2 seconds (generally in the order of 30 seconds).



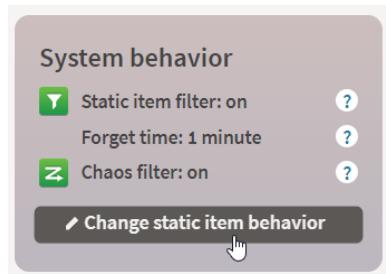
Other readers should be compatible with this implementation, by setting the SEL bits in the Query command to 'all' (00 or 01).

Chaos Filter

The last option is the Chaos Filter, this filters RFID labels that seem to move quickly between inside and outside the store. This is usually caused by reflections, and may cause false alarms when not filtered out. Be aware that even walking in and out the store one time with a certain label can already activate the Chaos Filter for that label.

Advanced settings

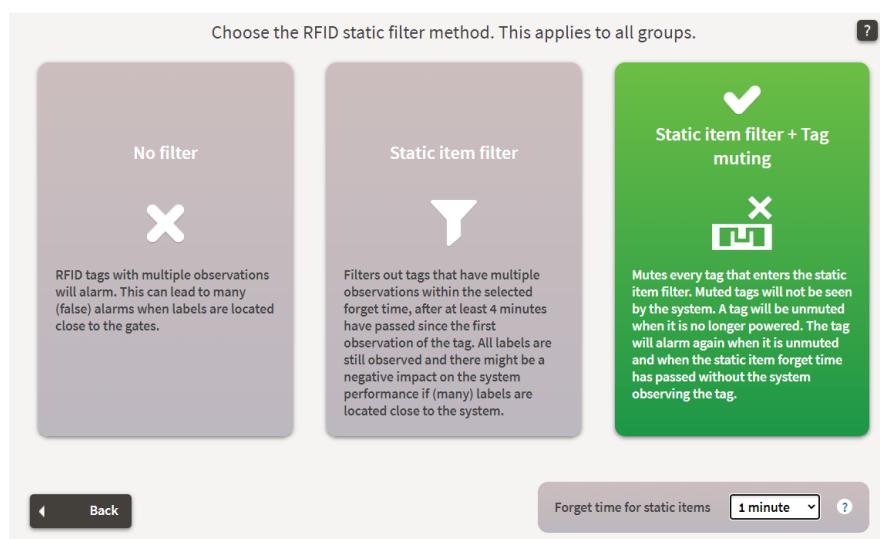
For advanced RFID technicians it is possible to change the Filter settings. This is normally not recommended however in some cases this might be necessary.



In this case there is an option to “Change static item behavior” in which:

- You can turn off Tag Muting
- Change the Forget time for static items

Contact Nedap Retail support for more information.



Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 24

Document Last modification date 16 February 2024

Document PDF Exported 5 April 2024 by Nedap Retail | Operations



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com



Connected Devices Guideline

iSense RFID - 8.2 MHz RF vs. UHF RFID

version 21, February 2024

Introduction	3
Field degradation	4
Reflections and interference	5
Shielding	6
Used abbreviations	7

Introduction

Almost all Nedap partners are experienced in installing RF-based 8.2 MHz EAS technology.

RFID technology can also be used for EAS applications, however, the behavior of the technology is completely different: not only the identification part is added, also the way the field works and which things can be problematic are different between both technologies.

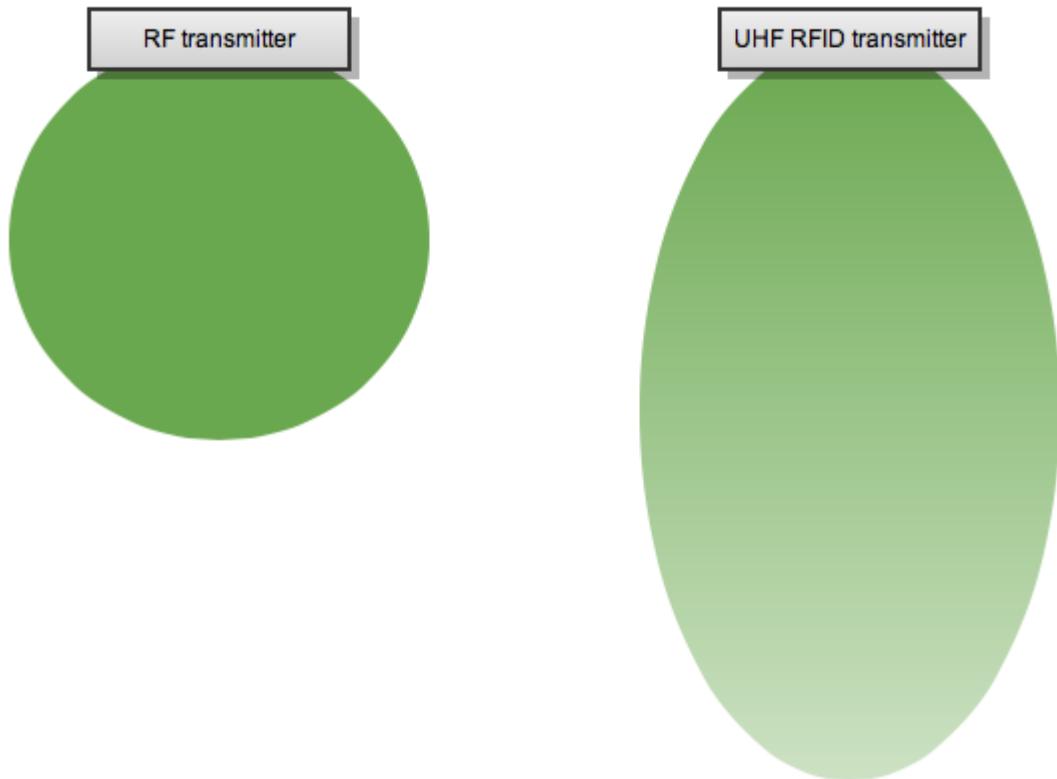
Standard RF technology operates at 8.2 MHz. RFID for retail applications operates at UHF frequencies, around 900 MHz - depending on the region and country. The different frequencies ensure different behavior. There are two main effects:

- The RFID field degrades slower compared to RF; The RFID detection field is less limited than a RF field.
- The RFID field is also reflected by surroundings, causing stray tag reads at locations you don't want it to be read.

First we will look at the behavior of a typical RFID reader. Then we will look at Nedap products, which try to solve issues using Advanced Tag Filtering (ATF) technology.

Field degradation

Components in a 8.2 MHz field are mostly magnetic, they degrade with a 3rd order speed. The components in a UHF RFID field around 900 MHz are mostly electric, so they degrade with a 2nd order speed. This is visualized in the following drawing (assuming no reflections and interference).

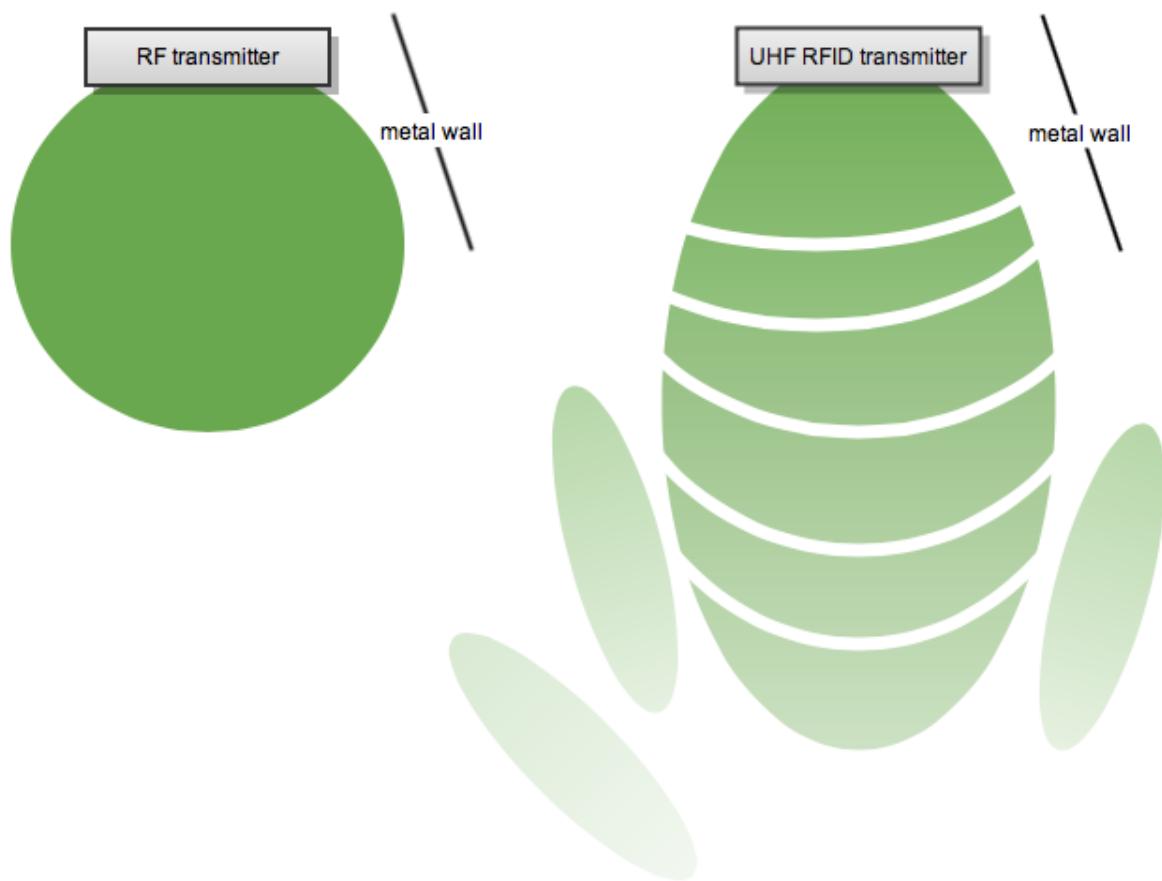


What this means, is the following:

- UHF RFID can have larger read distances compared to RF technology.
- However, with UHF RFID, at larger distances from the reader, the orientation of the label becomes important. In some orientations the label will be read, but in other orientations the label won't be read.

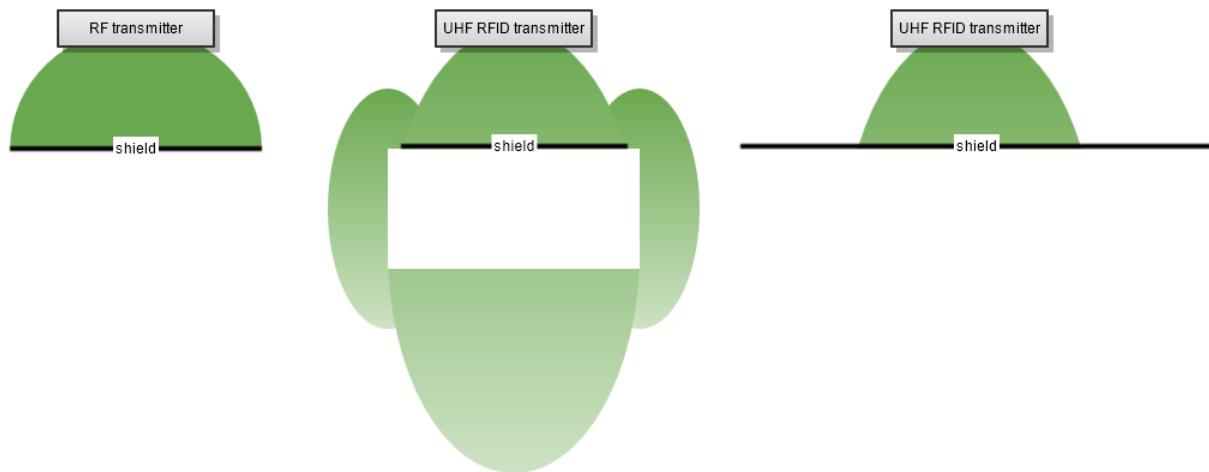
Reflections and interference

The way the field degrades is not the only difference between 8.2 MHz EAS and UHF RFID technology. The second issue is that UHF RFID is sensitive for reflections. Those reflections can be caused by metal materials. In the end, the reflections will cause interference. In practice you might experience this by reading labels at locations you won't expect them to be read, or not reading labels at locations you want it to be read. See the following picture for an explanation.



Shielding

With a 8.2 MHz RF-based system, it is possible to shield the field from reading items, by using a metal shield. When using UHF RFID technology, this is less of an issue. The shield should be much larger than the field, otherwise the field will go around the shield.



Shielding can also be experienced when a person stands in between the reader and the label; and the label is close to the human body: there is a chance that the label will not be read.



Please note that placing a shielding can cause additional reflection to the other side, as explained in the previous chapter. We always recommend to test specific set-ups in your office, before deploying in a retail store.

Used abbreviations

Standard terms may be abbreviated in this document. The following table shows the descriptions of the abbreviations used. RFID-specific abbreviations are highlighted.

Abbreviation	Description
API	Application Programming Interface - is a way for two or more apps to communicate with each other.
CC	Customer Counting
DM	Device Management
EAS	Electronic Article Surveillance
EPC (RFID)	The Electronic Product Code is one of the available formats for encoding identifiers on RFID tags. The EPC is a globally unique number that identifies a specific item in the supply chain.
External CC	External Customer Counting (e.g., Brickstream)
FRS	Fast Remote Service
GS1 (RFID)	(Global Standards 1) An international standards organization with member bodies in more than 100 countries worldwide. Nedap Retail follows the GS1 and RainRFID standards.
GTIN (RFID)	A Global Trade Item Number (GTIN) is a number that uniquely identifies a product. It can be found beneath the barcode of a product.
IO Box	Input/Output Electronics device
IR	Infra Red
MD	Metal Detection
RF	Radio Frequency
RFID	Radio Frequency Identification

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 21

Document Last modification date 16 February 2024

Document PDF Exported 16 February 2024 by Nedap Retail | Operations



support-retail@nedap.com



Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com

Nedap Sense Guideline

RFID EAS Performance Optimization

version 42, October 2024

Introduction	3
RFID Detection Performance in Device Management	3
Steps to improve performance.....	6
Advanced	9
Beam Steering v2	9
Beam Steering off	11
Median settings summary	11
Practical example	12
DM Performance Monitor	12
Solution	13

Introduction

Performance indicators can be monitored with the RFID performance tool in Device Management. This will help you get quick feedback on changed settings so that you can steer for the highest performance.

This document provides tips and tricks to improve the iSense RFID performance based on the indications in Device Management.

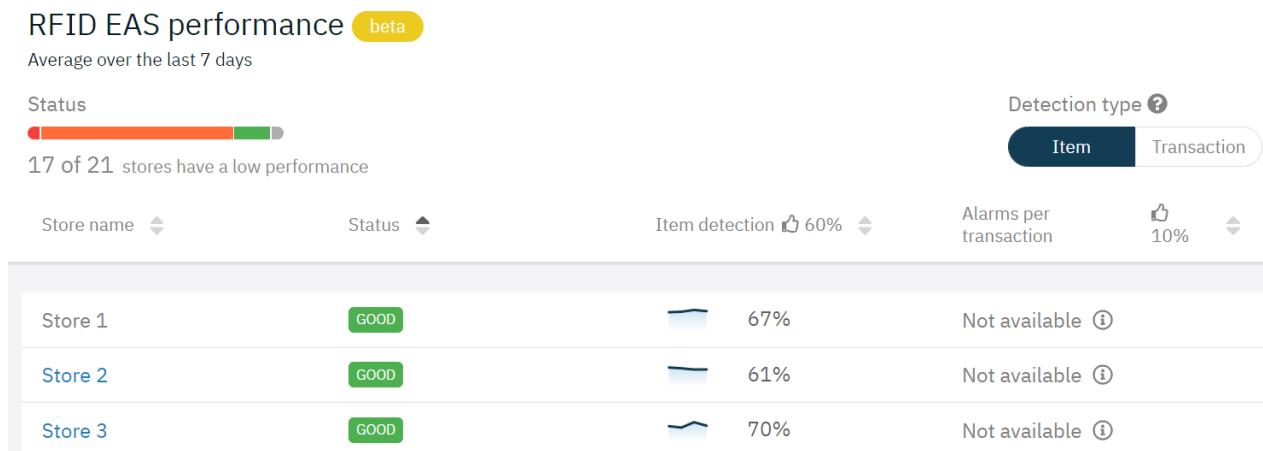
This document is focused on gates only.

Performance data in Device Management is only visible when:

- **Sales data** available in iD Cloud (e.g. with iD POS Pro)
- **SGTIN-coded labels** are used
- **Systems are connected** to Device Management
- **Fast Remote Service** is active (for Business Partners to view)
- **Support Package** is active (for Customers to view)

Performance is visible at the division and store levels. On store level in more detail.

RFID Detection Performance in Device Management



Store example:



There are two important values visible in the **Device Management** performance monitoring that are closely related to each other:

- **Alarms per transaction** (Number of alarms relative to the number of transactions)

Alarming

Alarms per transaction  10% 

- **Performance** (Item and Transaction)

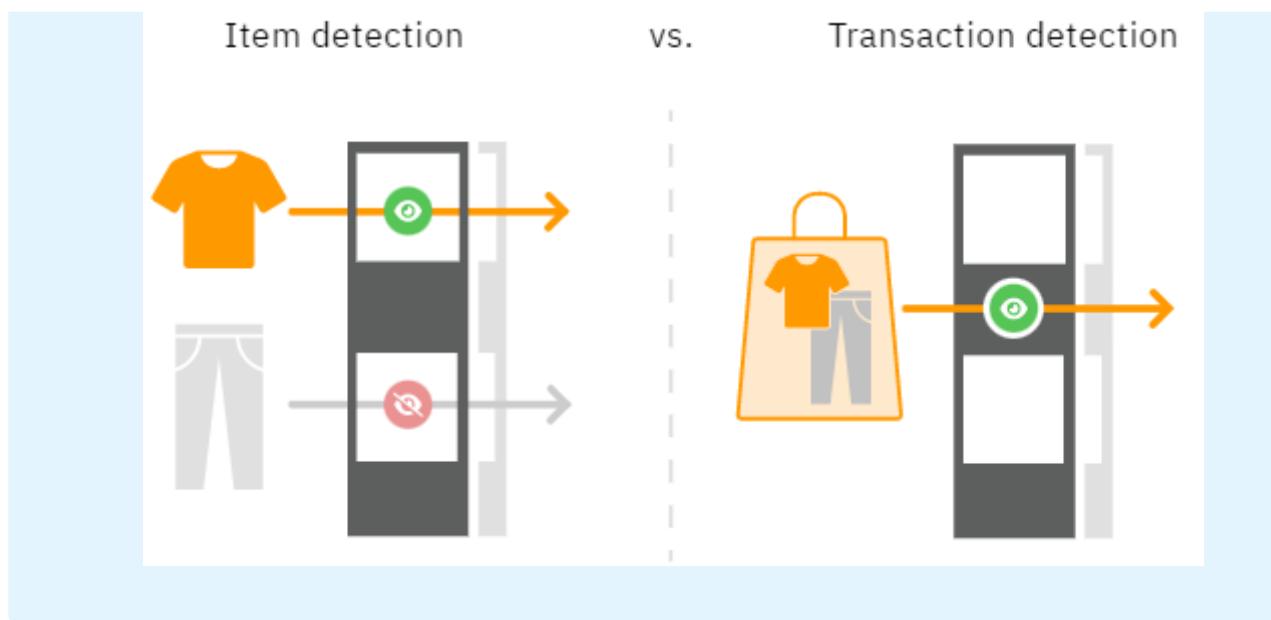
Detection

Item Detection  60% 

Detection

Transaction detection  60% 

- **Item-level performance** indicates how many unique items the system observes compared to items seen at the POS.
- **Transaction performance** Indicates how the system has observed transactions compared to items seen at the POS.



There is a balance between the false alarms and the performance. This also means that if the number of alarms per transaction is low, there is room for higher performance.

Detection performance is calculated once per day (overnight, based on local store time, between 2 AM and 6 AM).

Calculations are not repeated at a later point. So when data is delayed for a day, we will not recalculate performance for that store for that day.

Observations more than 5 minutes before any sale will be excluded from the performance calculations and will not contribute to the number of “Items seen at exit.”

Data retention is 6 months.

Steps to improve performance

Low-performance definition: <60% Item level detection and >10% Alarms per transaction

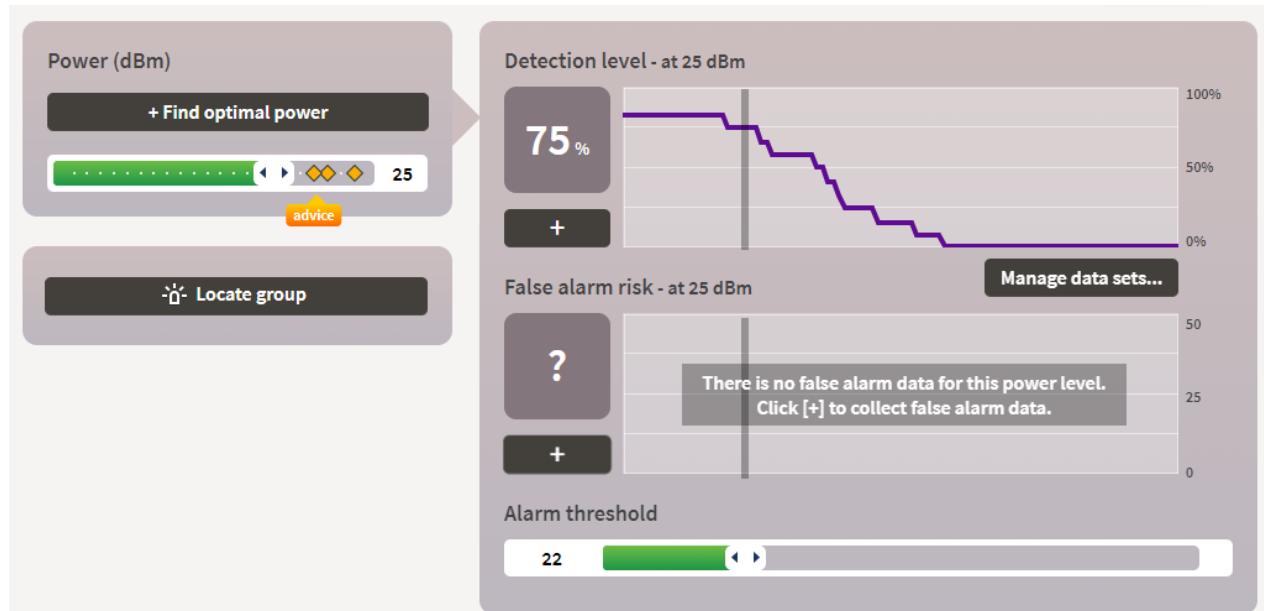
If the performance is too low, you can try following the basic steps below. This provides a step-by-step approach to finding the optimal point with the general settings (**Power** and **Alarm Threshold**).

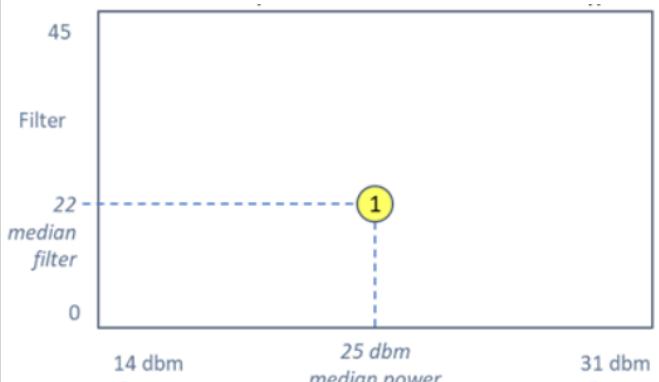
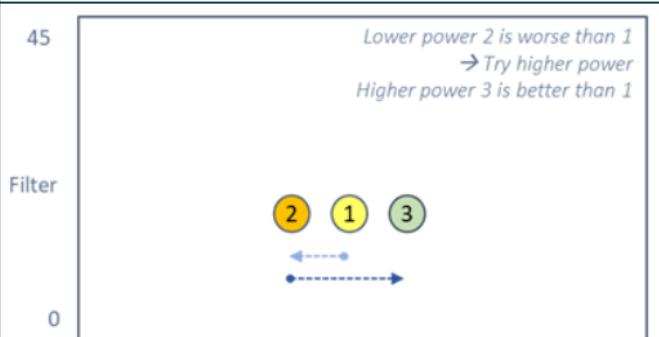
First, it is good to understand the most common (median) Power and Alarm Threshold settings:

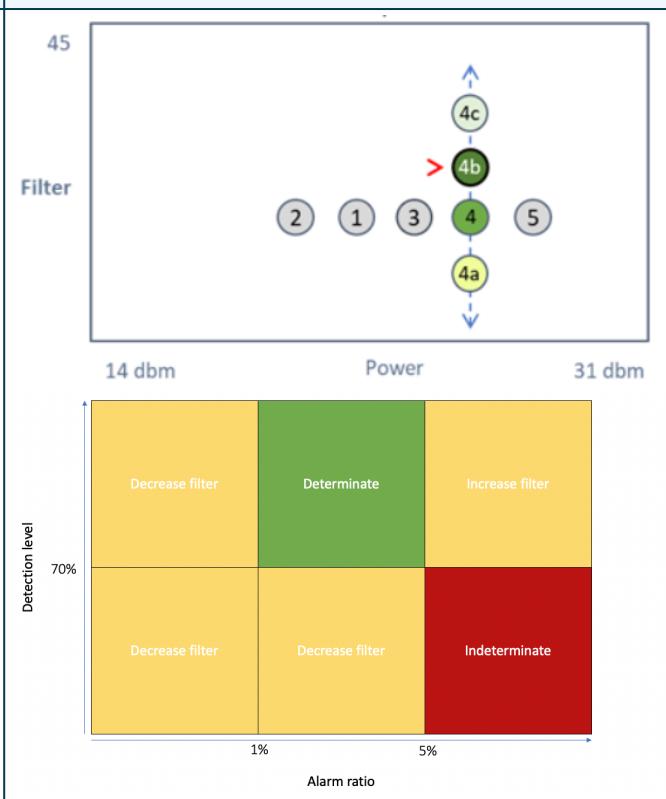
The median of **Power** setting that is used across the world is 25dBm

- Roadside stores may have a **Power** of **25dBm**
- Shopping mall stores **23dBm**

The median **Alarm Threshold** is **22%**, varies in general between 20% and 30%

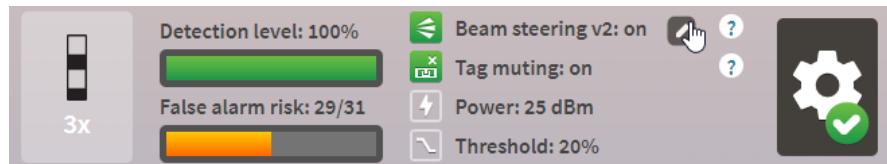


Step		
1	<p>Use the median Power and Alarm Threshold</p> <p>If this system performs well for 1 or 2 days, it can be left with the median settings. If not, continue with step 2 to set the power.</p> <p>If step 1 already gives too many alarms (>10% Alarms per transaction), increase the Alarm Threshold until the alarms are acceptable. Then, start increasing the power.</p>	
2	<p>Find power level</p> <p>Small steps from the median settings. First, lower the Power and check the Item/transaction detection level. If still low (<60% Item level), increase the Power.</p> <p>Keep increasing the Power until the Item/transaction detection level improves.</p>	 

Step		
3	<p>Find optimal filter settings for the found Power level</p> <p>Change the Alarm Threshold setting to find the optimal point (highest item performance with lowest number of alarms per transaction).</p>	 <p>The diagram illustrates the relationship between Filter, Power level, Detection level, and Alarm ratio.</p> <p>Filter: A vertical axis labeled "Filter" with values 45 at the top and 14 dbm at the bottom. A red arrow points upwards from 14 dbm towards 45, indicating increasing filter strength.</p> <p>Power: A horizontal axis labeled "Power" with values 14 dbm on the left and 31 dbm on the right. A green arrow points from 14 dbm towards 31 dbm, indicating increasing power level.</p> <p>Detection level: A vertical axis labeled "Detection level" with values 70% at the bottom and 45 at the top. A blue arrow points upwards from 70% towards 45, indicating increasing detection level.</p> <p>Alarm ratio: A horizontal axis labeled "Alarm ratio" with values 1% and 5% marked. A yellow arrow points from 1% towards 5%, indicating increasing alarm ratio.</p> <p>The diagram shows a grid of colored cells representing different combinations of these parameters:</p> <ul style="list-style-type: none"> Top row (Filter 45): Yellow (Decrease filter), Green (Determinate), Yellow (Increase filter). Middle row (Filter 14 dbm): Yellow (Decrease filter), Yellow (Decrease filter), Red (Indeterminate). Bottom row (Filter 14): Yellow (Decrease filter), Yellow (Decrease filter), Red (Indeterminate). <p>Specific points are highlighted: <ul style="list-style-type: none"> Point 4b: Located in the middle row, second column (Determinate). It is marked with a red arrow pointing towards it from the "Decrease filter" cell above it. Point 4a: Located in the bottom row, third column (Indeterminate). Point 4c: Located in the top row, first column (Decrease filter). </p>

Advanced

The Beam Steering configuration can also be changed if the general settings (**Power** and **Alarm Threshold**) do not deliver enough performance.



The default for gates is Beam Steering v1; there are two other options to use for gates;

- Beam Steering v2
- Beam Steering off

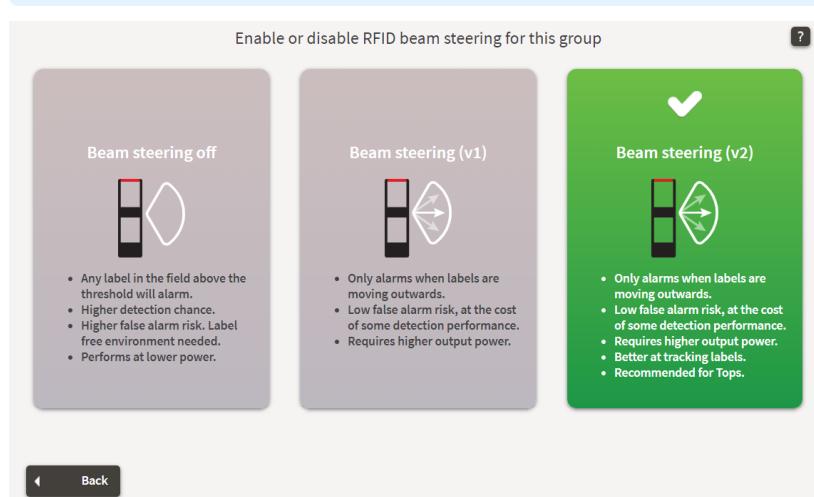
The default for iD Tops is Beam Steering v2, which should not be changed to v1

Beam Steering v2

This is another Beam Steering algorithm that can be useful if there are too many false alarms: use a higher **Power** with this setting. This algorithm is less sensitive on an essential basis but better with many false alarms.

The median settings for Beam Steering v2:

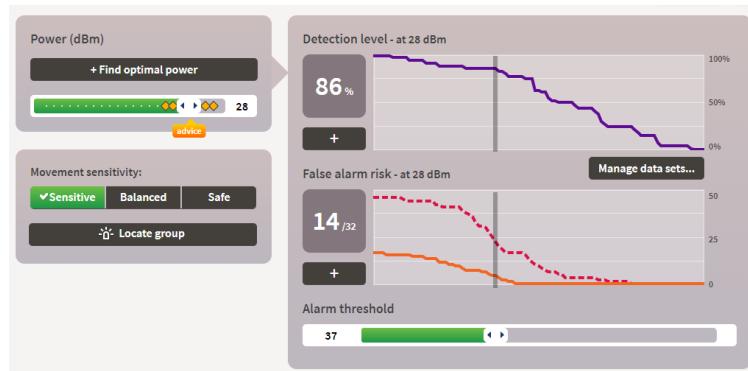
- **Power of 25dBm**
- **Alarm Threshold of 28%**
- **Movement sensitivity set to Sensitive**



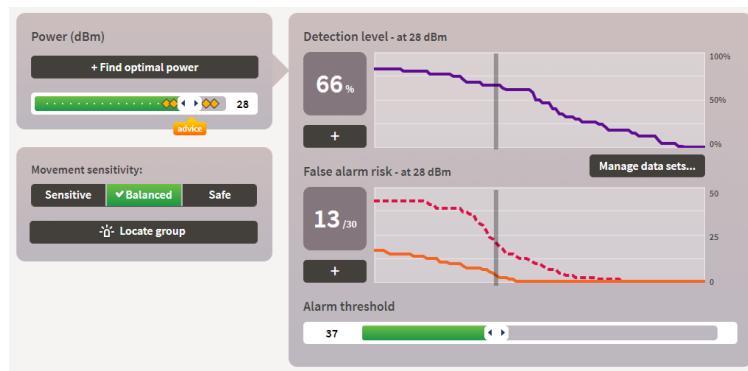
In the case of Beam Steering v2, another option, “Movement sensitivity,” will appear on the configuration screen.

This additional filter option is based on the gathered data graphs to find the optimal setting. Below, you can see one system with a change between the three options. Based on this setting, the sensitivity changes, causing lower item/transaction level performance and fewer false alarms.

Sensitive



Balanced



Safe

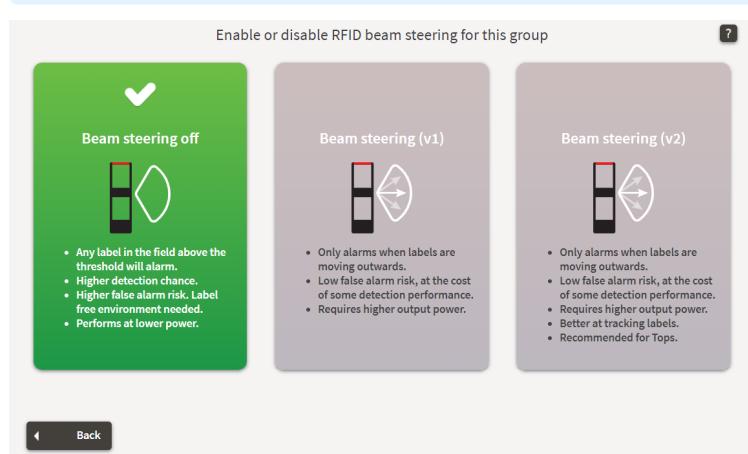


Beam Steering off

This will turn off the Beam Steering algorithm, making detecting labels and false alarms for close-by labels more sensitive. Therefore, it is needed to reduce **Power**.

The median settings for Beam Steering off:

- **Power of 19dBm**
- **Alarm Threshold of 30%**

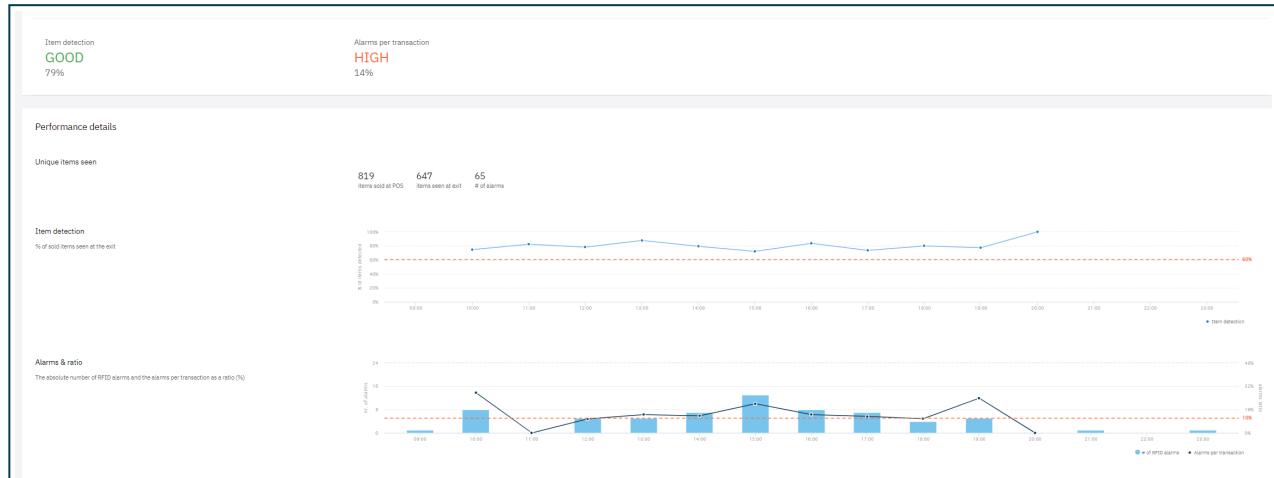


Median settings summary

Beam Steering	Power (DBm)	Alarm Threshold (%)	Movement Sensitivity
off	19	30	na
1	23-25	20-30	na
2	25	28	Sensitive

Practical example

DM Performance Monitor

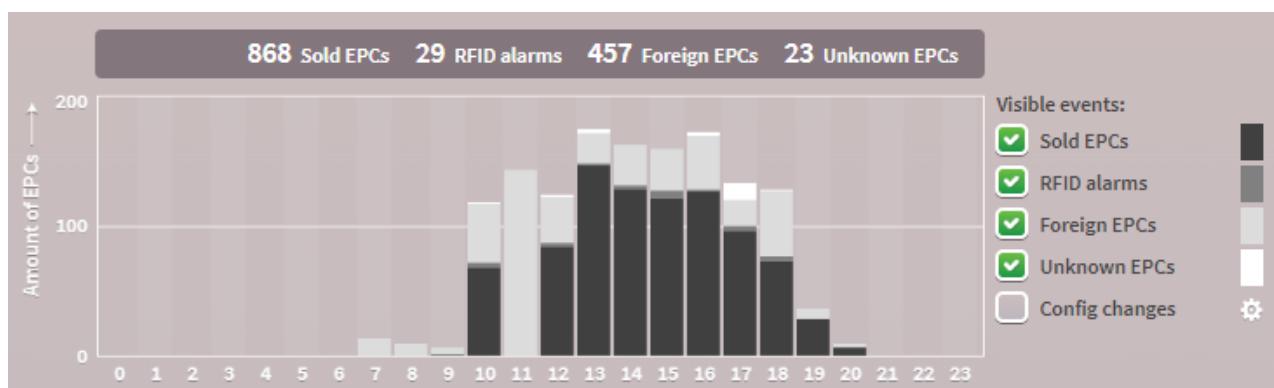


Based on the information above in Device Management (Alarms per transaction too high), you'd decide to squeeze the overall performance to reduce the alarm numbers. Before taking any action, it's essential to get an overview of the situation in the store.

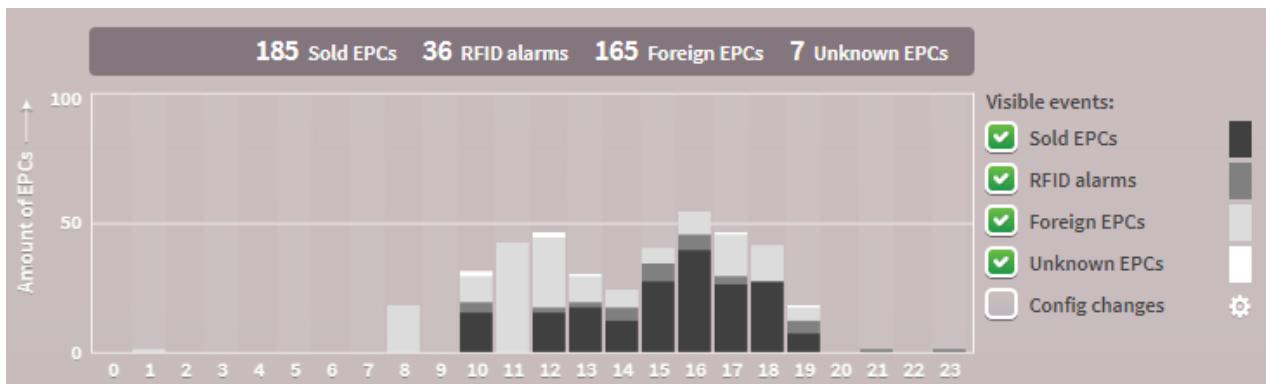
Check the **event list + graphs** & consult **uploaded documentation** in Device Management.

You won't get optimal results by simply reducing the **Alarm Threshold** of the system(s).

Graph entrance 1:



Graph entrance 2:



Entrance 2 has limited visitors but is responsible for more alarms than Entrance 1!

Solution

Since Entrance 2 only handles 15% of the store's traffic but has more alarms than Entrance 1, it is wise to focus on reducing alarm numbers in Entrance 2. This way, Entrance 1 can run at a higher sensitivity as 85% of the labels contributing to your performance figures pass via that exit.

Always analyze the situation before making changes

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 42

Document Last modification date 31 October 2024

Document PDF Exported 31 October 2024 by Nedap Retail | Operations



support-retail@nedap.com

Nedap Sense Guidelines

iSense RFID EAS methods

version 93, March 2025

Introduction	3
Method categories	4
Possible statuses	5
EPC Database	6
iD Cloud	7
EAS database	11
Customer specific	15
Without Database	16
EAS iD	16
Custom EPC prefix	17
Testing	18
Summary	19

Introduction

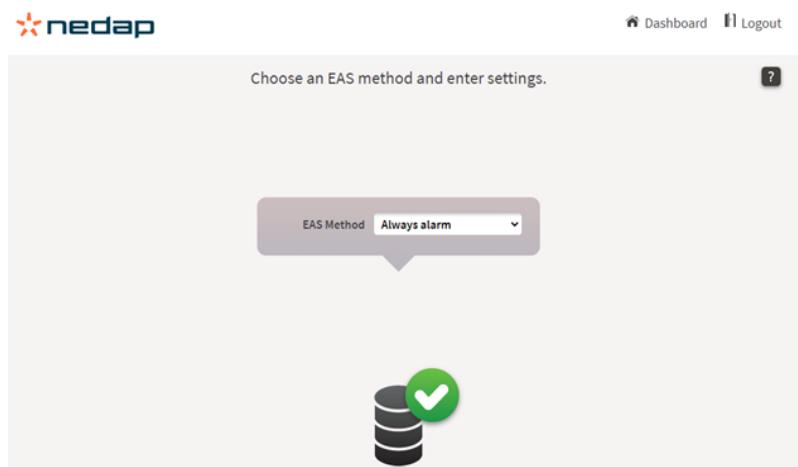
For a successful delivery of an iSense RFID system, it is required to select how the iSense RFID system should respond to specific RFID labels based on the corresponding code on the label: EPC. A correct setup is mandatory, as the iSense system should only alarm on the correct RFID labels. This all depends on the customer's requirements.

The system should generally alarm on “Unsold” items and not “Sold” items. In the iSense configuration wizard, this is called the “EAS Method.”



The “**EAS method**” is how the system determines whether a label is “**Sold**,” “**Unsold**,” or “**Foreign**.”

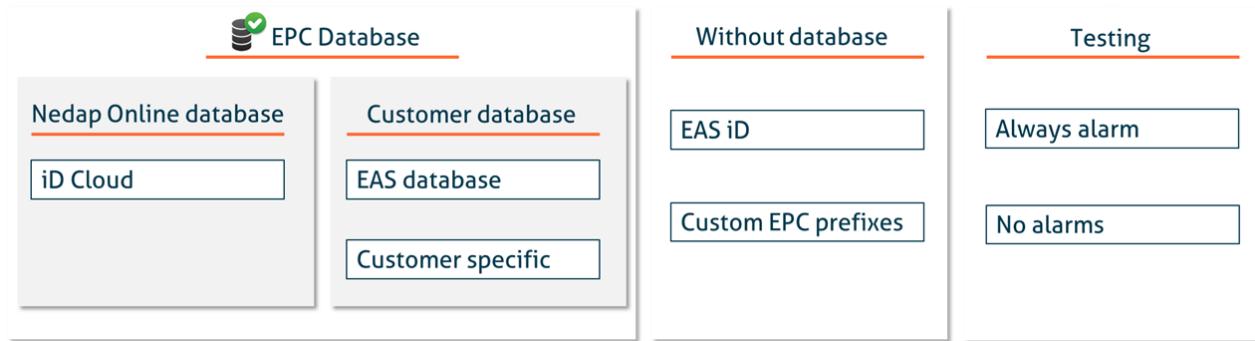
This document explains the possible RFID EAS “methods” that can be configured for iSense RFID systems.



A screenshot of a web-based configuration interface for the iSense system. At the top, there is a navigation bar with the nedap logo, a Dashboard link, and a Logout link. Below the navigation bar, a message says "Choose an EAS method and enter settings." On the right side of this message is a help icon (a question mark inside a circle). In the center, there is a dropdown menu labeled "EAS Method" with the option "Always alarm" selected. Below the dropdown is a large green circular button with a white checkmark inside, accompanied by two dark grey cylinder icons. The overall background of the interface is light grey.

Method categories

There are three main RFID method categories:



EPC Database

When using database deactivation, the iSense system should only make an alarm for labels that belong to that specific store, and others should be ignored. In practice:

1. Goods that arrive in a store should be marked in the database as “Unsold” (for example, they should be read with a handheld reader).
2. When they are sold, the status should change to “Sold.”
3. The iSense system only alarms for labels with an “Unsold” status.

The database options are:

- Nedap Online database (iD Cloud)
- General EAS database
 - Standard TCP
 - WebSocket
- Customer-specific database

Without database

In this case the specific EPC of a label will determine if it is “Sold” or “Unsold”, so without the using a database.

2 options:

- EAS iD
- Customer EPC prefixes

Testing

Specific methods in the system for troubleshooting:

- Always Alarm
- Never Alarm

Possible statuses

Depending on the method, the following statuses are possible in the iSense event list:

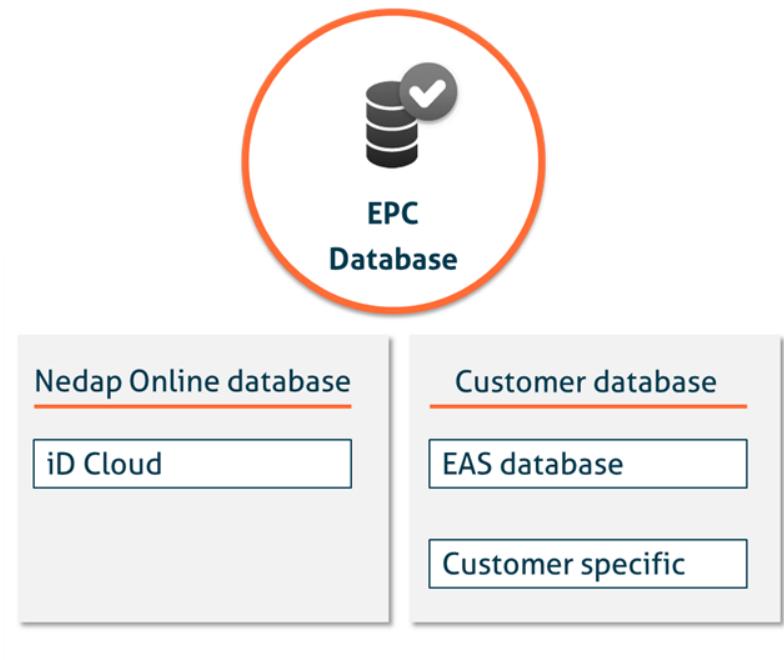
- **UNSOULD (Alarm)**
 - item has not been paid
- **SOLD (No alarm)**
 - item has been paid
- **FOREIGN (No alarm)**
 - This means that the EPC does not exist in the database
- **UNKNOWN (No alarm)**
 - This means that the connection was lost with the database (Or the EPC has a specific iD Cloud status; see iD Cloud chapter)

EPC Database

To use this method, a database should be maintained with all the EPCs currently present in the store. The list is altered basically in three ways:

- When new items arrive in the store, they should be set to “Unsold” so that customers are alarmed when they leave the store without being paid for.
- When sold, items should be set to “Sold”; they should not alarm anymore.
- When customers return items, they should be set back to “Unsold” because they should alarm from that moment on.

There are three options for the EPC database method:

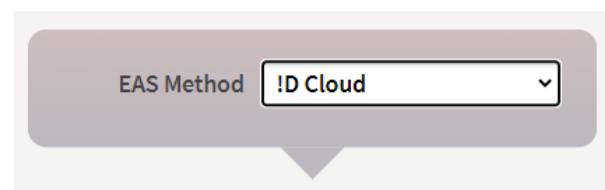
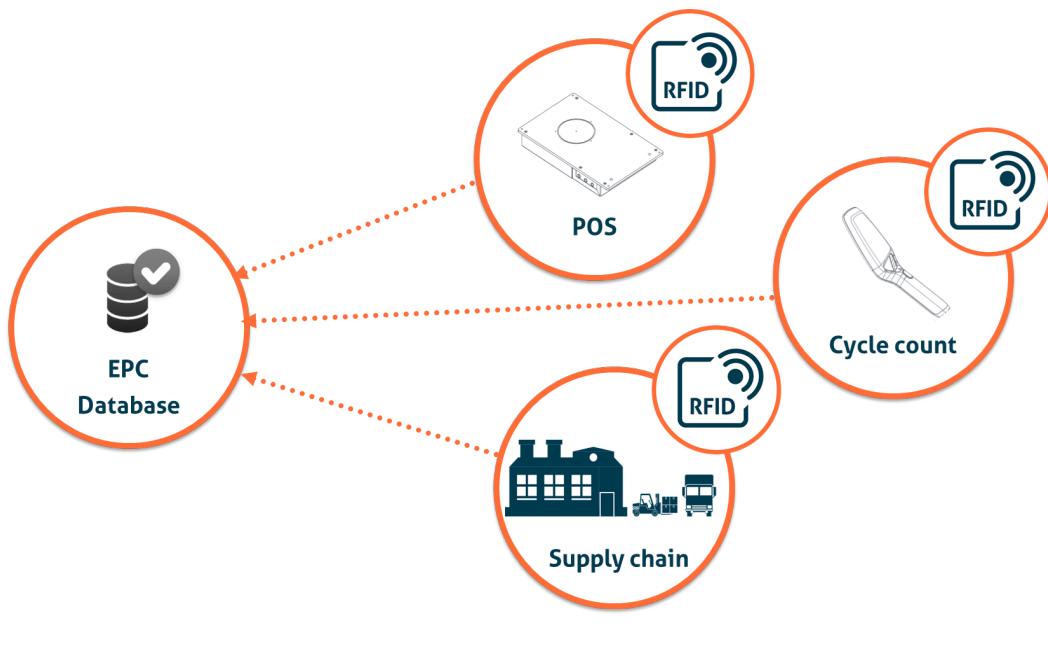


iD Cloud

iD Cloud is the Nedap online / cloud-based EPCIS database. To use iD Cloud as an EAS database, it is essential to keep the stock information updated when new items arrive in the store.

- This is not an issue if the stock information contains more items than are present in the store.
- If the stock information contains fewer items than those in the store, the missing items will be regarded as "Foreign" and are, therefore, not EAS protected.

It is also essential to have a Point Of Sale (POS) integration with iD Cloud to mark sold items as "Sold" and returned items as "Unsold" in the database.



Requirements

- Up-to-date stock information in iD Cloud
- Firmware 20.10 or higher
- POS integration with iD Cloud
- Stable network connection
- The store is connected to Device Management (Online)
- iD Cloud subscription

Nedap labels

Nedap pre-programmed labels also alarm automatically when the EAS method is set to iD Cloud based on the Nedap prefix.

The EPC for a Nedap preprogrammed label always starts with six predefined digits:

Length	Comment	Values
5	Nedap prefix	7EDA9 (fixed)
1	Type	<ul style="list-style-type: none">0 = UNSOLD Active security programmed tag1 = UNSOLD EAS test label; always alarms on Nedap RFID EAS systemsF = SOLD Deactivated security programmed tag

POS integration

The Point Of Sale (POS) must send sale and return information to iD Cloud in real-time: when an item has been sold, it will leave the store quickly.

iD Cloud supports the GS1 EPCIS standard for POS integrations (see for more information).



More detailed information about POS integration is available on request.

Store network requirements

The store needs a fast and reliable internet connection. If the POS cannot report a sale fast enough, the alarm will go off, even if items have been sold.



If the database query takes longer than **500ms**, there will be no alarm, leaving products unprotected.

The 500ms includes not only the database's response time but also the network speed and latency. On a fast internet connection, database query times of under 200ms can easily be achieved.

Store connected to Device Management

During installation, an iSense system is usually not yet associated with the correct store in Device Management. To configure the system correctly, iD Cloud will always return “Foreign” if an iSense system is not associated with a store. Once the system is associated with the correct store, it will use the stock information available in iD Cloud to determine the EAS status for each label seen by the iSense system. It may take a few minutes before the association changes and takes effect.



iD Cloud Subscription

Be aware that an active iD Cloud subscription is required in addition to a store association. If the store does not have a subscription, the EAS status will always be “Foreign.”

Summary

ISense Response	When
UNSOLD	<ul style="list-style-type: none">Status in iD Cloud (Disposition):<ul style="list-style-type: none">"urn:epcglobal:cbv:disp:sellable_accessible""urn:epcglobal:cbv:disp:sellable_not_accessible""urn:epcglobal:cbv:disp:active"
SOLD	<ul style="list-style-type: none">Status in iD Cloud (Disposition):<ul style="list-style-type: none">"urn:epcglobal:cbv:disp:retail_sold"
UNKNOWN	<ul style="list-style-type: none">Other statuses in iD Cloud (Dispositions)No connection to iD Cloud
FOREIGN	<ul style="list-style-type: none">EPC not in iD CloudNo iD Cloud subscription in Device ManagementThe system is not connected to the store in Device Management

EAS database

The EAS database works, in general, the same as the iD Cloud database integration. The major difference is that the EAS database is a protocol for integrating with a general database other than iD Cloud. This can be an online or local database.

There are two options for ‘EAS database’:

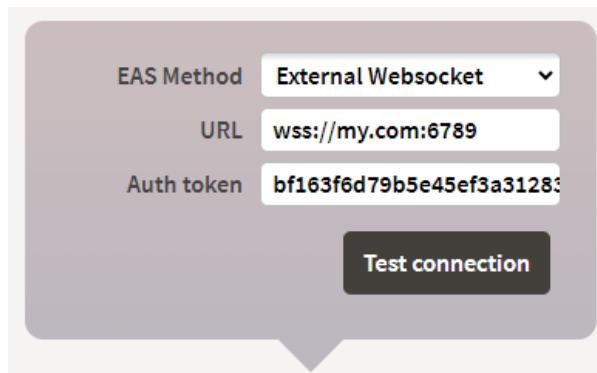
- External WebSocket (Preferred)
- Standard EAS database



It is recommended that you use the ‘External WebSocket’ because it offers added security and is faster and lighter to use.

External WebSocket

To use an external WebSocket, the `URL` and the `Auth token` can be set using the iSense configuration web interface:



Name	Description
<code>URL</code>	<p>It should always start with <code>wss://</code></p> <p>Examples:</p> <ul style="list-style-type: none">• <code>wss://nedap.com/ws/eas_status</code>• <code>wss://yourserver.here</code> <p> Optionally, a port can be added (default <code>443</code> when not entered):</p> <ul style="list-style-type: none">• <code>wss://my.com:6789</code>
<code>Auth token</code>	Any token cannot be empty.

The endpoint that our system will connect to will be in the following format based on the provided `URL` :

<URL>/<systemID>

The `systemID` will be added by the iSense system when a request is made, it is defined by the iSense system at the time it is configured.



A `systemID` might look like `f24c9761-7881-43fd-92cb-f9cac499235b`

When the iSense system requests the status of a label or tag, the full URL, using the examples above, would look like: `wss://my.com:6789/f24c9761-7881-43fd-92cb-f9cac499235b`

The contents of the message:

```
{  
  "epc": "1A2B3C4E5F67890ABCDEF"  
}
```

The WebSocket server should answer:

```
{  
  "epc": "1A2B3C4E5F67890ABCDEF",  
  "status" : "SOLD"  
}
```

Where:

Name	Description
epc	The EPC of the label or tag for which the status is requested
status	The current status of the EPC Either <code>SOLD</code> , <code>UNSOLD</code> , or <code>FOREIGN</code>

The WebSocket connection itself is encrypted but does not prevent anyone from creating a connection to the EAS database service. To improve security, authorization is added. The token is added, setting up the WebSocket connection with the following header:

`Authorization: Bearer <token>`

The actual token is provided through the configuration wizard.

⚠ The server must have a verified certificate, **not** a self-signed certificate. iSense does not accept self-signed certificates.

⚠ The server must have the entire certificate chain available, as the iSense system is not able to load intermediate certificates; this can be checked, for instance, with <https://www.ssllabs.com/ssltest/analyze.html>

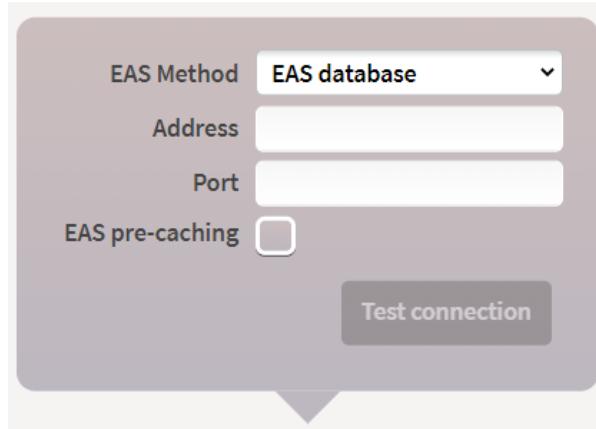
i The connection from iSense to the EAS WebSocket server is started as soon as the iSense system is started. It is checked every 10 seconds, and when it fails, the iSense system reconnects.

i If there is no reply within a 1-second timeout, it will result in `UNKNOWN` events and will not be requested again.

i Sample code of an EAS WebSocket implementation can be downloaded from our portal.

Standard EAS database

The iSense configuration web interface allows you to set the hostname and port number to use the standard EAS database over TCP.



i To prevent timeouts from DNS lookups, it is recommended to use an IP address rather than a hostname, as DNS server hostname resolution - particularly with external DNS servers - can significantly increase response times and risk exceeding the maximum allowed response time.

Connection

The iSense system and the EAS database communication is based on a **TCP socket** connection.

Request message format

```
<message-length-prefix>PTQ,<epc>,
```

Name	Description
message-length-prefix	Five digits, padded with zeros. This is the total message length, excluding this message-length-prefix.
EPC	EPC in binary hex encoding ending with a comma (,)

Request example

```
00029PTQ,3005FB63AC1F3841EC880467,
```

Response message format

```
<status>
```

The response is a number. The message must **not** end with a comma but with a new line.

Name	Description
status	0 = UNSOLD (Alarm) 1 = SOLD (No Alarm)

Response example

```
1
```



Responses should arrive within the 500 ms timeout. Responses that arrive outside this timeout are ignored. Eventually, an issue will also be reported in Device Management.

Cache

The result of the query is cached to reduce the number of database queries: by default, it is cached for 2 seconds for unsold items and 60 seconds for sold items.

Pre-caching

The iSense system also supports a feature called "pre-caching." Enabling this option improves the system's reaction time. Still, it increases the number of queries on the EAS database because it queries the database for labels as soon as it detects them, even if they are not going outside (before filtering).



Pre-caching can be used for a maximum of 8 gates/tops per system.



Sample code of an EAS database implementation can be downloaded from our portal.

Customer specific

This is very similar to the EAS database; however, the integration protocol with the customer database is more customer-specific. In the iSense wizard, you can find the specific names for that (e.g., Decathlon v2, Tyco, etc.). Please follow the key account guidelines to determine what is required.

For more details about these protocols, please contact Nedap Retail support.

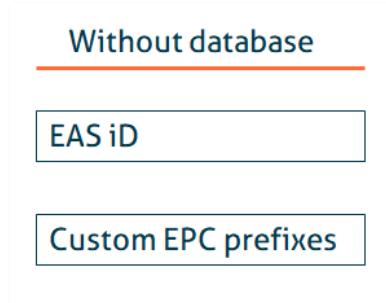


The Tyco database method also alarms on the Nedap prefix.

Without Database

When a standalone solution is required without a database, there are two options.

- EAS iD
- Custom EPC prefixes



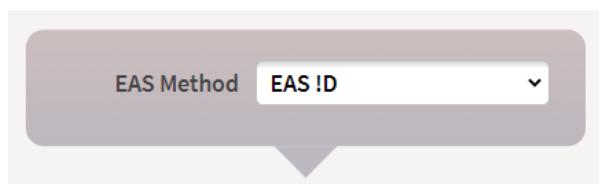
EAS iD

EAS iD is a Nedap-specific protocol that determines whether or not labels should alarm based on the EPC or code in the RFID label's USER memory.

The EPC for a Nedap preprogrammed label always starts with six predefined digits:

Length	Comment	Values
5	Nedap prefix	7EDA9 (fixed)
1	Type	<ul style="list-style-type: none">• 0 = UNSOLD Active security programmed tag• 1 = UNSOLD EAS test label; always alarms on Nedap RFID EAS systems• F = SOLD Deactivated security programmed tag

Pre-programmed EAS iD labels can be ordered at Nedap. When sold, the labels can be deactivated with the ID POS.



Usage of iD POS

The iD POS can be set to two different modes of operation:

- Deactivation - The label is set to `SOLD`
- Activation / Return - The label is set to `UNSOLED`



Not all RFID labels support iD POS deactivation; refer to the iD POS documentation for specific information.

Custom EPC prefix

Two other options are available that will specifically alarm based on the EPC, which is very useful for hard tags.

Custom EPC prefix

It is possible to set a custom EPC prefix. All EPCs that start with the set custom prefix(es) will alarm; all EPCs that begin with another prefix will not alarm.

For example, if the set prefix is 8EDA, then all labels with EPCs that start with 8EDA will raise an alarm, and other EPCs will not.

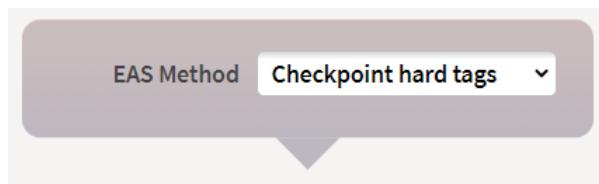


It is possible to add a maximum of 5 EPC prefixes.



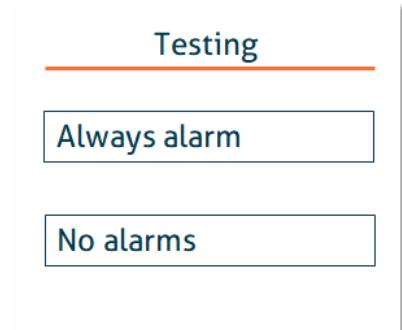
Checkpoint hard tags

Checkpoint RFID hard tags use a GIAI-96 encoding, with a specific Company Prefix. In HEX these EPCs always start with `340832B06124`, `E280` or `000000000000`. The system only alarms to those hard tags, not to other RFID labels.



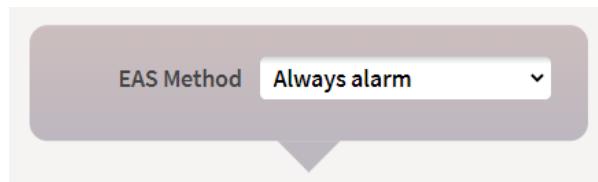
Testing

Testing is only meant for troubleshooting or testing. These methods should never be used as a fixed setup.



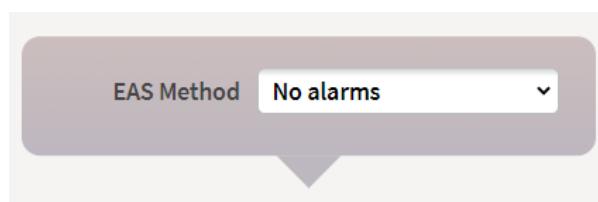
Always Alarms

Every RFID label will give an alarm.



Never Alarm

No RFID label will give an alarm.

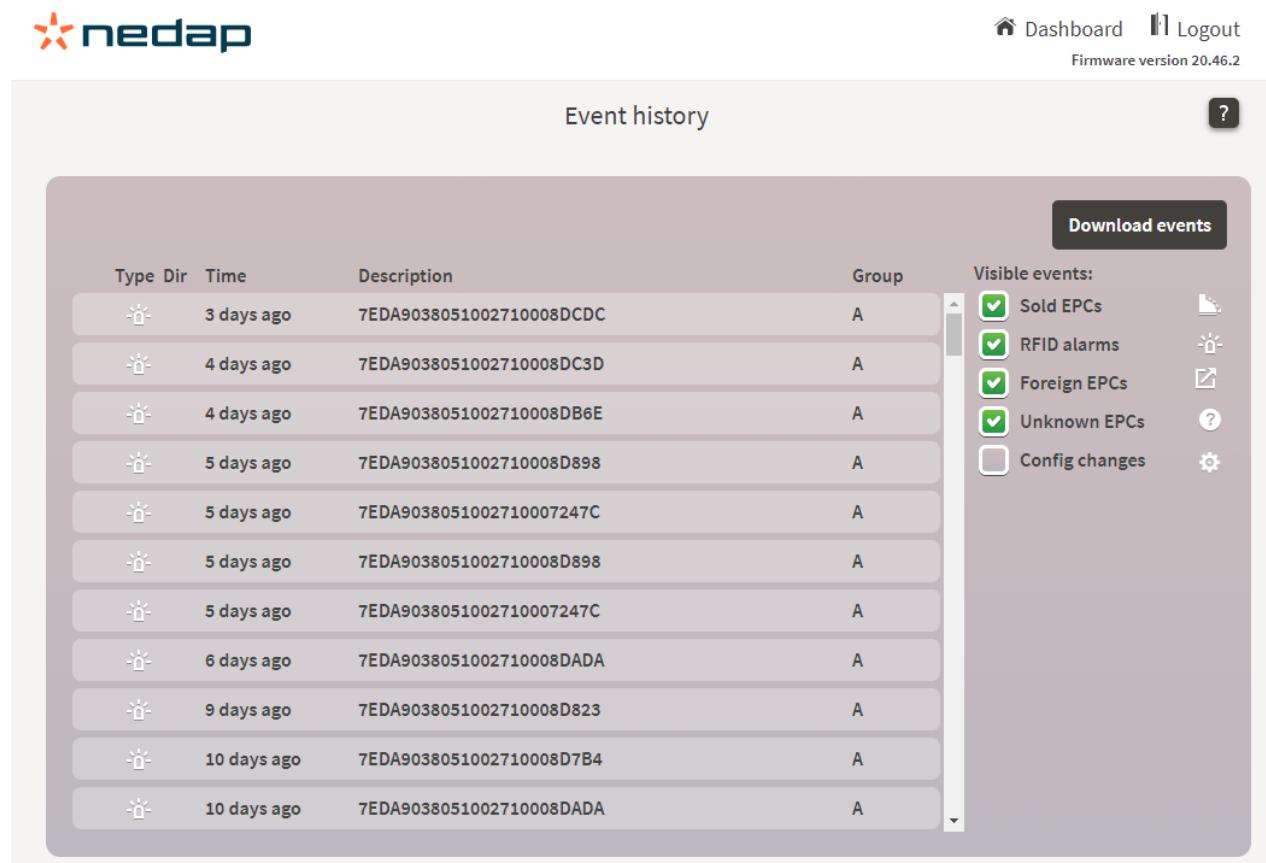


Summary

Summary of all methods and possible statuses in the event list.

Method	Category	Purpose	Possible Statuses (Event List)
iD Cloud	Database (Nedap online EPCIS database)	Alarm on specific labels that are in the database	<ul style="list-style-type: none"> • UNSOLD • SOLD • FOREIGN • UNKNOWN
EAS Database	Database (Customer-specific database based on Nedap protocol)	Alarm on particular labels that are in the database	<ul style="list-style-type: none"> • UNSOLD • SOLD • FOREIGN • UNKNOWN
Customer specific	Database (Customer specific database and customer-specific protocol; e.g., Decathlon v2)	Alarm on specific labels that are in the database	<ul style="list-style-type: none"> • UNSOLD • SOLD • FOREIGN • UNKNOWN
EASiD	Without database	The alarm on Nedap-specific label EPCs (e.g., Hard-tags)	<ul style="list-style-type: none"> • UNSOLD • FOREIGN
Custom EPC prefixes	Without database	Only alarm on specific EPC prefixes (e.g., Hard-tags)	<ul style="list-style-type: none"> • UNSOLD • FOREIGN
Always alarm	Testing	Testing only - alarm on all RFID labels	<ul style="list-style-type: none"> • UNSOLD
No alarms	Testing	Testing only - no alarm on all RFID labels	<ul style="list-style-type: none"> • SOLD

Events are visible in the iSense event list; see the example below.



The screenshot shows the 'Event history' section of the nedap iSense interface. At the top right are links for 'Dashboard' (with a house icon) and 'Logout'. Below that is the text 'Firmware version 20.46.2'. The main area is titled 'Event history' and contains a table of events. The columns are 'Type', 'Dir', 'Time', 'Description', and 'Group'. The 'Time' column shows dates from '3 days ago' to '10 days ago'. The 'Description' column lists EPC codes. A 'Download events' button is at the top right of the table. To the right of the table is a sidebar titled 'Visible events:' with checkboxes for 'Sold EPCs', 'RFID alarms', 'Foreign EPCs', 'Unknown EPCs', and 'Config changes'. The 'Config changes' checkbox is unselected.

Type	Dir	Time	Description	Group
!		3 days ago	7ED...DCDC	A
!		4 days ago	7ED...DC3D	A
!		4 days ago	7ED...DB6E	A
!		5 days ago	7ED...D898	A
!		5 days ago	7ED...7247C	A
!		5 days ago	7ED...D898	A
!		5 days ago	7ED...7247C	A
!		6 days ago	7ED...DADA	A
!		9 days ago	7ED...D823	A
!		10 days ago	7ED...D7B4	A
!		10 days ago	7ED...DADA	A

iSense Event List

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap NV 2025

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 93

Document Last modification date 25 March 2025

Document PDF Exported 25 March 2025 by Nedap Retail | Operations



support-retail@nedap.com

Connected Devices Guideline

iSense RFID Configuration and Trouble Shooting

version 127, June 2024



Introduction	3
RFID configuration Wizard	4
Preparation	4
Configuration steps	6
Nedap RFID test tag.....	19
Nedap RFID test tag behavior	19
How to use these Nedap RFID test tags?	19
Tag details	20
Ordering Nedap RFID test tags	20
RFID Troubleshooter	21
No Detection or unstable performance	21
False alarms	25



Introduction

This document explains in detail how to use the RFID configuration wizard for firmware version 20.46.2 and higher, including:

- Nedap RFID test tag
- RFID troubleshooting

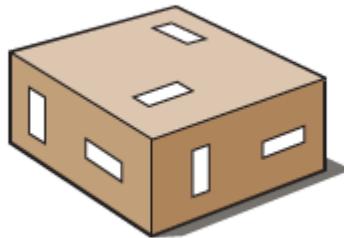
RFID configuration Wizard

To optimize and standardize RFID Electronic Article Surveillance (RFID EAS) installations, a configuration wizard is available.

Preparation

For a successful RFID EAS configuration, the following items are required:

- Carton test box (included with all iSense RFID products)
- A minimum of 6 RFID labels that are used in the store
- Tape (make sure not to use metal tape!)
- Prepare the box as instructed: place the labels on the indicated positions with tape to the box (about 10 cm apart)



(i) For an optimal configured system, it is recommended to use the same label types as used in the store. What labels to use for calibration?

- use (blank) RFID labels from the retailer
- use a stack of (removed) price tags from the retailer
- use a couple of (small) items from the retailer to stick the price tag to the calibration box (or a larger box if preferred)
- RFID labels for calibration are arranged by retailer and/or Nedap
- Perform calibration runs without the calibration box and use a shopping bag instead

(i) If multiple types of labels are used in the store, choose the most commonly used labels, as they have the largest impact on performance. The consequence may be that weak labels perform poor or that strong labels give more false alarms. Try to find the right balance.

⚠ If there are no usable labels in the store, a second store visit is needed, as this has a big impact on the behavior and settings of the system.



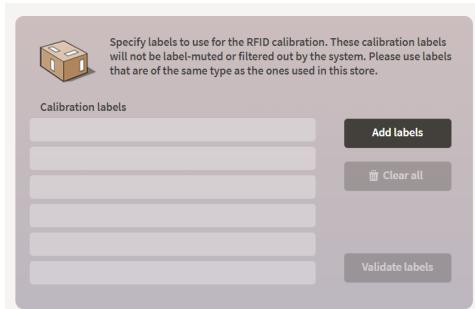
It is highly recommended to capture images of the store setup, encompassing the entrance(s) overview, power inserter placement, and nearby environmental factors (e.g., metal objects, tempered glass, close by self-checkout stations). These images can then be uploaded in PDF format to Device Management at the store level. This information will help significantly in case of support questions in a later stage.

Configuration steps

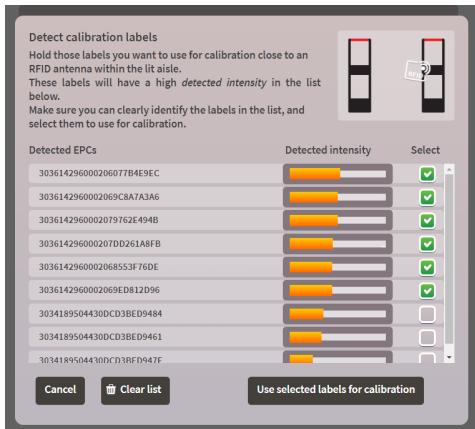
1. Select and verify test labels

Select the test labels to be placed on the test box (calibration labels).

- Click "Add labels" to add the calibration labels.



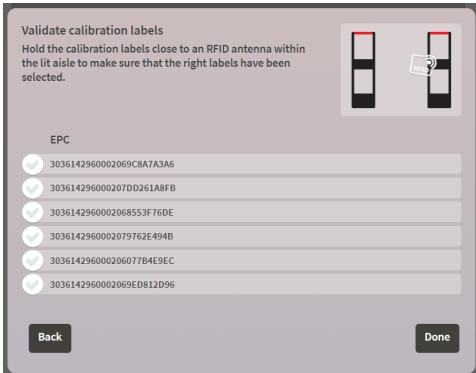
- Add calibration labels by rotating the calibration box close to the gate or top that is blinking red, so that you can easily find your calibration labels in the overview (recognized by the strongest signals). The strongest signals will be stored in the overview; turn the calibration box close to the antenna.



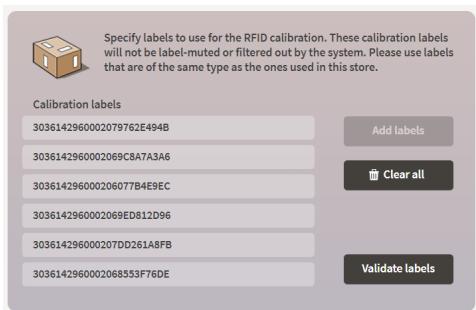
if you know the exact EPCs, you can also check that you have the correct labels based on the EPCs

- Select the 6 labels from the calibration box to be used for calibration. The 6 calibration labels on the box appear at the top of the list.
- Move the box at least a few feet/80-100 cm away from the gates, or tops, and click "Use selected labels for calibration" and continue.

- Validate if the selected labels are the labels on the test box. Move the box back to the gates or tops and check if they are all marked green.



- When the system has detected all calibration labels, the following screen is displayed.



The configured calibration labels are **never muted or filtered** by the system. They will always trigger an alarm, even after the configuration is complete. This will help to test the system and check the performance.

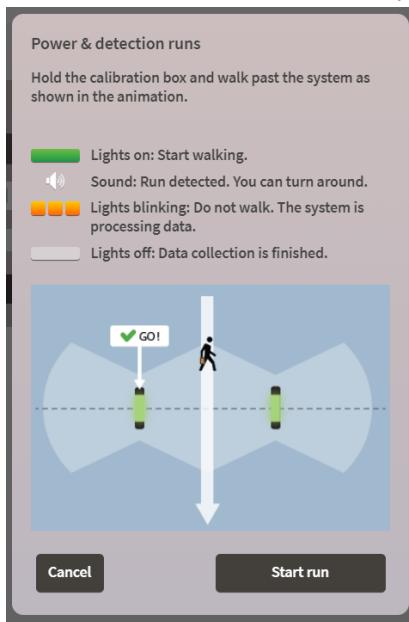
- The next screen provides an overview of all RFID settings per group and for the system that are relevant for label detection. To configure the specific group, press the configure button:



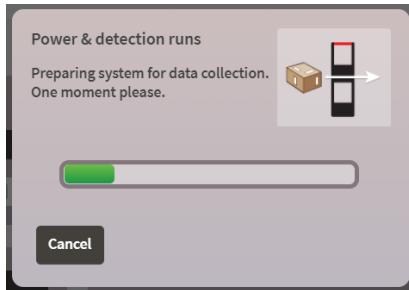
2. Optimal Power Finder

The system will help you find the best power setting, based on the calibration runs you make while walking with the calibration box.

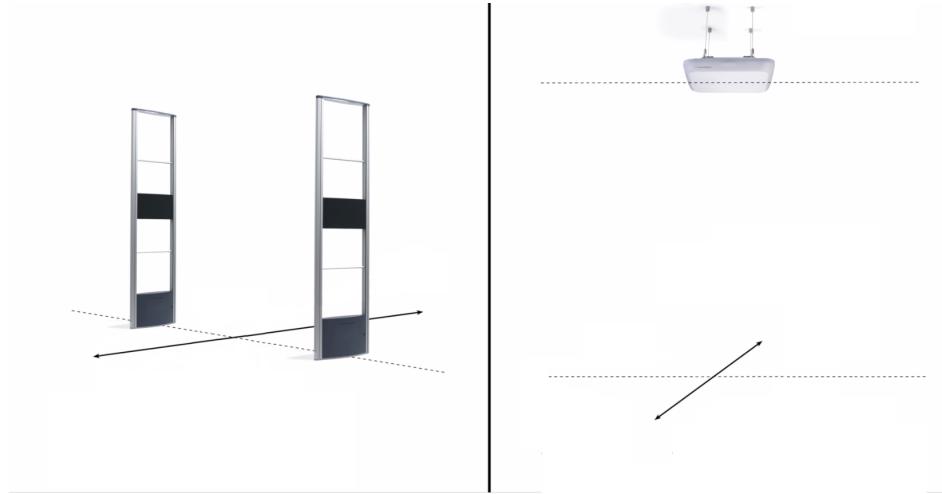
- Start the optimal power finder and read the instructions.
- Press the "Start run" button when you are ready to go.
- Follow the instructions. The complete procedure usually takes about 4 minutes.



- Wait for the system to be ready.



- Walk with the calibration box through the aisles (or under the top), when the lights are on according to the instructions. Hold the calibration box in a way that it resembles the customer behavior for this store. Keep walking until you hear the sound to turn around.



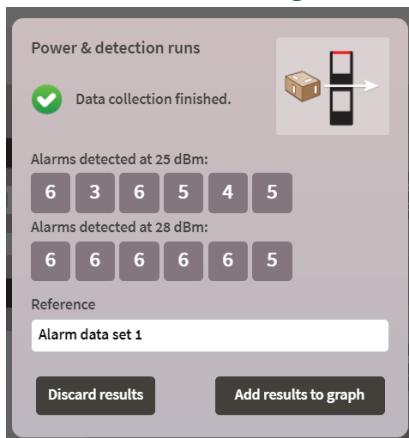
- With each run, the system shows the number of calibration labels it has detected. After a few runs, the power will be changed according to the labels collected in each run.



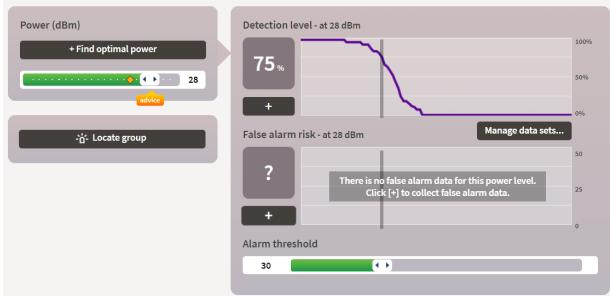
Changing the power takes some time. Carefully follow the signaling on the gates or tops and do not start walking while the lights are blinking.

- The power increases if the number of calibration labels is less than desired.
- If 6 calibration labels are displayed with each run, the power may be too high and the risk of false alarms will increase.
- It is important to have a balanced power setting.

- After the lights finally dim, you will see the “Data Collection Finished” screen which shows the number of labels detected during each run with the selected power.



- Click on the "Add results to graph" button.



(i) In the top left corner you will see the selected power level. In the same bar, the runs at the other power levels are visible as orange squares.

The "*Detection level*" diagram on the right shows the graph of the collected results for the selected power level.

With the "*Alarm threshold*" slider you can determine what the detection level will be. In this case 75%.

What does that mean? In this case, only 75% of all labels seen at this power level will generate an alarm. Moving the "*Alarm threshold*" slider to a lower value will improve on the detection level.

- Now you can change the Alarm threshold

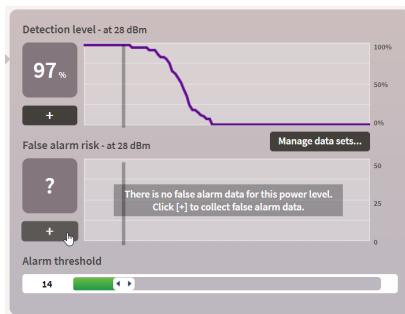


(i) In the example, the detection level is set to 97%. It is not clear at this moment if this is a save setting as it depends of the amount of false alarms.

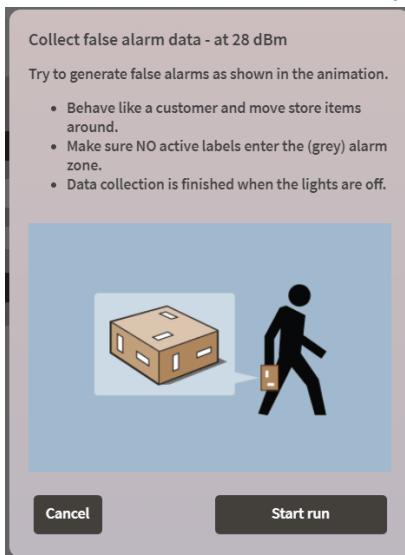
3. Retrieve False alarms

Now it is time to retrieve false alarms, read the instructions carefully.

- Press the “+” to start with the false alarms run



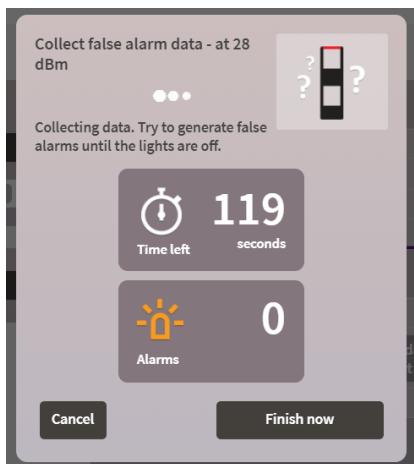
- Press the “Start run” button. The entire procedure takes 2 minutes. Make sure the calibration box is not too close to the antenna's when you start.



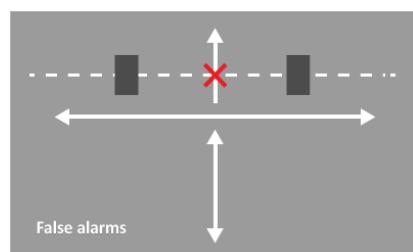
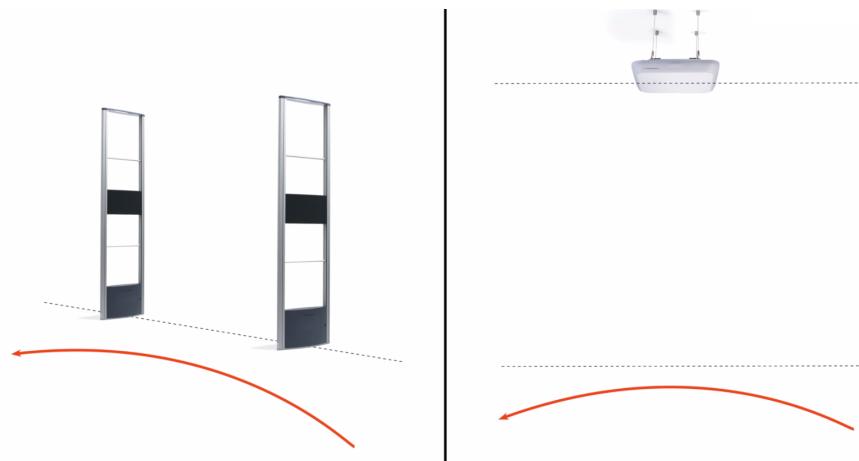
- The system prepares the False Alarms process.



- When it is ready, you can start walking according to the instructions. You have 2 minutes to complete the run.



Do not walk through the aisles with a label once the run has started!

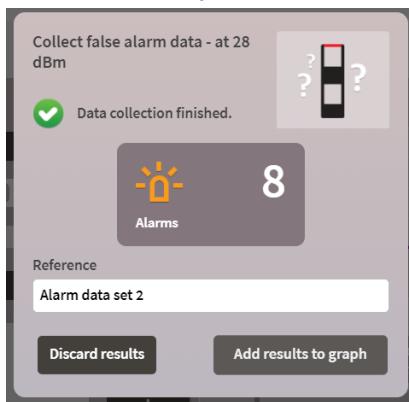


- Walk through the store and move around with items from the store to simulate real situations that should not generate a false alarm.
- Pretend what a customer would do in the store.
- The goal is to simulate normal customer behavior as much as possible and not necessarily have a large number of false alarms.

- If there are no labels close to the gates or tops, it is fine if few alarms are found during this test.



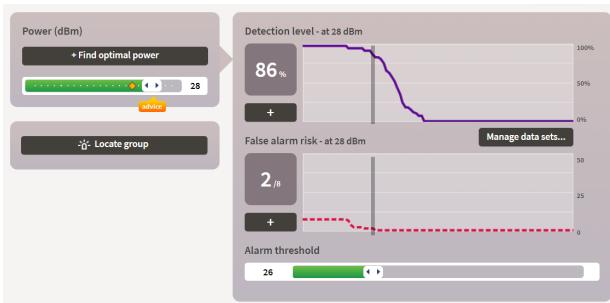
- After 2 minutes you will see the results of this run.



No false alarms during a run? It is a perfect store or you did not follow the procedure...

- Click on "Add results to graph" and you will see the updated overview.





i The "*False Alarm Risk*" diagram on the right shows the graph of collected results for the selected power level. The "*Alarm threshold*" slider allows you to determine the risk of detecting false alarms. In this case 8 out of 8.

What does that mean? With the current "*Alarm Threshold*" set to 97%, 97% of all labels at this power level will alarm, but the system will also alarm in all (8 out of 8) situations as created during the false alarm test.

It can be useful to add some extra runs by pressing the "+" button, this will add extra lines in the graphs. For instance with another walking position in the same group or with different labels/items.

- Does the output surprise you? Maybe something went wrong?
- Were the runs you made representative of how a normal customer would act?
- Are the labels from the store?
- Moving the "*Alarm Threshold*" slider to a higher value decreases the detection performance, but also reduces the risk of false alarms.

What is the best practice? The best practice can differ per store. Does the customer want an aggressive system with a higher risk of false alarms or perhaps a more defensive system?

- Test the system with the calibration labels and fine tune if necessary: choose a higher threshold to reduce false alarms and a lower threshold to reduce missed alarms.
- Changing the power level will not throw away the collected data as it will be stored with the corresponding power level, experimenting with the settings is allowed.

The button "*Manage datasets...*" allows you to see which datasets are collected and, if necessary, delete one or more datasets.

4. Repeat for all groups

- Press the "Apply changes" button.
- Press the "Finish group" button.



- Follow the same procedure for the other groups until they are all done.
- When all groups are finished, continue and perform the final test.

System behavior settings at the "Calibration overview" page

Static item filter Filters out RFID tags that are observed multiple times. These tags will not alarm. A tag enters the static item filter when it is seen for multiple times within the static item forget time and when at least 4 minutes have passed since the first observation of the tag. A tag is removed from the filter when the tag has not been seen during the static item forget time.

Forget time The static item filter filters tags that are seen for at least 4 minutes with breaks of no longer than <static item forget time>. When a tag becomes filtered, it needs to be unseen for <static item forget time> before it is removed from the filter.

Chaos filter Filters RFID tags that are moving rapidly between inside and outside the store.

- ##### To find muted labels use an iD Hand: Configure the iD Hand with the iD Hand App to read with **Session 1, Target A** and Select **Deasserted**.

5. Determine the final performance

- Walk out of the store with the calibration box and check in the "event list" how many labels have been detected.
- Repeat this 5 times and calculate the performance as follows:

$$(\text{[Number of EPC's seen in the event list]} / (\text{[Number of labels on the box] } \times \text{ [Number of runs]})) \times 100\% = \text{Performance \%}$$

In the example below you can find the 6 calibration labels in the test run, so in that case it is $(6 / 6) \times 100\% = 100\%$ EPC Level Performance



Type	Dir	Time	Description	Group
...	...	10 sec ago	3036142960002068553F76DE	A
...	...	10 sec ago	303614296000206077B4E9EC	A
...	...	10 sec ago	3036142960002079762E494B	A
...	...	10 sec ago	3036142960002069ED812D96	A
...	...	10 sec ago	3036142960002069C8A7A3A6	A
...	...	10 sec ago	303614296000207DD261A8FB	A
...	...	19 sec ago	303614296000206077B4E9EC	A
...	...	20 sec ago	3036142960002079762E494B	A
...	...	20 sec ago	3036142960002069ED812D96	A
...	...	20 sec ago	3036142960002069C8A7A3A6	A
...	...	20 sec ago	3036142960002068553F76DE	A

6. Summary

- Use 6 labels from the store
- Run the optimal power finder and use the advice of the finder
- Collect the complete false alarm run with customer behavior
- Choose a threshold that suits the customer's needs (performance vs false alarm risks)



It is recommended to do three test runs per group . For these test runs you may want to consider quoting 1 hour per store (+30 minutes per extra group).

Power

On the RFID calibration page, including all graphs, a button "Advanced" is located in the top right corner. This button allows you to view the power related to the number of labels in the field.

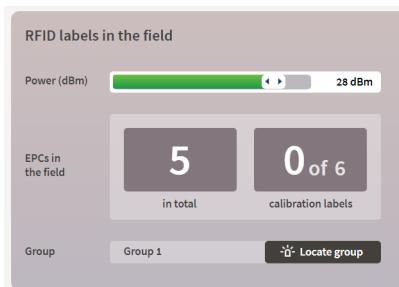


You can see the number of labels being read:

- *EPCs in the field - total:* all labels within the detection area
 - These labels will be, or are already muted by the system. If they are muted, they will **not** generate an alarm
 - If more than 15 labels are detected, the detection performance of the system will be affected
- *EPCs in the Field - Calibration Labels:* This shows how many of the calibration labels have been detected



It is important to understand that the other labels (except the 6 calibration labels) will be muted after the system is delivered, as they are constantly in the RFID field and therefore will **not** generate an alarm.



Low power

- Lower detection of shielded labels and labels in difficult orientations.
- Smaller area: Fewer labels in the store will be muted (not protected by EAS).
- Use low power when there are many labels around the system.

High power

- Better detection of shielded labels and labels in difficult orientations.
- Larger area: More labels in the store will be muted (not protected by EAS).
- Use high power when there are few labels around the system.

Beam Steering V2

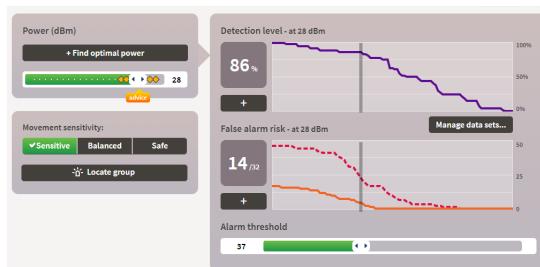
In case of Beam steering v2 (default for iD Tops), another option will show up on the configuration screen, which is “*Movement sensitivity*”.

This is an additional filter option to find the optimal setting based on the gathered data.



Below you can see an example with all 3 possible settings, the graph changes based on the selected filter so you can choose the optimal one for the store.

Sensitive



Balanced

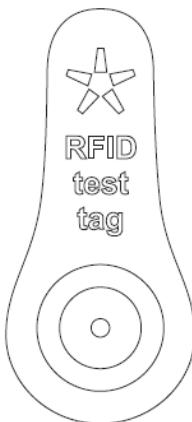


Safe



Nedap RFID test tag

Testing RFID systems can be difficult: when a store label is used for testing, the label could be *tag muted* when it was located close to the RFID system. In this case, no RFID alarm will be raised, however the RFID system could still be functioning perfect. Nedap RFID test tags make it possible to reliably test the RFID functionality.



Nedap RFID test tag behavior

The Nedap RFID test tags:

- **behave like regular tags:** in case of beam steering, they raise an alarm when they move from inside to outside the store, but not when they move in the opposite direction.
- will **never be tag muted** by the system.
- will still **raise an alarm** even if there is an issue with the configured EAS database.
- only function for iSense systems with firmware **16.30 or higher**.

How to use these Nedap RFID test tags?

- For demonstrating RFID functionality to a sales prospect or to a retailer when delivering a system.
- For troubleshooting RFID issues: If the Nedap RFID test tag raises an alarm but other tags do not, this is probably due to tag muting or to an EAS database issue. If the Nedap RFID test tag does not raise an alarm then this might indicate a power, hardware or configuration issue.



Leave a Nedap RFID test tag at a retailer after a system installation, so he or she can test whether the RFID system is functioning correctly.



Tag details

- The EPC of these Nedap RFID test tags starts with '**7EDA91**'.
- There is a Region 1 version and Region 2/3 version. Make sure to order Nedap RFID test tags that correspond to your region.

Ordering Nedap RFID test tags

They can be ordered via the Nedap Retail portal with the following article numbers:

- 9221433 (Region 1)
- 9221441 (Region 2+3)

RFID Troubleshooter

If the system does not function as expected, it could be for various reasons. There can be 2 major problems:

- No detection or unstable performance
- False alarms

Below are possible reasons and solutions to resolve these issues.

No Detection or unstable performance

See below the most common issues / errors for no detection or unstable performance.

Database

When a database is used, it is an essential part of EAS performance. If the database is not responding properly, it may cause poor performance.

The status of the database can be checked in the configuration wizard and information about the status of the database connection is also visible through Device Management.



The event download from iSense shows a column that shows the response-times for every database access. This can be very helpful

Problem	Solution
Incorrect selected EAS database	<ul style="list-style-type: none">• Select correct database in the RFID mini wizard• Set correct IP and port number in the RFID mini wizard
Wrong response from EAS database	<ul style="list-style-type: none">• Check if correct database is selected in the RFID mini wizard• Verify with Database responsible person (e.g. IT from Customer)
No response from EAS database	<ul style="list-style-type: none">• Check if network is setup correctly• Verify with Database responsible person (e.g. IT from Customer)
Slow response from EAS database	<ul style="list-style-type: none">• Check if network is setup correctly• Download the Event History and check the <code>Database response time (ms)</code> column• Verify with Database responsible person (e.g. IT from Customer)

System settings

The settings determine if the system will perform properly based on the environment of the store.

Problem	Solution
Low power value	<ul style="list-style-type: none"> Change settings in the RFID mini wizard
High filter value	<ul style="list-style-type: none"> Change settings in the RFID mini wizard
RFID reader errors	<ul style="list-style-type: none"> Check RFID hardware (RFID reader)
RFID coax cable error	<ul style="list-style-type: none"> Check cables and recheck RFID cable detection in the wizard

Improper testing

Problem	Solution
Improper test movement	<ul style="list-style-type: none"> Walk from in the store to completely out the store. From out the store to in the store will not raise an alarm (beam steering)
System is not alarming because of body shielding (RFID label is not visible for the system)	<ul style="list-style-type: none"> Test with RFID labels on the side of your body that is visible to the tops or gates
Muted labels	<ul style="list-style-type: none"> Move the labels far away from the system for more than 5 minutes before you test again Use the calibration labels or the Nedap RFID tag to test the system

Reflections

The system can alarm via reflections on items that are actually still in the store. This is because all beams can be reflected by an object to a label, the system concludes that this is a moving label when in fact it is not.

Finding reflections can be quite difficult, some tips that can help you find them:

- What happens in the store when the system triggers an alarm? (for example: do people walk in and out at that moment)
- Use an RFID power mapper to find hot spots
- Check the number of EPCs seen in the event list
- Do you see (metal) objects close to the system that might cause reflections

Problem	Solution
RFID reflections to metal objects	<ul style="list-style-type: none">• Change position of the gate/top• Move or remove reflective metal objects
Hot spots	<ul style="list-style-type: none">• Change position of the gate/top• Move or remove reflective objects• Move or remove labels from specific places

Labels

Problem	Solution
Muted labels	<ul style="list-style-type: none">Move the labels far away from the system for more than 5 minutes before you test again. Use the calibration labels or the Nedap RFID tag to test the systemLower power to prevent muted labels
Wrongly programmed	<ul style="list-style-type: none">Put system on “always alarm” to see if it alarmsCheck EPC codes to see if they match with expectations for database settings
Label Quality	<ul style="list-style-type: none">Test with wizard graphs to see general label performanceUse a reference label to see the performance

False alarms

See most common problems / mistakes for unwanted alarms below.

Database

Problem	Solution
Wrong feedback database sold / unsold status	<ul style="list-style-type: none">Check with IT department regarding the data in the EAS database (you can check the history first in the technical dashboard)
Wrong database selection (e.g. always alarm)	<ul style="list-style-type: none">Check RFID wizard for current settings

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Document Version 127

Document Last modification date 3 June 2024

Document PDF Exported 3 June 2024 by Nedap Retail | Operations

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.



support-retail@nedap.com



Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com

Nedap Sense Guideline

Roadmap for iSense RFID

installations

version 43, October 2024

Introduction	3
Training	4
Sales / Preparation	5
Customer understanding	5
RFID labels	6
EAS method and integrations	7
Example setups	8
Network	9
Products	9
Cabling	10
Store environment / Pre-store visit	10
Other / Customer Expectations	11
Installation.....	12
Physical Installation	12
Configuration	13
Hand over	14
After Care	15
Follow up	15

Introduction

This document explains the important points to realize successful iSense RFID EAS projects.

RFID EAS projects are generally more complex and require closer cooperation with the retailer (a more consulting role including expectation management).

- (i)** This document is created for local accounts where a Nedap-certified business partner is in the lead. This means this document is unrelated to global Nedap Retail RFID key account installations.

This document contains the most important points per phase:

- Training
- Sales / Preparation
- Installation
- Hand over
- After care

(i) For additional installation details, dimensions, precautions etc., please consult the manuals of the gates and iD Top, available at the Partner Portal.

(i) For additional details on the configuration, Device Management and network settings etc, please consult the available guidelines at the Partner Portal.

(i) For details on GTIN and EPC standards, please consult the available knowledge base documents at the Partner Portal.

Once the steps above have been completed, it would be helpful to meet with a Nedap representative who can assist and advise during the entire project.

Training

The basis for a successful RFID project is to have knowledge about iSense, iSense RFID, and RFID in general. To achieve this, the following information and trainings are available at the Partner Portal:

What
E-learning modules (online)
iSense classroom training (offline)
Technical documentation
Technical videos



To gain access to all relevant information you first need access to the Partner Portal!
The Nedap Retail Academy can only be accessed via the Partner Portal.



Based on finished trainings, more options might come available within your Nedap Retail Account.

Sales / Preparation

In the sales and preparation phase, it is important to get complete clarity about the customer's issues and problems that need to be solved (consultancy role).

Also, in this phase, managing expectations and defining a straightforward process is vital.

Customer understanding

One of the first things to find out, is how far the customer already is with RFID and their plan going forward in the following months / years. Based on the answers, what they are currently using to advise on the correct products to solve their problem needs to be clarified in detail.

What	Remarks
What is the main reason for the customer to work with RFID?	For example: <ul style="list-style-type: none">• Because they want to leverage source tagging for EAS to get rid of hard tags• They also want to use RFID for stock management• Prepared for future developments (e.g. self-checkout)• Having an open entrance (overhead solution)• etc.
Which products does the customer want to protect?	Understand the most important products / garments the retailer wants to protect. You can advise on suitable RFID labels / hard tags based on this information.

RFID labels

Find out what the customer has or will get regarding RFID labels. This is needed as input to set up the complete system and which products to choose.



Especially **Quality** and **Coding** of the labels is important to know

What	Remarks
Hard tags and / or labels?	This is required information to determine the best setup. For example, if hard tags are added to source-tagged items, the hard tags might also be RF. This can be facilitated with a Hybrid iSense system.
Type of label(s) (antenna, chip, supplier) ¹	To determine the label types used in the store to determine if the quality is similar for all labels in the store or not. This is important to know from a performance point of view. Label quality can also be tested at Nedap Retail.
Is the customer tagging the products (e.g. with Nedap preprogrammed labels / tags) or do they buy source tagged products from other brands?	It is important to know the range of company prefixes that are used in the store to know on which labels to alarm specifically.
Does the customer follow the GS1 standard correctly? ¹	All Nedap products follow the GS1 standard for Retail.

¹ Read the *RFID Knowledge base documents* on the *Partner Portal* for more information.

EAS method and integrations

Next is to determine how and when the system should alarm and if integrations are required. Best is to make a visual presentation of the setup.



EAS method is the way the system responds to a specific EPC, for more information see the RFID EAS Methods document on the Partner Portal

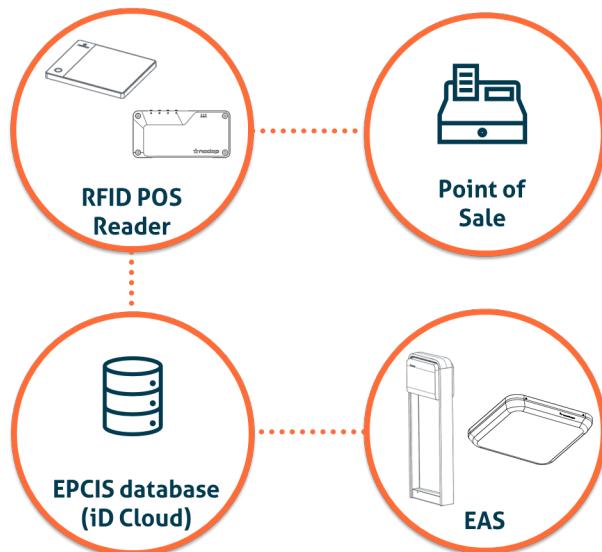
What	Remarks
Standalone EAS, or EAS Database involved? <ul style="list-style-type: none"> • iD Cloud* • Customer specific <ul style="list-style-type: none"> • General protocol • Key account protocol 	Standalone with hard tags or connected to a database. This has an impact on the configuration of the system. This may also require specific integrations.
POS integration required?	When a database is used, POS data must also end up in the same database to set items to “Sold”. This can be done with a 2D barcode scanner or a Nedap POS reader that is integrated with the POS.
Data integration needed? <ul style="list-style-type: none"> • Analytics API • Reporting (e-mail / SFTP) • iSense API 	External data required? This can be done in different ways. Discuss upfront with the customer if this is needed. This involves additional subscription fees (except for the iSense API).

*Alarming with iD Cloud can be done in 2 ways:

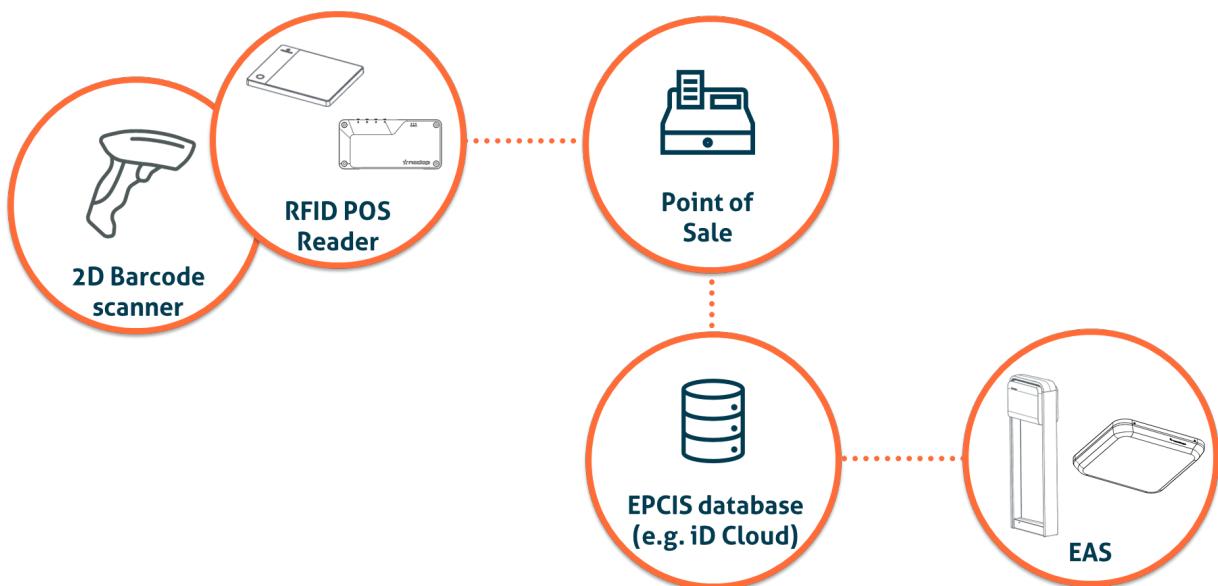
- Alarm on company prefix and exclude sold items at POS.
- Alarm on item level, which means that every item should be added to the database

Example setups

- Database connection via RFID POS reader



- Database connection via POS



Network

For most RFID EAS installations, an exemplary network setup is required. Make sure the details are discussed with the customer in an early stage.

What	Remarks
Network information from the customer (IP address, gateway, etc.)	Check the network availability and required settings with the customer. Also check if there are specific requirements (e.g. proxy)
Discuss firewall information with the customer	Make sure that the customer understands the information in the document " Online Services - Network Information and Connected Systems " which can be downloaded from the Partner Portal.
Database information (IP and port) if applicable	IP addressed is preferred over a hostname for Database connections to increase the speed of the connection.

Products

What	Remarks
Gate (which?) or iD Top installation	Depending on the store layout and wishes of the customer.
Other hardware / integrations? (e.g. RF, MD, IR CC, External CC, API, IO Box, Pager, etc.)	Depending on wishes of the customer.
Subscriptions (e.g. FRS, iSenseGo Analytics)	Depending on wishes of the customer.

Cabling

What	Remarks
Required number of power sockets available? (also on the correct place for the Power Inserter(s))	Always on power sockets is highly recommended
Network socket available?	Close to the Power Inserter / power socket is recommended
Cable conduits available? <ul style="list-style-type: none">• For network and coax cables (for gates)	

Store environment / Pre-store visit

What	Remarks
Width of the entrance / exit (gates and tops)	Width has an impact on the performance.
Height of the entrance / exit (tops)	Height has an impact on the performance.
Store environment observations <ul style="list-style-type: none">• Metal objects• Tempered glass• Other RFID devices• Other input	These objects may reflect the RFID signals. Avoid as much as possible, always discuss this with the customer upfront, so they are already aware of the risks
Sufficient Tag free zone available? If not; <ul style="list-style-type: none">• What is the distance?• Discussed with the customer?	

Other / Customer Expectations

What	Remarks
When will the installation be done?	<p>All prepared?</p> <ul style="list-style-type: none"> • Network / power sockets • IT setup • Make sure that labels / products are already in the store during installation. Otherwise, the system cannot be configured appropriately. Discuss with the retailer that an additional store visit might be needed to calibrate the system again.
Are there any specific expectations from the customer? (e.g. performance levels, how or when to do the installation, etc.)	
Do you expect any difficulties during this installation?	
Other comments or notes that are relevant	e.g. discussed points with the customer in pre-store visit
Make and pictures / drawings of the store	

Installation

Physical Installation

During the installation it is important to look back on the agreements made in the preparation phase.

What
Basics covered? <ul style="list-style-type: none">• Systems and gates orientation• Number of power inserters• Cabling requirements (length, cable type, etc.)
Is the store in line with the agreements you have made with the customer during the preparation / pre-store visit

Configuration

Configure the system to mimic the real situation in the store as much as possible for the best performance.

What
Configuration fully performed? <ul style="list-style-type: none">• Calibration box (always use store labels!)• Real alarm runs (on different power level)• False alarms runs (on different settings)
Check performance with event list <ul style="list-style-type: none">• Do you mostly see 6 out of 6 in the event list?
Have you been using special settings for this installation? <ul style="list-style-type: none">• Changes in muting forget time?• Beam steering V1 / V2 / off• Other?
Pictures of the store / system / environment

Hand over

Explain how the system works, leave test tags and setup Device Management

What	Remarks
Leave two RFID test tags in the store	Test tags are never muted and therefor ideal for testing.
Customer sign off	
Add system and store to Device Management	
Add required subscriptions	For example Fast Remote Service, iSense Dashboard or Analytics Theft.
Activate the relevant notifications within DM for pro-active monitoring (e.g. online status)	
Add installation document in Device Management	Also upload all relevant images and specific installation, and store details.

After Care

Follow up

Check if the settings need to be altered after some time.

What
Remotely check how the systems are doing (Performance, Alarms) e.g. 1 week after installation

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 43

Document Last modification date 9 October 2024

Document PDF Exported 9 October 2024 **by** Nedap Retail | Operations



support-retail@nedap.com



Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com

Release notes - iD POS Pro firmware 1.5.4+0EA2D402

Update-advice

 Recommended

Features

- POS API add continuously reading option for WebSocket
- improved network/ip selection
- Allow non-GS1 labels to be scanned and used (not send to iD Cloud if not valid SGTIN).
- Update initial setup wizard UI and Fixed IP option
- Add alternative DNS option

Bug fixes

- Ensure scanning is never stopped in always on mode. Add retry before stopping scanning in normal mode.
Clarify some logging.
- Ensure reboot abort does not abort transaction when in finalizing mode
- Fix EASiD after non-GS1 implementation
- Fixed iD Cloud api thread freeze causing reboot
- Made iD Cloud Slow metric solely dependant on sending tags to the iD Cloud
- Fixed an issue where a disconnect of the POS API would finalize all scanned items (and consequently send to the iD Cloud) instead of aborting the transaction.
- Change in RNDIS reconnect handling to fix windows sleep issues

Other

- Improve scanning stop reasons mainly for POS API send error if stop unexpected.
- Do not show default DNS port number 53
- Add "with DNS" to "Failed to resolve" system status to clarify it is an error for the DNS server
- Hide disposition sublocations in offline mode
- Add countries Kosovo, Lebanon, Moldova, Montenegro, Morocco, Ukraine and Uzbekistan
- Disable Button when POS API is enabled
- Update configuration card to Device and RF power card, Renamed Remote to Time Server, toggle system/network status in setup stage 1
- Device Manager Diagnostic event to POS on settings changes for faster settings synchronization
- Remove usage of "standalone" and set to "Offline"
- Removed "Short button press" in name for primary disposition
- Output antenna and RSSI in scan_event messages, also for IDPOS2
- Numerous enhancements and other bug fixes

Manuale Utente iD POS PRO

Vendita

- Premi brevemente il pulsante
- La luce diventa verde
- Posiziona gli articoli sul lettore



Reso

- Tieni premuto il pulsante per 2 scondi
- La luce diventa blue
- Posiziona gli articoli sul lettore

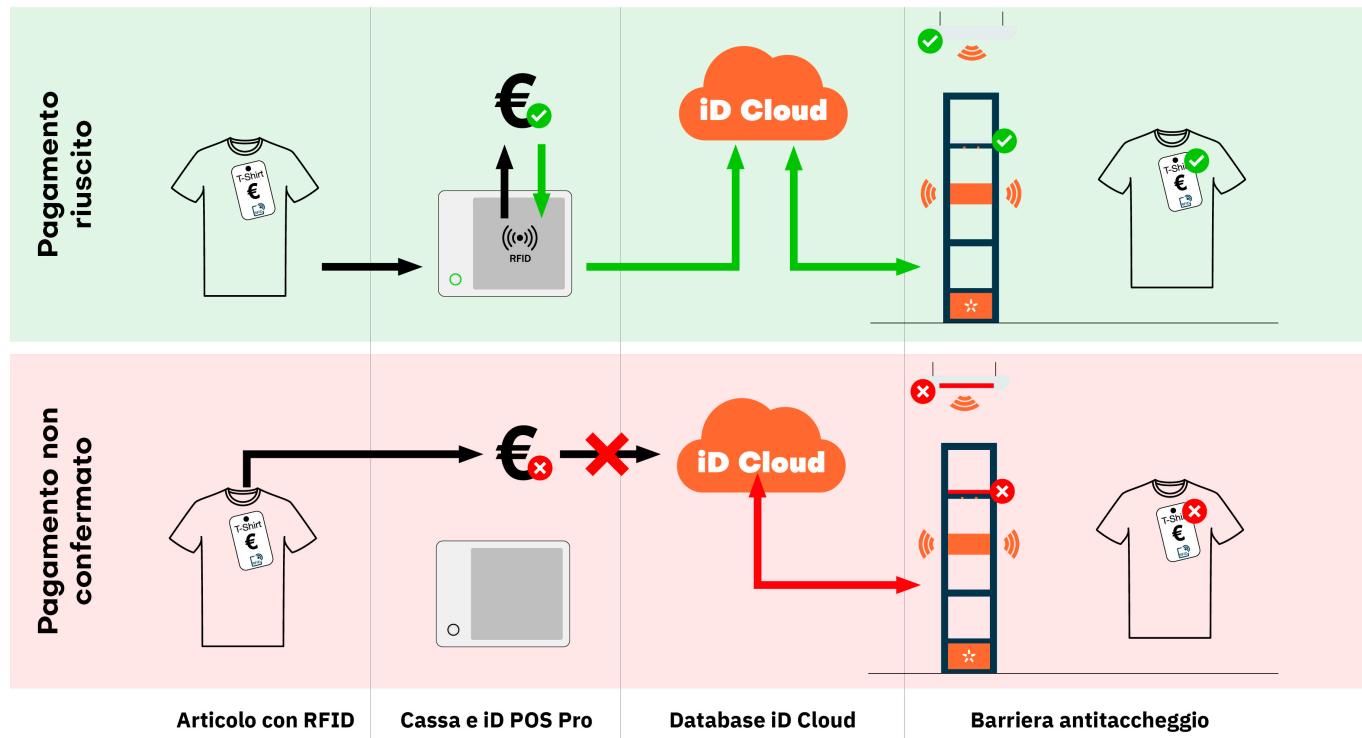


- A seconda delle impostazioni, la luce lampeggerà e il cicalino emetterà un segnale acustico per gli articoli letti.
- Un articolo non può essere letto di nuovo per 15 secondi o finché un'etichetta si trova sopra il lettore.
- Note: Luce arancione + segnali acustici brevi = nessuna connessione al database per la disattivazione.

Interrompere la lettura

- Premi brevemente il pulsante per spegnere il lettore oppure attendi 40 secondi (timeout di scansione).
- La luce si spegnerà.

iD POS Pro e EAS



Domande

Per qualsiasi domanda, contatta il tuo Partner Nedap Retail di riferimento.

User Manual iD POS PRO

Sell

- Short press the button
- The light will turn **green**
- Place items on the reader



Return

- Press and hold the button for **2 seconds**
- The light will turn **blue**
- Place items on the reader

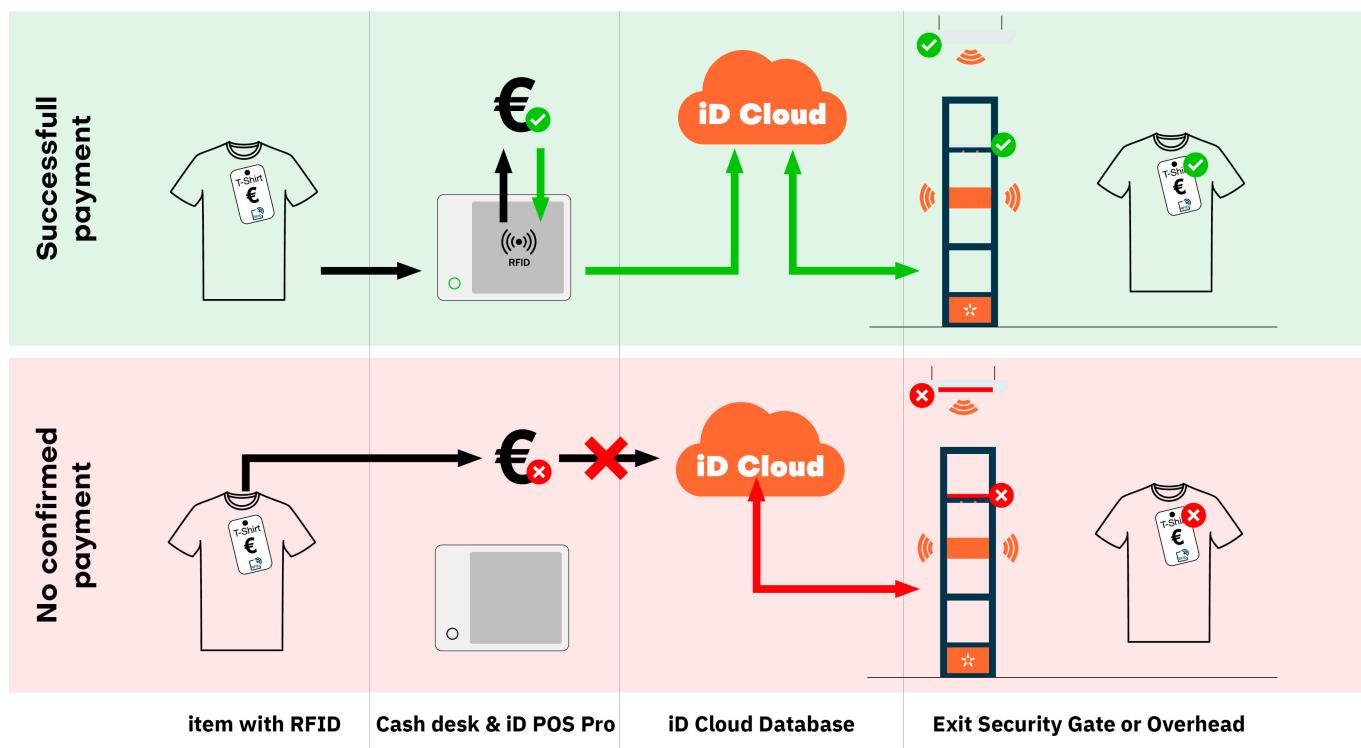


- Depending on the settings, the light will flash, and the buzzer will beep for scanned items.
- It cannot be scanned again for 15 seconds or as long as a label is on top of the reader.
- **Remark:** Orange light + short sounds: no connection to the database for deactivation

Stop reading

- Short press the button to turn off the reader or wait 40 seconds (Scan timeout)
- The light will turn off.

iD POS Pro and EAS



Questions

For questions, please contact your local Nedap Retail Partner.

Nedap Sense Knowledge Base

iD POS Pro & iD SCO Pro

WebSockets and Postman

version 25, April 2025



About Technical Documentation

This document highlights specific technical topics related to Nedap Sense products.

In addition to this guideline, other related documents, such as standard procedures, installation instructions, and settings, can be downloaded from the Technical section on the Partner Portal.

Links

- [Partner Portal](#)
 - [Technical Documentation](#)
 - [Commercial Documentation](#)
-

Installation / Project planning

Please visit the **Partnership Documents & Tools** portal page for information on project planning and all the steps to do a first-time-right installation.

Nedap Retail User Account

A Nedap Retail Portal account is required to enter the Partner Portal.

If you do not have access to specific accounts on the Partner Portal, you can request access at **support-retail@nedap.com**.

About Technical Documentation	2
Links	2
Installation / Project planning	2
Nedap Retail User Account	2
Introduction	4
1. Create a new collection	5
2. Add two variables	7
3. Add a WebSocket request.....	8
4. Enter the URL.....	9
5. Compose messages	10
Identify	10
Start	11
Stop	12
Sell	12
Return	12
Abort	13
6. Test	14

Introduction



This manual covers the operation and features of the iD POS Pro and the iD SCO Pro, which are largely identical. Most of the instructions, settings, and features described herein apply to both devices. Where there are differences between the two, these will be indicated. Please pay special attention to these notes to ensure proper usage of the specific device you are using.



Throughout this manual, the term “reader” is used as a generic reference to both iD POS Pro and iD SCO Pro.

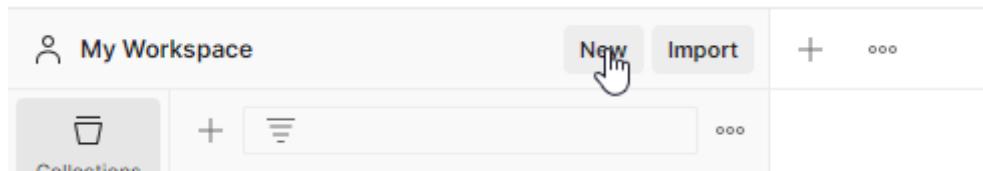


Postman is an API platform for building and using APIs.

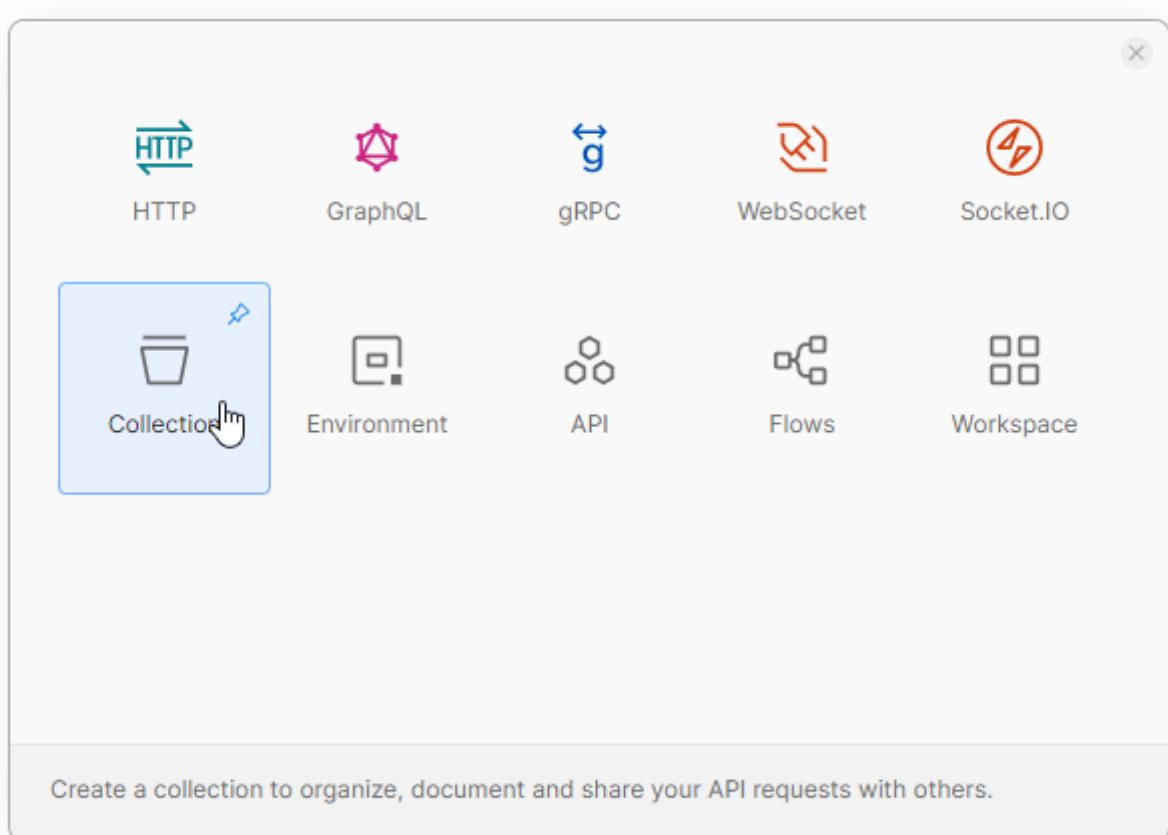
Postman added WebSockets functionalities to the API platform, **but does not support exporting (yet)**. This document describes a workaround for using WebSockets with a reader.

1. Create a new collection

≡ ← → Home Workspaces API Network Explore



Press the “New” button.



Press the “Collection” button.

And give the new collection a sensible name.

New Collection



...

iD POS2

Overview

Authorization

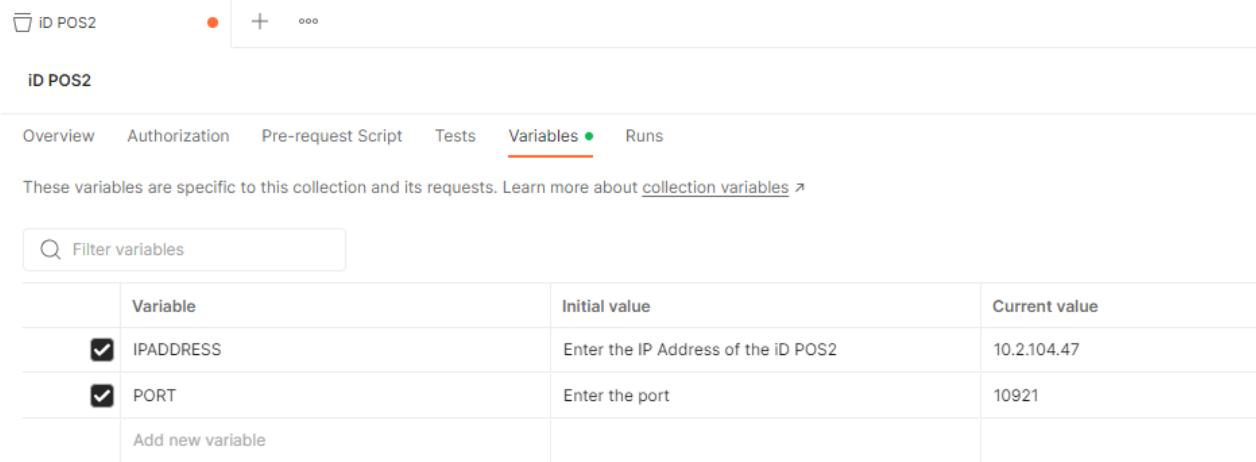
Pre-request Script

Tests

Variables

Runs

2. Add two variables



The screenshot shows a variable collection interface. At the top, there is a header with a trash can icon, a red dot, a plus sign, and three dots. Below the header, the collection name "ID POS2" is displayed. A navigation bar includes links for Overview, Authorization, Pre-request Script, Tests, Variables (which is underlined), and Runs. A note below the navigation states: "These variables are specific to this collection and its requests. Learn more about [collection variables](#) ↗". A search bar labeled "Filter variables" is present. A table lists the variables:

	Variable	Initial value	Current value
<input checked="" type="checkbox"/>	IPADDRESS	Enter the IP Address of the iD POS2	10.2.104.47
<input checked="" type="checkbox"/>	PORT	Enter the port	10921
	Add new variable		

Add “IPADDRESS”, being the IP address of the reader and “PORT”, being the port to be able to use the reader’s WebSocket.

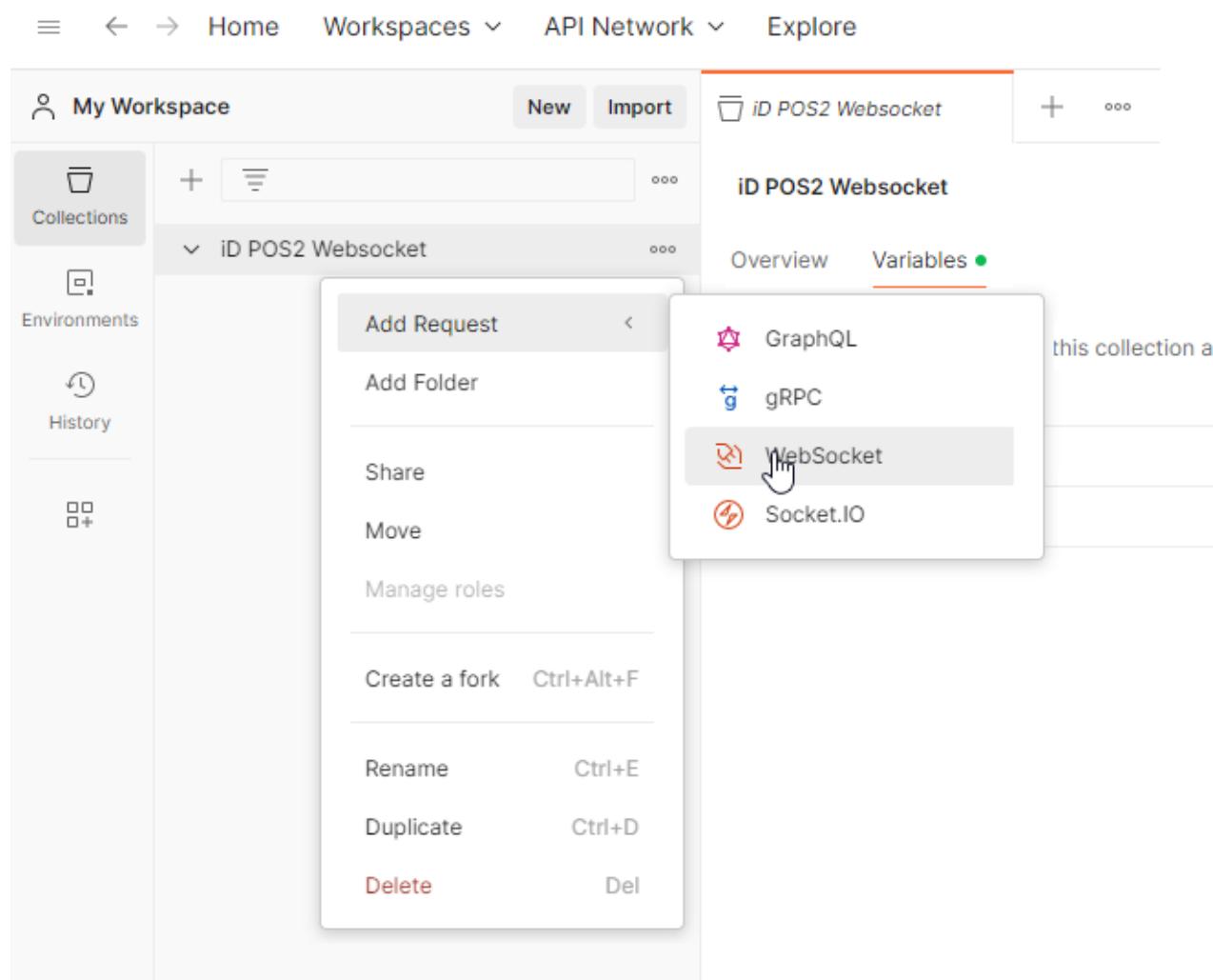
Change the “Current value” field to the values that you are using.

3. Add a WebSocket request

Press the three dots next to the newly created collection tab and press the “Add Request” button.

Choose “WebSocket”.

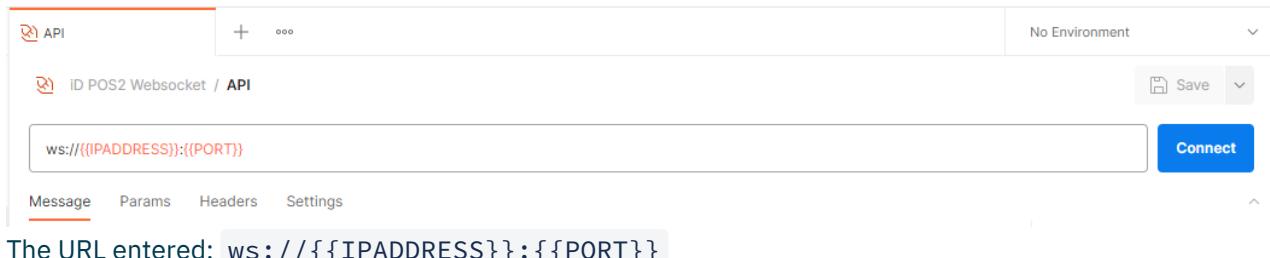
Give it a sensible name, like “API”.



The screenshot shows the API Network interface with the following details:

- Header:** Home, Workspaces, API Network, Explore.
- Left Sidebar:** Collections, Environments, History.
- Workspace Overview:** My Workspace, New, Import, iD POS2 Websocket (selected).
- Collection Details:** ID POS2 Websocket, Overview, Variables.
- Context Menu (Open):** Add Request, Add Folder, Share, Move, Manage roles, Create a fork (Ctrl+Alt+F), Rename (Ctrl+E), Duplicate (Ctrl+D), Delete (Del).
- Submenu (Visible):** GraphQL, gRPC, **WebSocket** (highlighted with a mouse cursor icon), Socket.IO.

4. Enter the URL



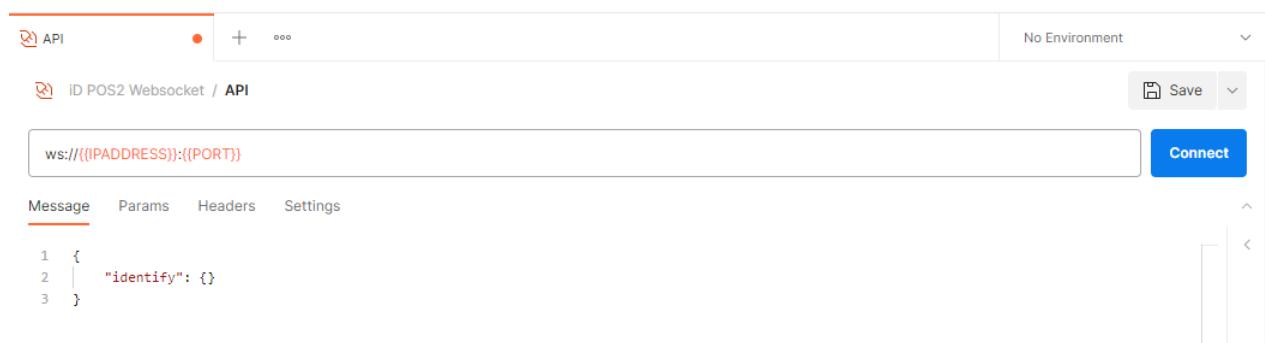
The URL entered: `ws://{{IPADDRESS}}:{{PORT}}`

5. Compose messages

To be able to execute some commands, a handful of messages need to be created.

The first one as an example.

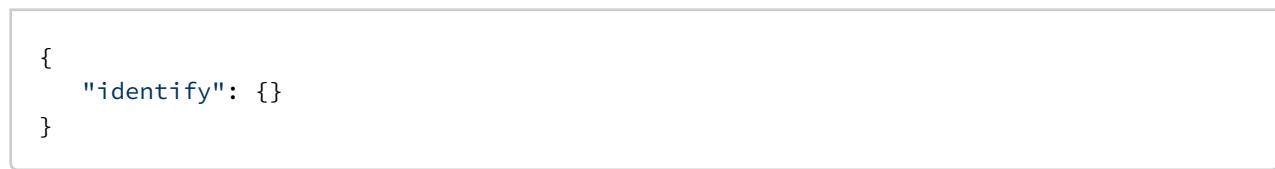
Identify



A screenshot of a WebSocket client interface. At the top, there's a header with 'API' and a red dot icon, followed by a '+' button and three dots. To the right is a dropdown menu set to 'No Environment'. Below the header is a status bar with 'ws://((IPADDRESS)):((PORT))' and a 'Save' button. The main area has tabs for 'Message', 'Params', 'Headers', and 'Settings', with 'Message' currently selected. A code editor shows the following JSON message:

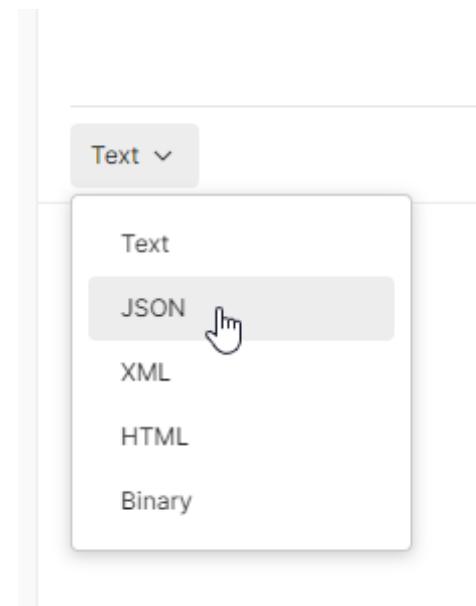
```
1 {  
2   "identify": {}  
3 }
```

For the first message, you can type directly in the “Message” field.

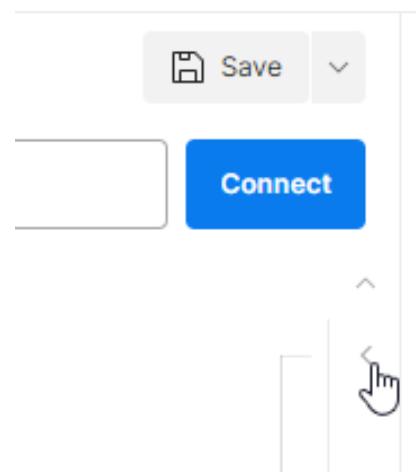


```
{  
  "identify": {}  
}
```

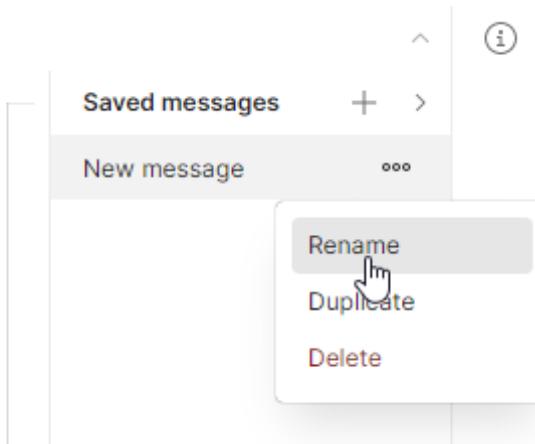
Change the Format to “JSON”



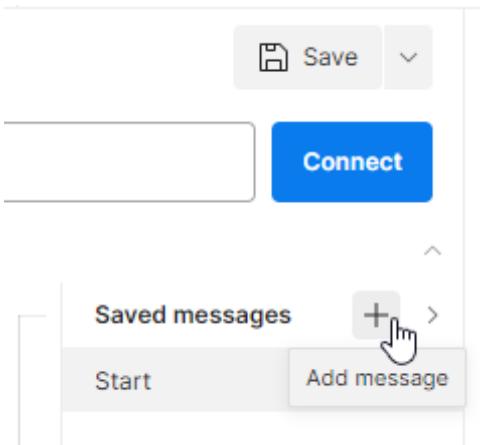
Then open the “save messages” pane by pressing the “<“ button.



Rename the newly created message to “Identify”.



By pressing the “+” button, you can add new messages.



Start

```
{  
  "start": {}  
}
```

Stop

```
// Instructions:  
// - enter the scan_id from the `scan_started` response  
{  
    "stop_scan": {  
        "scan_id": 0  
    }  
}
```

Sell

```
// Instructions:  
// - enter the scan_id from the `scan_started` response  
// - enter the epcs from the `scanned_tag` response  
{  
    "finalize_transaction": {  
        "scan_id": 0,  
        "identifiers": [  
            "epc1",  
            "epc2"  
        ],  
        "status": "retail_sold"  
    }  
}
```

Return

```
// Instructions:  
// - enter the scan_id from the `scan_started` response  
// - enter the epcs from the `scanned_tag` response  
{  
    "finalize_transaction": {  
        "scan_id": 0,  
        "identifiers": [  
            "epc1",  
            "epc2"  
        ],  
        "status": "sellable_accessible"  
    }  
}
```

Abort

```
{  
  "finalize_transaction": {  
    "status": "abort"  
  }  
}
```

6. Test

Time to perform a test run.

- Press the “Connect” button
 - Select the “Start” message
 - Press the “Send” button
 - Scan an RFID tag or two

The responses so far should look like:

- Select the “Stop” message
 - Change the `scan_id` into the `scan_id` that is shown in the "scan_started" response
 - Press the “Send” button
 - Select the “Sell” message
 - Change the `scan_id` into the `scan_id` that is shown in the "scan_started" response
 - Change `epc1` and `epc2` to the values received in the "scanned_tag" responses
 - Press the “Send” button

The responses so far should look like:

Response

Connected ▾

Search	All Messages ▾	Clear Messages
↓ {"finalized_transaction": {"scan_id": 4763, "timestamp": "2023-08-09T13:21:56Z"}}	15:21:56 ▾	
↓ {"finalizing_transaction": {"scan_id": 4763, "timestamp": "2023-08-09T13:21:56Z"}}	15:21:56 ▾	
↑ { "finalize_transaction": { "scan_id": 4763, "identifiers": ["urn:epc:id:sgtin:8058846.045424.34360000190", "ur...	15:21:55 ▾	
↓ {"stopped_scan": {"scan_id": 4763, "timestamp": "2023-08-09T13:20:54Z", "scan_count": 2}}	15:20:54 ▾	
↑ { "stop_scan": { "scan_id": 4763 } }	15:20:54 ▾	
↓ {"scanned_tag": {"scan_id": 4763, "timestamp": "2023-08-09T13:20:12Z", "epc_hex": "30347A142C224C20F7E32458", "pure_id...	15:20:12 ▾	
↓ {"scanned_tag": {"scan_id": 4763, "timestamp": "2023-08-09T13:20:12Z", "epc_hex": "3035EBDF782C5C080003FEBE", "pure_id...	15:20:12 ▾	
↓ {"scan_started": {"scan_id": 4763, "timestamp": "2023-08-09T13:20:11Z"}}	15:20:12 ▾	
↑ { "start_scan": {} }	15:20:11 ▾	
✓ Connected to ws://10.2.104.47:10921	15:20:10 ▾	

- Press “Disconnect”
- Press “Save”
- And exit Postman!

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap NV 2025

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 25

Document Last modification date 30 April 2025

Document PDF Exported 30 April 2025 by Nedap Retail | Operations



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com



Nedap Sense Guideline

iD POS Pro & iD SCO Pro

WebSockets

version 140, December 2024

Introduction	3
Modes	3
Configuring the reader	3
WebSocket concept	4
State Flow	4
Commands	6
Command: identify	6
Command: start_scan	7
Command: stop_scan	9
Command: finalize_transaction	10
Command: finalize_transaction (abort)	14
Response error	15
Elements	15
Examples.....	16
Selling	16
Returning	16
Aborting	17
Scanning always on.....	18
Offline configurations.....	19
Appendix A: Error codes.....	20
Appendix B: HTML/Javascript example code	21
Appendix C: Python example code.....	25

Introduction

This document outlines **integrating the iD POS Pro or iD SCO Pro device with a Point of Sale (POS)**.



This manual covers the operation and features of the iD POS Pro and the iD SCO Pro, which are largely identical. Most of the instructions, settings, and features described herein apply to both devices. Where there are differences between the two, these will be indicated. Please pay special attention to these notes to ensure proper usage of your specific device.



Throughout this manual, the term “reader” is used to refer to both iD POS Pro and iD SCO Pro.

Modes

When integrating the reader with the POS, the reader can operate in two modes;

1. the reader can finalize the transaction or
2. the POS can execute this.

Finalizing the transaction means calling the API and passing the EPC to set the status.

Configuring the reader

The reader must be configured to enable the POS to connect to the WebSocket.

CONNECTION TO POS

Connection type	<input type="text" value="Websocket"/>
	<input type="text" value="10921"/>
websocket POS API port (requires restart)	
Limit websocket POS API to USB	<input checked="" type="checkbox"/>
No duplicate filtering for POS API	<input type="checkbox"/>

The WebSocket connection can be addressed:

- through USB using `ws://192.0.2.1:10921`
- through the external network (when `Limit websocket POS API to USB` is OFF)
 - depending on the policy on the external network using its IP address `ws://x.x.x.x:10921`

- by its hostname using `ws://idpos000da01100c4.local:10921` for an iD POS Pro, or `ws://idsco000da001100c4.local:10921` for an iD SCO Pro
 - where the hostname is a concatenation of `idpos` or `idsco` and the mac-address of the unit
- by a generic hostname when only one iD POS Pro or iD SCO Pro is on the network: `ws://idpos2.local:10921` or `ws://idsco.local:10921`

WebSocket concept

The reader supports a WebSocket connection. WebSockets are low-level connections without flow control or message acknowledgments.

The protocol is set up so that all commands have a response. The response also indicates that the connection is valid and that the message has been received properly.

State Flow

A single transaction, from start to end, will look like this.

POS Command	Reader Response	Remarks
<code>identify</code>		Optional for identifying the connected reader
	<code>identification</code>	
<code>start_scan</code>		Start reading
	<code>scan_started</code>	Determines the <code>scan_id</code> for all commands and messages following it
	<code>scanned_tag</code>	For each tag read by the reader (can be zero)
<code>stop_scan</code>		Stop reading
	<code>stopped_scan</code>	Between <code>stop_scan</code> and <code>stopped_scan</code> , it is still possible to receive <code>scanned_tag</code> messages.

POS Command	Reader Response	Remarks
finalize_transaction		Update the transaction for all read RFID tags or just a subset.
	finalizing_transaction	After receiving, the reader is ready for a new start_scan
	finalized_transaction	Asynchronous, possibly delayed when the iD Cloud connection is interrupted
	error	Asynchronous, whenever an error occurs



It is crucial to design your system so that it remains robust and functional even as the protocol evolves. Protocols are often updated to add new commands, fields, or features to address new requirements, improve performance, or fix security vulnerabilities. An implementation that is not resilient to such changes may become obsolete or fail to interoperate with a future release. In short, be robust against adding new commands or fields by ignoring unknown commands and fields, and be flexible when parsing the messages.

Commands

Command: identify

This command can be used to identify the connected device.

```
{  
    "identify": []  
}
```

Response

```
{  
    "identification": {  
        "device_name": "Desk 3",  
        "mac_address": "00:0D:A0:11:12:34",  
        "system_id": "7e1d6794-7e8d-44c2-9d83-90558f54bb4d",  
        "state": "scanning"  
    }  
}
```

Elements

Element	Type	Description
device_name	string	The name of the device
mac_address	string	The MAC address of the device
system_id	string	The system identifier of the device in the Nedap Device Management servers
state	string	The current state: idle, scanning, finalizing, or unknown

Command: start_scan

This is the initial message to start a scan on the device. Once received, scanning starts, and a `scan_started` message is returned.

For every RFID tag detected, a `scanned_tag` message is returned until a `stop_scan` is sent.

```
{  
    "start_scan": {}  
}
```

Response scan_started

Reply from the device to the POS when the scan has started. This scan operation will have a unique `scan_id` used to stop or abort a scan when finalizing the transaction. This unique `scan_id` is returned, as well as the time at which the scan was started.

```
{  
    "scan_started": {  
        "scan_id": 2,  
        "timestamp": "2023-08-01T11:44:18Z"  
    }  
}
```

Elements

Element	Type	Description
<code>scan_id</code>	int32	The current scan identifier is needed in subsequent commands.
<code>timestamp</code>	ISO 8601 formatted date/time	The timestamp the scan was started

Response scanned_tag

The corresponding information is sent to the POS system whenever the device scans an RFID tag.



A unique tag is sent only once during a scan session unless the "Allow duplicate tags" option is enabled. When this option is turned on, the tag will appear every time the reader reads it.

Every tag is sent to the POS system containing the information as stated below.

```
{  
    "scanned_tag": {  
        "scan_id": 2,  
        "timestamp": "2023-08-01T11:44:19Z",  
        "epc_hex": "30347A12301D8EF84BC77670",  
        "pure_identity_uri": "urn:epc:id:sgtin:2000012.030267.241789531760",  
        "gs1_elementstring": "010200001230267121241789531760"  
    }  
}
```

Elements

Element	Type	Description
scan_id	int32	The current scan identifier
timestamp	ISO 8601 formatted date/time	The timestamp the RFID tag was read
epc_hex	string	The EPC of the RFID tag read
pure_identity_uri	string	The pure identity URI translation
gs1_elementstring	string	The gs1 translation

Command: stop_scan

A stop scan command is sent from the POS to the device to stop the current scanning of RFID tags.

```
{  
    "stop_scan": {  
        "scan_id": 2  
    }  
}
```

Elements

Element	Type	Description
scan_id	int32	The current scan identifier must match the value returned in the <code>scan_started</code> response

Response stopped_scan

Reply from the device on the `stop_scan` command, once the scan has stopped.

```
{  
    "stopped_scan": {  
        "scan_id": 2,  
        "timestamp": "2023-08-01T11:44:21Z",  
        "scan_count": 3  
    }  
}
```

Elements

Element	Type	Description
scan_id	int32	The current scan identifier
timestamp	ISO 8601 formatted date/time	The timestamp the scan was stopped
scan_count	int32	The number of unique RFID tags scanned



A `scanned_tag` can still be received while waiting for the `stopped_scan` message.

Command: finalize_transaction

Send from POS to the device, which tells the device to update the EAS database for the given RFID tags.

A scan should have been stopped and confirmed by the reader with a `stopped_scan` message before sending a `finalize_transaction` command.

`scan_id` should match the scan identifier of the scan at which the given RFID tags were read. This message can only be sent once per `scan_id`.

If `identifiers` is omitted or empty, the system will update all scanned tags in the database.

```
{  
    "finalize_transaction": {  
        "scan_id": 2,  
        "identifiers": [  
            "urn:epc:id:sgtin:2000012.030270.220538749701",  
            "urn:epc:id:sgtin:2000012.030267.241789531760"  
        ],  
        "status": "retail_sold"  
    }  
}
```

Elements

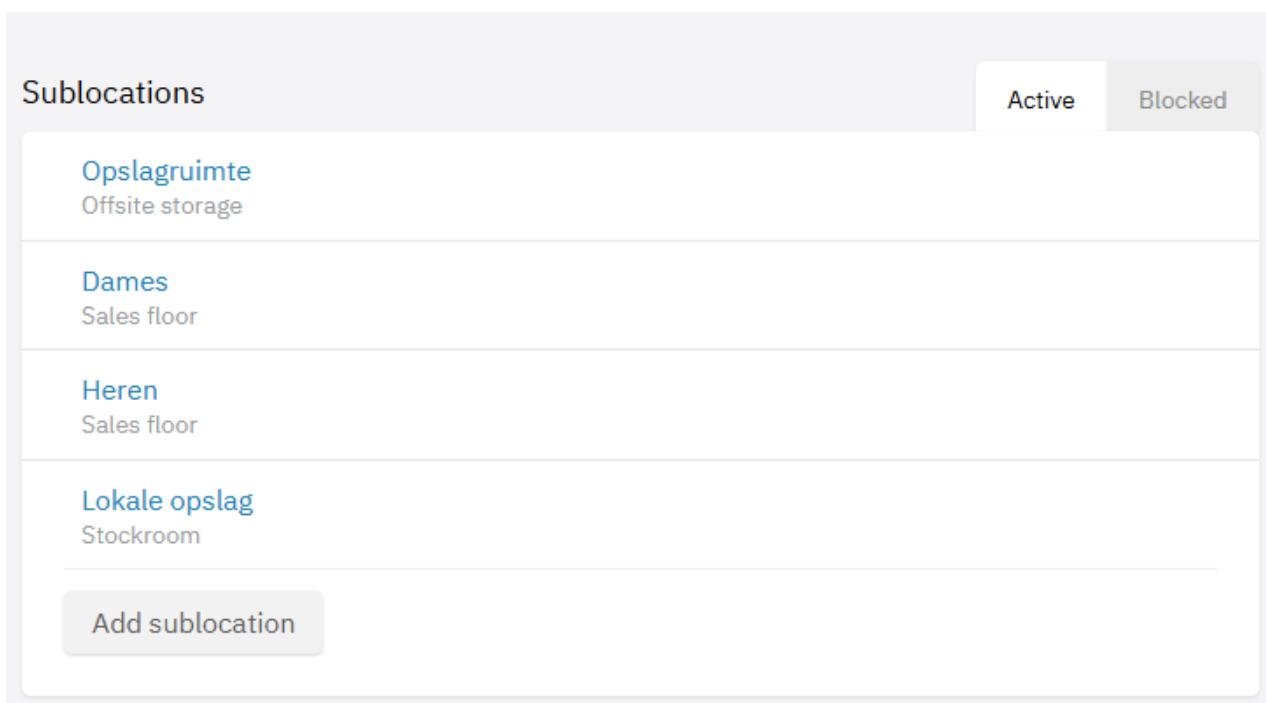
Element	Type	Description
<code>scan_id</code>	int32	The current scan identifier must match the value returned in the <code>scan_started</code> response
<code>identifiers</code>	string[]	An array of RFID tags will be used to finalize the transaction. Only add the RFID tags that should be updated in this field. The field can be left empty or even omitted when the action is for all the unique RFID tags scanned during this scan. <ul style="list-style-type: none">• Any of the three formats can be used here<ul style="list-style-type: none">• <code>"30347A12301D8EF84BC77670"</code> (<code>EPC_HEX</code>)• <code>"urn:epc:id:sgtin:2000012.030267.241789531760"</code> (<code>pure_identity_uri</code>)• or <code>"010200001230267121241789531760"</code> (<code>gs1_elementstring</code>)• Only scanned RFID tags are accepted, and only the added RFID tags in this field will be finalized.

Element	Type	Description
status	string	<p>retail_sold, sellable_accessible, or sellable_not_accessible for selling, returning to the Sales Floor, and returning to the Stockroom, respectively.</p> <p>Other options:</p> <ul style="list-style-type: none"> damaged - This is the status Damaged in iD Cloud non_sellable_other - This is the status Held in iD Cloud reserved - This is the status Reserved in iD Cloud

Business location

In the SCANNING section in the device's user interface, it is possible to change the sublocation (in iD Cloud, this is shown as the business location) to one of the available sublocations created in Device Management for the store.

In Device Management:



The screenshot shows the 'Sublocations' page in Device Management. At the top, there are two tabs: 'Active' (which is selected) and 'Blocked'. Below the tabs, there is a list of four sublocations:

- Opslagruimte** (Offsite storage)
- Dames** (Sales floor)
- Heren** (Sales floor)
- Lokale opslag** (Stockroom)

At the bottom left of the list, there is a button labeled 'Add sublocation'.

In the reader:

Short button press / Primary disposition

urn:epcglobal:cbv:disp:	retail_sold	▼
Sublocation	default	▼

Long button press / Secondary disposition

urn:epcglobal:cbv:disp:	sellable_accessible	▼
Sublocation	Opslagruimte	▼



The Primary disposition or Secondary disposition that matches the Status in the finalize_transaction message defines the Sublocation used in the communication towards iD Cloud.

For example, a finalized transaction with the status set to sellable_accessible will use “Opslagruimte” as its Sublocation.

Response finalizing_transaction

Reply from the device to notify the POS that the `finalize_transaction` call has been sent to iD Cloud for the given `scan_id`.

```
{  
    "finalizing_transaction": {  
        "scan_id": 2,  
        "timestamp": "2023-08-01T11:44:26Z"  
    }  
}
```

Elements

Element	Type	Description
<code>scan_id</code>	int32	The current scan identifier
<code>timestamp</code>	ISO 8601 formatted date/time	The timestamp the <code>finalize_transaction</code> was received

Response finalized_transaction

Reply from the device to notify the POS that the `finalize_transaction` call has been acknowledged by iD Cloud for the given `scan_id`. If iD Cloud is not used, this response follows directly after the `finalizing_transaction` response.



This is an asynchronous response. When the connection to iD Cloud is interrupted, new transactions (start, stop, finalize) can continue. As soon as the connection to iD Cloud is restored, even after a power cycle or reboot, transactions that were not yet finalized will be finalized, resulting in a delayed response with the old corresponding `scan_id` if the Websocket connection is open; otherwise, the update will occur silently.

```
{  
    "finalized_transaction": {  
        "scan_id": 2,  
        "timestamp": "2023-08-01T11:44:26Z"  
    }  
}
```

Elements

Element	Type	Description
scan_id	int32	The current scan identifier
timestamp	ISO 8601 formatted date/time	The timestamp the finalization was finished

Command: finalize_transaction (abort)

To abort any running scan, the status should be set to abort, scan_id or identifiers are not required. When needed, the command can be issued at any moment, the current state is not relevant.

```
{
    "finalize_transaction": {
        "status": "abort"
    }
}
```

Response finalized_transaction

```
{
    "finalized_transaction": {
        "scan_id": 2,
        "timestamp": "2023-07-14T13:25:56Z"
    }
}
```

Elements

Element	Type	Description
scan_id	int32	The current scan identifier
timestamp	ISO 8601 formatted date/time	The timestamp the scan was aborted



Closing the Websocket connection also aborts the current scan.

Response error

Reply from the device to notify the POS that an error was encountered. This message can be received anytime in the dialogue between POS and the device.

Error codes are described in “Appendix A: Error codes.”

```
{  
  "error": {  
    "scan_id": 2,  
    "code": -6,  
    "description": "Not scanning so cannot stop"  
  }  
}
```

Elements

Element	Type	Description
scan_id	int32	The current scan identifier
code	int32	The error code
description	string	Description of the error. This should provide some specific information about the problem, which is different from the error codes in Appendix A, which provide a general description.

Examples

Below a few examples of the flow for different transactions.

Selling

```
16:30:55 ---> {"start_scan":{}}
16:30:55 <--- {"scan_started":{"scan_id":269,"timestamp":"2024-12-04T15:30:56.700Z"}}
}
16:30:55 <--- {"scanned_tag":{"scan_id":269,"timestamp":"2024-12-04T15:30:56.865Z","epc_hex":"30347A12000005C00002254F","pure_identity_uri":"urn:epc:id:sgtin:2000000.00023.140623","gs1_elementstring":"010200000000023721140623"}}
16:30:55 <--- {"scanned_tag":{"scan_id":269,"timestamp":"2024-12-04T15:30:56.866Z","epc_hex":"30347A12000005C000022550","pure_identity_uri":"urn:epc:id:sgtin:2000000.00023.140624","gs1_elementstring":"010200000000023721140624"}}
16:30:57 ---> {"stop_scan":{"scan_id":269}}
16:30:57 <--- {"stopped_scan":{"scan_id":269,"timestamp":"2024-12-04T15:30:58.542Z","scan_count":2}}
16:30:59 ---> {"finalize_transaction":{"scan_id":269,"identifiers":[{"urn:epc:id:sgtin:2000000.00023.140623","urn:epc:id:sgtin:2000000.00023.140624"]},"status":"retail_sold"}}
16:30:59 <--- {"finalizing_transaction":{"scan_id":269,"timestamp":"2024-12-04T15:31:00.191Z"}}
16:31:00 <--- {"finalized_transaction":{"scan_id":269,"timestamp":"2024-12-04T15:31:01.966Z"}}
```

Returning

```
16:33:32 ---> {"start_scan":{}}
16:33:32 <--- {"scan_started":{"scan_id":270,"timestamp":"2024-12-04T15:33:33.576Z"}}
}
16:33:32 <--- {"scanned_tag":{"scan_id":270,"timestamp":"2024-12-04T15:33:33.741Z","epc_hex":"30347A12000005C000022550","pure_identity_uri":"urn:epc:id:sgtin:2000000.00023.140624","gs1_elementstring":"010200000000023721140624"}}
16:33:32 <--- {"scanned_tag":{"scan_id":270,"timestamp":"2024-12-04T15:33:33.742Z","epc_hex":"30347A12000005C00002254F","pure_identity_uri":"urn:epc:id:sgtin:2000000.00023.140623","gs1_elementstring":"010200000000023721140623"}}
16:33:35 ---> {"stop_scan":{"scan_id":270}}
16:33:37 <--- {"stopped_scan":{"scan_id":270,"timestamp":"2024-12-04T15:33:38.260Z","scan_count":2}}
16:33:37 ---> {"finalize_transaction":{"scan_id":270,"identifiers":[{"urn:epc:id:sgtin:2000000.00023.140624","urn:epc:id:sgtin:2000000.00023.140623"]},"status":"sellable_accessible"}}
```

```
16:33:37 <--- {"finalizing_transaction":{"scan_id":270,"timestamp":"2024-12-04T15:33:38.537Z"}}
16:33:38 <--- {"finalized_transaction":{"scan_id":270,"timestamp":"2024-12-04T15:33:40.069Z"}}
```

Aborting

```
16:34:06 ---> {"start_scan":{}}
16:34:06 <--- {"scan_started":{"scan_id":272,"timestamp":"2024-12-04T15:34:07.624Z"}}
16:34:06 <--- {"scanned_tag":{"scan_id":272,"timestamp":"2024-12-04T15:34:07.790Z","epc_hex":"30347A12000005C00002254F","pure_identity_uri":"urn:epc:id:sgtin:2000000.00023.140623","gs1_elementstring":"01020000000023721140623"}}
16:34:06 <--- {"scanned_tag":{"scan_id":272,"timestamp":"2024-12-04T15:34:07.791Z","epc_hex":"30347A12000005C000022550","pure_identity_uri":"urn:epc:id:sgtin:2000000.00023.140624","gs1_elementstring":"01020000000023721140624"}}
16:34:07 ---> {"finalize_transaction":{"status":"abort"}}
16:34:08 <--- {"finalized_transaction":{"scan_id":272,"timestamp":"2024-12-04T15:34:09.198Z"}}
```

Scanning always on

When `Always on` is configured, the behavior of the WebSocket API is slightly different. Commands are no longer needed as the device is constantly reading, and every tag read is transferred to the POS by means of the `scanned_tag` response.

In this mode, the POS updates iD Cloud or the local database.

`Update iD Cloud EPCIS` should be turned off when using `Always on`.



Offline configurations

When the device is configured to work offline, connections to iD Cloud, Device Management, BoschIoT (Firmware updates), and NTP services (optional) are disabled. Thus, setups that need an iD Cloud connection are not possible.

If there is no NTP connection, timestamps will be set to 0 .

Appendix A: Error codes

Error Code	Error Name	Description
0	NO_ERROR	OK value return
-1	INVALID_SCAN_ID	Scan id used is not current scan id. If scan id is unknown, please abort.
-2	INVALID_IDENTIFIER	One or more identifier(s) do not belong to Scan ID or are wrongly formatted.
-3	INVALID_FINALIZE	Cannot finalize transaction during running scan, except abort.
-4	INVALID_JSON	Given that JSON is not valid and cannot be parsed,
-5	NO_TAGS	Cannot finalize the transaction with retail_sold or sellable_accessible if no tags are given.
-6	NOT_SCANNING	Cannot stop scanning (no running scan).
-7	MAX_TAGS_SCANNED	The buffer containing tags is full.
-8	UNEXPECTED_ERROR	An unexpected error occurred.
-9	ALREADY_SCANNING	Cannot start scan, already started.
-10	CANNOT_SCAN	Cannot start, finalize previous scan first.
-11	CONFIGURATION	Transaction mode is disabled; this is more a warning than an error and should be guaranteed by the iD POS Pro never to happen.
-12	UNKNOWN_DISPOSITION	The disposition in the finalize message is unknown.
-13	SCAN_START_FAILED	Failed to start scanning (probably a radio issue).
-14	SCAN_STOP_FAILED	Failed to stop scanning (unlikely).
-15	SCAN_STOPPED	The scan stopped due to an error.



Appendix B: HTML/Javascript example code

- Get `iD POS Pro & iD SCO Pro example code.zip` from the Partner Portal; it should be on the same page where you found this Guideline
- Extract it
- In a Chromium-based browser, open the file
 - `<Ctrl>-O`
 - select `websocketPOS.html`
- After configuring the device to use WebSockets and changing the IP address in this test program to match with the device, press the `Open` and then the `Start` button, scan a few RFID tags, press the `Stop` button when done, and finally press the `Sell` button. The outcome should be like this:

Nedap iD POS Pro & iD SCO Pro WebSocket API Client

IP address: Port:

Labels seen: ScanID:

⚠ Please do not copy the code below, it results in syntax errors; instead find it on our Partner portal, see above.

iD POS Pro / iD SCO Pro example code

```
<!DOCTYPE html>
<!-- Check "Guideline - iD POS Pro & iD SCO Pro WebSockets" on https://
portal.nedapretail.com/technical/technical-idpos -->
<html>
    <head>
        <meta charset="UTF-8">
        <title>Nedap iD POS Pro & iD SCO Pro WebSocket API Client</title>
        <style>
            body {
                font-family: Arial, sans-serif;
                background-color: #F5F5F5;
                color: #023A4F;
            }
            h2 {
                color: #FF6C37;
            }
            input[type="text"] {
                padding: 5px;
                margin: 5px 0;
                border: 1px solid #023A4F;
                border-radius: 3px;
            }
            button {
                background-color: #FF6C37;
                color: white;
                border: none;
                padding: 10px 20px;
                margin: 5px 0;
                border-radius: 3px;
                cursor: pointer;
            }
            button:hover {
                background-color: #E55B2F;
            }
            #output {
                margin-top: 20px;
                padding: 10px;
                border: 1px solid #023A4F;
                background-color: #FFF;
            }
        </style>
        <script language="javascript" type="text/javascript">
```

```

let socket = null;
let scan_id = 0;
let epcs = "";

function log(message) { document.getElementById("output").innerHTML
+= new Date().toLocaleTimeString('en-GB') + " " + message + "<br>"; }
function clearLog() { document.getElementById("output").innerHTML
= ""; }
function send(message) { log('---> ' + message);
socket.send(message); }
function identify() { send('{"identify":{}}'); }
function startScan() { send('{"start_scan":{}}'); }
function stopScan() { send('{"stop_scan":{"scan_id":"' + scan_id +
'}}'); }
function finalizeSell() { send('{"finalize_transaction":{"scan_id":"' +
scan_id + ',"identifiers":[' + epcs.substr(1) + '],"status":"retail_sold"}}'); }
function finalizeReturn() { send('{"finalize_transaction":{"scan_id":"' +
scan_id + ',"identifiers":[' + epcs.substr(1) + '],"status":"sellable_accessible"}}'); }
function finalizeAbort() { send('{"finalize_transaction":
{"status":"abort"}}'); }

function openAPI() {
    if (socket) return;
    let url = "ws://" + document.getElementById("ipAddress").value + ":" +
+ document.getElementById("apiPort").value;
    socket = new WebSocket(url);
    socket.onopen = function(event) {
        log("[INFO] iD POS Pro / iD SCO Pro Connection established on " +
+ url);
    }
    socket.onmessage = function(event) {
        let message = JSON.parse(event.data);
        log("<--- " + event.data);
        if (message.hasOwnProperty("scan_started")) {
            epcs = "";
            scan_id = message.scan_started.scan_id;
            document.getElementById("scanID").value = scan_id;
        } else if (message.hasOwnProperty("scanned_tag")) {
            if (! epcs.includes(message.scanned_tag.pure_identity_uri))
epcs += ',' + message.scanned_tag.pure_identity_uri + '';
            ++document.getElementById("labels").value;
        } else if (message.hasOwnProperty("error")) {
            log("[ERROR] " + message.error.description);
        }
    }
    socket.onclose = function(event) { log("[INFO] Connection closed"); }
    socket.onerror = function(event) { log("[ERROR] Connection error"); }
}

```

```
}

function closeAPI() {
    if (socket == null) return;
    socket.close();
}
</script>
</head>
<body>
    <h1>Nedap iD POS Pro & iD SCO Pro WebSocket API Client</h1>
    IP address: <input id="ipAddress" type="text" value="192.0.2.1"/>&ampnbsp
    Port: <input id="apiPort" type="text" value="10921"/><br><br>
    <button onclick="openAPI()">Open</button>&ampnbsp
    <button onclick="clearLog()">Clear log</button>&ampnbsp
    <button onclick="closeAPI()">Close</button><br><br>
    <button onclick="identify()">Identify</button>&ampnbsp
    <button onclick="startScan()">Start</button>&ampnbsp
    <button onclick="stopScan()">Stop</button>&ampnbsp
    <button onclick="finalizeSell()">Sell</button>&ampnbsp
    <button onclick="finalizeReturn()">Return</button>&ampnbsp
    <button onclick="finalizeAbort()">Abort</button><br><br>
    Labels seen: <input id="labels" type="text" value="0"/>&ampnbsp
    ScanID: <input id="scanID" type="text" value="0"/><br><br>
    <div id="output"></div>
</body>
</html>
```

Appendix C: Python example code

- Get `iD POS Pro & iD SCO Pro example code.zip` from the Partner Portal; it should be on the same page where you found this Guideline
- Extract it
- select `POS API.py`
- After configuring the device to use WebSockets and changing the IP address in this test program to match with the device, run the Python code. The outcome should be like this:

```
--> Connection opened
--> {"start_scan":{}}
<-- {"scan_started":{"scan_id":215,"timestamp":"2024-11-19T08:55:41.624Z"}}
<-- {"scanned_tag":{"scan_id":215,"timestamp":"2024-11-19T08:55:44.267Z","epc_hex":"30347A142C224C20F7E32458","pure_identity_uri":"urn:epc:id:sgtin:2000139.035120.141597811800","gs1_elementstring":"010200013935120021141597811800"}}
--> {"stop_scan":{"scan_id":215}}
<-- {"stopped_scan":{"scan_id":215,"timestamp":"2024-11-19T08:55:44.306Z","scan_count":1}}
--> {"finalize_transaction":{"scan_id":215,"status":"retail_sold"}}
<-- {"finalizing_transaction":{"scan_id":215,"timestamp":"2024-11-19T08:55:44.384Z"}}
--> {"finalized_transaction":{"scan_id":215,"timestamp":"2024-11-19T08:55:45.015Z"}}
--> Connection closed
```

The code will:

- open the connection
- start a scan as soon as the connection is made
- stop the scan as soon as 1 RFID tag is read
- finalize the transaction as soon as the scan is stopped
- close the connection as soon as the transaction is finished in iD Cloud
- exit

iD POS Pro / id SCO example code

```
#!/usr/bin/python3

ip = "192.0.2.1"
port = 10921

import websocket
import json

def send(ws, message):
    print("--> " + message)
    ws.send(message)

def startScan(ws):
    send(ws, '{"start_scan":{}}')

def stopScan(ws, scan_id):
    send(ws, '{"stop_scan":{"scan_id":"' + str(scan_id) + '"}}')

def finalizeTransaction(ws, scan_id, status):
    send(ws, '{"finalize_transaction":{"scan_id":"' + str(scan_id) + '","status":"' + status + '"}}')

def on_open(ws):
    print("--> Connection opened")
    startScan(ws)

def on_message(ws, message):
    global scan_id
    global scanning

    print("<-- " + message)
    payload = json.loads(message)
    if "scan_started" in payload:
        scanning = True
        scan_id = payload["scan_started"]["scan_id"]
    elif "scanned_tag" in payload:
        if scanning:
            scanning = False
            stopScan(ws, scan_id)
    elif "stopped_scan" in payload:
        finalizeTransaction(ws, scan_id, "retail_sold")
    elif "finalizing_transaction" in payload:
        next
    elif "finalized_transaction" in payload:
        ws.close()
    elif "error" in payload:
        ws.close()
```

```
def on_error(ws, error):
    print("[ERROR] Connection error, code=" + error)

url = 'ws://' + ip + ':' + str(port)
ws = websocket.WebSocketApp(url, on_open=on_open, on_message=on_message, on_error=on_error)
ws.run_forever()
print("--> Connection closed")

# EOF
```

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2025

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 140

Document Last modification date 11 December 2024

Document PDF Exported 11 December 2024 by Nedap Retail | Operations



support-retail@nedap.com



Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com

Connected Devices Guideline

iD POS 2 Issues

version 32, February 2024

Introduction	3
Device Management - Store Assist	3
Device Management - History Page	4
Device Management - E-mail notifications	5
Analytics System Status Page	6
Issue classification	7
Timing	7
Issues	8
Not connected to Device Management	8
iD POS 2 management connection to Device Management is lost	9
iD POS 2 connection to iD Cloud is slow	10
iD POS 2 connection to iD Cloud is lost	11
iD POS 2 connection with the Firmware Update server is lost	12
Used abbreviations	13

Introduction

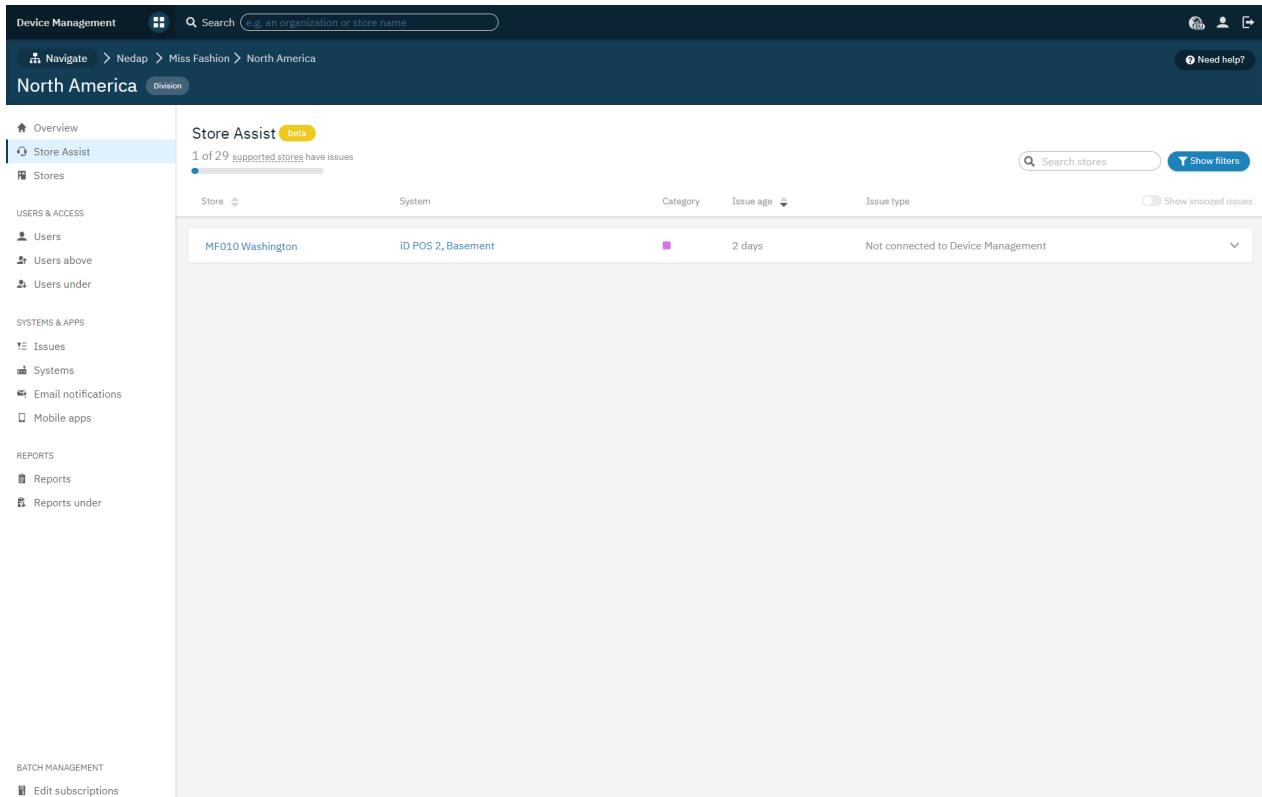
This document describes the messages, interpretation, and resolution of issues that can occur in Device Management (Store Assist and System Issues), Analytics and the iD POS 2 System.



In this document, Device Management is abbreviated to DM.

Device Management - Store Assist

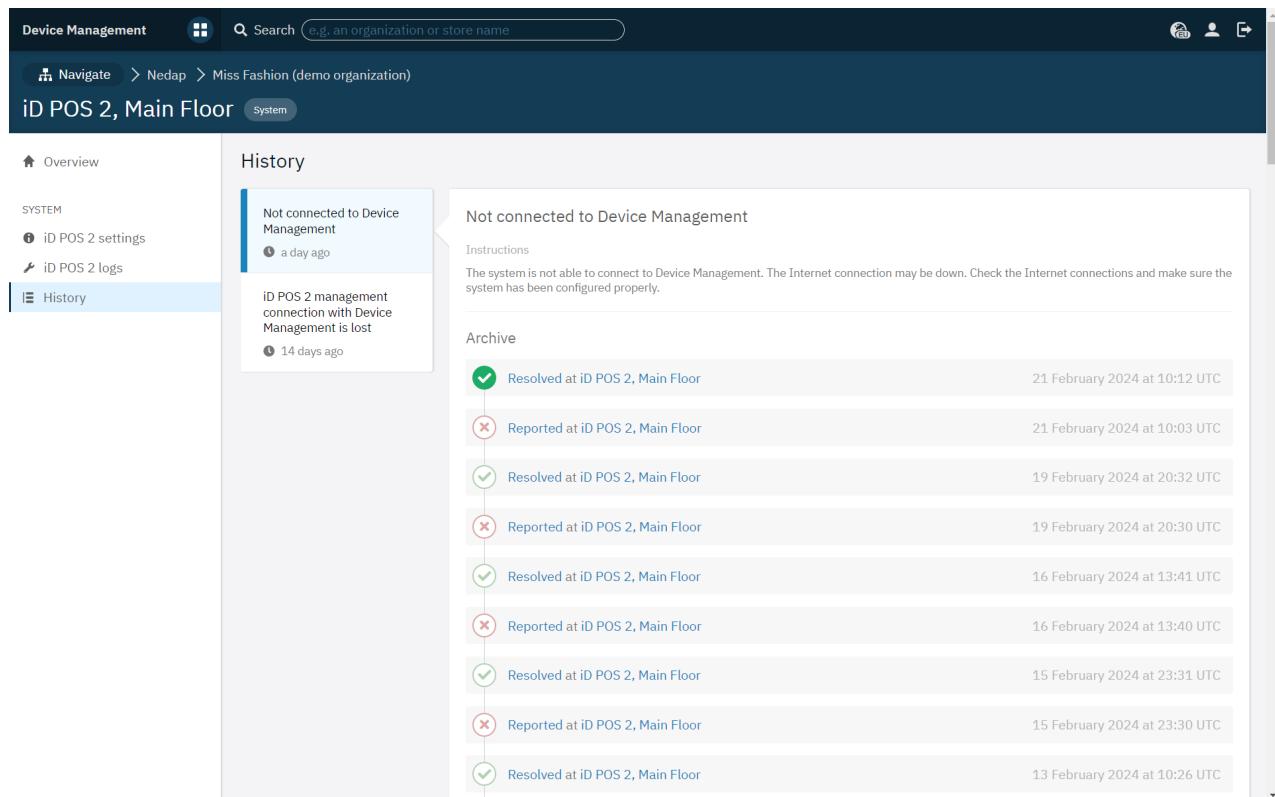
Store Assist shows the issues found for all systems in a division or at a certain level. It is a powerful tool to manage systems.

A screenshot of the Device Management software interface, specifically the Store Assist module. The top navigation bar includes 'Device Management', a search bar, and user account information. The main header says 'North America' and 'Division'. On the left, a sidebar menu lists categories like Overview, Store Assist (which is selected and highlighted in blue), Stores, USERS & ACCESS (with sub-options for Users, Users above, and Users under), SYSTEMS & APPS (with sub-options for Issues, Systems, Email notifications, and Mobile apps), and REPORTS (with sub-options for Reports and Reports under). The central content area is titled 'Store Assist (beta)' and shows a summary: '1 of 29 supported stores have issues'. Below this is a table with columns: Store, System, Category, Issue age, and Issue type. One row is visible: 'MF010 Washington' under 'System', with a pink square icon under 'Category', '2 days' under 'Issue age', and 'Not connected to Device Management' under 'Issue type'. There are also filters and search options at the top of the table area.

Device Management - History Page

The History Page shows the same information as the Store Assist page but adds a few details.

For most issues, the Device Management 'Description' and 'Instruction' should give you enough information about the issue to take action. Additional comments are added where necessary.



The screenshot shows the Device Management History Page for the organization 'Nedap'. The navigation bar includes 'Device Management', a search bar, and user icons. The breadcrumb path shows 'Navigate > Nedap > Miss Fashion (demo organization)'. The main content area displays the 'History' tab for 'iD POS 2, Main Floor'. A summary message indicates 'Not connected to Device Management' (a day ago) and 'iD POS 2 management connection with Device Management is lost' (14 days ago). The 'History' section lists events in a timeline:

Action	Date
Resolved at iD POS 2, Main Floor	21 February 2024 at 10:12 UTC
Reported at iD POS 2, Main Floor	21 February 2024 at 10:03 UTC
Resolved at iD POS 2, Main Floor	19 February 2024 at 20:32 UTC
Reported at iD POS 2, Main Floor	19 February 2024 at 20:30 UTC
Resolved at iD POS 2, Main Floor	16 February 2024 at 13:41 UTC
Reported at iD POS 2, Main Floor	16 February 2024 at 13:40 UTC
Resolved at iD POS 2, Main Floor	15 February 2024 at 23:31 UTC
Reported at iD POS 2, Main Floor	15 February 2024 at 23:30 UTC
Resolved at iD POS 2, Main Floor	13 February 2024 at 10:26 UTC

Device Management - E-mail notifications

It is possible to send automatic e-mail notifications for issues.

Navigate > Nedap Business Partner Demo > Netherlands

Netherlands Division

- [Overview](#)
- [Store Assist](#)
- [Stores](#)

- SYSTEMS & APPS**
- [Issues](#)
- [Systems](#)
- [RFID EAS performance](#)
- [Email notifications](#)
- [Mobile apps](#)
- [Ongoing firmware updates](#)

- REPORTS**
- [Reports](#)
- [Reports under](#)

Notifications beta

Add Notification

Show notifications: Under Netherlands Above Netherlands Search notifications

Recipient	Send delay	Issue type	Location	Creation date	Set by
Business Partner	30 minutes	Not connected to Device Management	Netherlands	Today at 12:28 PM	Business Partner X

nedap Privacy statement & disclaimer

Navigate > Nedap Business Partner Demo > Netherlands

Netherlands Division

- [Overview](#)
- [Store Assist](#)
- [Stores](#)

- SYSTEMS & APPS**
- [Issues](#)
- [Systems](#)
- [RFID EAS performance](#)
- [Email notifications](#)
- [Mobile apps](#)
- [Ongoing firmware updates](#)

- REPORTS**
- [Reports](#)
- [Reports under](#)

Set new email notification

Set for a different location? Use the [overview](#) to go to another location.

Which issue type(s) do you want to subscribe to?

<input type="checkbox"/> Not connected to Device Management
<input type="checkbox"/> Units inactive
<input type="checkbox"/> Units in RF maintenance mode
<input type="checkbox"/> RF extreme alarms
<input type="checkbox"/> High RF pulse interference
<input type="checkbox"/> RFID units are muted
<input type="checkbox"/> Units in RFID maintenance mode
<input type="checkbox"/> RFID false alarms suspected
<input type="checkbox"/> RFID EAS database error
<input type="checkbox"/> Key switch active
<input type="checkbox"/> Infrared beam sensors blocked
<input type="checkbox"/> IO box disconnected

After how long should the notification be sent?

Direct	30 minutes	1 hour	1.5 hours	2 hours	4 hours	12 hours	24 hours	48 hours
--------	------------	--------	-----------	---------	---------	----------	----------	----------



Analytics System Status Page

Analytics only shows generic messages of the issue. They have been added to this document to have everything together. The issue is derived from the problem in Device Management – no interpretation or timing differences.

The screenshot shows the 'System status' section of the Analytics System Status Page. On the left, a sidebar menu includes 'Overview', 'Alarms', 'Visitors', 'System status' (which is selected and highlighted in orange), and 'Occupancy'. The main content area displays 'Systems with issues' count as '0' of 0 systems. Below this, a red error icon and the text 'ID POS 2, Basement' followed by the message 'Integration related issues, to be investigated by the local Business Partner (installer)'.

Issue classification

Issues are classified in degrees / types of effort / action.

Category	Analytics Issue	Issues In This Category
Network	Network-related issues are to be investigated by the local Business Partner (installer); some may be resolved by in-store staff.	<ul style="list-style-type: none"> iD POS 2 connection to iD Cloud is slow iD POS 2 connection to iD Cloud is lost iD POS 2 management connection to Device Management is lost iD POS 2 connection to the Firmware Update server is lost
	System has been offline since {date} (UTC); check power cables and network connection; otherwise contact the local Business Partner (installer).	<ul style="list-style-type: none"> Not connected to Device Management

Timing

When the connection from the iD POS 2 to DM is interrupted, it takes some time before DM decides that the iD POS 2 should be marked as **Not connected to Device Management**.

In that period, other issues will not arrive at DM, so new issues, although noticeable in the store, will not be visible in DM, and resolved issues will also not be visual as resolved in DM.

Issues

Not connected to Device Management

Category

Network

Device Management Description

The system is not able to connect to Device Management. The Internet connection may be down.

Device Management Instruction

Check the Internet connections and make sure the system has been configured properly.

Device Management Notification

yes

Connection to POS

Any

Connection to iD Cloud

Any

Timing

Issue is shown after 10 minutes and removed immediately after the iD POS 2 reconnects.

Analytics Issue

System is offline since {timestamp} (UTC), check power cables and network connection, otherwise contact the local Business Partner (installer)



iD POS 2 management connection to Device Management is lost

Category

Network

Device Management Description

The connection from the iD POS 2 to Device Management is lost.

Device Management Instruction

Check the internet connection.

Device Management Notification

Yes

Connection to POS

Any

Connection to iD Cloud

Any

Timing

The issue is shown after 10 minutes and removed once the issue is resolved.

Analytics Issue

The network connection from the iD POS 2 to the Device Management servers has been interrupted since {timestamp} (UTC).

iD POS 2 connection to iD Cloud is slow

Category

Network

Device Management Description

iD Cloud did not respond within the timeout limit.

Device Management Instruction

Check the internet connection.

Device Management Notification

Yes

Connection to POS

Any

Connection to iD Cloud

Yes

Timing

The issue is shown after 10 minutes and removed once the issue is resolved and a SELL or RETURN event has occurred.

Analytics Issue

The network connection from the iD POS 2 to the iD Cloud servers is slow since {timestamp} (UTC).



iD POS 2 connection to iD Cloud is lost

Category

Network

Device Management Description

No response from iD Cloud.

Device Management Instruction

Check the internet connection.

Device Management Notification

Yes

Connection to POS

Any

Connection to iD Cloud

Yes

Timing

The issue is shown after 10 minutes and removed once the issue is resolved and a SELL or RETURN event has occurred.

Analytics Issue

The network connection from the iD POS 2 to the iD Cloud servers has been interrupted since {timestamp} (UTC).

iD POS 2 connection with the Firmware Update server is lost

Category

Network

Device Management Description

It was not possible to make a connection to the iD POS 2 update server; updates may not be installed

Device Management Instruction

Check the network connection.

Device Management Notification

Yes

Connection to POS

Any

Connection to iD Cloud

Any

Timing

The Firmware update server is checked about every 15 minutes, so that is the timing at which this metric is updated.

Analytics Issue

The network connection from the iD POS 2 to the Firmware update servers has been interrupted since {timestamp} (UTC).

Used abbreviations

Standard terms may be abbreviated in this document. The following table shows the descriptions of the abbreviations used. RFID-specific abbreviations are highlighted.

Abbreviation	Description
API	Application Programming Interface - is a way for two or more apps to communicate with each other.
CC	Customer Counting
DM	Device Management
EAS	Electronic Article Surveillance
EPC (RFID)	The Electronic Product Code is one of the available formats for encoding identifiers on RFID tags. The EPC is a globally unique number that identifies a specific item in the supply chain.
External CC	External Customer Counting (e.g., Brickstream)
FRS	Fast Remote Service
GS1 (RFID)	(Global Standards 1) An international standards organization with member bodies in more than 100 countries worldwide. Nedap Retail follows the GS1 and RainRFID standards.
GTIN (RFID)	A Global Trade Item Number (GTIN) is a number that uniquely identifies a product. It can be found beneath the barcode of a product.
IO Box	Input/Output Electronics device
IR	Infra Red
MD	Metal Detection
RF	Radio Frequency
RFID	Radio Frequency Identification

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 32

Document Last modification date 22 February 2024

Document PDF Exported 22 February 2024 **by** Nedap Retail | Operations



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com



Connected Devices Guideline

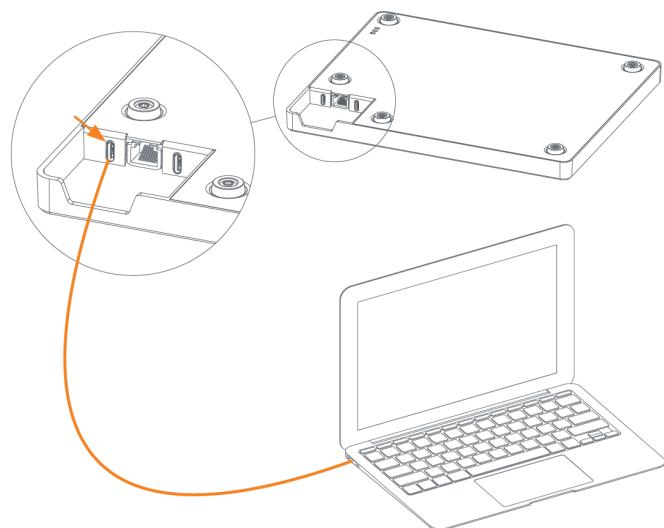
iD POS 2 - Windows driver installation

version 25, April 2024

Introduction	3
Installation of the Windows driver.....	4

Introduction

When first connecting to the iD POS 2 with a USB cable to a Microsoft Windows device, you sometimes need to install a driver to communicate with the iD POS 2.



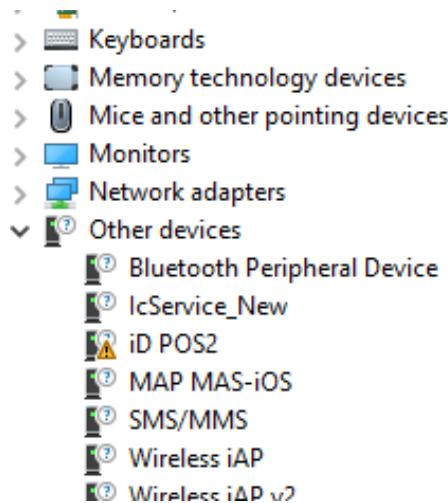
Installation of the Windows driver

Follow the next steps to install the Windows driver for the iD POS 2 reader connection via the USB service port 1 (port 1) to a Microsoft Windows-based computer:

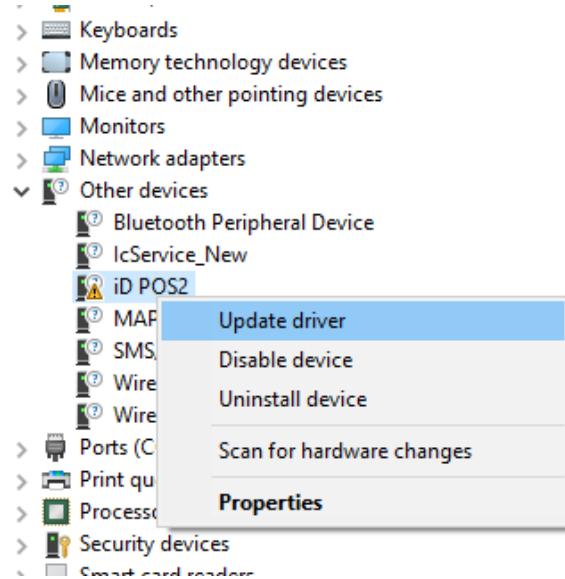
1. Insert the USB-c cable into the USB service port 1 on the back of the iD POS 2
2. Insert the other end of the USB cable into a free port on your laptop
3. Make sure the iD POS 2 reader is turned on
4. Open your browser and browse to this page <http://192.0.2.1>
 - a. If you get the Web interface of the iD POS 2, the driver is already installed. **There is no need to continue.**
 - b. If it does not open the Web interface of the iD POS 2, **continue with Step 5 below**
5. Go to **Device Manager**
6. Go to **Other devices**
7. Find **iD POS2**



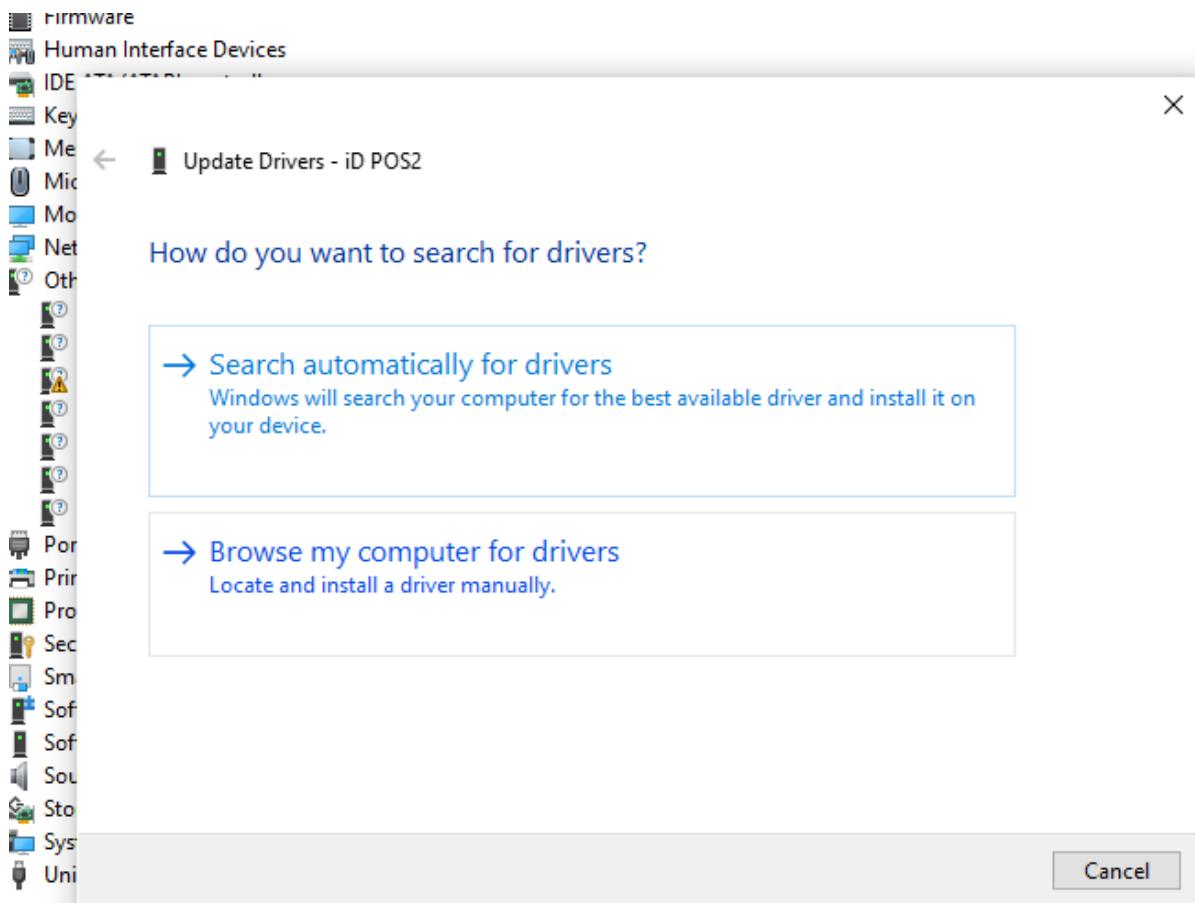
Be sure to check the **Other devices** section. The iD POS 2 also adds a HID Keyboard device in the Keyboards section, do **NOT** update this driver.



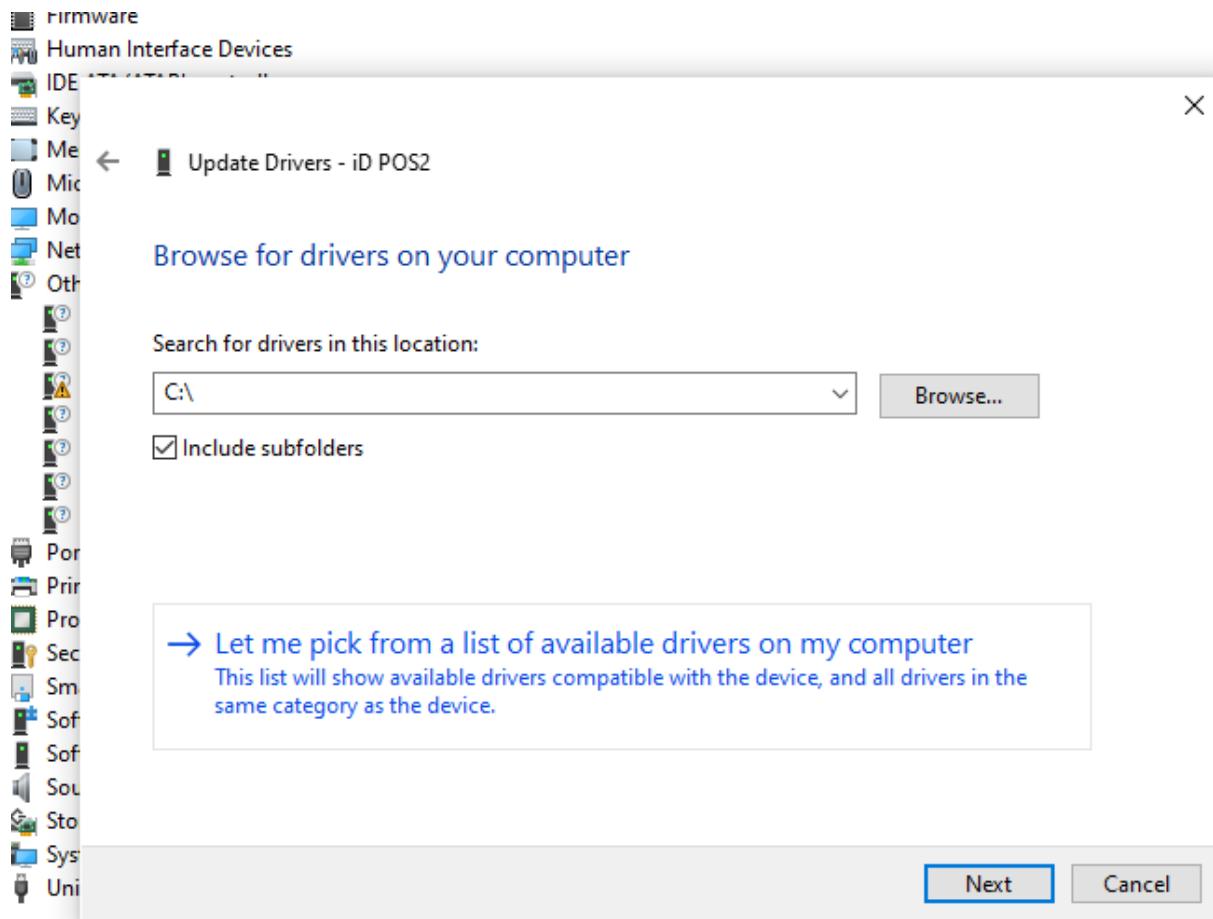
8. Right click and select Update driver



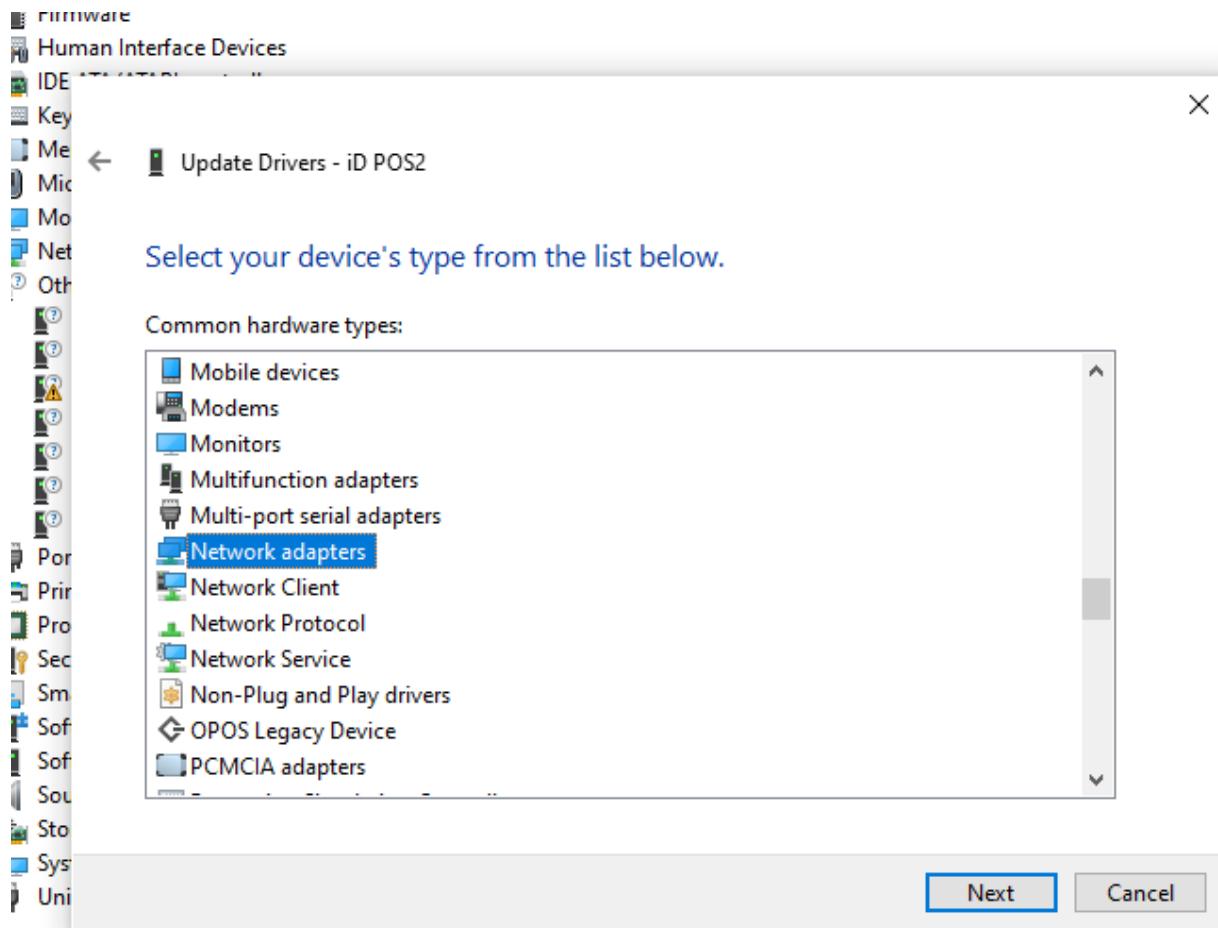
9. Select Browse my computer for drivers



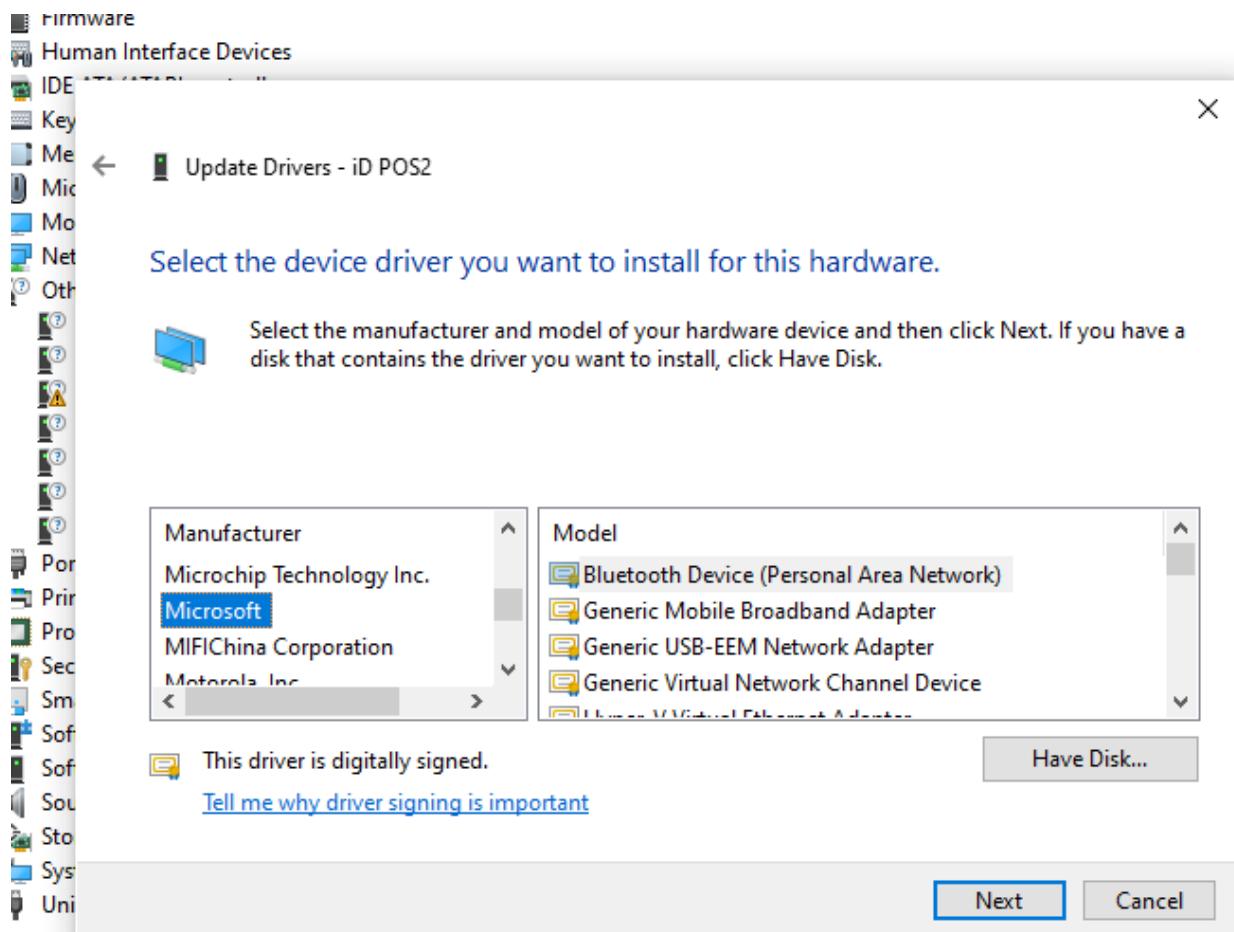
10. Select Let me pick from a list of available drivers on my computer



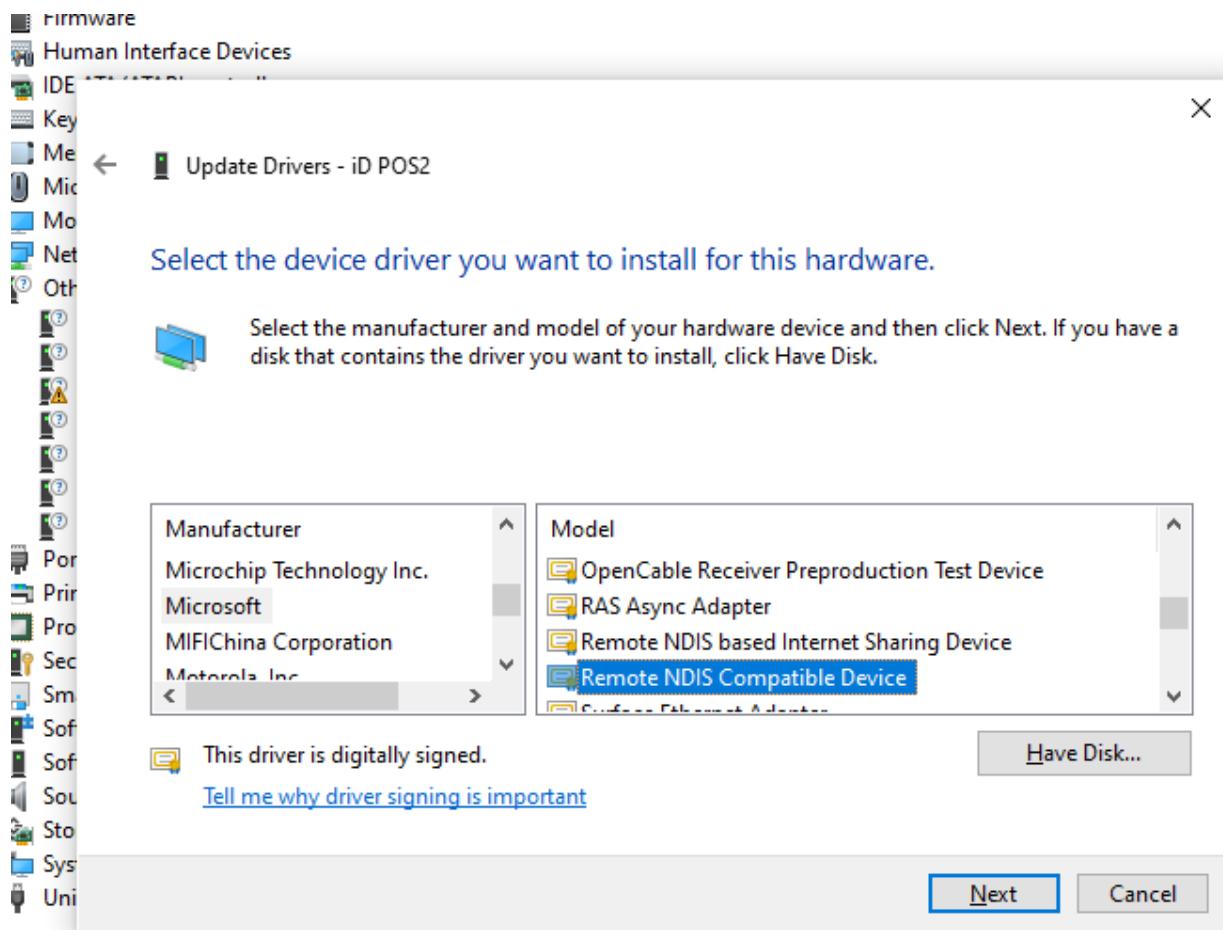
11. Find Network adapters and click it



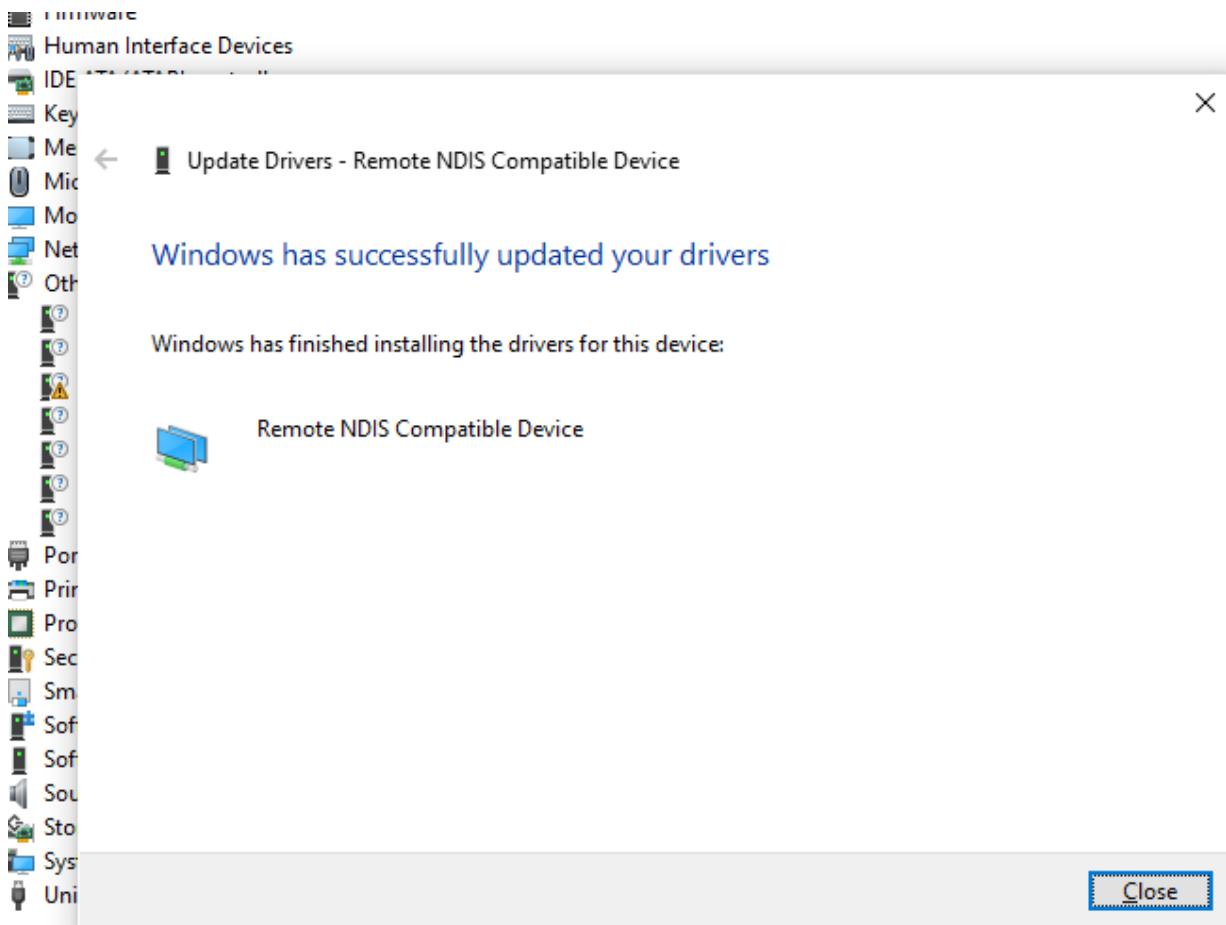
12. Find Microsoft and click it



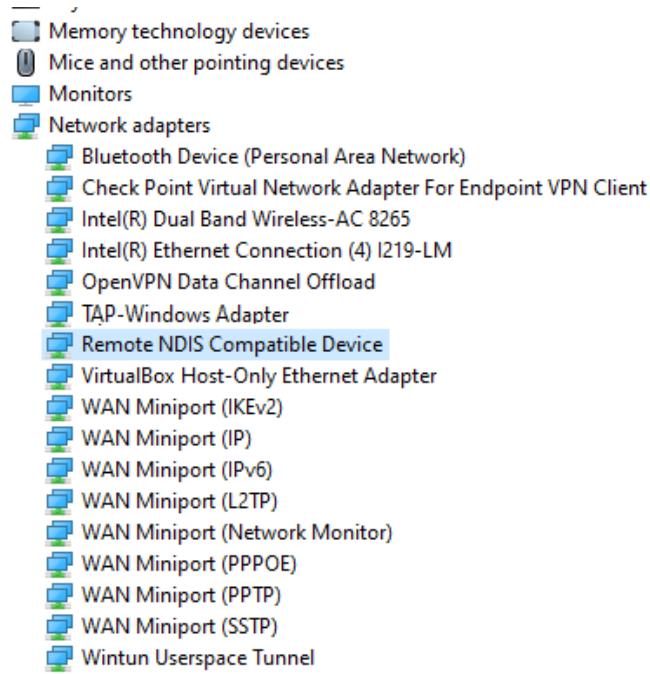
13. Find Remote NDIS Compatible Device and click it and press Next



14. Press Close



15. A network adapter is added



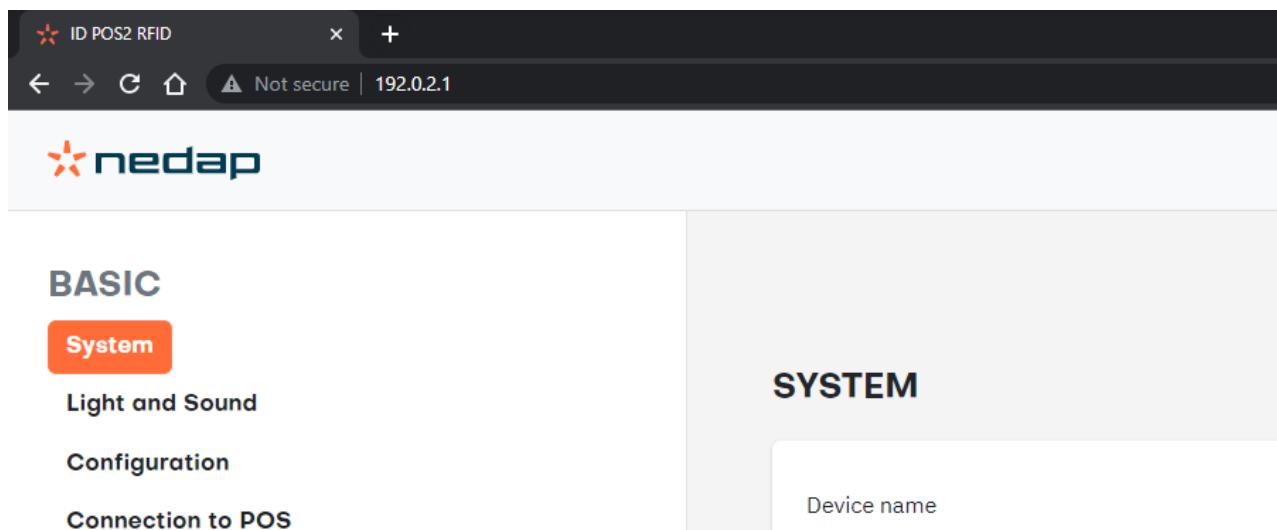
16. Your laptop receives 192.0.2.2 as its IP address from the iD POS 2

```
C:\>ipconfig
    //////
Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::da80:85b2:79e9:abea%26
IPv4 Address . . . . . : 192.0.2.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.0.2.1

Connection-specific DNS Suffix . : nedap.local
```

17. The iD POS 2 has IP address 192.0.2.1. Open your browser and go to this IP address



The screenshot shows a web browser window with the following details:

- Title Bar:** ID POS2 RFID
- URL Bar:** Not secure | 192.0.2.1
- Page Title:** ID POS2 RFID
- Left Sidebar (BASIC section):**
 - Selected:** System
 - Light and Sound
 - Configuration
 - Connection to POS
- Main Content Area (SYSTEM section):**
 - Section Title:** SYSTEM
 - Input Field:** Device name

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 25

Document Last modification date 5 April 2024

Document PDF Exported 5 April 2024 **by** Nedap Retail | Operations



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com



Nedap Sense Guideline

iD POS Pro & iD SCO Pro

OFFLINE Configuration

version 48, January 2025



Introduction	3
Available documentation	3
Connect to the iD POS Pro and iD SCO Pro.....	4
Driver installation - Microsoft Windows	4
First configuration.....	5
Predefined configuration.....	9
Configuration sections	10
Configuration section “Basic”	10
Configuration section “Advanced”	14
Common setups	18
Full setup via POS	19
Standalone	20
View and Edit settings.....	21

Introduction

This guideline describes the OFFLINE configuration of the Nedap Retail iD POS Pro / iD SCO Pro based on the **most common** setups.



This manual covers the operation and features of the iD POS Pro and the iD SCO Pro, which are largely identical. Most of the instructions, settings, and features described herein apply to both devices. Where there are differences between the two, these will be indicated. Please pay special attention to these notes to ensure proper usage of your specific device.

Available documentation

Next to some commercial documentation, the following technical documentation is available for the iD POS Pro and iD SCO Pro:

- iD POS Pro - Manual
- iD SCO Pro - Manual
- iD POS Pro & iD SCO Pro - Configuration
- iD POS Pro & iD SCO Pro - OFFLINE Configuration
- iD POS Pro & iD SCO Pro - Network information
- iD POS Pro & iD SCO Pro - WebSocket POS integration
- iD POS Pro & iD SCO Pro - WebSocket and Postman
- iD POS Pro & iD SCO Pro - Windows driver installation
- iD POS Pro & iD SCO Pro - Firmware and Settings API



This guideline only describes the OFFLINE setups for the iD POS Pro and iD SCO Pro.
ONLINE setups are described in the iD POS Pro & iD SCO Pro Configuration manual



This manual uses the term “reader” as a generic reference to both iD POS Pro and iD SCO Pro.

Connect to the iD POS Pro and iD SCO Pro

Connect a laptop to the service port on the reader using a USB cable with a USB-C connector.

-  Ensure the iD POS Pro is powered through standard Power over Ethernet (PoE) IEEE802.3af, class 0.
For the iD SCO Pro, exclusively use the included power supply.

-  A driver is required to configure the readers (see the list with available documentation)

Driver installation - Microsoft Windows

A Microsoft Windows driver needs to be installed to configure a reader. Please check the “*iD POS Pro & iD SCO Pro Windows driver installation*” manual for instructions.

-  At the moment, only Microsoft Windows is supported.

Once the Windows driver is installed, you can enter the configuration by opening your browser and navigating to <http://192.0.2.1>. This will open a webpage where you can complete the configuration.



First configuration

When entering the configuration for the first time, a short wizard will start setting some general settings and network configuration.

Enter the `Device name` (mandatory) and `installer notes`, and change the IP settings for the local network if necessary. Check all settings and adjust them where necessary. The “**Basic**” and “**Advanced**” chapters explain the sections below.

Factory reset Restart Identify unit Upload firmware

Device serial: ID POS2 R823 A 0051
Firmware version: 1.5.4+0EA2D402

Device name (required):

Installer notes:

IP setting: Automatic IP Configuration (DHCP)

IP address: 10.2.16.176

Subnet mask: 255.255.0.0

Gateway: 10.2.1.1

DNS server: 10.1.8.10

Alternative DNS server: 10.1.8.11:1664

MAC address: 00:0D:A0:11:00:B3

Please restart the device to apply these settings

Use alternative USB ethernet IP:

USB ethernet IP: 192.0.2.1

Enter the Device name and Installer notes.

Change the network settings, if needed, and press the Use Offline button to configure an OFFLINE reader.

A confirmation window pops up.

Factory reset Restart Identify unit Upload firmware

Device serial: iD POS2 R823 A 0051

Firmware version: 1.5.4+0EA2D402

Are you sure you want to use the device offline?

Choose the country this device is being used in and then press Yes, use offline to apply the network settings and continue without registering the device with Nedap Device Management.

The device will be limited to standalone functionality until a Factory Reset is performed. This means:

- No settings synchronization
- No remote device monitoring from Device Management
- No automatic firmware updates
- No connection to the iD Cloud EPC Information System

Operating country: --- COUNTRY ---

Password (required):

If you wish to use the device without these services, choose Yes, use offline.

Yes, use offline **No, go back**

Enter the Operating country to match the local RFID regulations.

Enter the Password (required).



The password is: NedapRetail123

Press the Yes, use offline button.



There will be no registration, authentication, iD Cloud connection, and Device Management connection. Also, it is not possible to update the reader over the air. NTP is optional.



Switching between an ONLINE and OFFLINE configuration is only possible by factory resetting the reader.

After the reader restarts, it is necessary to log in before being able to configure the reader. Use the same password as the one used in the wizard (see above).



Settings Scan events Logging

Login

X

Predefined configuration

A predefined configuration is much easier to use for larger installations. It prevents mistakes and makes the installations much quicker.

For OFFLINE systems, it is possible to use a “source” configuration file, which can be uploaded to every OFFLINE reader that needs to be a “clone” of this “source”.

- Create a “source” configuration file by configuring a reader and then saving its configuration by pressing the `Download` button.
- Upload the configuration from this “source” configuration file by using the `Upload` button to “clone” it into a new reader.

DEVICE

Device serial	iD POS2 R823 A 0068	
Device type	idpos2	
Current firmware version	1.5.2+0FA8553B	
Onboard logging level	Warning	<code>Download logs</code>
Upload configuration	Choose File	No file chosen
Download configuration	config.json	
Upload firmware	Choose File	No file chosen
<code>Restart</code> <code>Flush buffers</code> <code>Factory reset</code>		

Configuration sections

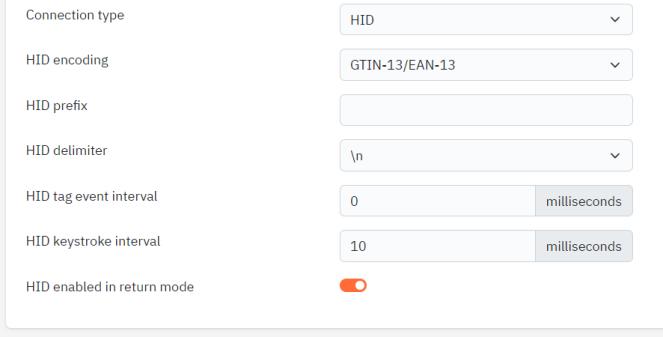
The configuration page is split up into 2 sections:

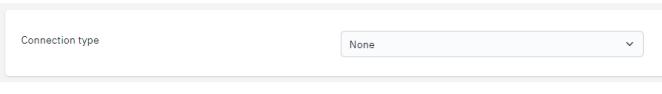
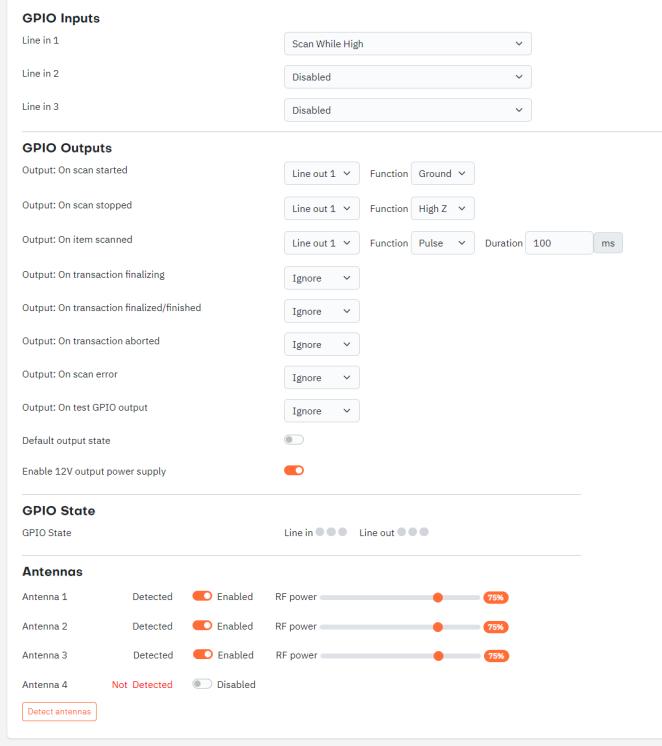
- Basic
- Advanced

Configuration section “Basic”

The following options are available under the “**Basic**” section.

Settings	Screen
SYSTEM <i>Basic system information and installer notes.</i> <i>The Device name is shown in Device Management as the Location</i> <i>The Operating country configures the RF to match the local regulations</i>	Device name <input type="text" value="First Floor POS 3"/> Installer notes <input type="text"/> Operating country <input type="text" value="NL"/>
LIGHT AND SOUND (iD POS Pro only) <i>Signaling settings with the option to test</i>	Light enabled <input checked="" type="checkbox"/> Sound volume <input type="range" value="75"/> <input type="button" value="Test light and sound"/>
RF POWER (iD POS Pro only) <i>RF Power to set the reading power. This impacts the reading distance.</i>	RF power <input type="range" value="100"/> 100%

Settings	Screen
<p>CONNECTION TO POS</p> <p>Type of setup and integration with the POS (Point of Sale)</p> <ul style="list-style-type: none"> • HID (Human Interface Devices) <ul style="list-style-type: none"> • USB connection to the POS to interface like a barcode scanner • A lot of settings are available <ul style="list-style-type: none"> • HID encoding defines the encoding used; see table below * • HID prefix and HID delimiter defining the way each tag is ‘packaged’ • HID tag event interval and HID keystroke interval allow for slowing down the speed at which the tag is transferred to the POS • Last but not least, HID enabled in return mode defines whether a return will also be visible in the POS. Independent of this setting, the event will always be transferred to iD Cloud if the iD Cloud feature is enabled • Websocket <ul style="list-style-type: none"> • USB or Network connection to the POS • Just two settings <ul style="list-style-type: none"> • Websocket POS API port (requires restart) defines the port at which the POS will communicate with the reader. 	 

Settings	Screen
<ul style="list-style-type: none"> • Limit websocket POS API to USB when turned on, disables the WebSocket connection to the external network interface. • Allow duplicate tags when turned on; will show the tag every time is read • Nedap EAS iD <ul style="list-style-type: none"> • Stand alone on Nedap pre-programmed labels • Just one setting • Allow return in Nedap EAS iD standalone mode enables the updating of the tag to the unsold state • None <ul style="list-style-type: none"> • No connection to the POS • No additional settings • Useless in OFFLINE mode 	 
<p>SELF CHECKOUT (iD SCO Pro only)</p> <p>With the settings in this block, it is possible to configure how the iD SCO Pro will interface with its general purpose in- and outputs.</p> <p>The way this is done is outside the scope of this document and will be discussed in the iD SCO Pro Manual.</p>	

* HID encoding options:

HID Encoding Options	Example Output
GS-1 Element String	010200013935120021141597811800
GTIN-12/UPC-12	200013935120
GTIN-13/EAN-13	2000139351200
GTIN-14/ITF-14	02000139351200
GTIN-14/GS1-128	0102000139351200
SGTIN Pure Identity URI	urn:epc:id:sgtin:2000139.035120.141597811800
EPC HEX	30347A142C224C20F7E32458 (shows the HEX data as read from the EPC field in the tag; this can be longer than the SGTIN conversion)



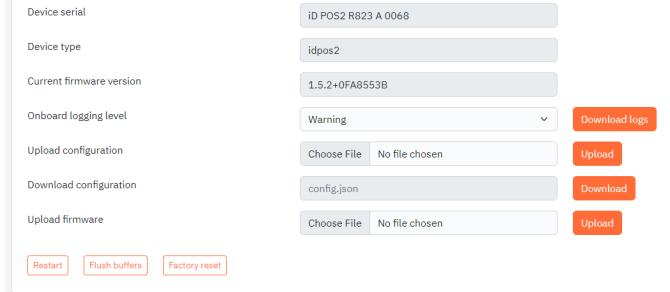
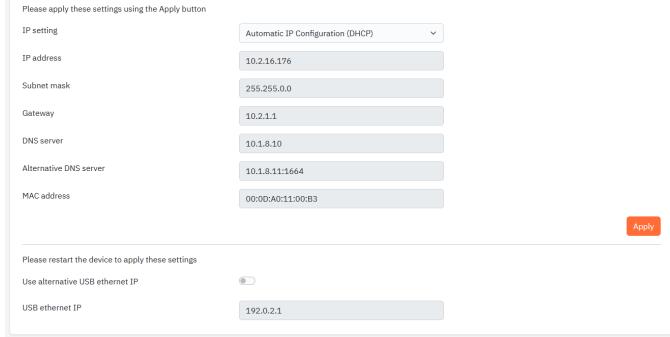
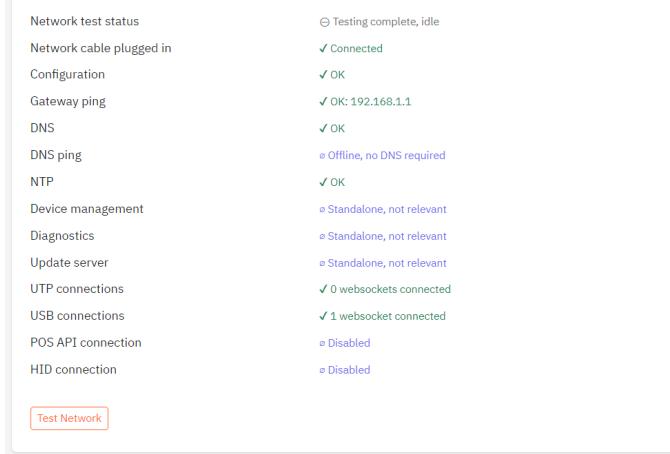
To better match the GS1 standards, the format of the GS1 Element String has been changed since ID POS Pro firmware versions 1.4.2

- before 1.4.2 : "(01)02000012302671(21)241789531760"
- 1.4.2 and up: "010200001230267121241789531760"

To create a robust implementation using GS1 Element String, it is advised to be able to handle both formats.

Configuration section “Advanced”

The following options are available in the “Advanced” section.

Settings	Screen
DEVICE <i>Basic device information and firmware options.</i> Onboard logging level to set the level of logging information saved in the reader Upload configuration allows you to upload a predefined setup Download configuration allows you to download the current configuration, which can be used for another reader to upload the same configuration Upload firmware . Upload a firmware file to go to a higher version of the firmware.	
NETWORK <i>Local network settings (Static IP or DHCP)</i> Use alternative USB ethernet IP allows the use of an alternative IP address for the USB network connection in case 192.0.2.x is already in use at the customers' network.	
SYSTEM STATUS <i>This section shows the status of all network-related connections. Press Test Network to start. Wait until Network test status shows Testing complete, idle</i>	

Settings	Screen
SECURITY Limit configuration access to USB <i>when turned on, disable the configuration through the IP address.</i>	<p>Limit configuration access to USB <input checked="" type="checkbox"/></p>

Settings	Screen
<p>SCANNING</p> <p><i>Options for scan/read behavior and to set the disposition options for the Primary and Secondary disposition and corresponding sublocations (Short and Long button press for iD POS Pro)</i></p> <p>Always on is an option to keep the Radio transmitter turned on for reading labels. Otherwise, it will automatically turn off after the Scan timeout</p> <p>Duplicate tag reading timeout prevents many reads of the same EPC</p> <p>Primary disposition & Long button press / Secondary disposition change the behavior of the button/web socket. Available dispositions are:</p> <ul style="list-style-type: none"> • retail_sold, sellable_accessible, or sellable_not_accessible for selling, returning to the Sales Floor, and returning to the Stockroom, respectively. <p>Other options:</p> <ul style="list-style-type: none"> • damaged • non_sellable_other • reserved <p>Transaction mode is set depending on the Connection to POS setting:</p> <ul style="list-style-type: none"> • HID and None <ul style="list-style-type: none"> • When turned ON, multiple items will be sent in one event towards iD Cloud when the transaction is finished (by pressing the key) instead of item per item when turned OFF • Websocket 	

Settings	Screen
<ul style="list-style-type: none"> • Forced ON • Nedap EAS iD • <i>not used</i> <p>With Minimum RSSI it is possible to filter on the RSSI value of the tag read. Tags read with an RSSI below this value are discarded.</p> <p>Allow non-GS1 labels to enable the reading of labels that are not formatted according to the GS1 standards. These labels are not transmitted to iD Cloud.</p> <p>With Radio on it is possible to turn the radio transmitter on once for reading labels; it will automatically turn off after the Scan timeout</p>	
REMOTE <p>Set a desired time server NTP server address (Network Time Protocol) for the correct event time with an NTP refresh interval on how often this should be synchronized.</p>	<p>NTP server address <input type="text" value="pool.ntp.org"/></p> <p>NTP refresh interval <input type="text" value="60"/> Minutes</p> <p><input type="button" value="Test time server"/></p>
RADIO <p>With Transmit RF mode, one can choose different RFID channels.</p> <p>Certification-related settings for the Region in which the iD POS Pro is used</p>	<p>Transmit RF mode <input type="text" value="Mode 285"/></p> <p>Region <input type="text" value="ETSI_LOWER"/></p>

Common setups

Description	Integration	ID POS Pro / ID SCO Pro Connected To POS	Database Connection	Integration Effort
Full setup via POS	HID or Websocket	Yes, HID (USB) or API (USB or local network)	POS takes care of status changes	oooo
Standalone	Nedap EASiD	No	Status is in the RFID tag	o

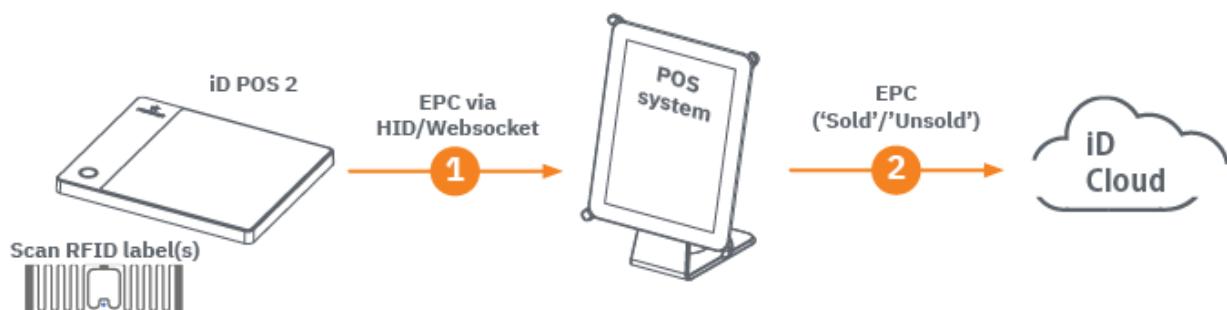
Full setup via POS

In this case, the reader's main task is to provide EPC information to the POS system. The POS system then updates iD Cloud with the relevant new disposition.

Instead of iD Cloud, a customer solution is also possible.

Pro: *Integrated with the POS so that it can replace a barcode scanner for fast checkout and is secure, because finalized payment can be required before setting to 'Sold' in iD Cloud*

Con: *It might be more difficult to implement this on the POS because of the integration towards iD Cloud for each POS EPC or other data format*



CONNECTION TO POS

Connection type	<input style="border: 1px solid #ccc; padding: 5px; width: 150px; height: 30px;" type="button" value="HID"/> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: -10px;"> GTIN-13/EAN-13 GS-1 Element String GTIN-12/UPC-12 GTIN-13/EAN-13 GTIN-14/ITF-14 GTIN-14/GS1-128 SGTIN Pure Identity URI EPC HEX </div>
HID encoding	<input style="border: 1px solid #ccc; padding: 5px; width: 150px; height: 30px;" type="button" value="GTIN-13/EAN-13"/> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: -10px;"> GTIN-13/EAN-13 GS-1 Element String GTIN-12/UPC-12 GTIN-13/EAN-13 GTIN-14/ITF-14 GTIN-14/GS1-128 SGTIN Pure Identity URI EPC HEX </div>
HID prefix	
HID delimiter	
HID tag event interval	<input style="width: 50px;" type="text" value="10"/> milliseconds
HID keystroke interval	<input style="width: 50px;" type="text" value="10"/> milliseconds
HID enabled in return mode	<input checked="" type="checkbox"/>

or

CONNECTION TO POS

Connection type	WebSocket
WebSocket POS API port (requires restart)	10921
Limit websocket POS API to USB	<input checked="" type="checkbox"/>
No duplicate filtering for POS API	<input type="checkbox"/>

Standalone

This is a use case in which the reader only updates the RFID tags itself with a 'Sold' flag. This setup requires the use of EASiD Nedap tags. There is no connection to a POS system or EAS database.

Pro: Straightforward and quick to set up.

Con: Something separate is required for the POS (e.g., a barcode scanner). This only works for preprogrammed Nedap labels.

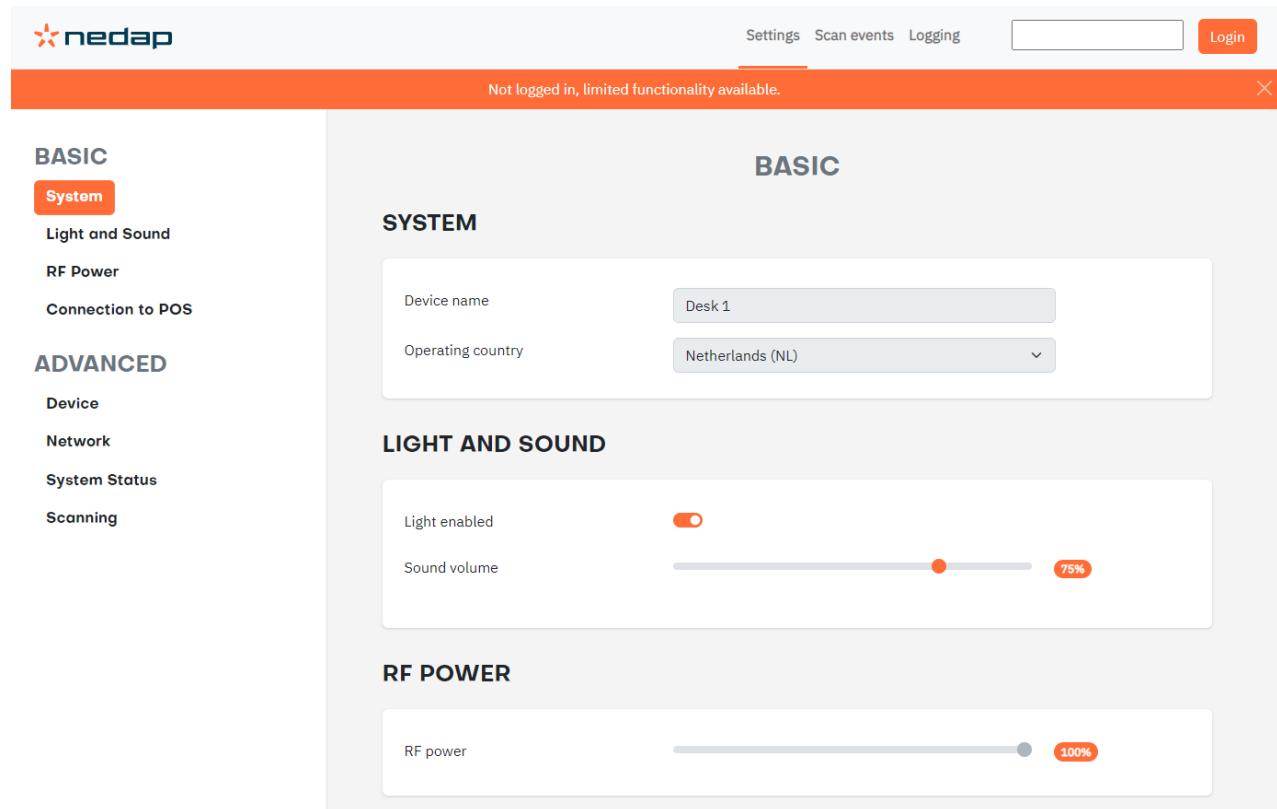


CONNECTION TO POS

Connection type	Nedap EAS iD
Allow return in Nedap EAS iD standalone mode	<input type="checkbox"/>

View and Edit settings

With an OFFLINE setup, you will have to log in to be able to change its settings when connected to the local interface on 192.0.2.1



The screenshot shows the nedap offline settings interface. The left sidebar has two main sections: **BASIC** (with **System** selected) and **ADVANCED** (with **Device**, **Network**, **System Status**, and **Scanning**). The main content area is divided into sections: **SYSTEM** (Device name: Desk 1, Operating country: Netherlands (NL)), **LIGHT AND SOUND** (Light enabled: On, Sound volume: 75%), and **RF POWER** (RF power: 100%). A status bar at the top indicates "Not logged in, limited functionality available." and includes links for Settings, Scan events, Logging, a search bar, and a Login button.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2025

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 48

Document Last modification date 6 January 2025

Document PDF Exported 6 January 2025 **by** Nedap Retail | Operations



support-retail@nedap.com

Nedap Sense Guideline

iD POS PRO & iD SCO Pro Configuration

version 123, January 2025

Introduction	3
Available documentation	3
Connect to the iD POS Pro and iD SCO Pro.....	4
Driver installation - Microsoft Windows	4
First configuration.....	5
Predefined configuration.....	9
Configuration sections	10
Configuration section “Basic”	10
Configuration section “Advanced”	17
Common setups	22
Simple setup with POS system integration	23
Simple setup without POS system integration	25
Full setup via POS	26
Full setup via iD POS Pro or iD SCO Pro	29
Standalone	31
View settings	32

Introduction

This guideline describes the configuration of the Nedap Retail iD POS Pro and iD SCO Pro based on the **most common** setups.



This manual covers the operation and features of the iD POS Pro and the iD SCO Pro, which are identical. Most of the instructions, settings, and features described herein apply to both devices. Differences between the two will be indicated. Please pay special attention to these notes to ensure proper usage of your specific device.

Available documentation

Next to some commercial documentation, the following technical documentation is available for the iD POS PRO and iD SCO PRO:

- iD POS PRO - Manual
- iD SCO PRO - Manual
- iD POS PRO & iD SCO PRO - Configuration
- iD POS PRO & iD SCO PRO - OFFLINE Configuration
- iD POS PRO & iD SCO PRO - Network information
- iD POS PRO & iD SCO PRO - WebSocket POS integration
- iD POS PRO & iD SCO PRO - WebSocket and Postman
- iD POS PRO & iD SCO PRO - Windows driver installation
- iD POS PRO & iD SCO PRO - Firmware and Settings API



This guideline only describes the ONLINE setups for the iD POS Pro and iD SCO Pro. OFFLINE setups are described in the iD POS Pro & iD SCO Pro OFFLINE Configuration manual



Throughout this manual, the term “reader” refers to both iD POS Pro and iD SCO Pro.

Connect to the iD POS Pro and iD SCO Pro

Connect a laptop to the service port on the reader using a USB cable with a USB-C connector.

⚠ Ensure the iD POS Pro is powered through standard Power over Ethernet (PoE) IEEE802.3af, class 0.

For the iD SCO Pro, exclusively use the included power supply.

⚠ A Nedap Retail account is required to configure the readers.

⚠ A driver is required to configure the readers (see the list with available documentation)

Driver installation - Microsoft Windows

To configure a reader, a Microsoft Windows driver must be installed. For instructions, please refer to the “*iD POS Pro & iD SCO Pro Windows driver installation*” manual.

⚠ At the moment, only Microsoft Windows is supported.

Once the Windows driver is installed, you can enter the configuration by opening your browser and navigating to <http://192.0.2.1>; this will open a webpage where you can configure it.



First configuration

When entering the configuration for the first time, a short wizard will start to set some general settings, set network configuration, and link to the correct store in Device Management.

Enter the `Device name` (mandatory, shown in the `Location` field in Device Management), `Installer notes`, and IP settings. Check all settings and change where needed. The “**Basic**” and “**Advanced**” chapters explain the various sections.

Factory reset Restart Identify unit Upload firmware

Device serial: ID POS2 R823 A 0051
Firmware version: 1.5.4+0EA2D402

Device name (required):

Installer notes:

IP setting: Automatic IP Configuration (DHCP) ▾
IP address: 10.2.16.176
Subnet mask: 255.255.0.0
Gateway: 10.2.1.1
DNS server: 10.1.8.10
Alternative DNS server: 10.1.8.11:1664
MAC address: 00:0D:A0:11:00:B3

Apply settings

Show network status

Please restart the device to apply these settings

Use alternative USB ethernet IP:

USB ethernet IP: 192.0.2.1

Use offline **Register device**

Enter the **Device name** and **Installer notes**.

Change the network settings, if needed, and press the **Register device** button to configure an ONLINE reader.

The reader must then be linked to a store in Device Manager. A link easily links the reader to the correct store.



FINALIZE REGISTRATION

[Factory reset](#) [Restart](#) [Identify unit](#)

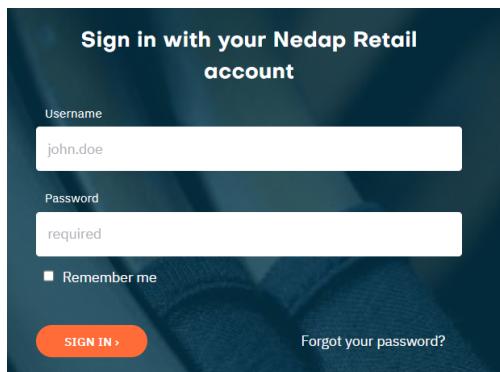
Please finalize the registration by assigning the device to a store using the following link:

https://devices.nedapretail.com/authenticate_system/0e35e49e-dbdc-40cb-9bcf-4096d100bcea



Press the link; you will get the opportunity now if you are not logged in.

Log in with your Nedap Retail Account:



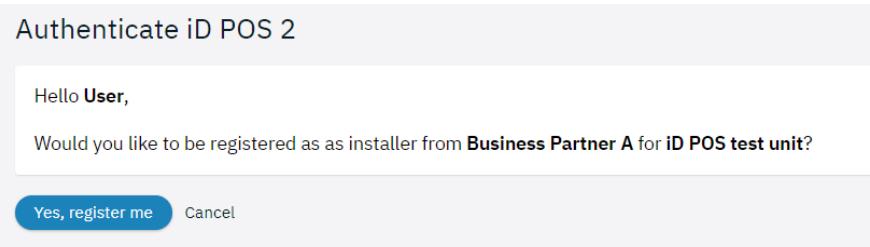
The form is titled "Sign in with your Nedap Retail account". It has two input fields: "Username" containing "john.doe" and "Password" containing "required". There is a "Remember me" checkbox and a "SIGN IN >" button. A "Forgot your password?" link is located below the button.



The following Device Management permission is required to configure the iD POS Pro:

- Manage Systems

Register the reader:



The form is titled "Authenticate iD POS 2". It displays a message "Hello User," and a question "Would you like to be registered as as installer from **Business Partner A** for **iD POS test unit**?". At the bottom are two buttons: "Yes, register me" and "Cancel".

Link the reader to the correct store in Device Management:

Authenticate system

💡 You have been successfully registered as an installer for this iD POS Pro. Please follow the steps below to authenticate your device.

Store		System information	
Select the store this system should be placed in.		Name	iD POS test unit
Nedap Companies	CUSTOMER ORGANIZATION	Firmware	1.0.0+E7E585B
Nv Groenlo	DIVISION	version	
Division A	DIVISION	Device serial	idpos-2 R823 A 0051
Store 1	STORE	MAC address	00:0D:A0:11:00:B3

Registration notes (optional)

Authenticate system **Cancel**

Predefined configuration

It is much easier to use a predefined configuration for higher quantities of installations. This prevents mistakes and makes the installation much quicker.

- Retrieve the configuration from a Device Management preset (At this moment, only for Nedap key accounts) [Import from Device Management](#)

DEVICE

Device serial	iD POS2 R823 A 0068
Device type	idpos2
Current firmware version	1.5.2+0FA8553B
Onboard logging level	Warning
Upload firmware	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/>
<input type="button" value="Restart"/> <input type="button" value="Flush buffers"/> <input type="button" value="Factory reset"/>	

Configuration sections

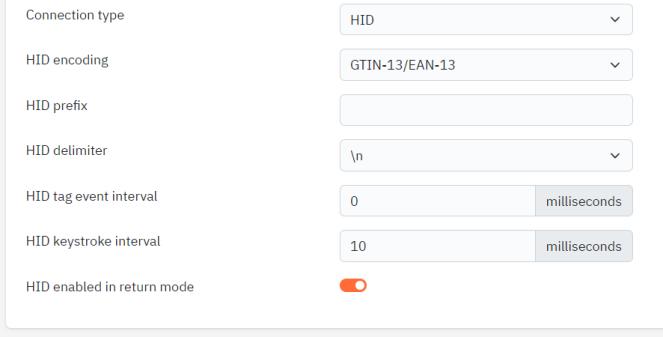
The configuration page is split up into two sections:

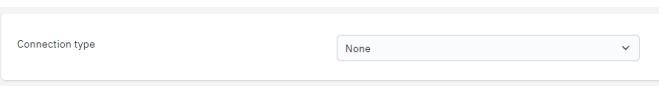
- Basic
- Advanced

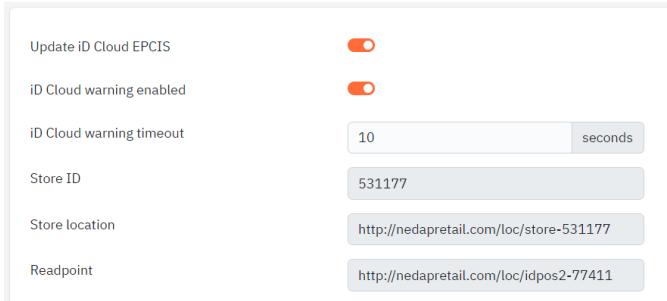
Configuration section “Basic”

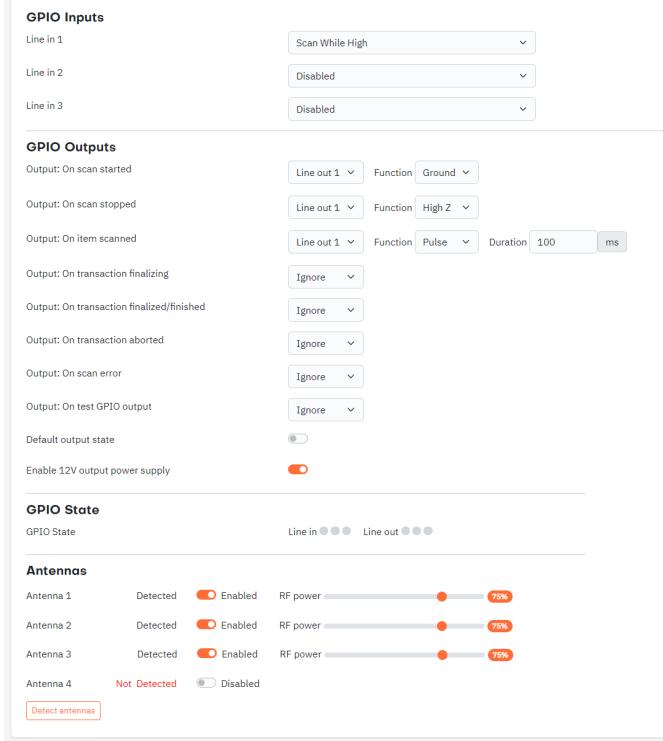
The following options are available under “Basic”:

Settings	Screen
SYSTEM <i>Basic system information and installer notes.</i> <i>The Device name is shown in Device Management as the Location</i> <i>The System ID is used in Device Management to identify the device</i> <i>The Operating country configures the RF to match the local regulations</i>	<div data-bbox="767 822 1421 1057"> <p>Device name <input type="text" value="Test 1.3.2"/></p> <p>Installer notes <input type="text"/></p> <p>System ID <input type="text" value="ab7743a1-2861-40d4-a169-f4f8db197b2a"/></p> <p>Operating country <input type="text" value="NL"/></p> </div>
LIGHT AND SOUND (iD POS Pro only) <i>Signaling settings with the option to test</i>	<div data-bbox="767 1264 1421 1421"> <p>Light enabled <input checked="" type="checkbox"/></p> <p>Sound volume <input type="range" value="75%"/></p> <p><a data-bbox="790 1376 906 1401" href="#">Test light and sound</p> </div>
RF POWER (iD POS Pro only) <i>RF Power to set the reading power. This impacts the reading distance.</i>	<div data-bbox="767 1444 1421 1522"> <p>RF power <input type="range" value="100%"/></p> </div>

Settings	Screen
<p>CONNECTION TO POS</p> <p>Type of setup and integration with the POS (Point of Sale)</p> <ul style="list-style-type: none"> • HID (Human Interface Devices) <ul style="list-style-type: none"> • USB connection to the POS to interface like a barcode scanner • A lot of settings are available <ul style="list-style-type: none"> • HID encoding defines the encoding used; see table below * • HID prefix and HID delimiter defining the way each tag is ‘packaged’ • HID tag event interval and HID keystroke interval allow for slowing down the speed at which the tag is transferred to the POS • Last, HID enabled in return mode defines whether a return will be visible in the POS. Independent of this setting, the event will always be transferred to iD Cloud if the iD Cloud feature is enabled • Websocket <ul style="list-style-type: none"> • USB or Network connection to the POS • Just two settings <ul style="list-style-type: none"> • The Websocket POS API port (which requires restart) defines the port at which the POS will communicate with the reader. 	 

Settings	Screen
<ul style="list-style-type: none"> • Limit websocket POS API to USB when turned on, disables the WebSocket connection to the external network interface. • Allow duplicate tags. When turned on, it will show the tag time as long as it is read. When turned off, the tag will only come up once per session. • Nedap EAS iD <ul style="list-style-type: none"> • Stand alone on Nedap pre-programmed tags • Just one setting <ul style="list-style-type: none"> • Allow return in Nedap EAS iD standalone mode, which enables updating the tag to the unsold state. • None <ul style="list-style-type: none"> • No connection to the POS • No additional settings 	 

Settings	Screen
<p>iD CLOUD</p> <p><i>iD Cloud information and settings</i></p> <p><i>Update iD Cloud EPCIS when set enables the connection of the reader to iD Cloud</i></p> <p><i>iD Cloud warning enabled when set, the LED will turn red, and the reader will start to beep when no response is received from iD Cloud</i></p> <p><i>The iD Cloud warning timeout is the time of no response before it starts signaling</i></p> <p><i>Store ID is the store identifier used at the Device Management and iD Cloud servers</i></p> <p><i>Store location shows the URL being used at the iD Cloud servers, where it is named Location Identifier</i></p> <p><i>Readpoint is the URL that defines this reader as part of the store at the Location Identifier</i></p> <p><i>When the connection to iD Cloud is interrupted, the transactions are saved until the connection is restored, even after a power cycle. The buffer for this is about 32k tags big. Once this limit is reached, new tags are dropped. The buffer can be emptied by pressing the Flush buffers button in the DEVICE section.</i></p>	

Settings	Screen																				
<p>SELF CHECKOUT (<i>iD SCO Pro only</i>)</p> <p>With the settings in this block, the <i>iD SCO Pro</i> can be configured to interface with its general-purpose inputs and outputs.</p> <p>GPIO Inputs</p> <p>Any input can be used to trigger the following options:</p> <ul style="list-style-type: none"> • Disabled - if unused • Scan While High - As long as this input is High Z, the scanning continues • Scan While High With Finish - Same, but once the input becomes Ground, the scan is finished (transferred to <i>iD Cloud</i>) • Start Scan - Start a scan, stopped when either a Stop Scan is executed or when the Scan Timeout is reached • Stop Scan - Stop the scanning of tags • Finish - Finish the transaction (transfer to <i>iD Cloud</i>. This can only be done after a Start Scan and a subsequent Stop Scan) • Toggle Scan - Combination of Start Scan and Stop Scan • Toggle Scan With Finish <ul style="list-style-type: none"> • Combination of Start Scan, Stop Scan and Finish • Abort - Cancels the current scan • Trigger Test Output - For test purposes <p>GPIO Outputs</p> <p>In this section, you can configure what event is done with a specific output.</p> <p>Available events:</p>	 <p>The screenshot shows the configuration interface for the <i>iD SCO Pro</i>. It includes sections for GPIO Inputs and GPIO Outputs, and a separate Antennas section.</p> <p>GPIO Inputs:</p> <ul style="list-style-type: none"> Line in 1: Scan While High Line in 2: Disabled Line in 3: Disabled <p>GPIO Outputs:</p> <ul style="list-style-type: none"> Output: On scan started: Line out 1 (Function: Ground) Output: On scan stopped: Line out 1 (Function: High Z) Output: On item scanned: Line out 1 (Function: Pulse, Duration: 100 ms) Output: On transaction finalizing: Ignore Output: On transaction finalized/finished: Ignore Output: On transaction aborted: Ignore Output: On scan error: Ignore Output: On test GPIO output: Ignore Default output state: Off Enable 12V output power supply: On <p>GPIO State:</p> <p>GPIO State: Line in 0 0 0 0 Line out 0 0 0 0</p> <p>Antennas:</p> <table border="1"> <thead> <tr> <th>Antenna</th> <th>Detected</th> <th>Enabled</th> <th>RF power</th> </tr> </thead> <tbody> <tr> <td>Antenna 1</td> <td>Detected</td> <td>Enabled</td> <td>75%</td> </tr> <tr> <td>Antenna 2</td> <td>Detected</td> <td>Enabled</td> <td>75%</td> </tr> <tr> <td>Antenna 3</td> <td>Detected</td> <td>Enabled</td> <td>75%</td> </tr> <tr> <td>Antenna 4</td> <td>Not Detected</td> <td>Disabled</td> <td></td> </tr> </tbody> </table> <p>Detect antennas</p>	Antenna	Detected	Enabled	RF power	Antenna 1	Detected	Enabled	75%	Antenna 2	Detected	Enabled	75%	Antenna 3	Detected	Enabled	75%	Antenna 4	Not Detected	Disabled	
Antenna	Detected	Enabled	RF power																		
Antenna 1	Detected	Enabled	75%																		
Antenna 2	Detected	Enabled	75%																		
Antenna 3	Detected	Enabled	75%																		
Antenna 4	Not Detected	Disabled																			

Settings	Screen
<ul style="list-style-type: none"> On scan started , On scan stopped , On item scanned , On transaction finalizing , On transaction finalized/finished , On transaction aborted , On scan error, and On test GPIO output - <p><i>Each of these events can trigger an action on an output. Only one output can be triggered by each event; the same output, however, can be triggered by as many events as needed.</i></p>	
<p>Every output can be configured as:</p> <ul style="list-style-type: none"> Toggle - On the selected event, the output will toggle Pulse - On the chosen event, the output will pulse with a selectable Duration Ground - On the chosen event, the output will go to the Ground level High Z - Same, but then to the 'High Z' state <p>Two extra options for all outputs:</p> <ul style="list-style-type: none"> Default output state - The default state is Ground for Pulse and Toggle . When setting this to true , the default state becomes High Z Enable 12V output power supply - This enables the 12V on the GPIO connector <p>GPIO State</p> <p>This shows the current state of the GPIO in- and outputs</p> <p>Antennas</p> <p>The iD SCO Pro can interface with a maximum of 4 antennas, which can be Enabled per antenna. The RF power can be configured.</p>	

Settings	Screen
Detect antennas allow you to find the connected antennas.	

* HID encoding options:

HID Encoding Options	Example Output
GS-1 Element String	010200013935120021141597811800
GTIN-12/UPC-12	200013935120
GTIN-13/EAN-13	2000139351200
GTIN-14/ITF-14	02000139351200
GTIN-14/GS1-128	0102000139351200
SGTIN Pure Identity URI	urn:epc:id:sgtin:2000139.035120.141597811800
EPC HEX	30347A142C224C20F7E32458 (shows the HEX data as read from the EPC field in the tag; this can be longer than the SGTIN conversion)

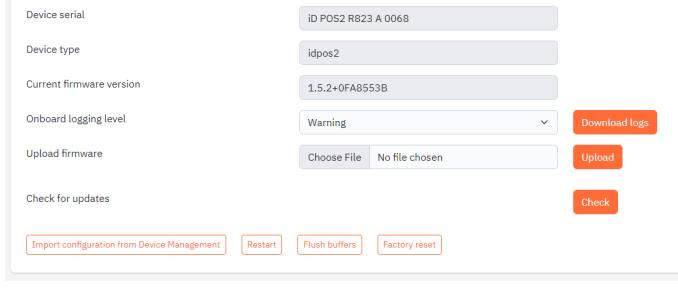
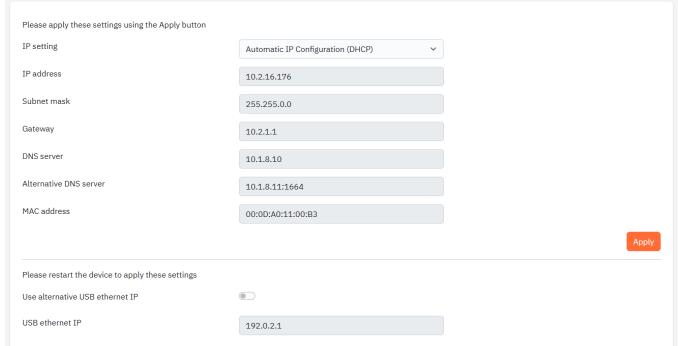
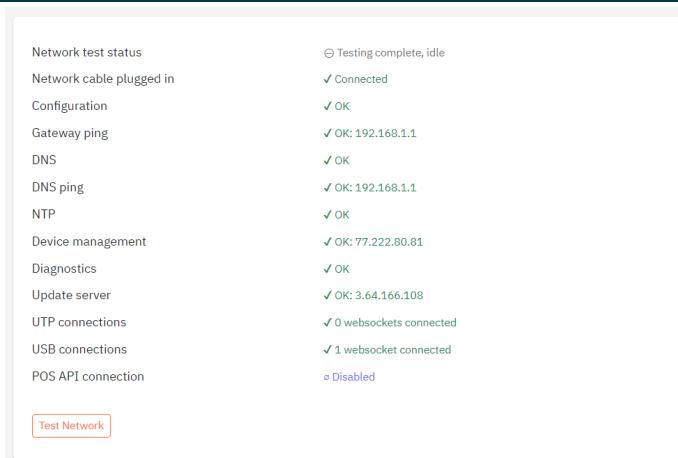


- To better match the GS1 standards, the format of the GS1 Element String and GTIN-14/GS1-128 has been changed since iD POS Pro firmware versions 1.4.2
 - before 1.4.2 : "(01)02000012302671(21)241789531760"
 - 1.4.2 and up: "010200001230267121241789531760"

To create a robust implementation using GS1 Element String or GTIN-14/GS1-128, it is advised to be able to handle both formats.

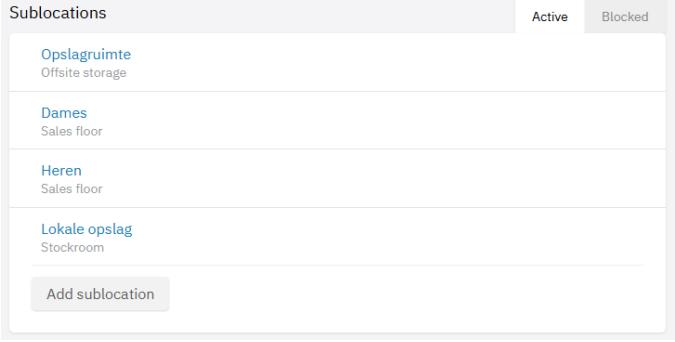
Configuration section “Advanced”

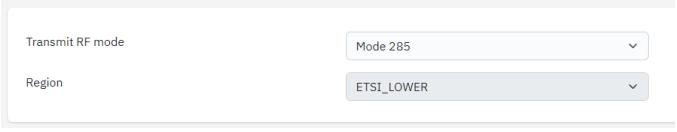
The following options are available under “Advanced”:

Settings	Screen
DEVICE <i>Basic device information and firmware options.</i> <i>Onboard logging level to set the level of logging information saved in the reader</i> <i>Upload firmware ; upload a firmware file to go to a higher version of the firmware</i> <i>Check for updates to see if they are available. When they are available, installation can be started by pressing the button.</i>	
NETWORK <i>Local network settings (Static IP or DHCP)</i> <i>Use alternative USB ethernet IP allows the use of an alternative IP address for the USB network connection in case 192.0.2.x is already in use at the customer's network.</i>	
SYSTEM STATUS <i>This section shows the status of all network-related connections. Press Test Network to start. Wait until Network test status shows Testing complete, idle</i>	

Settings	Screen
<p>SECURITY</p> <p><i>When turned on, limit configuration access to USB and disable the configuration through the IP address.</i></p>	<p>Limit configuration access to USB <input checked="" type="checkbox"/></p>

Settings	Screen
<p>SCANNING</p> <p><i>Options for scan/read behavior and to set the disposition options for the Primary and Secondary disposition and corresponding sublocations (Short and Long button press for iD POS Pro)</i></p> <p><i>Always on is an option to keep the Radio transmitter turned on for reading tags. Otherwise, it will automatically turn off after the Scan timeout</i></p> <p><i>Duplicate tag reading timeout A tag is re-read if it re-enters the RFID field after the set time. Ignored in Websocket POS connections.</i></p> <p><i>Primary disposition & Long button press / Secondary disposition change the behavior of the button/Websocket. Available dispositions are:</i></p> <ul style="list-style-type: none"> • <code>retail_sold</code>, <code>sellable_accessible</code>, or <code>sellable_not_accessible</code> for selling, returning to the Sales Floor, and returning to the Stockroom, respectively. <p><i>Other options:</i></p> <ul style="list-style-type: none"> • <code>damaged</code> - This is the status Damaged in iD Cloud • <code>non_sellable_other</code> - This is the status Held in iD Cloud • <code>reserved</code> - This is the status Reserved in iD Cloud 	

Settings	Screen
<p>The Sublocation can be changed from 'default' to one of the specific sublocations as optionally defined in Device Management (see example on the right) for the store. This sublocation will be used as the business location for the disposition in iD Cloud.</p> <p>Transaction mode is set depending on the Connection to POS setting:</p> <ul style="list-style-type: none"> • HID and None <ul style="list-style-type: none"> • When turned ON, multiple items will be sent in one event towards iD Cloud when the transaction is finished (by pressing the button) instead of item per item when turned OFF • Websocket <ul style="list-style-type: none"> • Forced ON • Nedap EAS iD <ul style="list-style-type: none"> • not used <p>With Minimum RSSI, it is possible to filter by the RSSI value of the tag read. Tags read with an RSSI below this value are discarded.</p> <p>Allow non-GS1 labels to enable the reading of tags that are not formatted according to the GS1 standards. These tags are not transmitted to iD Cloud.</p> <p>With Radio on, it is possible to turn the radio transmitter on once for reading tags; it will automatically turn off after the Scan timeout</p>	
<h3>REMOTE</h3> <p>Set a desired time server NTP server address (Network Time Protocol) for the correct event time and an NTP refresh interval for how often this should be synchronized.</p>	

Settings	Screen
<p>RADIO</p> <p><i>With Transmit RF mode, one can choose different RFID channels.</i></p> <p><i>Certification-related settings for the Region in which the iD POS Pro is used</i></p>	

Common setups

Description	Integration	Reader Connected To POS	Reader Connected To ID Cloud	Integration Effort
Simple setup with POS system integration	HID	Yes, HID (USB)	Yes (local network)	oo
Simple setup without POS system integration	None	No	Yes (local network)	o
Full setup via POS	HID or Websocket	Yes, HID (USB) or API (USB or local network)	No, POS takes care of status changes	oooo
Full setup via reader	WebSocket	Yes, API (USB or local network)	Yes (local network)	ooo
Standalone	Nedap EASiD	No	No, the status is in the RFID tag	o

Default business steps and dispositions used for iD Cloud:

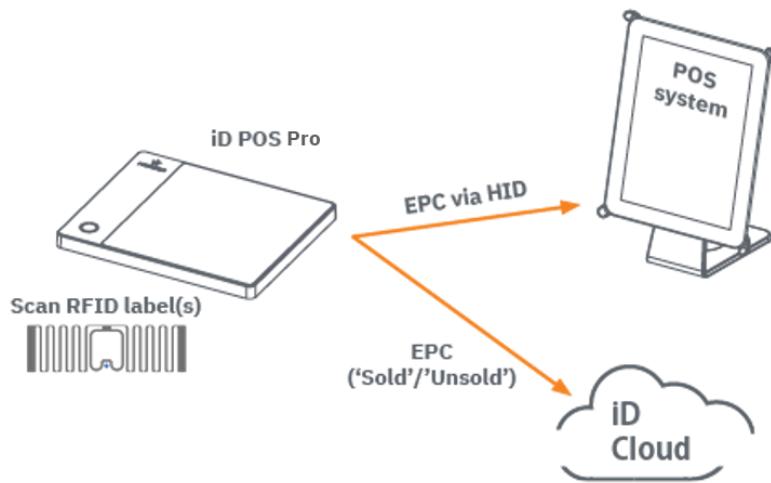
Functionality	Biz_step	Disposition
Sell items	urn:epcglobal:cbv:bizstep:retail_selling	urn:epcglobal:cbv:disp:retail_sold
Return items	urn:epcglobal:cbv:bizstep:retail_selling	urn:epcglobal:cbv:disp:sellable_accessible

Simple setup with POS system integration

They are intended to be used in pilots or during the start of a project. The aim is to have a reader working with as little integration needed as possible. The reader is connected to the POS via a USB HID interface and to iD Cloud using the Ethernet interface. The user sets the mode (Sell, Return) with a button.

Pro: Quick to set and integrated with the POS, so that it can replace a barcode scanner for fast checkout

Con: Items are directly set to 'Sold' in iD Cloud when the payment process on the POS is not complete yet



CONNECTION TO POS

Connection type	HID
HID encoding	GTIN-13/EAN-13
HID prefix	GS-1 Element String GTIN-12/UPC-12 GTIN-13/EAN-13 GTIN-14/ITF-14 GTIN-14/GS1-128 SGTIN Pure Identity URI EPC HEX
HID delimiter	
HID tag event interval	10 milliseconds
HID keystroke interval	
HID enabled in return mode	<input checked="" type="checkbox"/>

ID CLOUD

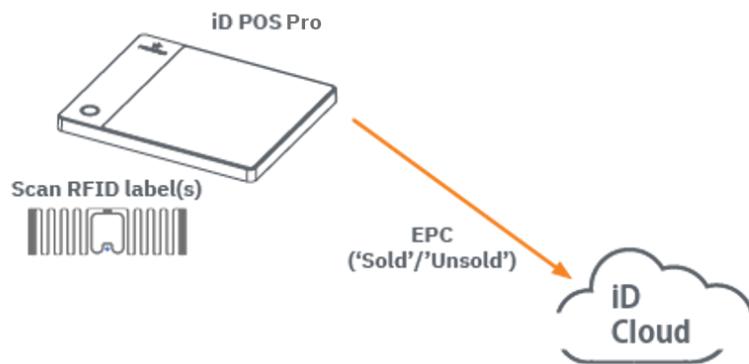
Update iD Cloud EPCIS	<input checked="" type="checkbox"/>
iD Cloud warning enabled	<input checked="" type="checkbox"/>
iD Cloud warning timeout	10 seconds
Store ID	531177
Store location	http://nedapretail.com/loc/store-531177
Readpoint	http://nedapretail.com/loc/idpos2-764

Simple setup without POS system integration

This is the same as the standard simple integration, except that the USB HID keyboard interface is not connected to the POS system. This is the most straightforward possible integration.

Pro: Straightforward and quick to set up

Con: Items are directly set to 'Sold' in iD Cloud when the payment process on the POS is not complete yet, and still something separate is required for the POS (e.g., barcode scanner)



CONNECTION TO POS

Connection type

None

ID CLOUD

Update iD Cloud EPCIS



iD Cloud warning enabled



iD Cloud warning timeout

10

seconds

Store ID

531177

Store location

<http://nedapretail.com/loc/store-5311>

Readpoint

<http://nedapretail.com/loc/idpos2-764>

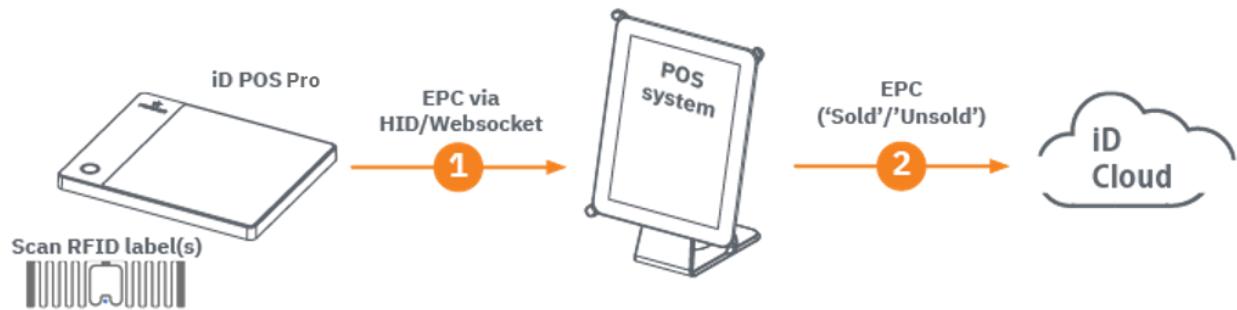
Full setup via POS

In this case, the reader's main task is to provide EPC information to the POS system. The POS system then updates iD Cloud with the relevant new disposition.

Instead of iD Cloud, a customer solution is also possible.

Pro: *Integrated with the POS so that it can replace a barcode scanner for fast checkout and is secure because finalized payment can be required before setting to 'Sold' in iD Cloud*

Con: *It might be more challenging to implement this on the POS because of the integration towards iD Cloud for each POS EPC or other data format.*



CONNECTION TO POS

Connection type	HID
HID encoding	GTIN-13/EAN-13
HID prefix	GS-1 Element String
	GTIN-12/UPC-12
	GTIN-13/EAN-13
HID delimiter	GTIN-14/ITF-14
	GTIN-14/GS1-128
HID tag event interval	SGTIN Pure Identity URI
	EPC HEX
HID keystroke interval	10 milliseconds
HID enabled in return mode	<input checked="" type="checkbox"/>

ID CLOUD

Update iD Cloud EPCIS	<input type="checkbox"/>
iD Cloud warning enabled	<input type="checkbox"/>
iD Cloud warning timeout	10 seconds
Store ID	531177
Store location	http://nedapretail.com/loc/store-5311
Readpoint	http://nedapretail.com/loc/idpos2-764

or

CONNECTION TO POS

Connection type

WebSocket

WebSocket POS API port (requires restart)

10921

Limit websocket POS API to USB



No duplicate filtering for POS API



ID CLOUD

Update iD Cloud EPCIS



iD Cloud warning enabled



iD Cloud warning timeout

10

seconds

Store ID

531177

Store location

<http://nedapretail.com/loc/store-5311>

Readpoint

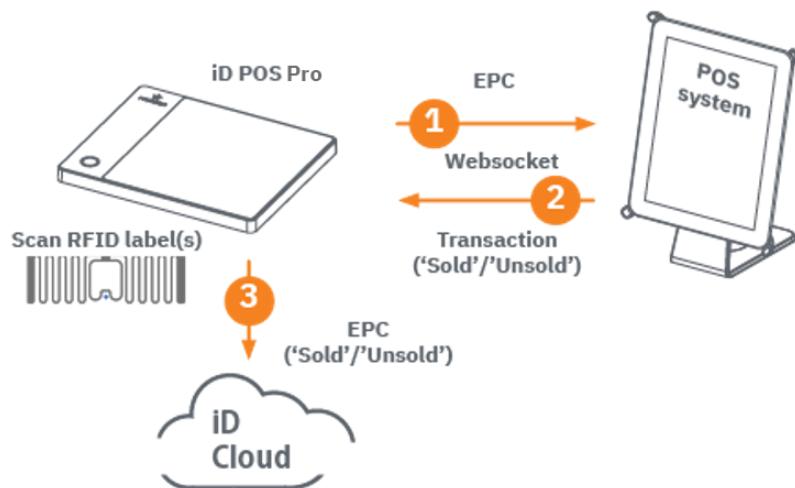
<http://nedapretail.com/loc/idpos2-764>

Full setup via iD POS Pro or iD SCO Pro

It is similar to the *Full setup via POS*, with the addition that the reader is also responsible for updating the EAS database. The POS system initiates this by returning the disposition to the reader once a transaction has been completed. The reader is now responsible for updating iD Cloud with the relevant new disposition.

Pro: *Integrated with the POS so that it can replace a barcode scanner for fast checkout, and it is secure because the payment process is required before setting to 'Sold' in iD Cloud*

Con: *It might be more challenging to implement this on the POS because of integration with the reader*



CONNECTION TO POS

Connection type

WebSocket

▼

WebSocket POS API port (requires restart)

10921

Limit websocket POS API to USB



No duplicate filtering for POS API



ID CLOUD

Update iD Cloud EPCIS



iD Cloud warning enabled



iD Cloud warning timeout

10

seconds

Store ID

531177

Store location

<http://nedapretail.com/loc/store-5311>

Readpoint

<http://nedapretail.com/loc/idpos2-764>

Standalone

This is a use case in which the reader only updates the RFID tags itself with a ‘Sold’ flag. This setup requires the use of EASiD Nedap tags. There is no connection to a POS system or EAS database.

Pro: Straightforward and quick to setup

Con: Something separate is required for the POS (e.g., a barcode scanner). This only works for preprogrammed Nedap tags.



CONNECTION TO POS

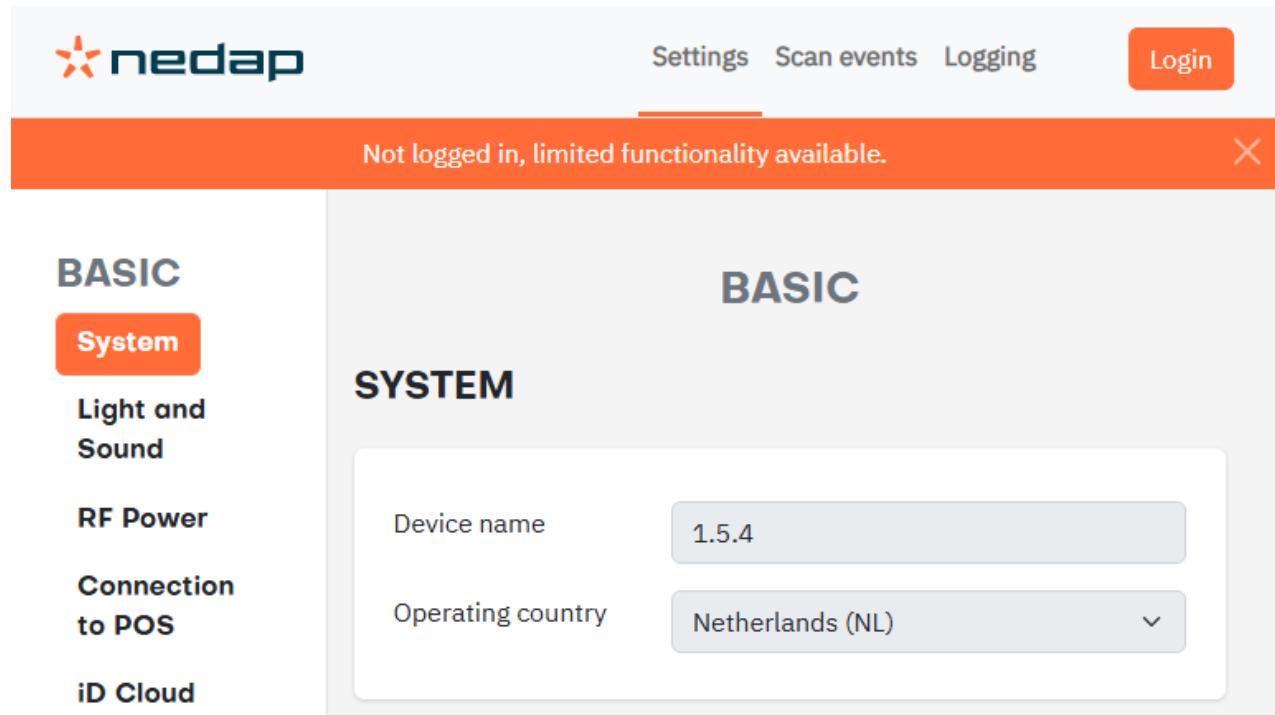
Connection type	Nedap EAS iD
Allow return in Nedap EAS iD standalone mode	<input checked="" type="checkbox"/>

ID CLOUD

Update iD Cloud EPCIS	<input checked="" type="checkbox"/>
iD Cloud warning enabled	<input checked="" type="checkbox"/>
iD Cloud warning timeout	10 seconds
Store ID	531177
Store location	http://nedapretail.com/loc/store-5311
Readpoint	http://nedapretail.com/loc/idpos2-764

View settings

When the configuration is done, it is possible to see a subset of the settings when not logged in:



The screenshot shows a web-based configuration interface for a nedap device. At the top, there is a navigation bar with the nedap logo, "Settings", "Scan events", "Logging", and a "Login" button. A prominent orange banner across the top states "Not logged in, limited functionality available." with a close button "X". On the left, a sidebar titled "BASIC" contains links for "System" (which is highlighted with an orange border), "Light and Sound", "RF Power", "Connection to POS", and "iD Cloud". The main content area is titled "SYSTEM" and displays two configuration fields: "Device name" set to "1.5.4" and "Operating country" set to "Netherlands (NL)" with a dropdown arrow. The overall layout is clean and modern, using a light gray background and orange accents for the unlogged-in state.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2025

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 123

Document Last modification date 16 January 2025

Document PDF Exported 16 January 2025 by Nedap Retail | Operations



support-retail@nedap.com

Nedap Sense Guideline

iD POS Pro & iD SCO Pro

Network Information

version 70, December 2024



Introduction	3
Monitoring	3
Technical operation	4
Device Management, NTP server, and Bosch IoT Servers	4
How to connect the system to the internet	9
Security information	10
Disclaimer	10
Security information	11

Introduction



This manual covers the operation and features of the identical iD POS Pro and iD SCO Pro. Most of the instructions, settings, and features described herein apply to both devices. Where there are differences between the two, these will be indicated. Please pay special attention to these notes to ensure proper usage of your specific device.



Throughout this manual, the term “reader” is used to refer to both iD POS Pro and iD SCO Pro.

Every Nedap Retail reader has to be connected to the online Device Management platform to ensure that systems can be managed remotely and work optimally globally.

The Nedap Device Management service provides four main functions on system level:

- **Monitoring:** Critical reader parameters are monitored 24/7. If a reader has issues, an alert is generated and sent to the supporting partner.
- **Firmware Update:** an authorized Nedap-certified engineer can install new firmware releases remotely using the Device Management website.
- **Sales data:** in case the reader is configured to transfer sales data to the iD Cloud platform.

This document describes essential IT information related to the Nedap Retail reader and online environment.

Monitoring

The status of each reader is continuously monitored and transmitted to the Device Management server.

The following items are monitored:

- Whether the reader is connected to the Device Management server.
- Is the reader still connected to the POS?
- Whether the API connections are still present.

Technical operation

The reader connects to the Device Management server over a secure HTTPS connection to set up the connection.

To use Device Management, the reader must be able to communicate with Nedap servers. Please inform the IT department to set up the firewall according to the information in this document **before the installation.**

Device Management, NTP server, and Bosch IoT Servers



Firewall recommended connections, allowing:

- outbound TCP port 443 traffic to *.nedapretail.com (for Monitoring and iD Cloud)
- outbound TCP port 443 traffic to *.bosch-iot-rollouts.com (for Firmware update)
- outbound UDP port 123 traffic to pool.ntp.org (for Time synchronization)



Or more specific as:

- outbound HTTPS port 443 traffic to api.nedapretail.com (for Monitoring)
- outbound HTTPS port 443 traffic to eas.nedapretail.com (when using: for iD Cloud)
- outbound HTTPS port 443 traffic to device.eu1.bosch-iot-rollouts.com and cdn.eu1.bosch-iot-rollouts.com (for Firmware Update)
- outbound NTP port 123 traffic to pool.ntp.org (for Time synchronization)



If whitelisting based on hostnames is not possible, please use the following list of IP addresses instead:

- 77.222.68.161 - 77.222.68.190 (77.222.68.160/27)
- 77.222.80.1 - 77.222.80.30 (77.222.80.0/27)
- 77.222.80.33 - 77.222.80.62 (77.222.80.32/27)
- 77.222.80.65 - 77.222.80.94 (77.222.80.64/27)
- 87.249.123.1 - 87.249.123.126 (87.249.123.0/25)
- 144.2.168.1 - 144.2.171.254 (144.2.168.0/22)
- 149.3.168.1 - 149.3.168.254 (149.3.168.0/24)
- 213.126.140.97 - 213.126.140.126 (213.126.140.96/27)
- 213.160.213.81 - 213.160.213.94 (213.160.213.80/28)
- 217.114.110.33 - 217.114.110.62 (217.114.110.32/27)
- **IP addresses for firmware update and time synchronization servers are NOT available.**



IP Addresses

The IP address list is subject to change depending on external parties.

We cannot specify the IP addresses for NTP and BoschIoT as this is outside our control.



NTP

The reader must connect to an NTP server—defaults to `pool.ntp.org` port 123.

The NTP organization advises to have a timeserver available within the customer's network.

If that is available, please use that server instead of `pool.ntp.org`

The reader synchronizes with the time server every hour as default.



Bosch IoT

IP addresses are not available; use `*.bosch-iot-rollouts.com` instead.

The rules for this connection depend entirely on the requirements of this third party.



DNS

The reader needs to be able to resolve the DNS names of the used servers, so either a suitable internal DNS server must be present or outbound UDP port 53 traffic to an external DNS server needs to be open.



Transport Layer Security

TSL 1.2 is needed. Support for TLS 1.0 and TLS 1.1 is not available.



IP Addresses used by the iD POS Pro for configuration via USB connection

The reader configures the following IP address range via its USB connection.

- `192.0.2.0 .. 192.0.2.255`

In case this default range interferes with the IP address range in use at the customer's network, this can be changed into

- `192.168.133.0 to 192.168.133.255`



Ports used by the iD POS Pro

The reader uses the following local ports. These ports should **NOT** be added to the firewall.

- 53 = DNS
- 67 and 68 = if used: DHCP
- 80 and 8085 = configuration of the reader (HTTP and WebSocket port)
- 4242 and 5353 = MDNS

- 10921 = If used: WebSocket POS connection, it is possible to change the used port in the configuration



Proxy

The reader is **NOT** designed to be used in environments that dictate the use of a proxy.



Speed and EAS

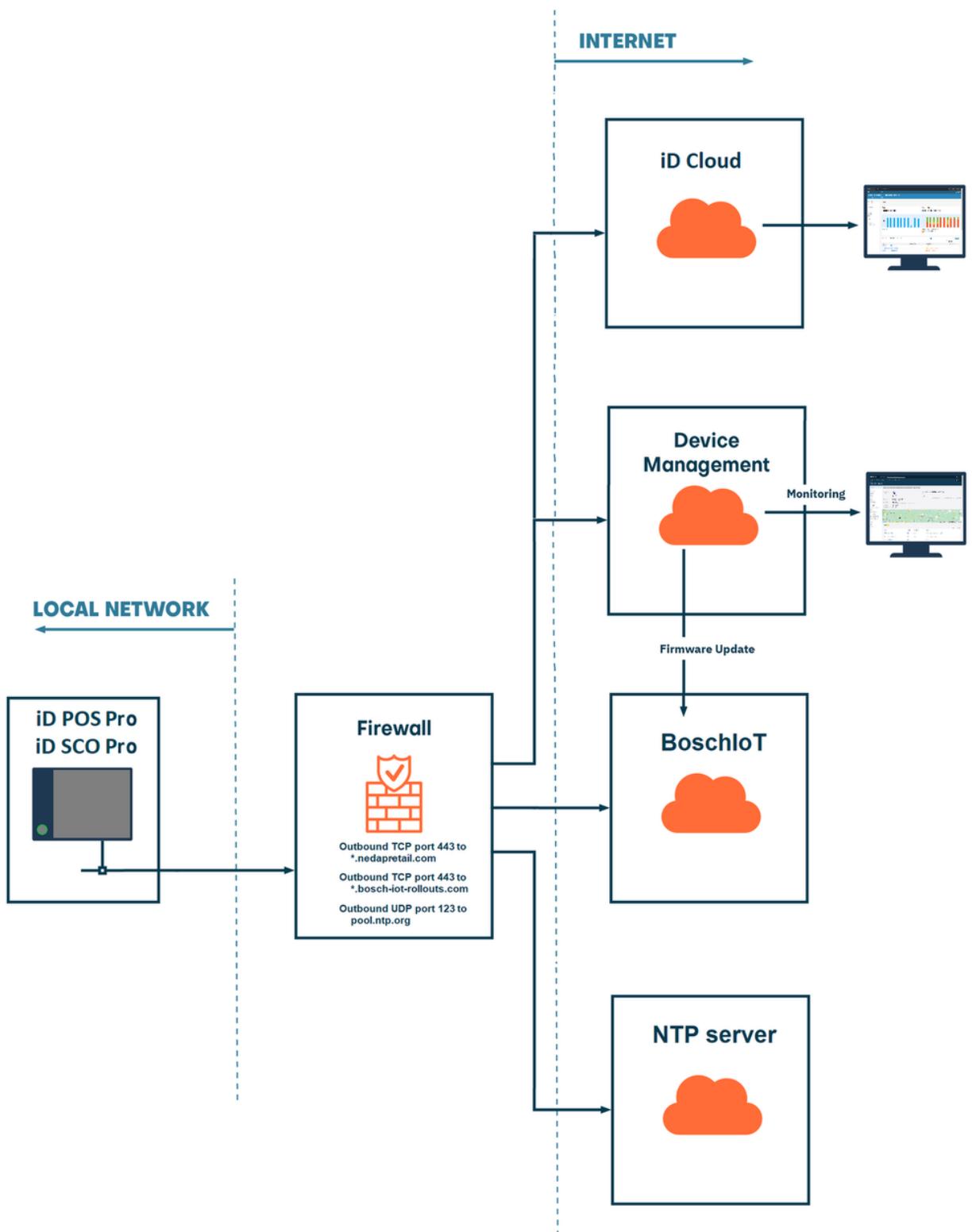
When Loss Prevention is part of the in-store infrastructure, it is important that the network connections are fast enough to ensure that the EAS system will receive an updated status for the RFID tags it detects, to ensure that an appropriate response is made.

If the status of an RFID tag is not updated quickly enough after it has been sold, the EAS system will receive an incorrect status for it, resulting in a false alarm when the tag is exited.



Offline configuration

When the reader is configured to work offline, connections to iD Cloud, Device Management, BoschIoT (Firmware updates), and NTP services (optional) are disabled. Thus, setups that need an iD Cloud connection are not possible.



Test the firewall and connection.



You can test this by connecting a PC or laptop to the network connection and opening <https://api.nedapretail.com> in a browser.

If you see the login screen for a Nedap Retail account, the connection was successful. However, remember that this is not a full firewall test; it only tests the connection to one of the servers.

How to connect the system to the internet

The easiest way to connect a reader to the Device Management server is via an in-store network.



VLAN

We recommend placing the reader in a different VLAN to enhance security.

If the system cannot be connected to the in-store network or does not provide access to the Internet, it is also possible to connect via a 3G/4G modem.



Direct internet connection

Never connect the systems directly to the Internet (e.g., via port forwarding), as this poses a severe **security risk**.



Security information

Disclaimer

- The user interface during configuration uses HTTP traffic on port 80 and a websocket connection on port 8085.
- When no user is authenticated, the user interface is restricted to some very basic settings, like the sound volume.
- Logging into the user interface is only possible by trained technicians using OAuth2 authentication for **Online** readers. For **Offline** readers, a password login is required.
- Firmware updates are only possible with signed firmware images.
- The WebSocket API from Point Of Sale (PoS) to the iD POS Pro or iD SCO Pro, when using it, is not encrypted.
- All traffic to our Nedap Retail services and to Bosch IoT Rollouts are encrypted HTTPS connections on port 443.

Security information

At Nedap (Retail), we understand the importance of protecting the confidentiality, integrity, and availability of systems and data, ensuring business continuity, and maintaining your trust in our products and services. Cybersecurity is one of our top priorities, and we continuously invest in comprehensive measures to protect our systems, the information we process, and the products and services we provide to our clients.

Our commitment to cybersecurity involves a combination of robust technical and organizational measures. We strongly believe cybersecurity is about the right mixture of People, Processes, and Technology (PPT). We employ state-of-the-art security technologies, regularly update our systems, and periodically conduct risk and vulnerability assessments to proactively identify and mitigate potential risks. Third parties and suppliers are included in these risk and vulnerability assessments. We have implemented strict access controls, ensuring only authorized personnel can access our most critical systems or sensitive data. We use MFA and SSO for primary and secondary, as well as facilitating systems and applications. Our employees receive regular training to keep up-to-date and aware of cyber threats. We follow industry best practices and compliance standards to safeguard our products and services.

To ensure resilience against potential vulnerabilities and cyber attacks, we have robust risk management and change management policies and processes in place. These processes enable us to identify, assess, and address security risks promptly and effectively. Moreover, we continuously evaluate our security controls and improve our policies to adapt to evolving cyber threats.

Infrastructure & Hosting

Within Nedap, we use the services of a specialized and dedicated internal hosting team to manage our platform infrastructure. The data centers we use hold various relevant security certifications, such as ISO27001, ISAE3402 type II, and SOC2 type II. Nedap's internal hosting team works closely with Nedap Retail's own DevOps and Development teams to manage and monitor the hosting infrastructures' performance and security continuously. A SIEM and multiple other tools are used for log analysis, monitoring system events, and alerting if thresholds are exceeded or anomalies are detected.

The hosting infrastructure is completely separated from the Nedap office environment and is only accessible by authorized personnel based on their role/function. Access is only possible using non-domain-joined jump hosts and Multi-Factor Authentication (MFA). To ensure secure server configuration at all times, we use Infrastructure-as-Code. Any suggested change is well-documented, goes through a 4-eyes principle (at least), and must be explicitly approved before implementation. Any manual system or configuration change that did not follow this process is automatically being reverted.



Application Security

Multiple software development teams within Nedap Retail develop our applications, such as Device Management, APIs, Loss Prevention, iD Cloud Web, and mobile apps. These teams focus on their specific area and collaborate closely. Our developers all hold higher degrees in software development and share the same robust development principles.

We care a lot about secure and high-quality code. Therefore, we also apply the 4-eyes principle to all changes within our source code. Every Pull Request (PR) must be reviewed and approved by another (senior) developer before being merged. Besides reviewing all code through this 4-eyes principle, we continuously improve our tools and practices to identify and prevent any possible issues as soon as possible in the CI/CD pipeline (shifting security left). We do unit and integration tests, have full traceability of who made what change and why, and use various tooling for Continuous Integration (CI) services so that PRs can only be merged after all tests have passed. We use Software Bill of Materials (SBOM) and Software Composition Analysis (SCA) to gain insight into possible security issues introduced using third-party libraries. Furthermore, we use Dynamic Application Security Testing (DAST) tooling to scan our staging environment for potential vulnerabilities weekly. If any serious security issues are identified, these will be resolved before the code is deployed to production.

Penetration Testing

Besides all the effort we put in ourselves to keep our hosted platform secure, we also engage a reputable cyber security firm to either perform an annual penetration test or to do Agile Security Testing throughout the year (consisting of code reviews and manual hands-on penetration testing, in intervals of several weeks). Our iD Cloud Web environment, Device Management, and our APIs are within the scope of these tests. Resulting reports are assessed and discussed, and any findings are treated following our Information Security Policy, meaning that at least all critical or high-risk findings must be resolved within two weeks.

Certification & Assurance

Our iD Cloud EU platform (including Device Management and our APIs) successfully passed a SOC2 type I attestation, and we are currently in the process of obtaining a SOC2 type II report and a SOC1/ISAE3402 type II report covering our Year-End Count service. In addition to all technical controls, these attestations include relevant organizational aspects assessed by independent external auditors, both in design and effectiveness.

Should you have any questions or concerns regarding our cybersecurity practices, we encourage you to contact your business contact within Nedap (Retail). They will be more than happy to work with you and answer your questions.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Document Version 70

Document Last modification date 2 December 2024

Document PDF Exported 2 December 2024 **by** Nedap Retail | Operations

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.



support-retail@nedap.com

Nedap Sense Manual

iD POS PRO

version 204, March 2025

Introduction	5
Features of the iD POS PRO	5
About this Manual	5
Disclaimers & Safety Precautions	6
Disclaimers	6
Safety precautions	6
RFID Regions	6
Product Overview	7
Box contents	7
Technical specifications	8
RFID Specifications	10
Connections	11
Hardware status	12
Preparing the installation.....	13
RFID installation requirements.....	14
Metal surfaces	14
Detection distance	14
Label-free zone	14
Distance to adjacent iD POS PRO	15
Power over Ethernet	16
Cabling.....	17
Shielded Ethernet Cable	17
USB-Cable	17
USB-Cable + Filter	18
Configuration.....	19
Connecting a laptop to the iD POS PRO	19
Supported web browsers	20
Driver installation - Microsoft Windows	20
Entering the configuration	21
Operation	22
Light and sound signaling	23



Disclaimer	24
Nedap Device Management	24
Firmware update	24
Reset to Factory default	25
Replacement	26
Troubleshooting.....	27
Warranty and spare parts.....	28
Regulatory information	29
FCC and IC Compliance Statement	29
FCC and IC Radiation Exposure Statement	29
FCC Information to the user	29
Information for Taiwan	30
CE WEEE	30
CE - UKCA Declaration of Conformity	31
Disposal of this product	31
About Nedap.....	32
Together, we make merchandise simply available	32
Our vision for inventory visibility	32
Contact	32



Introduction

The Nedap iD POS PRO is an RFID reader that reads RFID tags attached to articles in a retail/fashion environment. The iD POS PRO can be used for “sell” and “return” functionalities, after which the data can be sent to the POS or a database.

Features of the iD POS PRO

- It is fitted with a shielded RFID antenna that only reads items above it while ignoring items below or next to the antenna.
- State-of-the-art RFID reader and antenna design, ensuring optimal read performance, even in challenging environments.
- All integrated functions are included in 1 device, antenna, processor, reader, audio/visual.
- Equipped with Ultra High Frequency (UHF) RFID technology, designed for in-store retail applications.
- It can be mounted on top, in, or underneath a desk.
- Powered through standard Power over Ethernet (PoE) (not included in the box).
- It can be connected/integrated to the Point of Sale (POS) over ethernet or USB.
- Remote capabilities to communicate with iD Cloud and Device Management.
- Easy to install and configure.
- Firmware updates can be triggered from Device Management and in-store.

About this Manual

This manual provides specifications, installation basics, and configuration setups for the iD POS PRO and the phased-out iD POS 2. For more details, consult the additional documentation at the Nedap Retail Partner Portal.

Disclaimers & Safety Precautions

Disclaimers



Nedap intends to make this manual accurate and complete. However, Nedap does not warrant that the information contained herein covers all details, conditions or variations, nor does it provide for every possible contingency in connection with the installation or use of this product. Nedap disclaims any liability for damage to property or personal injury resulting, in whole or in part, from improper installation, modification, use, or misuse of its products. The information contained in this document is subject to change without notice.



This equipment should only be installed, operated, serviced, and repaired by skilled personnel. The installation and interconnection of this equipment to facility wiring and other equipment must be done by a competent, skilled craftsperson familiar with applicable standards and codes governing the installation. Installation methods, practices or procedures that are unauthorized or done improperly are dangerous and could result in serious personal injury or damage to property and equipment.

Safety precautions



Do not place cards equipped with a magnetic strip or chip (i.e., ID, travel, debit, and credit cards) close to the equipment to avoid possible card failures.



To avoid potential interference with medical devices (pacemakers, cochlear implants, etc.), keep a distance of at least 20cm (8 inches) between them and the equipment.

RFID Regions

Region 1: Europe, Eastern Europe, Middle East, Africa and India

Region 2: North America and South America

Region 3: Asia and Oceania

Product Overview

Box contents

Article Number	Article Name	(Box) Label Description	Box Contents
9567278	iD POS PRO RFID Black Region 1	ASSY PS25 RFID R1 BLACK	<ul style="list-style-type: none"> • iD POS PRO Region 1 • 4x Mounting clip • 4x Screw torx T20 (4.0x20) • 1x Quick Reference
9567291	iD POS PRO RFID Black Region 2	ASSY PS25 RFID R2 BLACK	<ul style="list-style-type: none"> • iD POS PRO Region 2 • 4x Mounting clip • 4x Screw torx T20 (4.0x20) • 1x Quick Reference
9567437	iD POS PRO RFID Black Region 3	ASSY PS25 RFID R3 BLACK	<ul style="list-style-type: none"> • iD POS PRO Region 3 • 4x Mounting clip • 4x Screw torx T20 (4.0x20) • 1x Quick Reference
9567372	Bracket Black for iD POS PRO RFID	BRACKET ASSY PS25 RFID RAL7021	<ul style="list-style-type: none"> • Mounting bracket



A PoE power supply is not included and should be sourced locally.



A USB-C cable for configuration and/or communication to the POS is not included.

Technical specifications

Manufacturer	Nedap NV
Air Interface Protocol	EPC global UHF Class 1 Gen 2 / ISO 18000-6C
Antenna Type	Archimedean Spiral antenna internal
Connectivity	Ethernet, USB-C
Management Interfaces	Configuration tool and firmware update via USB and Ethernet
Dimensions	255mm x 210mm x 20.1mm 10.04" x 8.27" x 0.79"
Weight	approx. 1.0 kg approx. 2.20 lbs
Power Supply	PoE Power-supply adapter 802.3af, class 0
Power Consumption	13 W max.
Operating Temperature	0 .. 40°C, 32 .. 104°F
Humidity	<93% non-condensing
Environment	In-door use
IP Protection Class	IP42
Mounting Option	Mounting on top, in or beneath a desk ¹

¹ additional measures may be required to achieve this solution

Dimensions



RFID Specifications

Region 1

Frequency Band	865.7 – 867.5MHz FHSS
Channels	4 (1: 865.7; 2: 866.3; 3: 866.9; 4: 867.5)
Channel Spacing	600kHz
Output Power Radiated	<ul style="list-style-type: none"> Europe (ETSI EN 302 208): 2W ERP max.

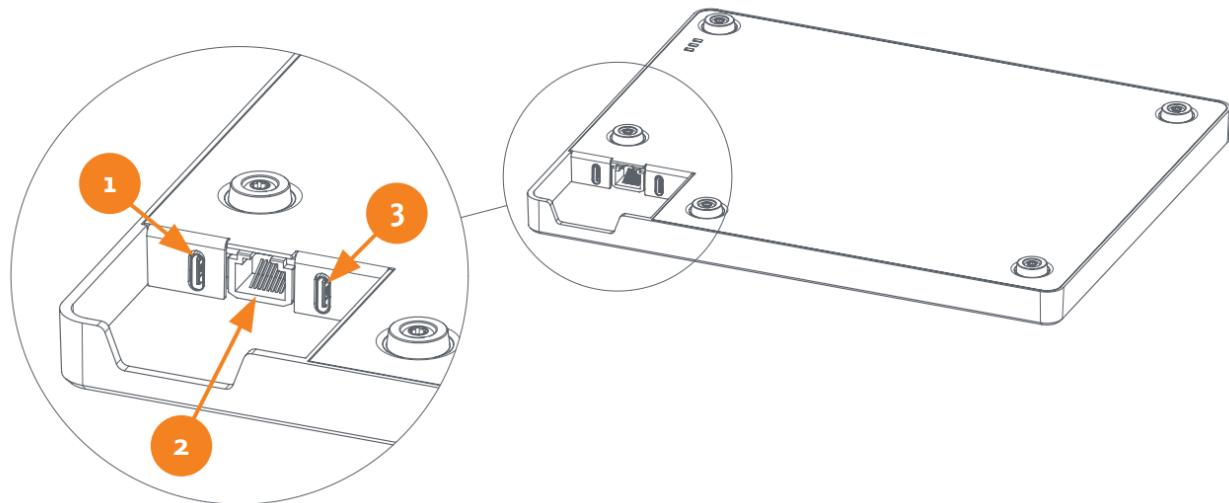
Region 2

Frequency Band	902 – 928MHz
Channels	50
Channel Spacing	500kHz
Output Power Radiated	<ul style="list-style-type: none"> United States (FCC Part 15.247): 4W eirp Canada (RSS210): 4W eirp

Region 3

Frequency Band	Depending on the country of installation, please contact Nedap Retail Support for more information.
Channels	
Channel Spacing	
Output Power Radiated	

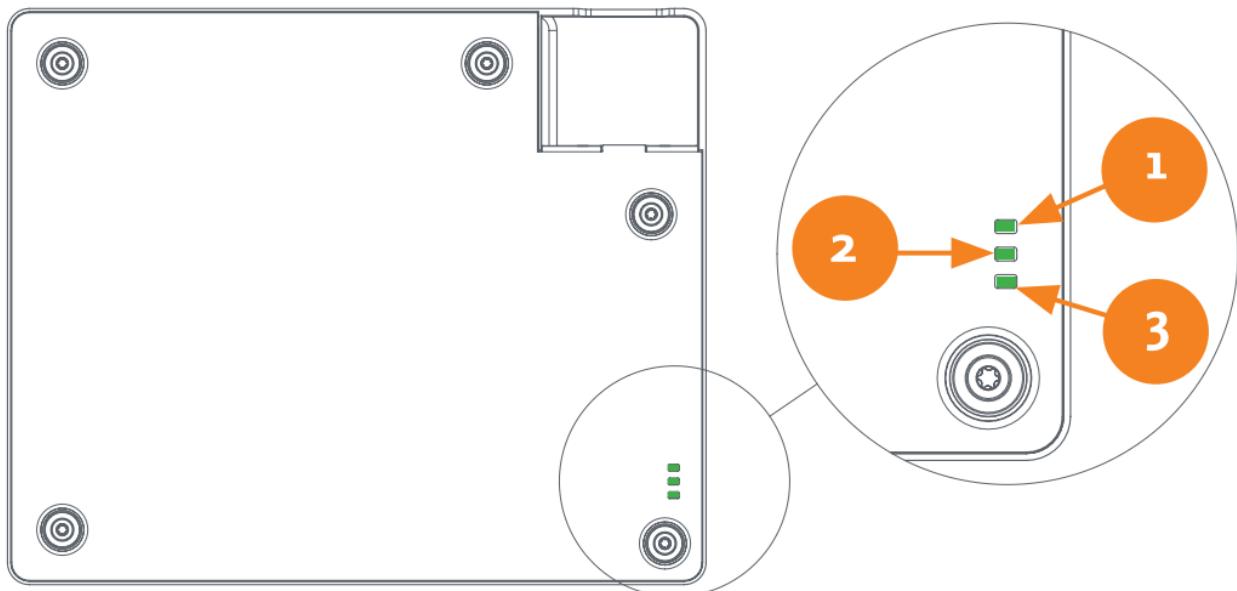
Connections



Number	Meaning	Remark
1	Service port / HID POS	USB-C
2	Power & Ethernet	RJ45 PoE IEEE 802.3af, class 0
3	Not in use	

Hardware status

The iD POS PRO is fitted with three status LEDs at the bottom of the housing.



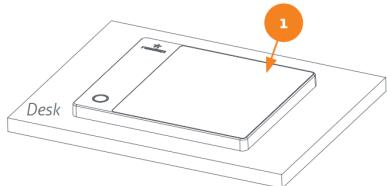
Number	Meaning	Remark
1	Power	“ON” when lit
2	Debug	For development purposes only
3	Ethernet	<ul style="list-style-type: none">• “ON”: the link is established• “Blink”: when data is transferred

Preparing the installation

When preparing an iD POS PRO installation, the following requirements should be taken into account:

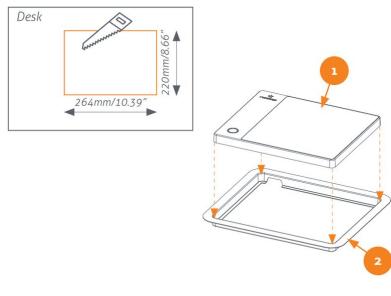
- A Power over Ethernet adapter is required (not included in the package)
- Network/USB-Connection for integration with a checkout system (USB cable not included)
- PoE access, including an Internet connection for configuring the iD POS PRO, Device Management, and/or connection to the iD Cloud. If no PoE connection is available, PoE switches need to be ordered.
- Number of checkouts required
- See “iD POS PRO & iD SCO Pro Network information” for the customer's network and firewall settings.
- Where and how the iD POS PRO will be mounted:

On top of the sales desk



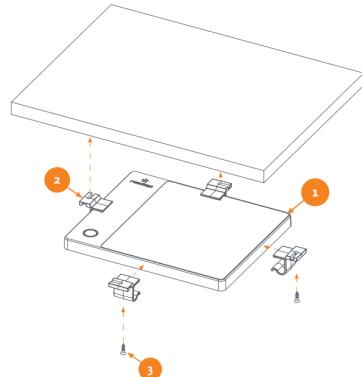
1. iD POS PRO

In the sales desk



1. iD POS PRO
2. Table mounting bracket
(mounting bracket not included; it can be ordered as a separate spare part)

Underneath the sales desk



1. iD POS PRO
2. Mounting clip
3. Screw torx T20 (4.0x20)



The iD POS PRO must be securely placed or mounted to prevent it from falling down the table. Any fall or impact on the floor can cause significant damage to the reader, which is not covered under warranty. Ensure the reader is installed stably and securely.



When the iD POS PRO is mounted underneath the sales desk, the button is not available, and configurations that require it to function cannot be used.

RFID installation requirements

Metal surfaces

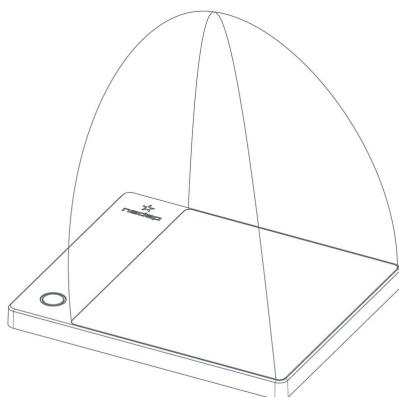
Metal surfaces can reflect or block the RFID field, impairing the iD POS PRO performance. It is strongly advised to avoid metal surfaces, such as metal desktops or objects containing metal parts, near the iD POS PRO.



Metal items above the reader surface of the iD POS PRO will partially or entirely block the RFID signals.

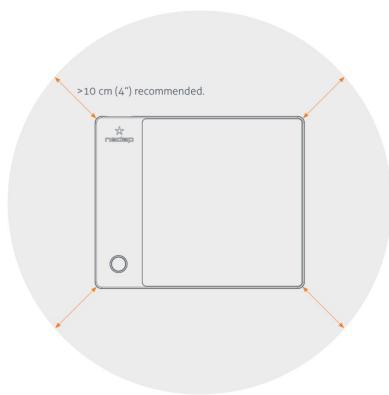
Detection distance

Depending on the configured power settings, label type(s), orientation, and other factors, the detection distance varies from approximately 10 cm to 50 cm (4 up to 20 inches). The beam is narrow directly above the iD POS PRO, preventing cross-reads.



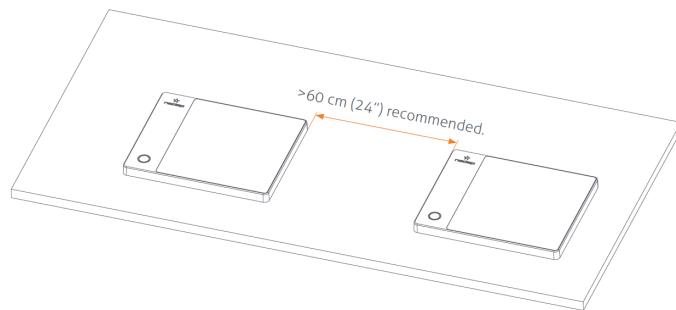
Label-free zone

A label-free zone of at least 10 cm (4 inches) is recommended around the iD POS PRO.



Distance to adjacent iD POS PRO

Although the iD POS PRO is impervious to nearby iD POS PROs, it is recommended that they be placed at least 60 cm (24 inches) apart.



Power over Ethernet

The iD POS PRO is powered through standard Power over Ethernet (PoE) **IEEE802.3af, class 0**.



A power-over-Ethernet **adapter is not included!**

PoE to the iD POS PRO can be arranged in 2 ways:

- Use a **PoE router/switch** that is already available in the store
- Use a **PoE injector**. As an example of a PoE injector, the TP-Link TL- POE150S can be used:



Cabling

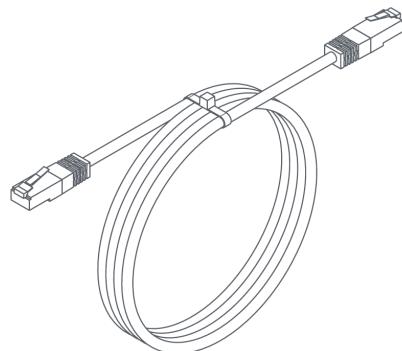
The cabling must be set up when the placement and orientation are precise.

Shielded Ethernet Cable

For power and network, a shielded ethernet cable is needed.

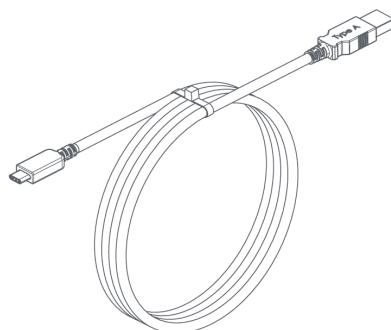
Use a standard shielded ethernet cable, or keep the following in mind when making a cable yourself:

- Use shielded ethernet Cat 5e with a stranded copper core and a 24 AWG (0,51 mm) core diameter.
- Use the connectors that are to be used with the chosen cable.
- We recommend a higher quality cable, like a Cat 6 cable, to cover a greater distance.
- Standard shielded ethernet cabling limits must be applied.



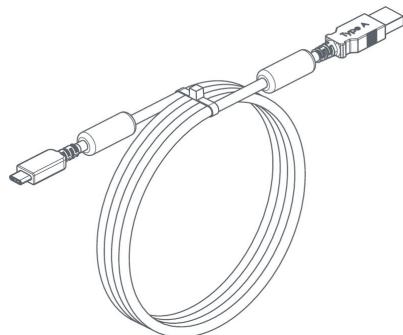
USB-Cable

When the iD POS PRO is connected to the POS, a USB cable is needed, and on the iD POS PRO side, there is a USB-C connector.



USB-Cable + Filter

Use a USB cable with ferrite filters for cables longer than 2 m (6.6 ft.).



Configuration

To complete the configuration and registration, the following is required:

- iD POS PRO is connected to the internet.
- USB-(x) to USB-C (iD POS PRO side) cable.
- Laptop with installed driver and the latest version of the internet browser (preferably Google Chrome).

The iD POS PRO can be configured as an **Online** or **Offline** reader. The choice depends on the required solution.



For the online mode: An internet connection is required from the iD POS PRO to Device Management. For the network configuration, please check the guidelines on the Partner Portal:

- iD POS PRO & iD SCO Pro Network information



For the online mode: A Nedap Retail Account is needed to login to the iD POS PRO with the following permission: ‘Manage systems’ (to be able to link the iD POS PRO to a store)



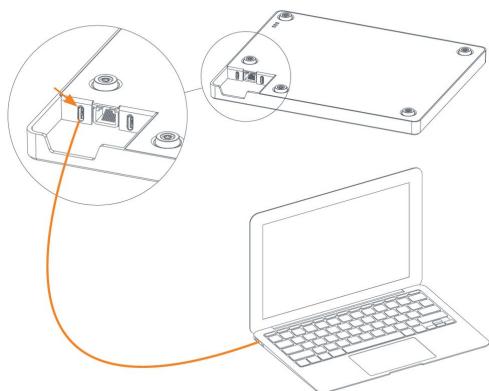
The iD POS PRO has several operation modes, depending on the selected mode (online/offline) and the type of integration required with the POS (Point of Sale).

For further information, it is essential to check the relevant guidelines on the Partner Portal:

- iD POS PRO & iD SCO Pro - Configuration
- iD POS PRO & iD SCO Pro - OFFLINE Configuration

Connecting a laptop to the iD POS PRO

Connect a laptop via a USB Cable to the service port on the iD POS PRO. The iD POS PRO is fitted with a USB-C connection.



Supported web browsers

To configure the system, the latest versions of the following browsers are officially supported:

- Chrome (and other Chrome-based browsers)
- Firefox
- It has not been tested, but in principle, every modern browser that supports JavaScript should work.

If you don't have one of these browsers installed on your laptop, please install them before the installation.

Driver installation - Microsoft Windows

To configure an iD POS PRO, a Microsoft Windows driver must be installed. Please check the “*iD POS PRO & iD SCO Pro Windows driver installation*” manual for instructions.



At the moment, only Microsoft Windows operating systems are supported



Entering the configuration

Once the steps to install the Windows driver are finished, you can enter the configuration by opening your browser and navigating to:

http://192.0.2.1



- Ensure that no other network connections are active in the same range. If the customer's network is in the 192.0.2.x range, it is possible to change the default IP address to 192.168.133.1

Follow the steps in the configuration.

When the installation has been completed and delivered, monitoring the installation via Nedap Device Management for **Online** readers is possible.

Operation

In setups where a WebSocket connection is used, the button on the iD POS PRO is not used.

For the other setups, the button on the iD POS PRO is used to determine the action:

Action	
Sell	Short press the button, the light will turn green
Return	Press and hold the button for 2 seconds ; the light will turn blue (when enabled)
Stop	Short-press the button to stop the scanning of tags, or wait 45 seconds (default, configurable), and the light will turn off.



It cannot be scanned again for 15 seconds (default, configurable) **or** if a label is on top of the RFID reader.

Light and sound signaling

Feedback is given with light and sound, both of which are configurable. The light can be turned on and off, and the sound volume can be changed.

When an RFID tag is detected, the light will flash, and a sound is played.



Signaling		Meaning
Green		Selling
Blue		Returning
Orange		The iD POS PRO is in its power-up phase
Orange + short sounds		No connection to the database
Purple		The iD POS PRO is not configured yet
Red		Error during firmware update



Disclaimer

- The user interface during configuration uses HTTP traffic on port 80 and a websocket connection on port 8085.
- When no user is authenticated, the user interface is restricted to some very basic settings, like the sound volume.
- Logging into the user interface is only possible by trained technicians using OAuth2 authentication for **Online** readers. For **Offline** readers, a password login is required.
- Firmware updates are only possible with signed firmware images.
- The WebSocket API from Point Of Sale (PoS) to the iD POS Pro or iD SCO Pro, when using it, is not encrypted.
- All traffic to our Nedap Retail services and to Bosch IoT Rollouts are encrypted HTTPS connections on port 443.

Nedap Device Management

The following features are available via Nedap Device Management.

- System monitoring via some key metrics. The following key metrics are available:
 - Not connected to Device Management
 - Update server not reachable
 - iD POS PRO has no HID connection
 - iD POS PRO WebSocket connection to the POS offline
 - Slow or no connection to iD Cloud

Firmware update

A firmware update can be done in the following ways:

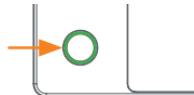
- Triggered remotely via Device Management
- Local:
 - Via the USB service port connection
 - Via local network

Reset to Factory default

The iD POS PRO can be reset to its factory settings using 2 different methods:

- Factory reset by use of the user interface
- Factory reset by use of the button

The LED around the button shows the progress.



The steps to take to execute a button factory reset by the use of the button:

1. *Power off the reader*
2. *Press and hold the button*
3. *Power on the reader*
4. *Keep the button pressed during boot → after 30 seconds, the red LED will start blinking.*
5. *Release the button within 10 seconds → The LED will now blink orange*
6. *Within 10 seconds, press the button for at least 3 seconds → the LED will now be solid yellow, and the reader will factory reset, followed by an automatic reboot*

The process can be interrupted at any time by not executing the next step.



Replacement

When an iD POS PRO needs to be replaced due to issues, a new one must be installed.

Every (more extensive) customer will have a fixed setup. This setup can be pushed into the new reader.

Troubleshooting

Some general troubleshooting tips.

- Try to define where things go wrong.
 - Is the iD POS PRO powered?
 - Have the EPCs not been received by the POS?
 - Have the EPCs not been received in the iD Cloud?
- Check the power
- Check the network cable
- Does the iD POS PRO react on pressing the button?



Warranty and spare parts

- Please consult the Nedap Retail Business Partner from whom you purchased this product regarding the applicable warranty conditions.
- This product cannot be used for any other purpose described in this document.
- If the product is not installed according to this document, the warranty provided is not applicable.
- At the sole discretion of Nedap N.V., Nedap N.V. may decide to change the conditions of Page 7 of 19 Compliance information for technical manuals warranty policy.
- You agree that Nedap N.V. can compensate you for the pro-rata value of the warranty involved rather than replacing or repairing the product based on its technical or economical value.
- Prior to applying the warranty, please verify that you comply with the warranty conditions of the warranty policy and that you can successfully apply for the replacement or repair of a defective part.
- Parts can only be replaced with original Nedap parts; otherwise, the warranty policy will not apply to the product.
- If the warranty is applicable, please contact the dealer or send the defective parts to the dealer.

Regulatory information

FCC and IC Compliance Statement

This device complies with part 15 of the FCC Rules and RSS210 of Industry Canada. 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.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Cet appareil se conforme aux normes CNR210 exemptés de license du Industry Canada. L'opération est soumis aux deux conditions suivantes:

- (1) cet appareil ne doit causer aucune interférence, et*
- (2) cet appareil doit accepter n'importe quelle interférence, y inclus interférence qui peut causer une opération non pas voulu de cet appareil.*

Les changements ou modifications n'ayant pas été expressément approuvés par la partie responsable de la conformité peuvent faire perdre à l'utilisateur l'autorisation de faire fonctionner le matériel.

FCC and IC Radiation Exposure Statement

This equipment complies with FCC and Canadian radiation exposure limits for an uncontrolled environment. It should be installed and operated with a minimum distance of 20 cm between the radiator and your body. This transmitter must not be co-located or operated with any other antenna or transmitter.

Cet équipement est conforme a CNR102 limites énoncées pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et votre corps.

This Class B digital apparatus complies with Canadian ICES-3. Cet appareil numérique de Classe B est conforme à la norme Canadienne NMB-3.

FCC Information to the user

Note: This equipment has been tested and found to comply with the limits for class B digital devices, according to part 15 of the FCC Rules. These limits are designed to protect reasonably against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency

energy and, if not installed and used following the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. Suppose this equipment does not cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on. In that case, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from the receiver's.



Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. To ensure compliance with FCC regulations, use only the shielded interface cables provided with the product or additional specified components or accessories that can be used to install the product.

Information for Taiwan

第十二條 經型式認證合格之低功率射頻電機，非經許可，
公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；
經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。
低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

CE WEEE

This European Standard specifies a marking:

- of electrical and electronic equipment following Article 11(2) of Directive 2002/96/EC (WEEE); This is in addition to the marking requirement in Article 10(3) of this Directive, which requires producers to mark electrical and electronic equipment put on the market after 13 August 2005 with a 'crossed-out wheeled bin' symbol.
- that applies to electrical and electronic equipment falling under Annex IA of Directive 2002/96/EC, provided the equipment concerned is not part of another type of equipment that does not fall within the scope of this Directive. Annex IB of Directive 2002/96/EC contains an indicative list of the products that fall under the categories set out in Annex IA of this Directive;



- that identifies the equipment producer clearly and that the equipment has been put on the market after 13 August 2005.

CE - UKCA Declaration of Conformity

With this, Nedap N.V. declares that the subject equipment is in compliance for CE with directives 2014/53/EU (Radio Equipment Directive) and 2011/65/EU (RoHS). And for UKCA with SI 2017/1206 (radio Equipment Regulations 2017) and with SI 2012/3032 UK Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 (RoHS). The full text of the declarations of conformity is available at the following internet address: <https://portal.nedapretail.com/>, where, if applicable, REACH information can also be found.

Disposal of this product

This product's owner or last user is responsible for properly disposing of (parts of) the product as required by local rules and regulations.





About Nedap

Together, we make merchandise simply available

At Nedap, we believe in ‘Technology for Life’. Nedap Retail enables retailers to serve their customers better. Using technology, we allow for perfect inventory visibility, total control, no waste, and no losses.

Our vision for inventory visibility

Today, established retailers need more information about where their items are. Without this knowledge, providing an omnichannel experience leads to heavy overstocking, waste, and eroding margins. Solving this requires a fundamental change in the retailers’ supply chain and information systems.

Our mission is to simplify the process of ensuring that retailers always have the right products available at the right place and time.

We do this by giving retailers perfect inventory visibility for a seamless shopping experience. This way, retailers can meet the changing consumer needs while remaining profitable.

Nedap works with the largest and most successful retailers in the world. We take complete ownership of our projects—failure is never an option. A unique combination of the best technology and industry teams at Nedap Retail achieves this.

Nedap solutions are built upon 45 years of global experience, market expertise, and close cooperation with leading retailers. A flexible network of certified partners worldwide supports our worldwide operations. Nedap systems are future-proof (RFID-ready), cost-efficient, and Eco-friendly. Our mission is to ensure retailers' customers maintain the best shopping experience while we help retailers protect their profits.

Contact

If you need further details or help preparing, executing, or servicing an installation, please contact our support team at support-retail@nedap.com.

Suggestions for improving our products and documentation are much appreciated.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Document Version 204

Document Last modification date 25 March 2025

Document PDF Exported 25 March 2025 by Nedap Retail | Operations

Copyright © Nedap NV 2025

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.



support-retail@nedap.com



**Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands**

nedap-retail.com

Nedap Sense Guideline

iSense External Customer Counter Integration – XOVIS

Xovis Customer Counting

version 66, March 2025

About this document	3
Introduction	4
Behavior	5
Network setup	6
Configuring iSense (part 1)	7
Configuring Xovis	9
1. Connect the sensor with your laptop	9
2. Firmware update	10
3. Configuring the network	12
4. Connect the sensor to the customer's network	13
5. Configuring the sensor	14
6a. Single sensor	16
6b. Multi sensor	24
Configuring iSense (part 2)	35
Status and troubleshooting	37
iSense	37

About this document

This document describes the installation and configuration of the **Xovis PC2SE** sensors in combination with a Nedap iSense system.

- i Xovis devices can be ordered via Xovis wholesaler Vemco in Denmark at a special Nedap project price. Consult the commercial documentation on the Partner Portal for more information.
- i A Xovis account is advised, as it gives you access to Xovis documentation and support. Please contact Xovis directly via support@xovis.com to get an account.
- i An Xovis device does not have a **power supply** included and should be sourced locally. This should be a Power over Ethernet, Class 0 IEEE 802.3af PoE Class 2 or higher.

Introduction

Next to Nedap integrated customer counters, it is possible to connect *external* customer counters to iSense. External customer counters are, for example, a good solution with iSense - iD Tops. This setup shows the visitor data from the external counters in Nedap Retail Analytics and the local iSense dashboard.



This document describes how to integrate the **Xovis PC2SE** sensor with iSense.

Behavior

- With this integration, *visitor counting* data via Xovis sensors will be visible in Analytics. Other features like queue detection are not supported.
- In this setup, each Xovis sensor sends the number of incoming and outgoing customers to the iSense system per minute.
- Visitor data will also be shown in the local iSense dashboard graphs.



Per integrated Xovis sensor, a one-time fee will be charged automatically when the system is connected to Device Management: External CC Integration (6670059). Also, an iSenseGo Analytics Visitor (6669549) subscription is required to see the data in Analytics.



When replacing Xovis sensors in an existing installation, give the new unit the same name as the replaced unit.



Counts made by Xovis sensors are *not* available in the iSense API; they are available in the Analytics API.



Counts can *not* be used as a trigger for a pager or IO box.



Xovis sensors are available in iSense as of firmware version 24.16.1



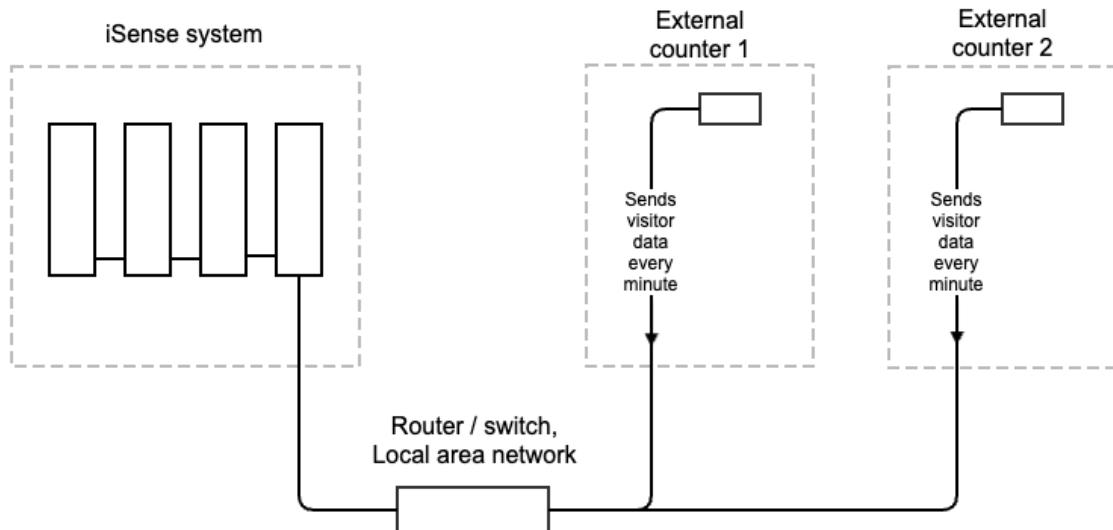
Xovis sensors are not suitable for determining the store's occupancy.



It can take 1 to 2 days before the first counts show up in Analytics

Network setup

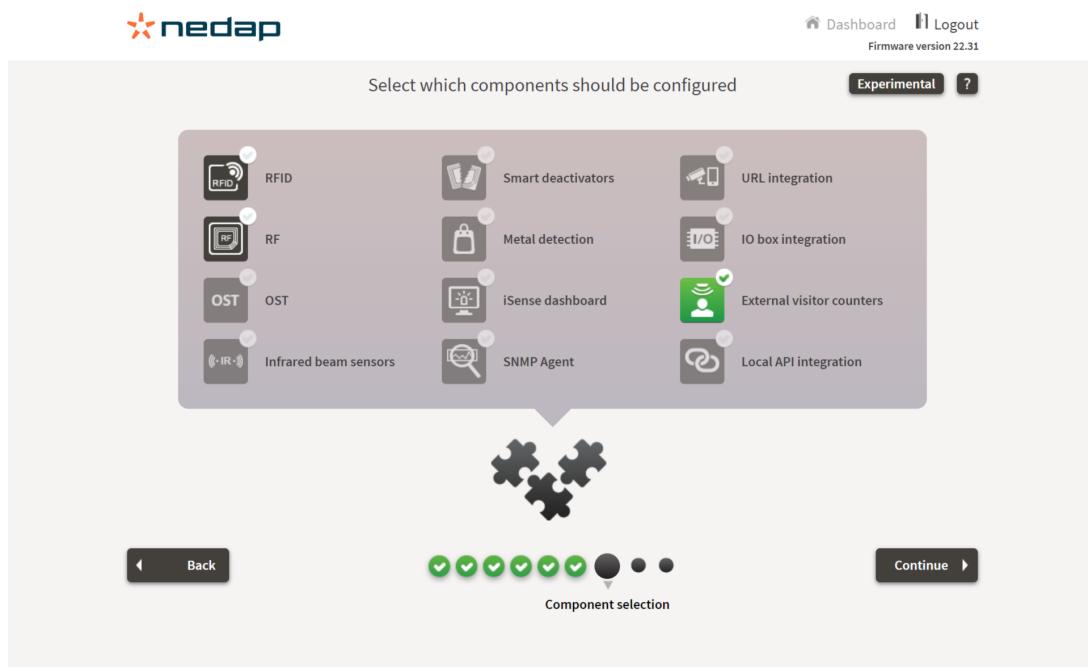
Connect each Xovis sensor to the local area network. The iSense system (which can contain multiple gates or iD tops) must also be connected to this same local area network:



When the connection between the Xovis sensor and the iSense system is down for any reason, the visitor data collected during this downtime will **not** be saved. This data will not be shown in Analytics and in the local iSense dashboard.

Configuring iSense (part 1)

Install and configure the iSense system. In the 'Component selection page', choose '*External visitor counters*':



The external customer counter configuration page will provide setup instructions. Write down the system's IP address.



Receive external customer data in Renos and Analytics

1

Configure each external camera:

- Follow the steps as described in the document 'How to connect external customer counters with iSense'. This can be found on the partner portal.
- The IP address of this system is: 192.168.1.116

Device:

Status of last minute:

2

Make sure the device shows up on the right side. This can take a minute.

3

Confirm the amount of devices when all cameras are connected.

Confirm 0 connected cameras



 Back

Continue 



Configure external customer counters

We will now need to configure each Xovis sensor.

Configuring Xovis

1. Connect the sensor with your laptop

- Connect the sensor and your laptop to the same isolated network



The simplest way is to have a Power over Ethernet switch that will power the sensor and connect to your laptop

- Configure your laptop's network interface:
 - IP address: in the **192.168.1.x** range (x should **not** be **168 or 255**)
 - Netmask: **255.255.255.0**
- Open your browser and connect to the Xovis web interface
- To access the Xovis web interface, use the default IP address: **192.168.1.168**



It can take a few minutes before the sensor is up and running

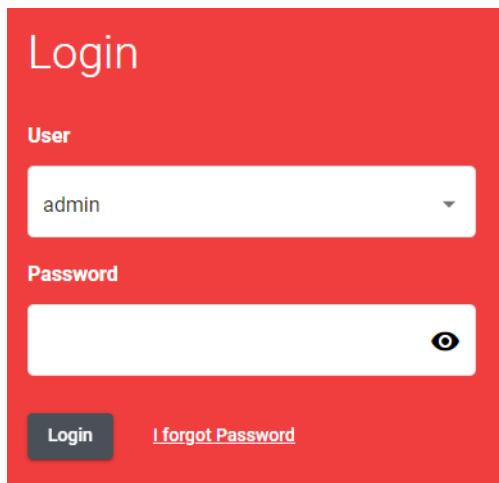
- Enter username and password.



Sensor defaults:

- IP address: **192.168.1.168**
- Username: **admin**
- Password: **pass**

Cameras purchased from Vemco have **installer** as its password



The image shows a red-themed login interface. At the top center, it says "Login". Below that is a "User" field containing "admin". Below the user field is a "Password" field with a small eye icon to the right. At the bottom left is a "Login" button, and at the bottom right is a link "I forgot Password".

⚠ Changing the password for the Xovis device is strongly advised. This will prevent changes by unauthorized access.

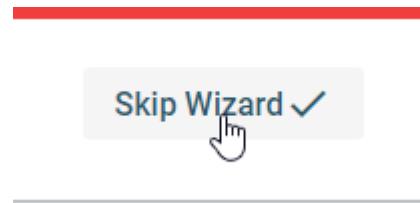
2. Firmware update

- i** Make sure that you use the advised Xovis firmware version, to be found on our portal: <https://portal.nedapretail.com/technical/technical-isense-integrations>

Wizard

Feel free to use the Wizard, but to use the configuration below, both on the first run and all subsequent runs, we will skip the Wizard and configure section by section.

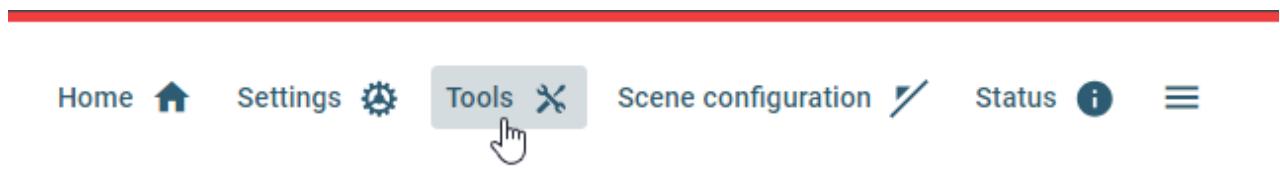
- Press Skip Wizard



Firmware upgrade

Make sure that you use the advised Xovis firmware version.

- Press Tools



- Press Firmware update

Tools

Firmware update



Diagnostics

Sensor explorer

Stereo image

Lens check

Visualization maps

Historical count data

Backup & restore

Recordings

Launch wizard

Reboot

Reset

- Check Currently installed

Firmware update

To update your sensor you can either choose one of the listed firmware versions below or upload another firmware (.xfw file). The update will take several minutes to complete, during which the sensor will not be available. At the end of the update, the sensor will reboot and you will have to log in again.

Currently installed

5.2.0-f757509538

Update firmware

- If it matches 5.5.6-450cf850b1, skip to the next chapter else continue to update the firmware with the following steps
- Press Update firmware
- Press Browse file or drag and drop the file
- Press Open
- Press Install
- Wait until the process finishes
- Login

3. Configuring the network

General

- Press **Settings**



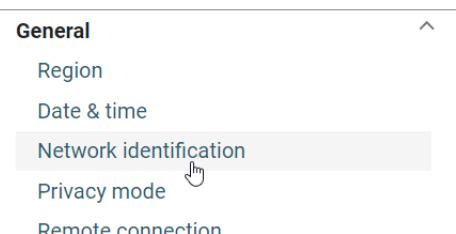
- Press **General**

Settings

- General
 - Region
 - Date & time
 - Network identification
 - Privacy mode
 - Remote connection
 - User management
 - Licenses
 - Advanced network properties
 - Legacy support

Network identification

- Press **Network identification**



- Copy the **Hostname** into the **Name** field. This ensures that the device name is the same in both the iSense wizard and the network.
- Change **DHCP** if needed, and in that case, enter all the network parameters
- Press **Save**

Network identification

Specify your network settings and, if desired, sensor naming and group here.

Name	Group	Hostname
XS-SENSOR-D60B17		XS-SENSOR-D60B17

IPv4

IPv4 with DHCP is the default network setting. Please be aware, if you change your IP settings here, you will lose access to the current view. In that case, please be prepared to re-open the sensor web-interface by typing in the new IP address in your web browser.

DHCP Fallback to 192.168.1.168

Save

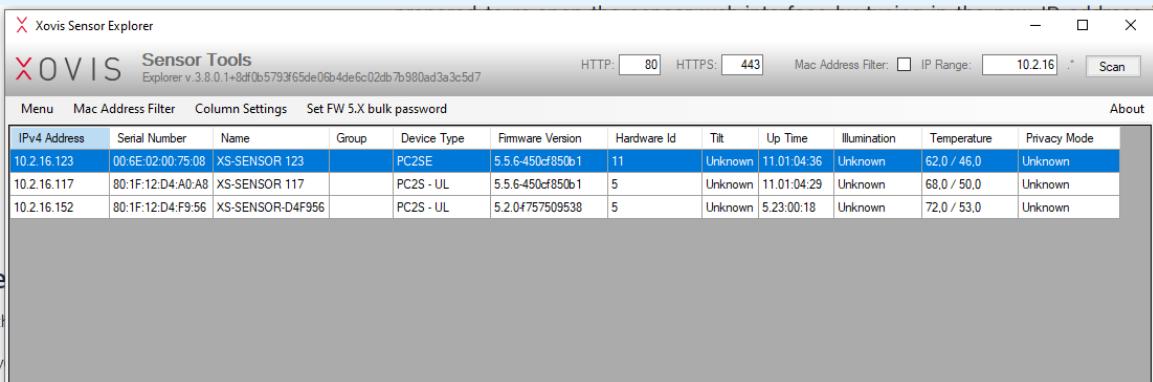
4. Connect the sensor to the customer's network

Connect the sensor (and your laptop) to the customer's network.

- Configure your laptop's network interface to network settings that will make a connection possible to the sensor when both are in the customer's network
- Connect the switch to the customer's network
- Open your browser and enter the IP address of the sensor



An alternative is to use a handy utility (`XovisSensorExplorer.exe`) to find the Xovis sensors in the current network. It can be requested via Xovis directly.



You will have to fill in the IP Range and then press Scan . Double-clicking a sensor opens a webpage for that sensor.

5. Configuring the sensor

We'll continue configuring the sensor.

- Press **Settings**
- Press **General**

Region

- Press **Region**

General ^

Region
Date & time
Network identification

- Enter the **Country**
- Enter the **Language**
- Enter the **Power frequency**
- Enter the **Measuring unit**
- Press **Save**

Region

Country

Netherlands

Language

English

Power frequency ?

50 Hz

Measuring unit

Metric (cm)

Xovis product improvement program

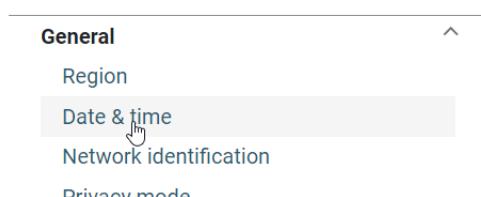


[Find out more](#)

Save

Date & time

- Press Date & time



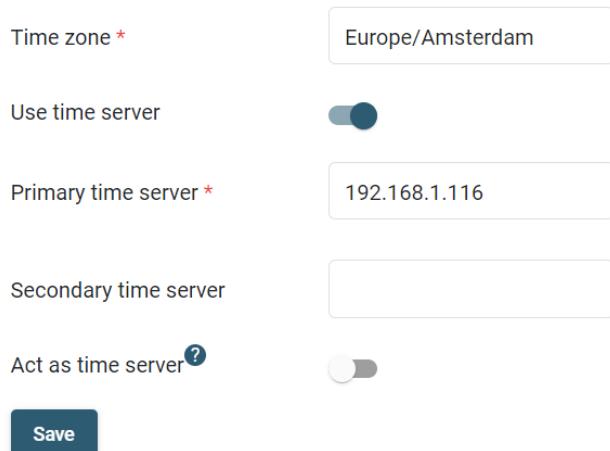
The screenshot shows a navigation menu with the following items:

- General
- Region
- Date & time (highlighted with a mouse cursor)
- Network identification
- Privacy mode

- Enter the Time zone
 - Make sure this matches the iSense system it is sending its data to
- Enter the iSense IP address in the Primary time server
- Press Save

Date & time

Specify the date and time settings here. Whenever possible it is recommended to use a time server instead of specifying the time manually.

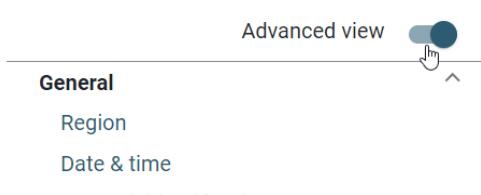


The form contains the following fields:

- Time zone *: Europe/Amsterdam
- Use time server:
- Primary time server *: 192.168.1.116
- Secondary time server: (empty input field)
- Act as time server ?
- Save button

Legacy support

- Turn on Advanced view



The screenshot shows a navigation menu with the following items:

- Advanced view (highlighted with a mouse cursor)
- General
- Region
- Date & time

- Press Legacy support

Advanced view

General ^

- Region
- Date & time
- Network identification
- Privacy mode
- Remote connection
- User management
- Licenses
- Advanced network properties
- Legacy support 

- Turn on **Enable legacy support**

Legacy support

Setting this option, enables legacy logics and legacy data pushes from former version 3 or version 4. If you migrated your sensor with configured data from one of those versions, the switch will be enabled. Sensors having version 5 installed from production, have the switch disabled. Please be aware, that legacy support may be dropped in future versions.

Enable legacy support



- When installing **one Xovis sensor for the exit/entrance**, continue with Chapter **6a. Single sensor**
- When installing **more than one Xovis sensor for the same exit/entrance**, continue with Chapter **6b. Multi sensor**

6a. Single sensor

Now configure the Single sensor:

- Press **Singlesensor**

Singlesensor ^

- Mounting height & tilt
- Image setup
- Recalibration
- Data push
- Path stitcher
- Tracking area
- Blocked space trigger
- Advanced options

Mounting height & Tilt

- Press Mounting height & tilt



- Change Sensor mounting height to match with the height at which the sensor is mounted
- Press Overwrite
- Press Save

Mounting height & tilt

For the best tracking results, make sure to set the correct mounting height of the sensor and set tilt corresponds closely with measured tilt.

Sensor mounting height

 cm

Tilt setup mode

Live tilt measured by the sensor 

0.1° / 9.7°

Tilt set in the sensor:

0.1° / 9.7°

Image setup

- Press Image setup



- Press Draw floor mask

Image setup

Draw floor mask: Cover the whole visible floor for best tracking results. Avoid drawing the floor mask over objects such as tables, flower pots or stairs.

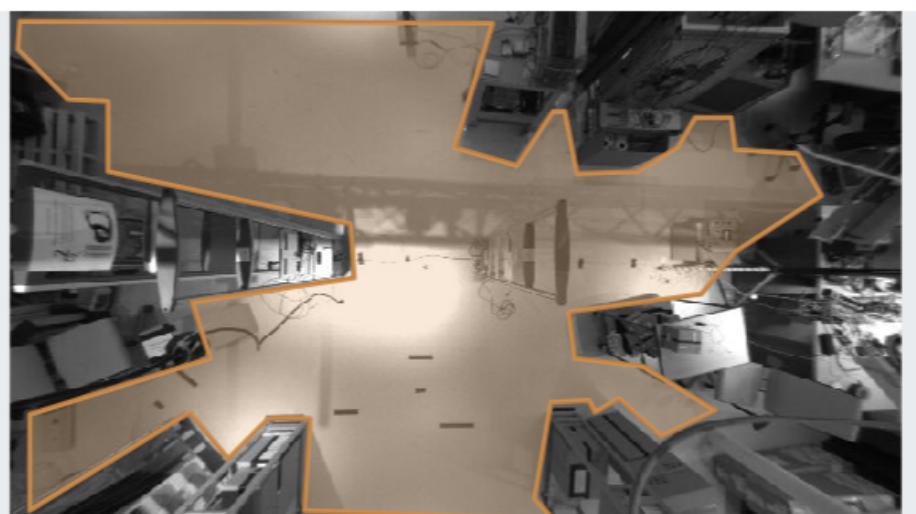
Draw taboo mask: Masked areas are ignored for image processing. Use carefully! To suppress tracks in specific areas use exclusion masks in the 'Scene Configuration'.

Draw illumination mask : Disturbing light sources can optionally be covered with illumination masks.

After any change in the image setup, the sensor will compile a new recalibration algorithm that need to be applied manually in the recalibrations menu.



- Start by clicking the first point where the floor meets an object and then move to the next point
- Repeat until done, double-click the last point or press ESC



- The example picture does not look too nice since it is taken from our lab, but the idea is to have the mask covering the floor
- Individual points can be moved
- Press Save

Recalibration

- Press Recalibration

Singlesensor ^

Mounting height & tilt

Image setup

Recalibration 

Data push

- Press **Apply**

Recalibration

After height, tilt or image setup changes, the sensor automatically computes a new recalibration. If the tracking quality is insufficient, a new recalibration should be applied.

 No recalibration is applied

 New recalibration can be applied **Apply**

Data push

- Press **Data push**

Singlesensor ^

Mounting height & tilt

Image setup

Recalibration

Data push 

Path stitcher

- Press **Add connection +**
- Select **HTTP / HTTPS connection**
- Change **Server URI** to **http://<iSense IP address>/integrations/xovis**
 - Replace **<iSense IP address>** to the IP address of the iSense system where the events should be delivered
- Press **Save**

Data push Singlesensor

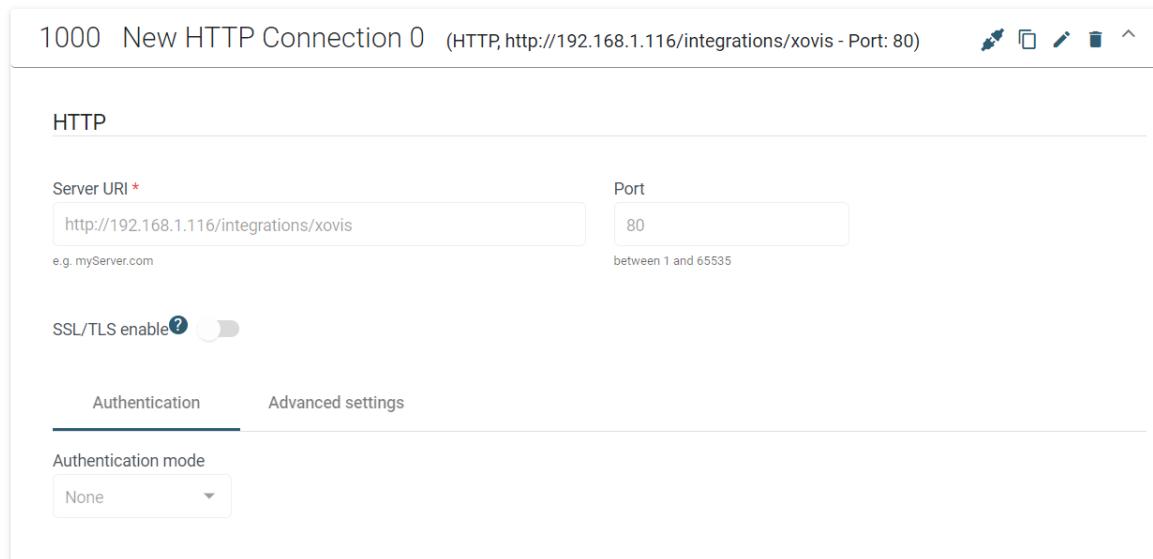
Push the data gathered on this sensor to the endpoints of your choice. Manage your connections to be used in the Data Push agent configuration below. Create at least one connection to be able to push data, otherwise localhost will be used by default. You may deactivate and reactivate Data Push agents using the toggle switch next to them. Both connections and Data Pushes can be edited and deleted here.

Configure here your data push setting for all data gathered by the Singlesensor. Connections and Agents are completely separated between Singlesensor and Multisensor.

Connections

Add connection +

1000 New HTTP Connection 0 (HTTP, http://192.168.1.116/integrations/xovis - Port: 80)



The form shows an 'HTTP' connection configuration. It includes fields for 'Server URI *' (http://192.168.1.116/integrations/xovis), 'Port' (80), and 'SSL/TLS enable?' (disabled). Below these are tabs for 'Authentication' (selected) and 'Advanced settings'. Under 'Authentication mode', a dropdown menu shows 'None'.

Agents

Add new agent +

There are no agents created yet

- Press **Connection test**

Add connection +



Connection test

- It should result in OK

Connection test

Status: OK
Server code: 200
Server info: OK

Retry

Close

- Press `Add new agent +`
- Select `Line count`
- Select the newly created connection in `Connection`
- Change `Format` to `JSON`
- Press `Save`
- Turn on the newly created agent

Data push Singlesensor

Push the data gathered on this sensor to the endpoints of your choice. Manage your connections to be used in the Data Push agent configuration below. Create at least one connection to be able to push data, otherwise localhost will be used by default. You may deactivate and reactivate Data Push agents using the toggle switch next to them. Both connections and Data Pushes can be edited and deleted here.

Configure here your data push setting for all data gathered by the Singlesensor. Connections and Agents are completely separated between Singlesensor and Multisensor.

Connections

[Add connection +](#)

1000 New HTTP Connection 0 (HTTP, http://192.168.1.116/integrations/xovis - Port: 80)



Agents

[Add new agent +](#)

1000 New Line Count Agent (Legacy push)



Data push type
Legacy push

Connection *

1000 - New HTTP Conne...

Data type

Line count

Interval

1 minute

Granularity

1 minute

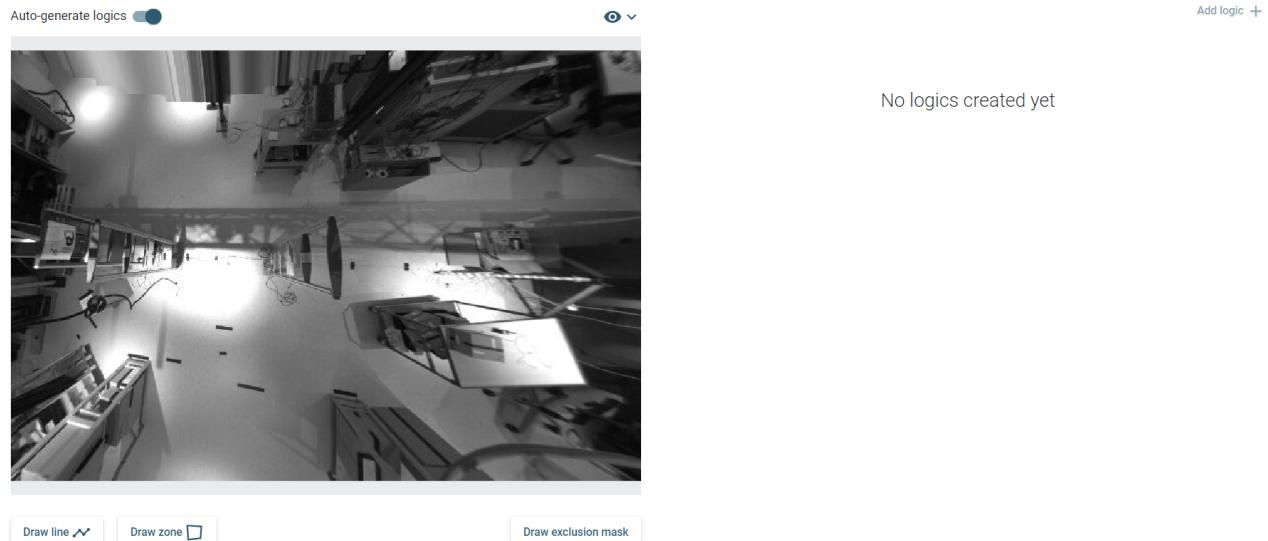
Format

JSON

Scene configuration

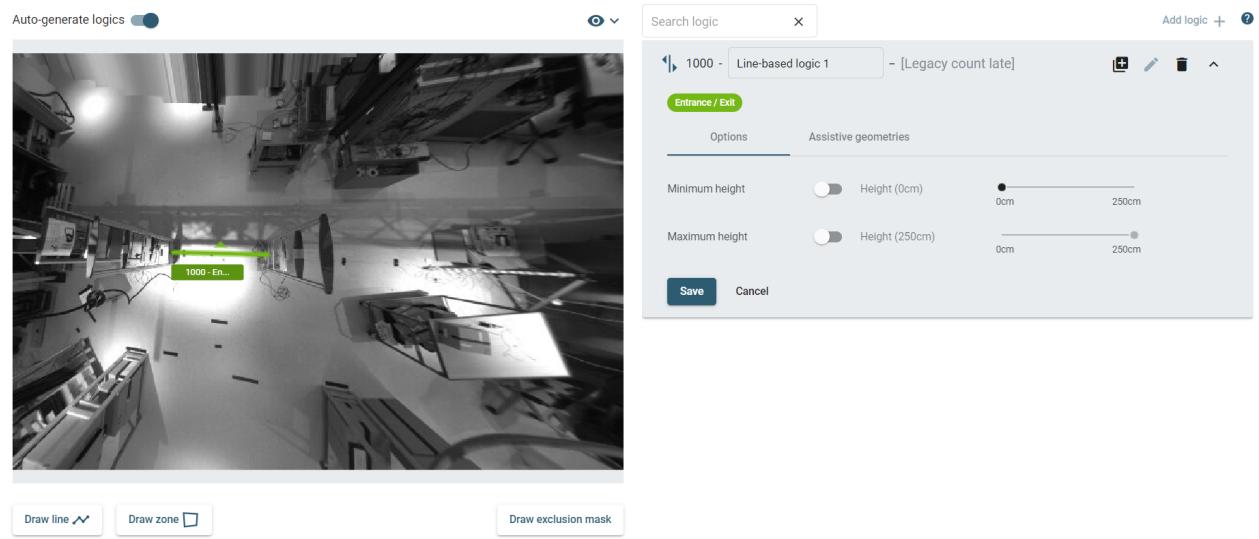
- Press `Scene configuration`
- Make sure `Auto-generate logics` is turned `on`
- Press `Draw line`

Scene configuration



- Start by clicking the first point where the entrance/exit starts and then move to the next point
- Repeat until done; double-click the last point or press ESC
- The green arrow points in the direction that counts incoming customers; you can change the direction with the **Invert direction** button
- Enter **Geometry name**
- For **Logic type**, enter **Legacy count late**
- Press **Save**

Scene configuration



- Logic is automatically generated
- Press **Save**

Privacy mode



Nedap Retail uses Xovis Sensor technology in the Overhead Customer Counting application. The Xovis Sensor technology is a device purchased by the end-customer. Nedap Business Partners install the Xovis 3D Sensor at the premises of the end-customer in one of the configurations as advised by Xovis and as instructed by end-customer, so customers cannot be identified. At all times the end-customer, as a data controller, will be responsible for the compliance with privacy legislation. Any changes made after the installation, will be at the account of the end-customer.



To reduce the privacy level, the sensor master key is required which can be obtained via the local supplier.

- Press General
- Press Privacy mode
- Press Level 2

Privacy mode

Choose the level of privacy you want to operate with. Attention: Lowering the level of privacy always requires the sensor master key to be entered!



- Press Save

(Almost) Ready



Since you configured a single sensor, skip Chapter **6b. Multi sensor** and continue with Chapter **7. Configuring iSense (part 2)**

6b. Multi sensor

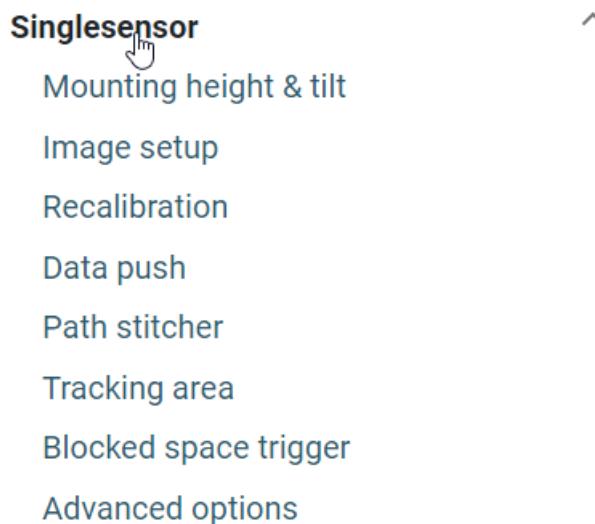
When installing more than one Xovis sensor for the same exit/entrance, you will have to choose one of the Xovis sensors as being the parent sensor for all the Xovis sensors that make up the exit/entrance.

Parent and Child sensors



First, do the following steps for **ALL** Xovis sensors (**parent** and **children**) that belong to this exit/entrance, maximum is 9 Xovis sensors.

- Press `Singlesensor`



Mounting height & Tilt

- Press `Mounting height & tilt`



- Change `Sensor mounting height` to match with the height at which the sensor is mounted
- Press `Overwrite`
- Press `Save`

Mounting height & tilt

For the best tracking results, make sure to set the correct mounting height of the sensor and set tilt corresponds closely with measured tilt.

Sensor mounting height

 cm

Tilt setup mode

Live tilt measured by the sensor 

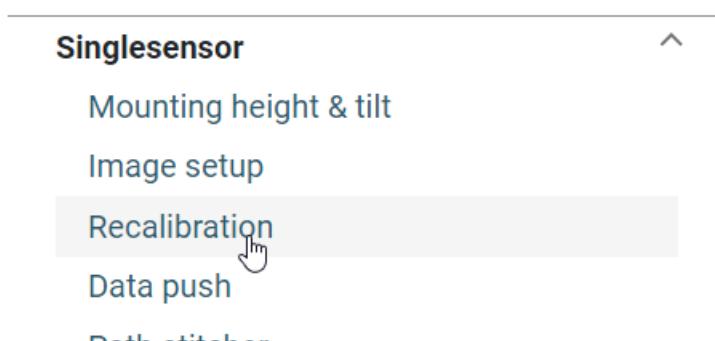
0.1° / 9.7°

Tilt set in the sensor:

0.1° / 9.7°

Recalibration

- Press



- Press

Recalibration

After height, tilt or image setup changes, the sensor automatically computes a new recalibration. If the tracking quality is insufficient, a new recalibration should be applied.

 No recalibration is applied

 New recalibration can be applied

- Repeat this for ALL sensors that make up this exit/entrance

Parent sensor



Do the following for the **parent** sensor only.

- Press
- Press

Multisensor

Rotation

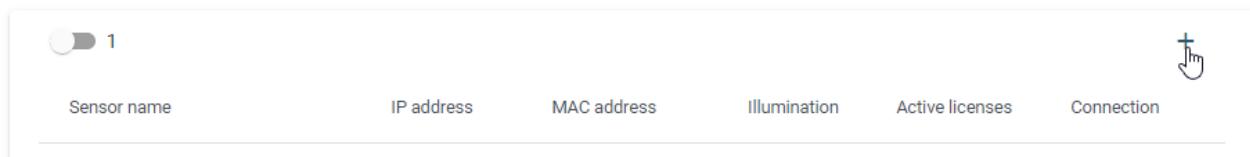
Multisensor

Data push

- Press +

Multisensor

Live scene images from multiple sensors can be combined to create a larger scene image to cover a wider viewing area. Logics and other scene configurations, as well as data push options, can be configured for this Multisensor in the same way as for a Singlesensor. Set up the Multisensor in a few minutes by connecting to the existing sensors using their IP address and credentials. Please make sure that all sensors are in operation.



- Press + Add sensor

- Enter IP address
- Enter Username
- Enter Password

Adding sensor 1 of 9

IP address (required if no MAC)

MAC address

Protocol

Port

Username

Password

 **Add****Close**

- Do this for ALL Xovis sensors (Parent and Children)
- Press **Close**
- Press every Xovis sensor once to fill every slot

Multisensor stitcher - 1

XS-SENSOR 117

C X Curr



Preview 2

C X



Stitch

Good

Sensors: 2/9

Search by name, ip or mac address



Ref: No ref

XS-SENSOR 117

C :

Sensor selected in preview 1

Online

Admin

🔗 http://10.2.16.117:80

MAC: 80:1F:12:D4:A0:A8

XS-SENSOR

Online

Admin

🔗 http://10.2.16.123:80

MAC: 00:6E:02:00:75:08

- Press Stitch

Multisensor stitcher - 1

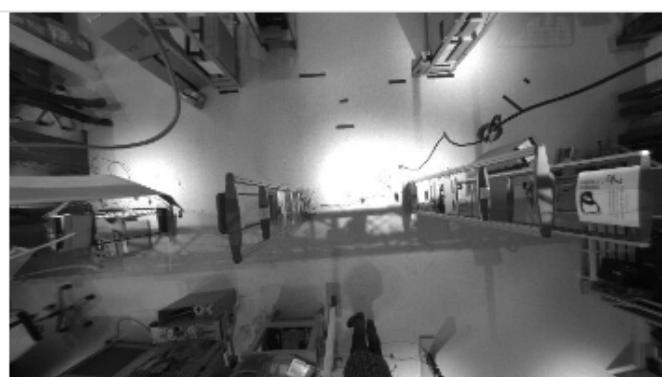
XS-SENSOR 117

C X



XS-SENSOR

C X



Stitch



Open camera 0 / 0 Search by name or IP address

- Choose and click 3 points that form a large triangle to enable good stitching of the images of each Xovis sensor. One point at a time.
- Press Save

Stitching sensors

XS-SENSOR 117



Stitching point pairs: Point 1 (29 cm) Point 2 (49 cm) Point 3 (41 cm)

[Save](#) [Cancel](#)

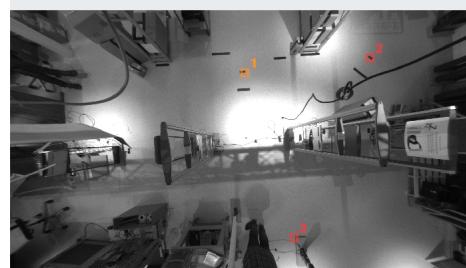
- Press **Apply computation**

Stitch points: 3/6

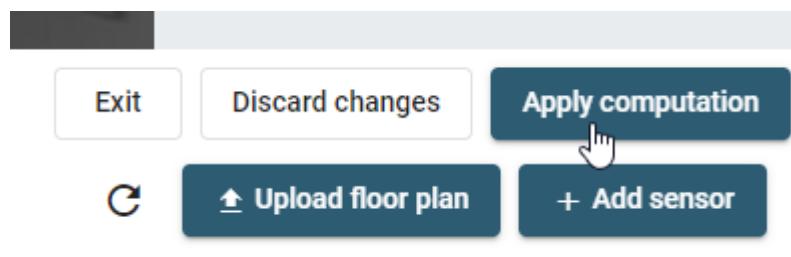
Accuracy
Difference between pair points in centimeters

- Info not available
- Good (less than 10 cm)
- Valid (less than 30 cm)
- Bad (more than 30 cm)

XS-SENSOR

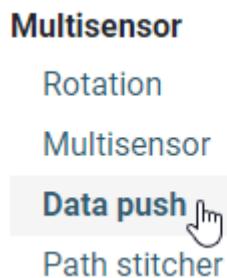


Stitching point pairs: Point 1 (29 cm) Point 2 (49 cm) Point 3 (41 cm)



Data push

- Press **Settings**
- Press **Multisensor**
- Press **Data push**



- Press **Add connection +**
- Select **HTTP / HTTPS connection**
- Change **Server URI** to `http://<iSense IP address>/integrations/xovis`

- Replace <iSense IP address> to the IP address of the iSense system where the events should be delivered
- Press Save

Data push Multisensor

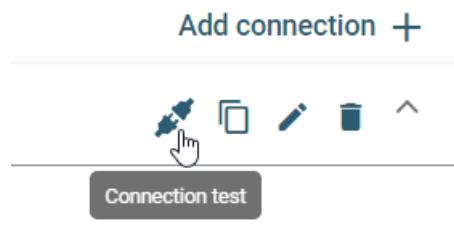
Push the data gathered on this sensor to the endpoints of your choice. Manage your connections to be used in the Data Push agent configuration below. Create at least one connection to be able to push data, otherwise localhost will be used by default. You may deactivate and reactivate Data Push agents using the toggle switch next to them. Both connections and Data Pushes can be edited and deleted here.

Configure here your data push setting for all data gathered by the Multisensor. Connections and Agents are completely separated between Multisensor and Singlesensor.

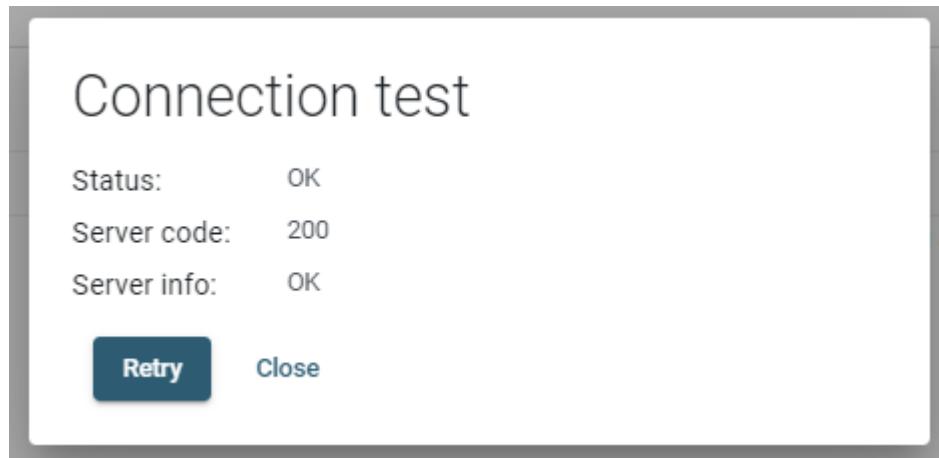
Connections

1000	New HTTP Connection 0	(HTTP, http://10.2.16.18/integrations/xovis - Port: 80)	Add connection +
HTTP			
Server URI! *	<input type="text" value="http://10.2.16.18/integrations/xovis"/>		Port <input type="text" value="80"/> between 1 and 65535
SSL/TLS enable?	<input checked="" type="checkbox"/>		
Authentication	Advanced settings		
Authentication mode	<input type="button" value="None"/>		
<input type="button" value="Save"/> <input type="button" value="Discard"/>			

- Press Connection test



- It should result in OK



- Press Add new agent +
- Select Line count
- Select the newly created connection in Connection

- Change Format to JSON
- Press Save
- Turn on the newly created agent

Data push Multisensor

Push the data gathered on this sensor to the endpoints of your choice. Manage your connections to be used in the Data Push agent configuration below. Create at least one connection to be able to push data, otherwise localhost will be used by default. You may deactivate and reactivate Data Push agents using the toggle switch next to them. Both connections and Data Pushes can be edited and deleted here.

Configure here your data push setting for all data gathered by the Multisensor. Connections and Agents are completely separated between Multisensor and Singlesensor.

Connections

Add connection +

1000 New HTTP Connection 0 (HTTP, http://10.2.16.18/integrations/xovis - Port: 80)				
------------------------------------------------------------------------------------	--	--	--	--

Agents

Add new agent +

1000 New Line Count Agent (Legacy push)				
Data push type Legacy push				
Connection * 1000 - New HTTP Conne...				
Data type	Interval	Granularity		
Line count	1 minute	1 minute		
Format				
JSON				

Scene configuration

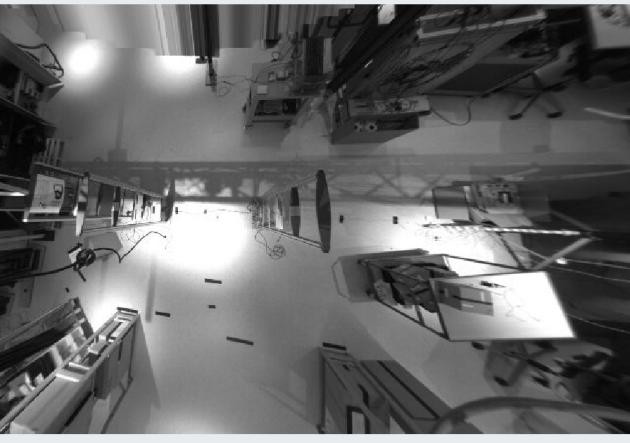
- Press Scene configuration
- Make sure Auto-generate logics is turned on
- Press Draw line

Scene configuration

Auto-generate logics

Add logic +

No logics created yet



Draw line ↘

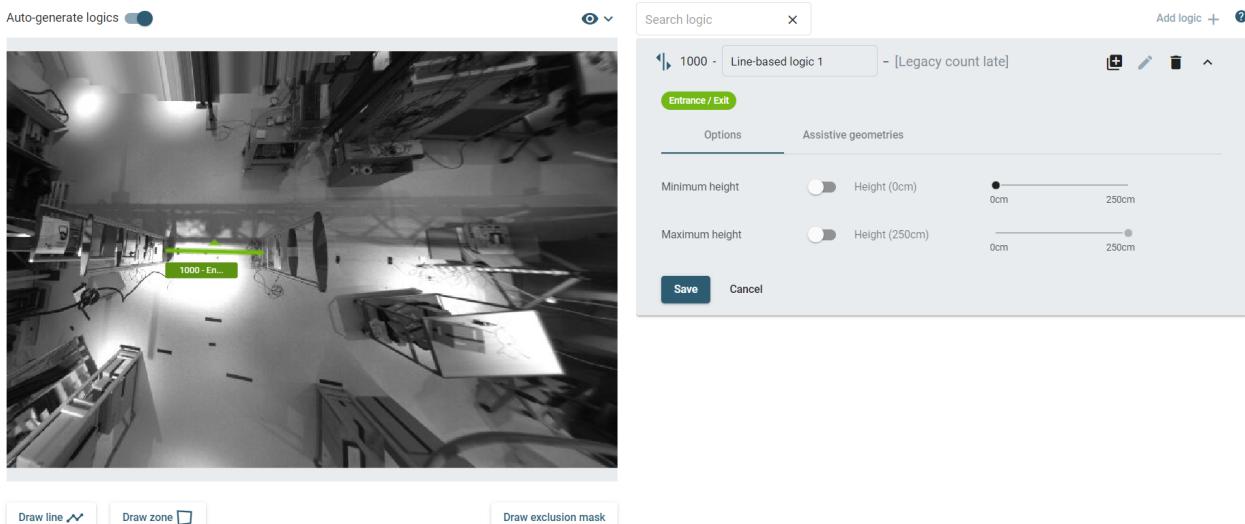
Draw zone □

Draw exclusion mask

- Start by clicking the first point where entrance/exit starts and then move to the next point
- Repeat until done, double-click the last point or press ESC

- The green arrow points in the direction that counts incoming customers; you can change the direction with the **Invert direction** button
- Enter **Geometry name**
- For **Logic type**, enter **Legacy count late**
- Press **Save**

Scene configuration



- Logic is automatically generated
- Press **Save**

Privacy mode



In Multisensor mode, there is no explicit option for enabling privacy mode as this is done by default.

Configuring iSense (part 2)

After saving the Xovis settings, switch back to the iSense configuration wizard. The Xovis sensor should show up here.



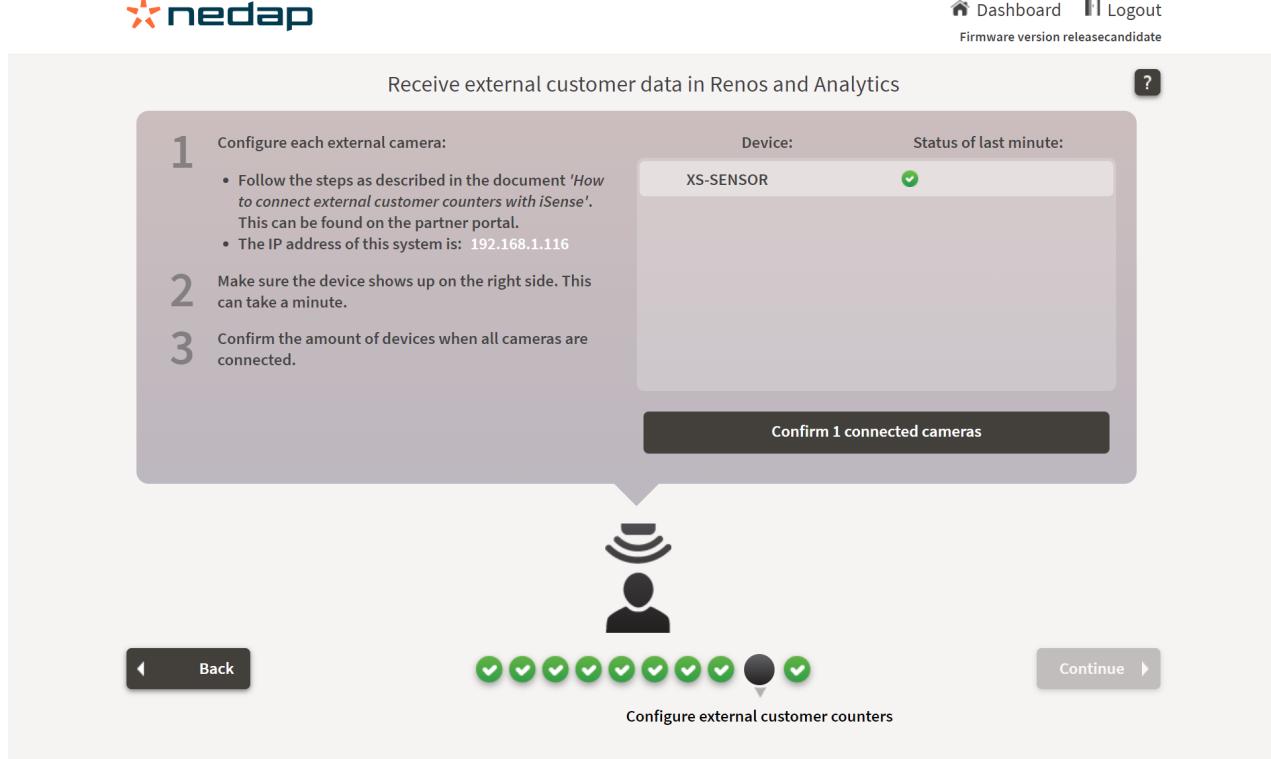
The Xovis sensors will only show up in the iSense configuration wizard when the sensor is completely configured (including the counting lines in the configuration of the sensor)



Because the device sends its counts to iSense every minute, it can take up to a minute before the device shows up.



If still not shown, create an event by passing the count lines and checking that the sensor has incremented the counts.



The screenshot shows the 'Configure external customer counters' step of the iSense configuration wizard. At the top, there's a header with the nedap logo, a dashboard link, a logout link, and a firmware version indicator ('Firmware version releasecandidate'). Below the header, the page title is 'Receive external customer data in Renos and Analytics'. A large callout box on the left provides instructions for connecting cameras:

- Configure each external camera:
 - Follow the steps as described in the document 'How to connect external customer counters with iSense'. This can be found on the partner portal.
 - The IP address of this system is: 192.168.1.116
- Make sure the device shows up on the right side. This can take a minute.
- Confirm the amount of devices when all cameras are connected.

To the right of the callout box is a table showing a single device entry:

Device:	Status of last minute:
XS-SENSOR	✓

A large button at the bottom of the callout box says 'Confirm 1 connected cameras'. Below the callout box is a central icon of a person with a signal wave above it. At the bottom of the page are navigation buttons for 'Back' and 'Continue', and a progress bar consisting of several green circles with checkmarks.

After configuring all Xovis sensors, ensure each shows up in the device list on the right side of the page. If this is correct, confirm the shown devices by clicking the '*Confirm X connected sensors*' button. The iSense system now remembers which devices are configured and will notify Nedap Device Management when one of these devices is no longer sending data.

 Receive external customer data in Renos and Analytics ?

1 Configure each external camera:

- Follow the steps as described in the document 'How to connect external customer counters with iSense'. This can be found on the partner portal.
- The IP address of this system is: 192.168.1.116

2 Make sure the device shows up on the right side. This can take a minute.

3 Confirm the amount of devices when all cameras are connected.

Device:	Status of last minute:
XS-SENSOR	✓

Confirm 1 connected cameras



Back Continue ▶

Configure external customer counters

Continue the configuration of the iSense system. When visitors are counted, an external count event is visible in the event list of the technical dashboard:

 1 minute ago Customers in: 1. Customers out: 0. Device id: XS-SENSO...

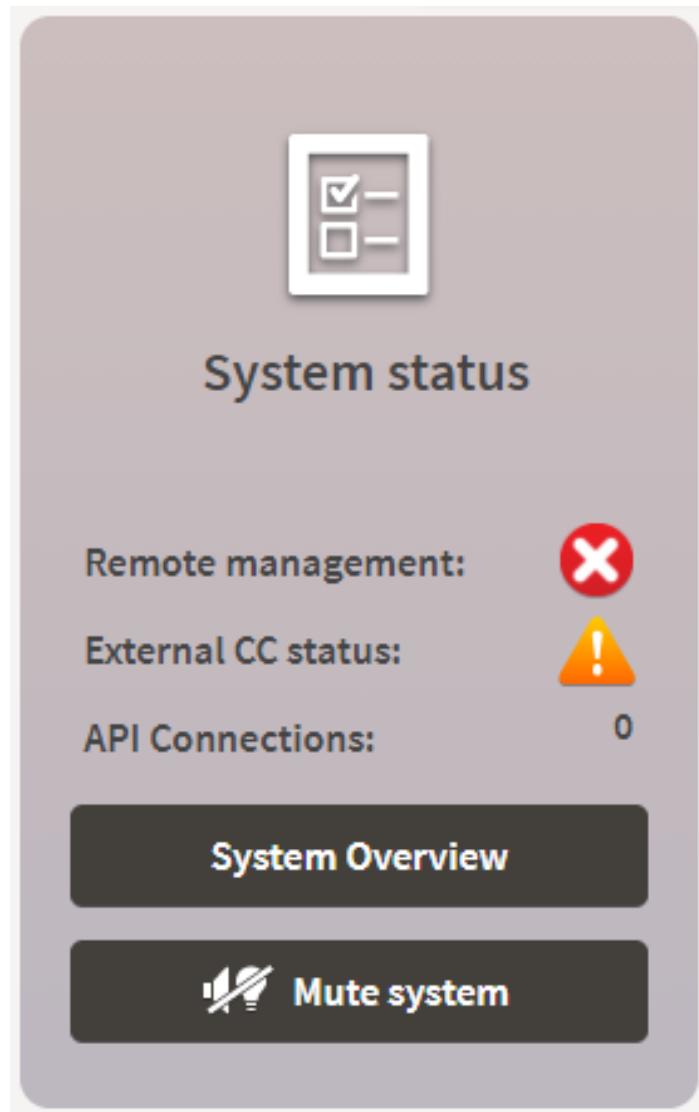
 When no visitors are counted, no event will be shown.

You have now successfully integrated Xovis sensors with iSense!

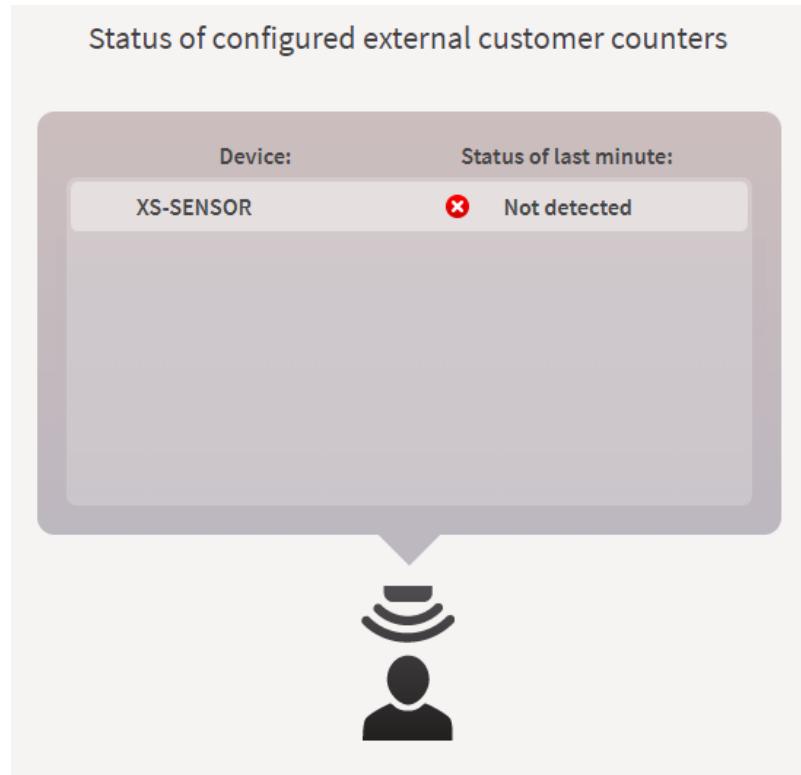
Status and troubleshooting

iSense

The status of the configured customer counters is shown in the technical dashboard - See *External CC* status in the following image. When something is wrong, the warning/error icon is clickable.



This will display a detailed list with the status of each configured device:



Possible statuses are:

- **OK** - the device is sending data to iSense every minute.
- **Not detected** - iSense has not received data from this device in the last two minutes. Ensure the Xovis sensor is powered and running and that the Xovis sensor and the iSense system are connected to the same Local Area Network.

If the “Not Detected” status is displayed, an issue is displayed for this store/system in Nedap Device Management.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap NV 2025

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 66

Document Last modification date 21 March 2025

Document PDF Exported 26 March 2025 by Nedap Retail | Operations



support-retail@nedap.com

Nedap Sense Guideline

iSense External Customer Counter Integration – Brickstream

Brickstream Customer Counting

version 156, March 2025

About this document	3
Introduction	4
Behavior	5
Network setup	6
Configuring iSense (part 1)	7
Configuring Brickstream.....	9
1. Update firmware	9
2. Configure IP settings	11
3. Configure Time server	12
4. Configure Sensor ID and Data format	14
5. Reboot	15
6. Configure Count area	16
7. Configure Data Delivery	18
8. Checking Diagnostics [Optional]	20
9. Privacy settings	22
10. Add login/password	23
11. Clear the buffer [Optional]	24
Configuring iSense (part 2)	25
Status and troubleshooting	27
iSense	27
Brickstream	29

About this document

This document describes the installation and configuration of the Brickstream 3D customer counters in combination with a Nedap iSense system.

- Model **2510M-25W/B** (White / Black) Brickstream 3D Gen 2, 2.5mm Lens

The guideline Brickstream: Pricing—Ordering—Connection is available for the commercial part of the project next to this document. It is available in the Commercial download section on the Partner Portal.



A Brickstream account is advised, which will give you access to Brickstream documentation and support. Please contact Brickstream directly to get an account via <https://flir.custhelp.com/app/ask>.



A Brickstream device does not have a **power supply** included and should be sourced locally (Power over Ethernet, IEEE 802.3af, Class 2 or higher)

Introduction

In addition to Nedap integrated customer counters, *external* customer counters can be connected to iSense. External customer counters are, for example, a good solution with iSense iD Tops. This setup shows the visitor data from the external counters in Nedap Retail Analytics and the local iSense dashboard. Currently, only *Brickstream 3D* customer counters are supported.



This document describes how to integrate these Brickstream 3D counters with iSense.

Behavior

- With this integration, *visitor counting* data via Brickstream 3D counters will be visible in Analytics. Other Brickstream features, like queue detection, are not supported.
- Each Brickstream customer counter sends the number of incoming and outgoing customers to the iSense system per minute in this setup.
- Visitor data will also be shown in the local iSense dashboard graphs.



Per integrated Brickstream device, a one-time fee will be charged automatically when the system is connected to Device Management: External CC Integration (6670059). Also, an iSenseGo Analytics Visitor (6669549) subscription is required to see the data in Analytics.



When replacing Brickstream 3D units in an existing installation, name the new unit the same as the old unit.



Counts made by Brickstream 3D counters are *not* available in the iSense API; they are available in the Analytics API.



Counts can *not* be used as a pager or IO box trigger.



Brickstream 3D counters are available in iSense as of firmware version 18.41



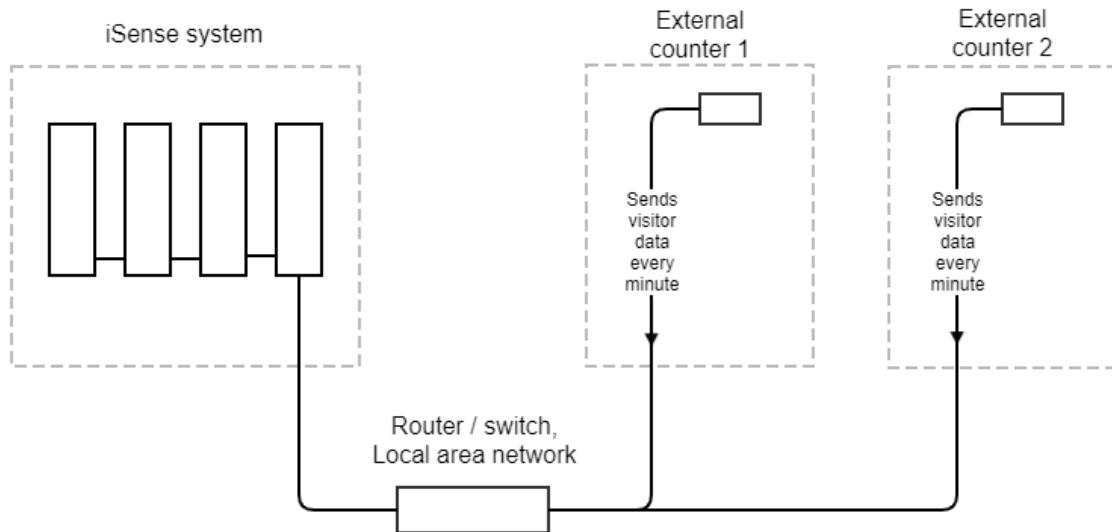
Brickstream 3D counters are not suitable for determining the stores' occupancy.



It can take 1 to 2 days before the first counts show up in Analytics

Network setup

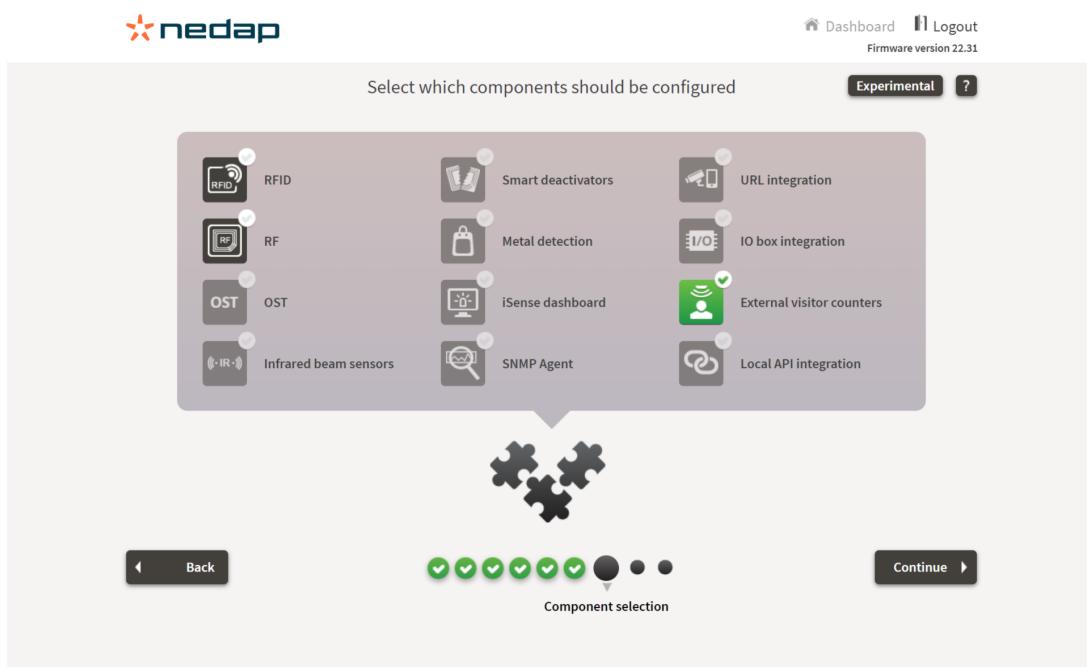
Connect each Brickstream 3D counter to the local area network. The iSense system (which can contain multiple gates or iD tops) must also be connected to this same local area network:



When the connection between the Brickstream device and the iSense system is down for any reason, the visitor data collected during this downtime will **not** be saved and will not be shown in Analytics and the local iSense dashboard..

Configuring iSense (part 1)

Install and configure the iSense system. In the 'Component selection page,' choose '*External visitor counters*':



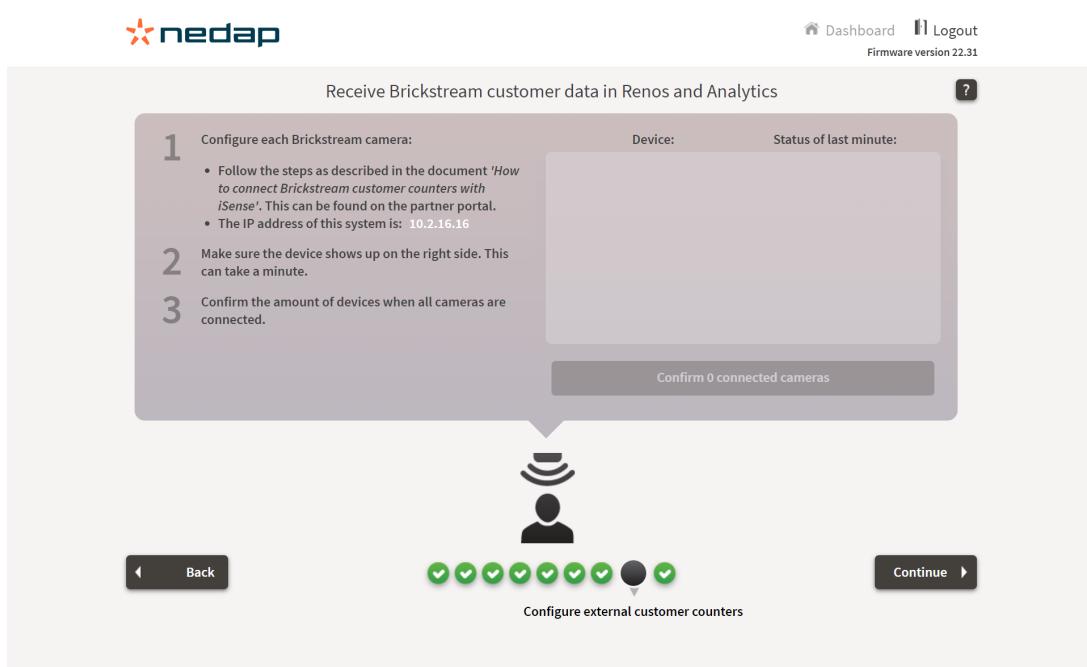
Select which components should be configured

Dashboard Logout Firmware version 22.31

Experimental ?

Component selection

The external customer counter configuration page will provide setup instructions. Write down the system's IP address.



Receive Brickstream customer data in Renos and Analytics

Configure each Brickstream camera:

- Follow the steps as described in the document 'How to connect Brickstream customer counters with iSense'. This can be found on the partner portal.
- The IP address of this system is: 10.2.16.16

Device: Status of last minute:

Configure external customer counters

Component selection



We will now need to configure each Brickstream device.

Configuring Brickstream

Open the browser and connect to the Brickstream web interface.

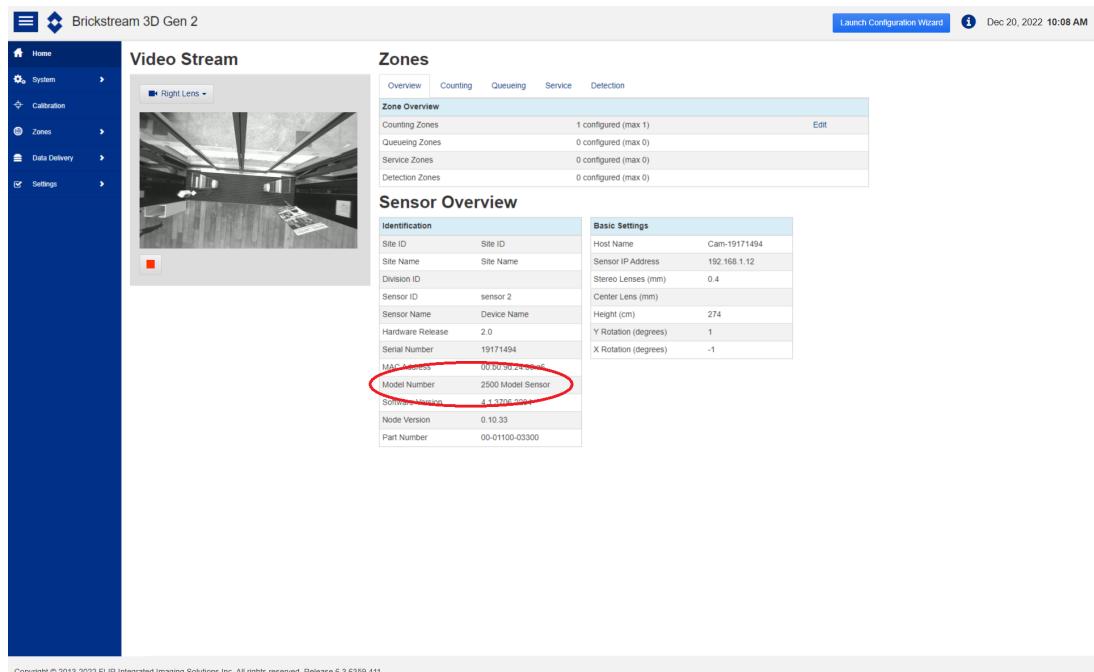
Use the default IP address, 192.168.1.7, to access the Brickstream web interface. This address is included in the shipment of all sensors.

1. Update firmware



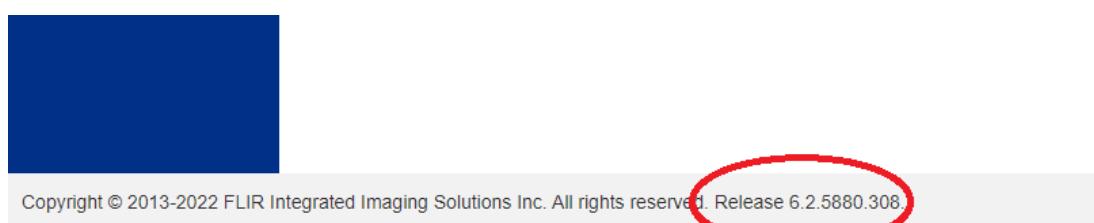
Make sure that you use the advised Brickstream firmware version, to be found on our portal:
<https://portal.nedapretail.com/technical/technical-isense-integrations>

- There are two different Brickstream models used. First, find out which model you are working with
- Choose **Home**



The screenshot shows the 'Brickstream 3D Gen 2' web interface. On the left is a dark sidebar with navigation links: Home, System, Calibration, Zones, Data Delivery, and Settings. The main area has tabs for 'Video Stream' and 'Zones'. Under 'Video Stream', there's a preview window showing a room interior. Under 'Zones', there's a table for 'Zone Overview' with rows for Counting Zones, Queueing Zones, Service Zones, and Detection Zones. Below that is a 'Sensor Overview' table divided into 'Identification' and 'Basic Settings' sections. The 'Identification' section includes fields like Site ID, Site Name, Division ID, Sensor ID, Sensor Name, Hardware Release, Serial Number, MAC Address, Model Number (circled in red), Software Version, Node Version, and Part Number. The 'Basic Settings' section includes Host Name, Sensor IP Address, Center Lens (mm), Height (cm), Y Rotation (degrees), and X Rotation (Degrees). At the bottom of the page, a copyright notice reads: 'Copyright © 2013-2022 FLIR Integrated Imaging Solutions Inc. All rights reserved. Release 6.3.6359.411.'

- Find the Model Number: either 2500 or 2510
- Verify the current Brickstream firmware version; it is shown in the bottom line.



The screenshot shows the same 'Brickstream 3D Gen 2' web interface as above, but with a large red circle highlighting the footer text. The footer text reads: 'Copyright © 2013-2022 FLIR Integrated Imaging Solutions Inc. All rights reserved. Release 6.2.5880.308.'

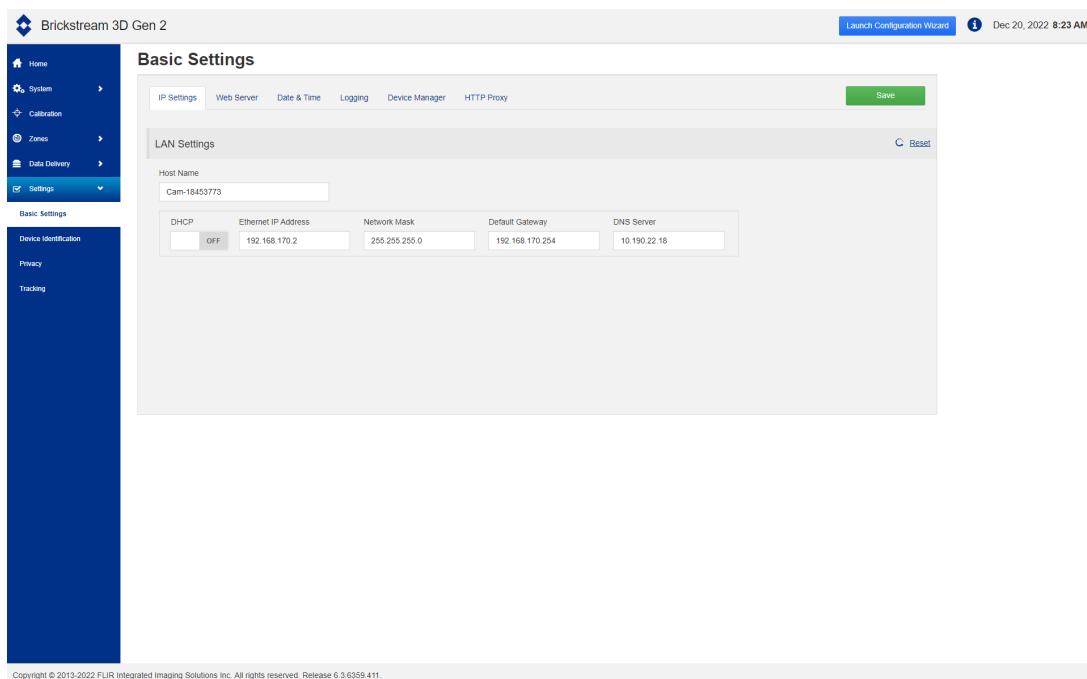


If it differs from the versions below, change the firmware to match this with the following steps.

- Choose **system> Upgrade**
- Press **Browse**
- Select the downloaded firmware file
 - For the 2510M-25W and 2510M-25B: **CountingApp2510_6.3.6324.410.bin**
 - For the 2500-25W: **CountingApp2500_6.3.6359.411.bin**
- Press **Upgrade**
- Follow the instructions and wait until the process finishes

2. Configure IP settings

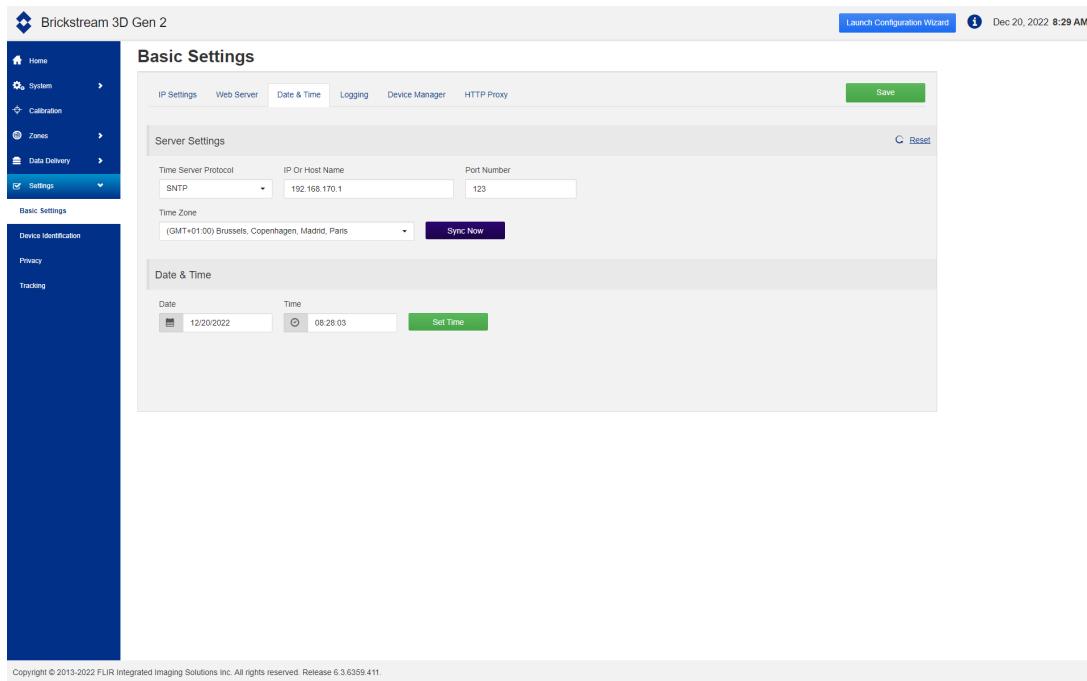
- Choose **Settings > Basic Settings**
- Select the **IP Settings** tab
- Enter the network settings as agreed with the customer
- Press **Save**
- The Brickstream camera will reboot now
- Please wait a few minutes and then connect to it with the new IP address



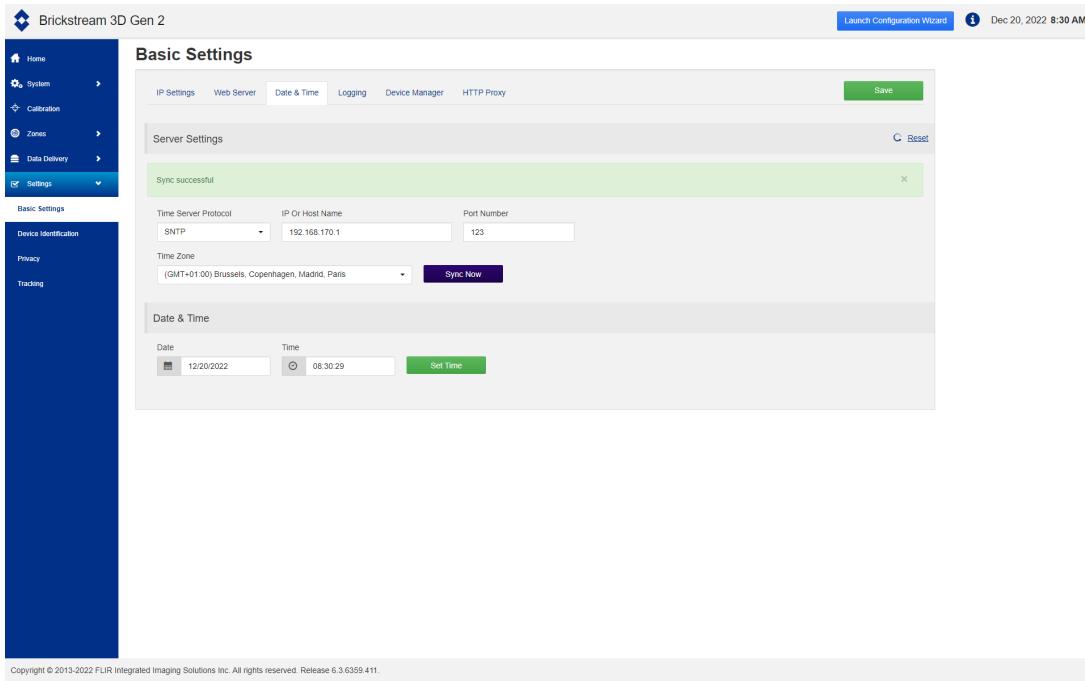
3. Configure Time server

The integration between the Brickstream device and iSense only works when the time server is set correctly so that the Brickstream device has the right time. The iSense system has a time server that should be used for the integration.

- Choose **Settings > Basic Settings**
- Select the **Date & Time** tab
- Time zone: select the time zone of the store's country/location
- Time Server Protocol: **SNTP**
- Time Server: the *IP address* of the iSense system that you wrote down in *Configuring iSense (part 1)*
- Port: **123**
- Press **Save**



Now verify the settings by pressing **Sync Now**. It should result in a 'Sync successful' message.



Errors as a result of the test will be shown in a red banner.



Validate that the displayed Date and Time are correct.



With an incorrectly configured time server, the wizard's status will change to "Receiving old data," **meaning** counts are never displayed!

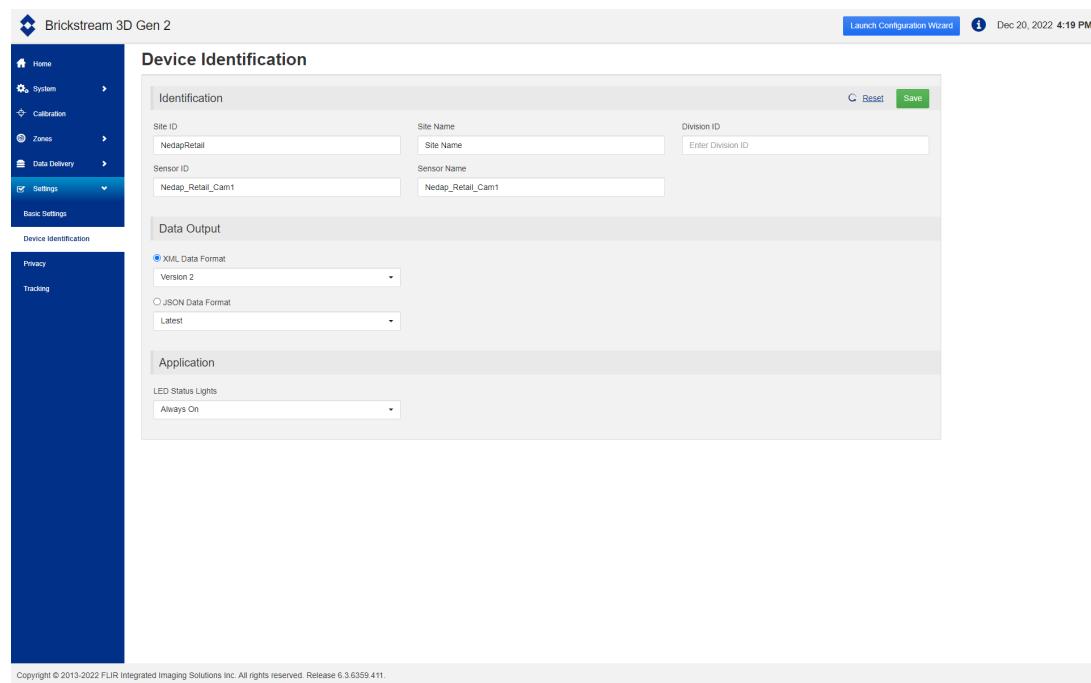
4. Configure Sensor ID and Data format

Now choose **Settings > Device Identification**

- Enter relevant values for **Site ID**, **Site Name**, **Division ID**, and **Sensor Name**
- Copy the **Host Name** found in **Settings > Basic Settings > IP Settings**.
- Paste the copied hostname to the **Sensor ID**, This ensures that the device name is the same in both the iSense wizard and the network.
- Select **XML Data Format** and set it to **Version 2**.
- Press **Save**.



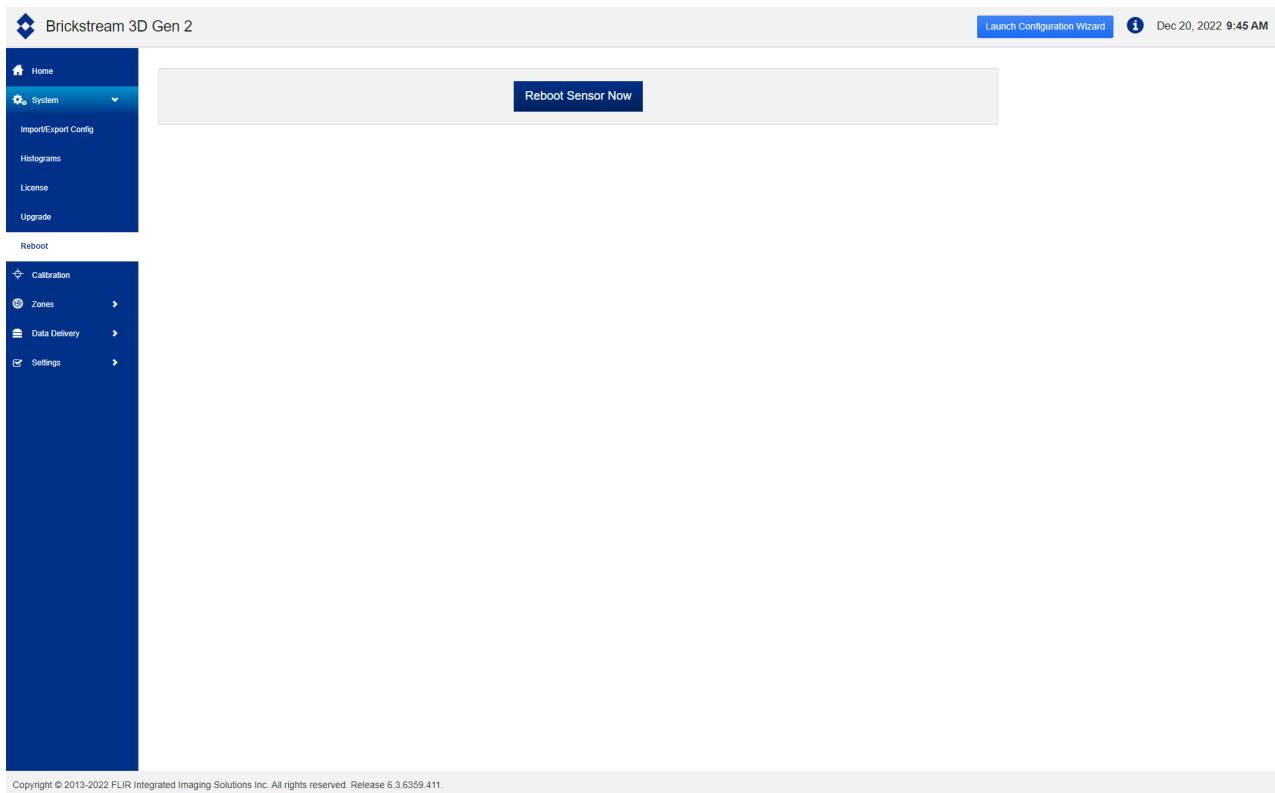
Setting **XML Data Format** to the incorrect version leads to disconnected Brickstream units after some time, although a delivery test will pass.



The screenshot shows the 'Device Identification' configuration page for a Brickstream 3D Gen 2 unit. The left sidebar has a dark blue background with white icons and text for Home, System, Calibration, Zones, Data Delivery, Settings (which is currently selected), and Basic Settings. The main area is titled 'Device Identification' and contains three sections: 'Identification', 'Data Output', and 'Application'. In the 'Identification' section, Site ID is set to 'NedapRetail', Site Name is 'NedapRetail', and Division ID is 'Enter Division ID'. Sensor ID is set to 'Nedap_Retail_Cam1' and Sensor Name is 'Nedap_Retail_Cam1'. Under 'Data Output', XML Data Format is selected and set to Version 2. JSON Data Format is set to Latest. In the 'Application' section, LED Status Lights are set to Always On. At the top right, there are 'Launch Configuration Wizard', a gear icon, and the date 'Dec 20, 2022 4:19 PM'. At the bottom, a copyright notice reads 'Copyright © 2013-2022 FLIR Integrated Imaging Solutions Inc. All rights reserved. Release 6.3.6359.411.'

5. Reboot

Changing the XML format and the Time Zone requires a reboot: **System > Reboot > Reboot Sensor Now.**

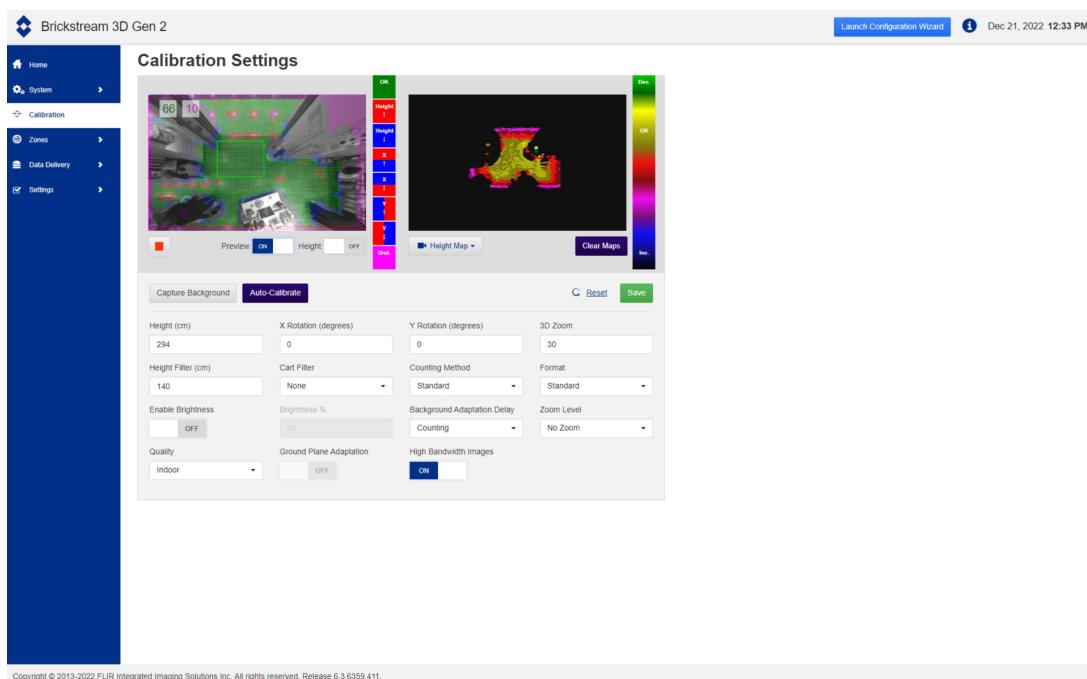


6. Configure Count area

Now **configure the cameras' count area** as described in the Brickstream documentation available on our Partner Portal.

As a summary:

- Move or change the green calibration box so that it contains only the floor and no walls or other objects, and minimal or no pink-shaded (undefined) areas
- Press **Calibration**
- Turn on **Preview**
- Press **Auto-Calibrate**
- Press **Capture Background**
- Check that most of the floor is green
- Press **Save**



- Press **Zones**
- Press **Counting**
- Add a new zone by pressing **Add**
- Draw enter and exit lines, taking care of the direction
- Draw a filter zone, optional but beneficial in cases of false counts
 - for a customer to be counted as entering the store, the customer should come from the yellow filter zone and then pass the green enter line in the correct direction

- for a customer to be counted as leaving the store, the customer should pass the blue exit line in the correct direction and then leave through the yellow filter zone
- The filter zone should cover the entire entering/leaving area!

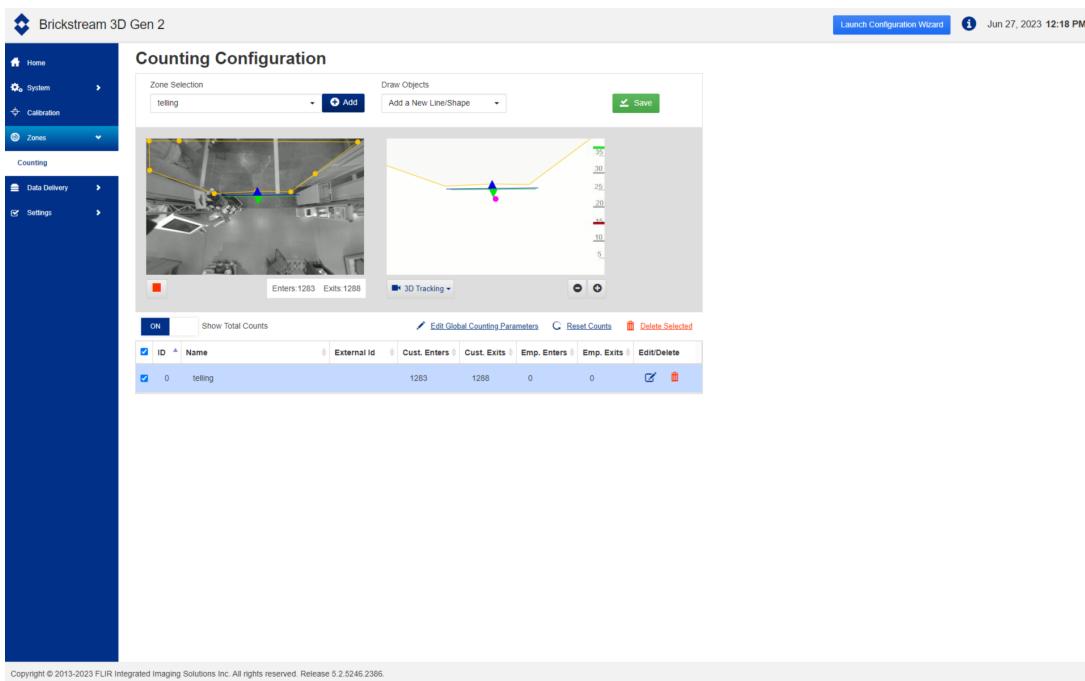


Make sure the lines and filter zone only cover the floor and no walls or other objects.

- Press **Save**
- Verify the counts



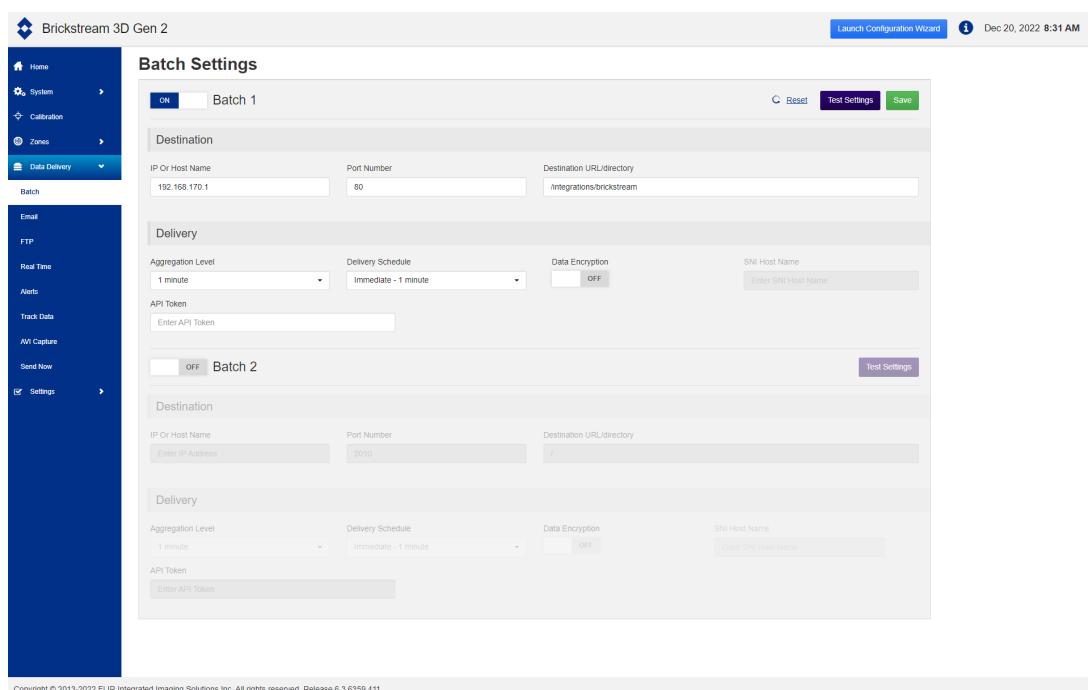
If this is your first installation with a Brickstream counter or if the situation is complex, please contact support!



7. Configure Data Delivery

Choose **Data Delivery > Batch**. Fill in the following settings:

- Batch1: **on**
- IP Or Hostname: the *IP address* of the iSense system that you wrote down in *Configuring iSense (part 1)*
- Port Number: **80**
- Destination URL/directory: **/integrations/brickstream**
- Aggregation Level: **1 minute**
- Delivery Schedule: **Immediate - 1 minute**
- Data Encryption: **off**
- Press **Save**



Brickstream 3D Gen 2

Batch Settings

Batch 1

Destination

IP Or Host Name: 192.168.170.1 | Port Number: 80 | Destination URL/directory: /integrations/brickstream

Delivery

Aggregation Level: 1 minute | Delivery Schedule: Immediate - 1 minute | Data Encryption: OFF | SNI Host Name: Enter SNI Host Name

API Token: Enter API Token

Batch 2

Test Settings

Destination

IP Or Host Name: Enter IP Address | Port Number: 2010 | Destination URL/directory: /

Delivery

Aggregation Level: 1 minute | Delivery Schedule: Immediate - 1 minute | Data Encryption: OFF | SNI Host Name: Enter SNI Host Name

API Token: Enter API Token

Now verify the settings by pressing **Test Settings**. It should result in a 'Test successful' message.



Test Settings only tests the **IP Or Hostname**.

The result will be successful even if the **Destination URL/directory** is wrong!

Double-check that it matches */integrations/brickstream*

Brickstream 3D Gen 2

Launch Configuration Wizard | Dec 20, 2022 8:32 AM

Batch Settings

Test successful.

Batch 1

Destination

IP Or Host Name: 192.168.170.1 Port Number: 80 Destination URL/directory: /integrations/brickstream

Delivery

Aggregation Level: 1 minute Delivery Schedule: Immediate - 1 minute Data Encryption: OFF SNI Host Name: Enter SNI Host Name

API Token: Enter API Token

Batch 2

Destination

IP Or Host Name: Enter IP Address Port Number: 2019 Destination URL/directory: /

Delivery

Aggregation Level: 1 minute Delivery Schedule: Immediate - 1 minute Data Encryption: OFF SNI Host Name: Enter SNI Host Name

API Token: Enter API Token

Test Settings Save

Reset

Batch

Home System Calibration Zones Data Delivery Email FTP Real Time Alerts Track Data AVI Capture Send Now Settings

Errors as result of the test will be shown in a red banner.

Server Error: connect to socket error #-1: No route to host

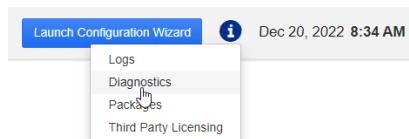
8. Checking Diagnostics [Optional]

You might want to check the Diagnostics page to be even more sure.

- Press the  in the top right corner.



- Then select **Diagnostics**



This page shows a collection of diagnostics that can be helpful in debugging issues.

Please check if the date and time shown in the upper right-hand corner of the Last Success column match within 1 minute.



Type	Successes	Last Success	Failures	Last Failure
Time Syncs	565	12/20/2022 08:30:56	0	-
Data Delivery				
Real Time 1	506524	12/20/2022 08:35:41	253261	12/20/2022 08:35:40
Batch 1	8462	12/20/2022 08:35:05	0	-
Administration				
Web Server	4230	12/20/2022 08:34:00	7	12/18/2022 08:52:10

Also, on the **Data Delivery > Batch** page, a message with the results of the latest delivery is shown.





As the delivery is once per minute, these values can take 1 minute to be updated. A page refresh might be needed.

9. Privacy settings



Nedap Retail uses Brickstream 3D Sensor technology in the Overhead Customer Counting application.

The Brickstream 3D Sensor technology is a device purchased by the end customer. Nedap Business Partners installs the Brickstream 3D Sensor at the end customer's premises in one of the configurations advised by Brickstream and as instructed by the end customer so customers cannot be identified.

As a data controller, the end customer is always responsible for compliance with privacy legislation.

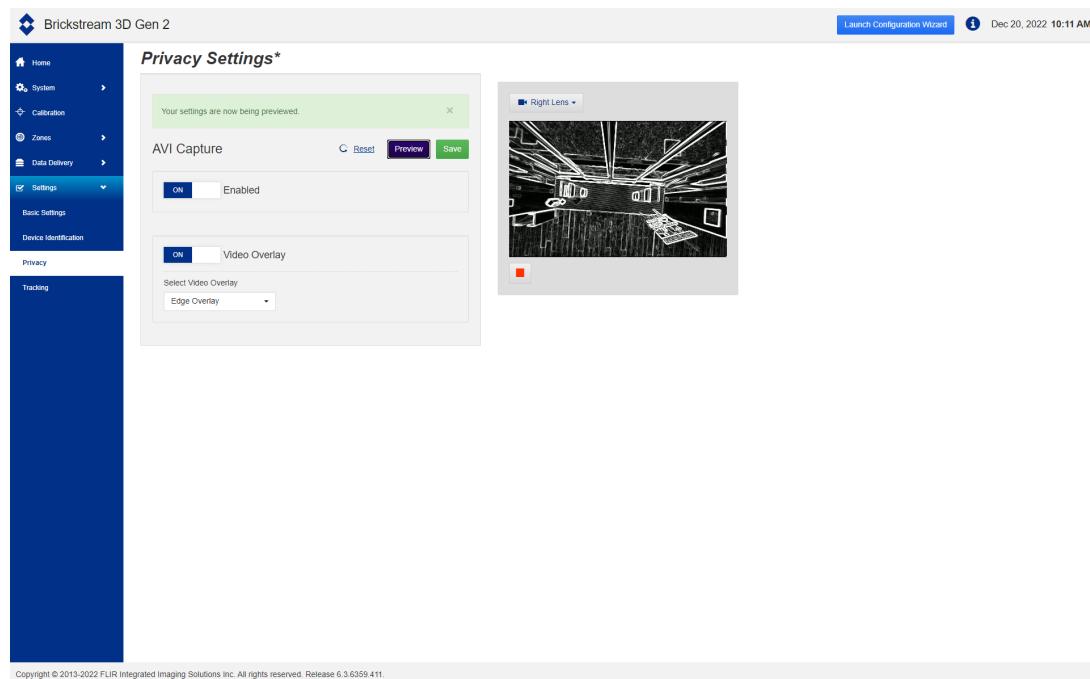
Any changes made after the installation will be charged to the end customer's account.



Disabling privacy mode is only possible on-site by using the hardware reset procedure.

Choose **Settings > Privacy** to turn off the video capture option and to set a video overlay.

- Set the **Video Overlay** to **ON**
- By pressing **Preview**, you can check the image before you save
- Press **Save**



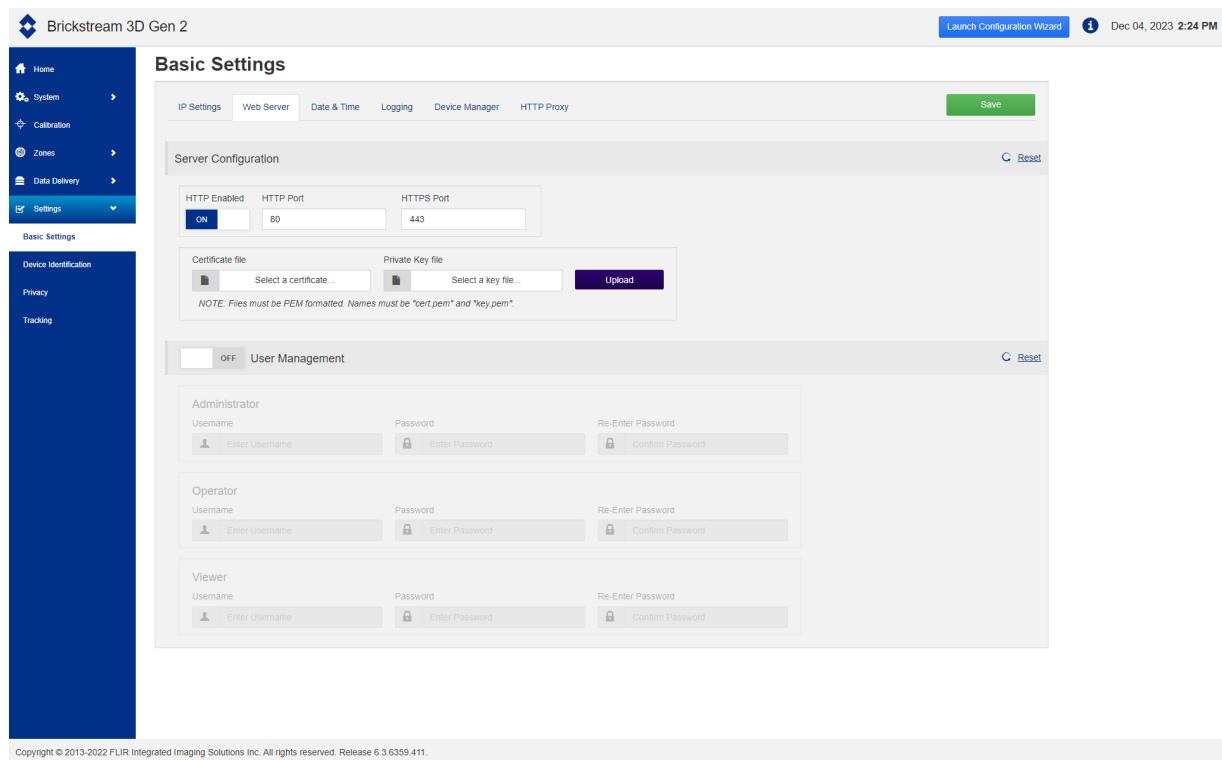
10. Add login/password



It is strongly advised to add an account for the administration of the Brickstream device. This will prevent changes by unauthorized access.

Choose **Settings > Basic Settings > Web Server** to turn on user authentication.

- Set **User Management** to **ON**
- Please enter a **Username and password** (and **Re-Enter the Password**) and save them in your password manager. (Get one if you're not already using one!)
- Press **Save**



The screenshot shows the 'Basic Settings' page of the Brickstream 3D Gen 2 configuration interface. The left sidebar has 'Basic Settings' selected under 'Settings'. The main tab is 'Web Server'. The 'User Management' section is turned 'ON'. It includes fields for 'Administrator', 'Operator', and 'Viewer' accounts, each with 'Username', 'Password', and 'Re-Enter Password' fields. A note at the bottom says 'NOTE: Files must be PEM formatted. Names must be "cert.pem" and "key.pem".' There is a 'Save' button at the top right.

11. Clear the buffer [Optional]

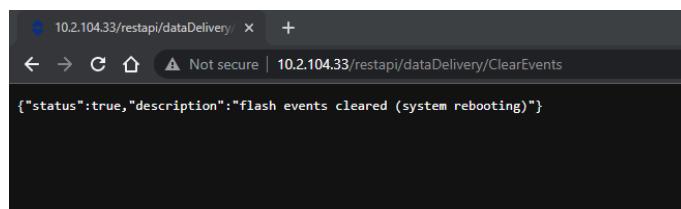
The Brickstream device will buffer events until it can deliver them to the iSense system. These 'late-delivery' events will be marked as 'Receiving old data' in the iSense system until up-to-date events are received again. The buffer in the Brickstream devices is extensive, and it can take several hours before the first up-to-date event is sent to the iSense system. This is especially the case when the iSense system has been unreachable by the Brickstream device for quite some time.

Unless the time server settings (step 2) are wrong, the 'Receiving old data' will be removed, and a green check mark will eventually appear. If you do not want to wait that long, you can clear the Brickstream buffer.

The way to do this is by accessing a specific page on the Brickstream: browse to

<http://<ip address>/restapi/dataDelivery/ClearEvents>

Replace '<ip address>' with the IP address of the Brickstream device.



Accessing this page clears the buffer, and a green check mark replaces the 'Receiving old data' message on the iSense system.

Configuring iSense (part 2)

After saving the Brickstream settings, switch back to the iSense configuration wizard. The Brickstream device should show up here.



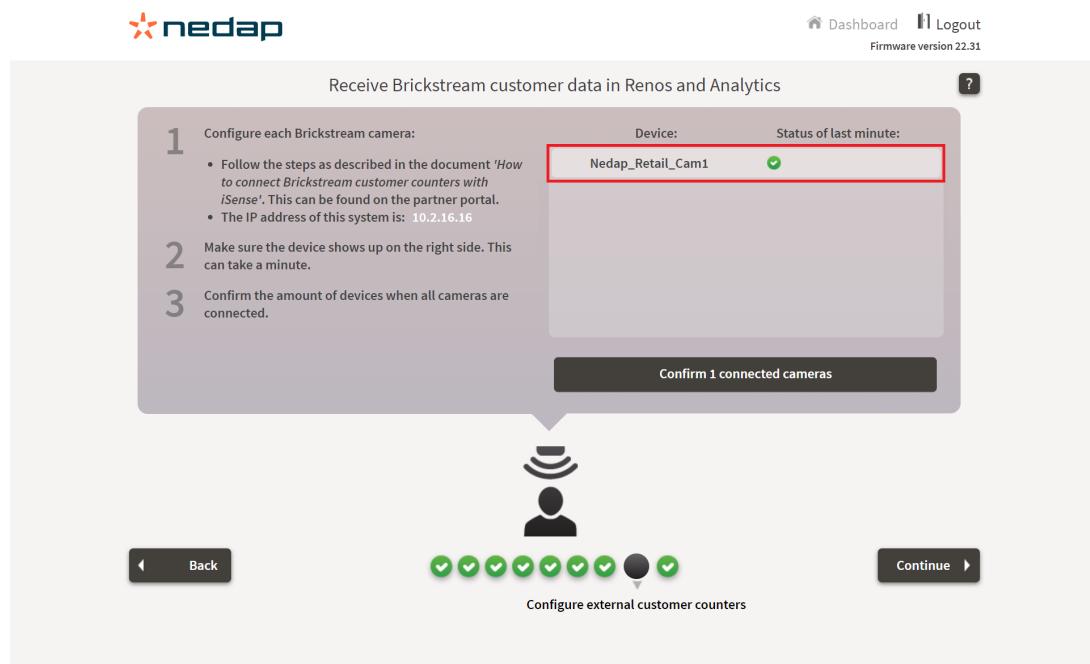
The Brickstream devices will only show up in the iSense configuration wizard when the Brickstream is completely configured (including the counting lines in the configuration of the Brickstream).



Because the device sends its counts to iSense every minute, it can take up to a minute for the device to show up.



If it still hasn't been shown, create an event by passing the count lines and checking that the camera has incremented the counts.



The screenshot shows a web-based configuration interface for the iSense system. At the top, there's a navigation bar with the nedap logo, a Dashboard link, a Logout link, and a Firmware version 22.31 notice. Below the navigation, a header reads "Receive Brickstream customer data in Renos and Analytics".

The main content area contains a step-by-step guide:

- Configure each Brickstream camera:
 - Follow the steps as described in the document 'How to connect Brickstream customer counters with iSense'. This can be found on the partner portal.
 - The IP address of this system is: 10.2.16.16
- Make sure the device shows up on the right side. This can take a minute.
- Confirm the amount of devices when all cameras are connected.

To the right of the steps, there's a table with two columns: "Device:" and "Status of last minute:". A red box highlights the "Device:" column for "Nedap_Retail_Cam1" and the "Status of last minute:" column, which shows a green checkmark. Below this table is a button labeled "Confirm 1 connected cameras".

At the bottom of the screen, there's a summary section with a user icon and the text "Configure external customer counters". It shows a progress bar with 10 green dots, one of which is darkened, and a "Continue" button to the right.

After configuring all Brickstream devices, ensure each appears in the device list on the right side of the page. If this is correct, confirm the devices shown by clicking the '*Confirm X connected cameras*' button. The iSense system now remembers which devices are configured and will notify Nedap Device Management when one of them no longer sends data.

Receive Brickstream customer data in Renos and Analytics

?

1 Configure each Brickstream camera:

- Follow the steps as described in the document 'How to connect Brickstream customer counters with iSense'. This can be found on the partner portal.
- The IP address of this system is: 10.2.16.16

2 Make sure the device shows up on the right side. This can take a minute.

3 Confirm the amount of devices when all cameras are connected.

Device: Nedap_Retail_Cam1 Status of last minute: 

Confirm 1 connected cameras

?

Back Continue

Configure external customer counters



The screenshot shows a configuration interface for integrating Brickstream customer counters with iSense. It includes a sidebar with navigation links like Dashboard and Logout, and a footer indicating Firmware version 22.31. The main content area displays a step-by-step guide for connecting cameras, a summary of one connected device, and a final confirmation button. Below this, there's a section for configuring external customer counters. A red box highlights the 'Confirm 1 connected cameras' button. A large blue arrow points downwards from the summary box towards the next section.

Continue the configuration of the iSense system. When visitors are counted, an external count event is visible in the event list of the technical dashboard:



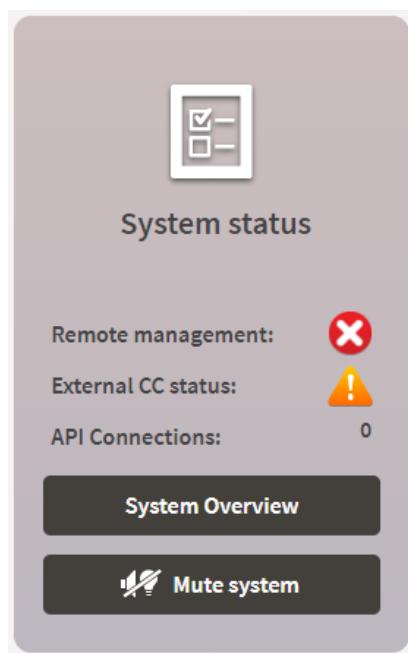
 When no visitors are counted, no event will be shown.

You have now successfully integrated Brickstream customer counters with iSense!

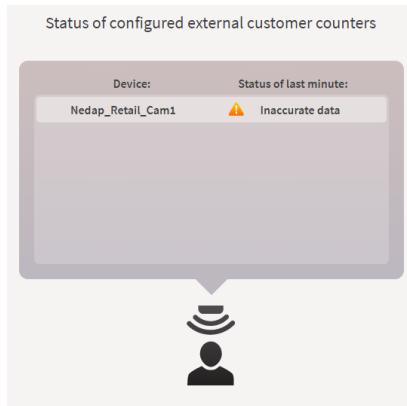
Status and troubleshooting

iSense

The technical dashboard shows the status of the configured customer counters. See the *External CC* status in the following image. When something is wrong, the warning/error icon is clickable.



This will display a detailed list with the status of each configured device:



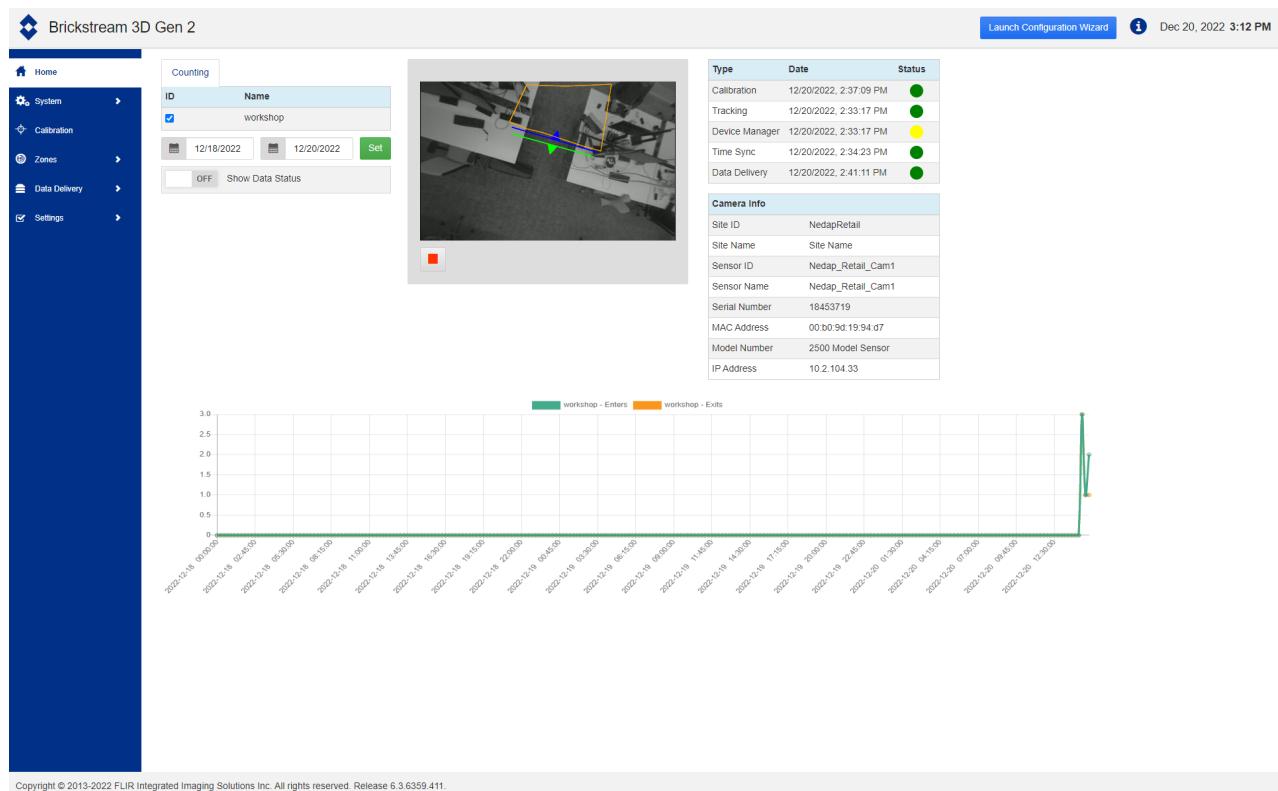
Possible statuses are:

- **OK** - the device is sending data to iSense every minute.
- **Inaccurate data**—The Brickstream device is sending data, but this data might not be accurate. For instance, it might happen at night, when the store environment is too dark to count visitors correctly. Move the mouse over the status to see a detailed message.
- **Receiving old data** - when the connection between a Brickstream and iSense is down for longer, the Brickstream device will send this data again once the connection is established. This old data is **not** saved on iSense, but the system still receives old messages. After receiving all old messages, the connection will be back to OK. This can take up to 9 hours in extreme cases!! If the Brickstream device has 1 day's worth of old data, it will take approximately 6 minutes to synchronize. This status can also be due to a poorly configured time server. Double-check the timeserver settings to ensure they are set up correctly.
- **Error**—The Brickstream device encountered an error. Click on this status to see a detailed message.
- **Not detected** - iSense has not received data from this device in the last two minutes. Ensure the Brickstream device is powered and running and that the Brickstream system and the iSense system are connected to the same Local Area Network. Also, ensure the XML version is set to "Version 2". With the wrong XML version, the "Test Settings" for the batch delivery returned successfully, but the camera still might end with a "Not detected" message in the iSense Dashboard.

In Nedap Device Management, an issue is displayed for this store/system if an error or unrecognized status is present.

Brickstream

The Brickstream homepage shows the camera's status; green dots are okay. The yellow dot for the Device Manager can be ignored; it is not configured.



Copyright © 2013-2022 FLIR Integrated Imaging Solutions Inc. All rights reserved. Release 6.3.6359.411.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Document Version 156

Document Last modification date 21 March 2025

Document PDF Exported 26 March 2025 **by** Nedap Retail | Operations

Copyright © Nedap NV 2025

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com



ioLogik E1214

Remote Ethernet I/O with 2-port Ethernet switch, 6 DIs, and 6 relays



- Built-in 2-port Ethernet switch for daisy-chain topologies
- Free support of Moxa's push-based Active OPC Server Lite
 - Seamlessly connect to any SCADA system
 - Save 80% on network bandwidth
 - I/O response that's seven times faster
- User-defined Modbus/TCP addressing
- MXIO programming library for Windows and WinCE VB/VC.NET and Linux C APIs
- Web configuration with Import/Export function

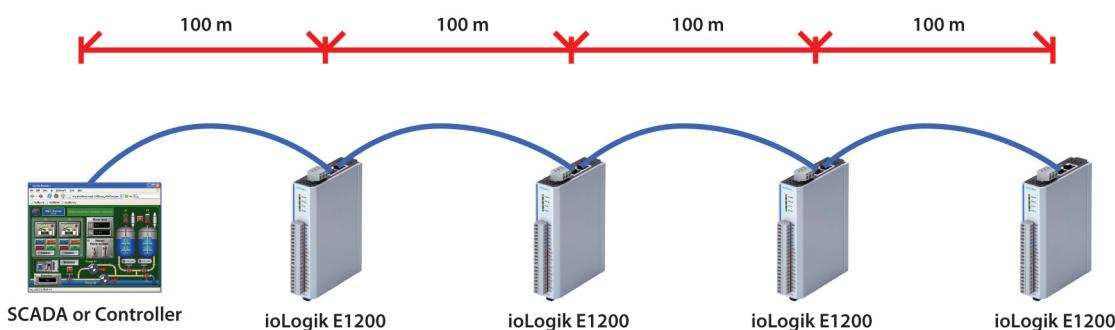


Introduction

Daisy-chained Ethernet I/O Connection

A new daisy-chained Ethernet I/O concept is now available. The ioLogik E1214 industrial remote Ethernet I/O has two embedded Ethernet switch ports that allow information to flow to another local Ethernet device or connect to the next ioLogik in the daisy-chain. Applications such as factory automation, security and surveillance systems, and tunnel monitoring, can make use of daisy-chained Ethernet for building multi-drop I/O networks over standard Ethernet cables. Many industrial automation users are familiar with the multi-drop configuration

typically used in fieldbus applications. The daisy-chain function on the remote Ethernet I/O ioLogik E1214 not only increases the connection between machines and panels, but also lowers the cost of buying separate Ethernet switches, and at the same time reduces labor fees and cabling by a large percentage. For example, if a production facility contains 700 stations (20 points per station), the wiring cost reduction can reach 15% of the total implementation cost.



Specifications

LAN

Ethernet: 2 x 10/100 Mbps switch ports, RJ45

Protection: 1.5 KV magnetic isolation

Protocols: Modbus/TCP, TCP/IP, UDP, DHCP, Bootp, HTTP

Digital Input

Sensor Type: NPN, PNP, and Dry contact

I/O Mode: DI or Event Counter

Dry Contact:

- Logic 0: short to GND

- Logic 1: open

Wet Contact:

- Logic 0: 0 to 3 VDC

- Logic 1: 10 to 30 VDC (DI COM to DI)

Isolation: 3K VDC or 2K Vrms

Counter/Frequency: 250 Hz, power off storage

Relay Output

Type: Form A (N.O.) relay outputs, 5A

Contact Rating: 5 A @ 30 VDC, 5 A @ 250 VAC, 5 A @ 110 VAC

Inductance Load: 2 A

Resistance Load: 5 A

Breakdown Voltage: 500 VAC

Relay On/Off Time: 1500 ms (Max.)

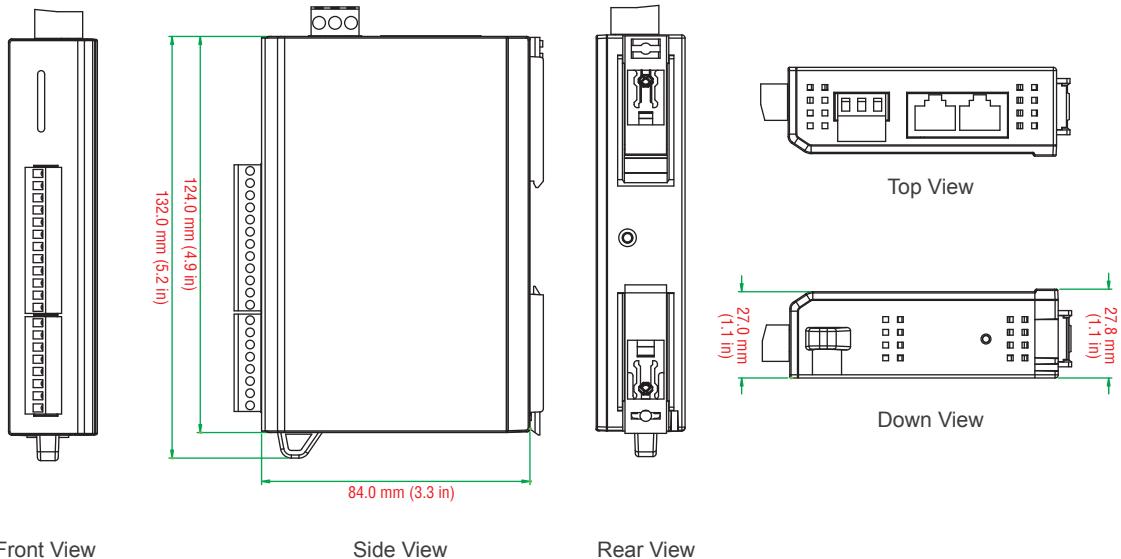
Initial Insulation Resistance: 1G min. @ 500 VDC

Expected Life: 100,000 times (Typical)

Initial Contact Resistance: 30 milli-ohms (Max.)

Pulse Output: 0.3 Hz at rated load

Dimensions



Power Requirements

Power Input: 24 VDC nominal, 12 to 36 VDC

Power Consumption: 130 mA typical @ 24 VDC

Physical Characteristics

Wiring: I/O cable max. 14 AWG

Dimensions: 27.8 x 124 x 84 mm (1.09 x 4.88 x 3.31 in)

Weight: under 200 g

Environmental Limits

Operating Temperature: -10 to 60°C (14 to 140°F)

Storage Temperature: -40 to 85°C (-40 to 185°F)

Ambient Relative Humidity: 5 to 95% (non-condensing)

Regulatory Approvals

EMI: FCC Part 15, CISPR (EN55022) class A

EMS: IEC 61000-4, IEC 61000-6

Safety: UL508

Shock: IEC 60068-2-27

Freefall: IEC 60068-2-32

Vibration: IEC 60068-2-6

Note: Please check Moxa's website for the most up-to-date certification status.

Warranty

Warranty Period: 2 years

Details: See www.moxa.com/warranty

Ordering Information

Available Models

ioLogik E1214: Remote Ethernet I/O with 2-port Ethernet switch, 6 DIs, and 6 Relays

Connected Devices Guideline

iSense Integration I/O box

with Moxa IOLogik E1214

version 135, February 2024

Introduction	3
Preparation	4
Required products	5
Installation.....	6
USB options	7
Network options	9
Connecting the IO box	10
Configuration.....	11
Input Event.....	14
Name	15
Action	15
Invert	15
Gate Range	15
Output Event	16
Name	17
Event	17
Invert	17
Gate Range	17
Delivery test	18
Test your integration and check if it works as expected.	18
Appendix Moxa ioLogik E1214	19
Specifications	19
Dimensions	22
Used abbreviations	23

Introduction

Integrating an IO box, enables a large number of interfacing possibilities. This document describes how to install and configure an IO box.

Preparation

Determine the equipment to interface with the IO box (to be defined by the project manager)



Nedap Retail only supports the "Moxa IOLogik E1214" IO Box.

1. Determine which outputs and inputs of the IO box will be used.
2. Check the specifications of the Moxa IOLogik E1214 IO box at moxa.com.
 - a. Determine whether the input and output signals of the IO box and the hardware to be connected match or whether these must be converted by additional hardware.
3. Choose an appropriate power supply for the IO box. (12 .. 36V DC)



Moxa IOLogik IO Box

Required products

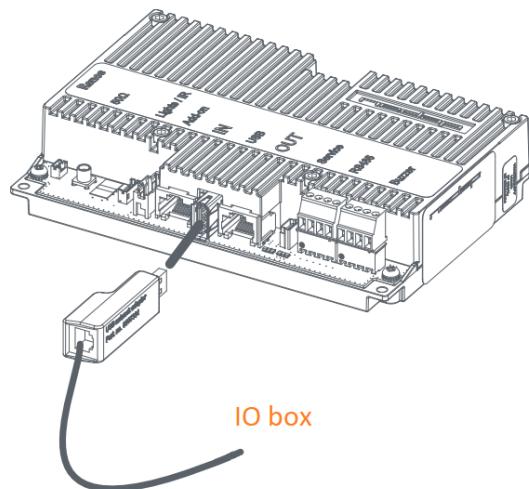
1. iSense system
2. USB network-adapter
3. IO box (Moxa IOLogik E1214)
4. External Power supply (12 .. 36V DC not supplied with the IO box)
5. Standard Installation tools and materials to create a network cable (Network cable Cat 5E or better, Filters, UTP connectors, Crimp tool, Cable tester)
6. Powered USB hub (Needed when an RFID reader is also installed in the system)

Installation

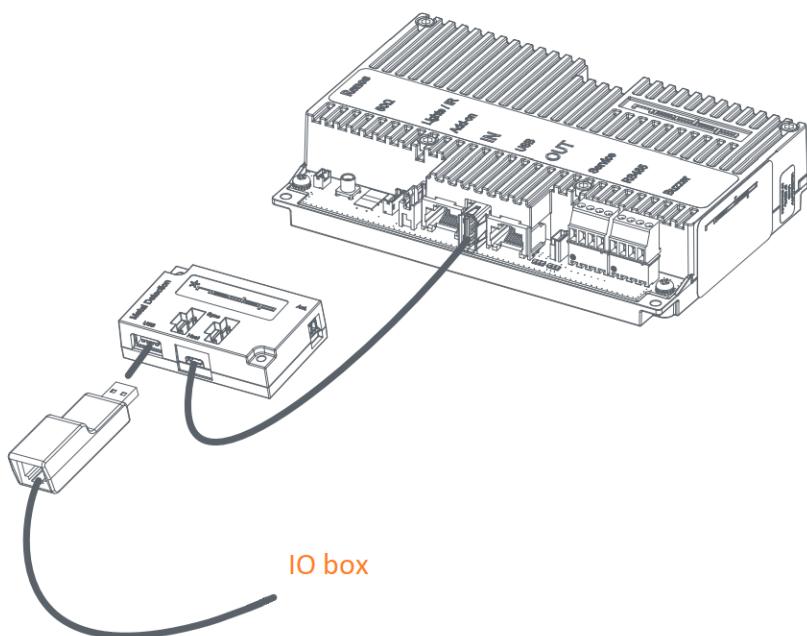
1. Power
 - a. Connect Power to the IO box power Connector using the correct polarity.
2. From external hardware to the IO box
 - a. Connect the external input(s) (e.g. roller shutter switch) to Input 0-5 according to DI Dry contact connection in the schematic diagram.
 - b. Connect the external devices to output 0-5. The outputs are "Normally Open/NO" relay contacts.
3. IO box to iSense.
 - a. Create a network cable for connecting the network adapter from the iSense unit to the IO box using two filters.
 - b. Connect the UTP cable to Port 1 of the IO box and place one filter as close as possible to the IO box.
 - c. Connect the other end of the UTP cable to the USB network-adapter, place the second filter as close as possible to it and connect it to the iSense USB Host port if available. In case you have a system with RFID, a powered USB hub is needed. Find the different setups below.

USB options

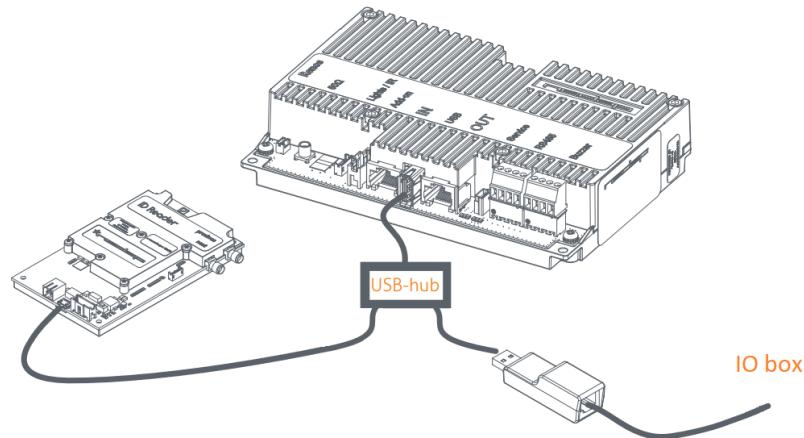
If there is no RFID reader and no Metal Detection unit installed, use the USB Host port on the iSense unit to connect the USB network-adapter:



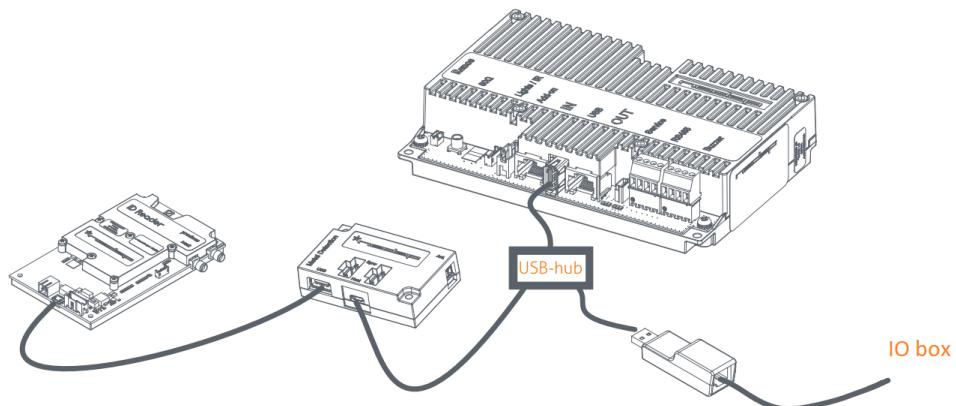
In combination with a Metal Detection unit, use the USB Host port on the Metal Detection unit to connect the USB network-adapter:



In combination with an RFID reader, add a powered USB hub to connect the RFID reader and the USB network-adapter:



And finally, in combination with an RFID reader and a Metal Detection unit, add a powered USB hub to connect the Metal Detection unit with the RFID reader and the USB network-adapter:



- (i)** The powered USB hub does not need to be powered.
Not every USB Hub will work, test before using!

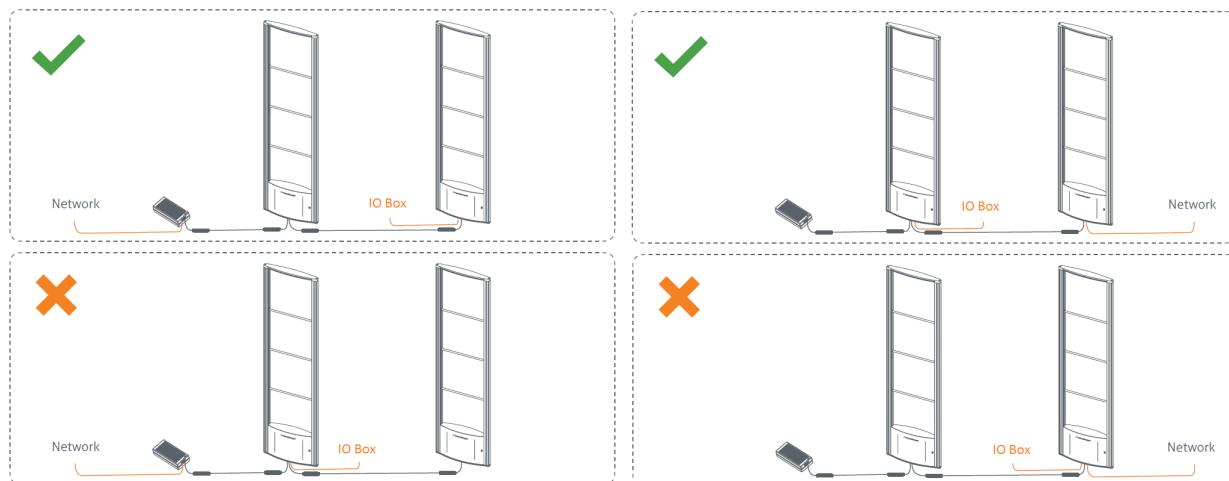
Network options



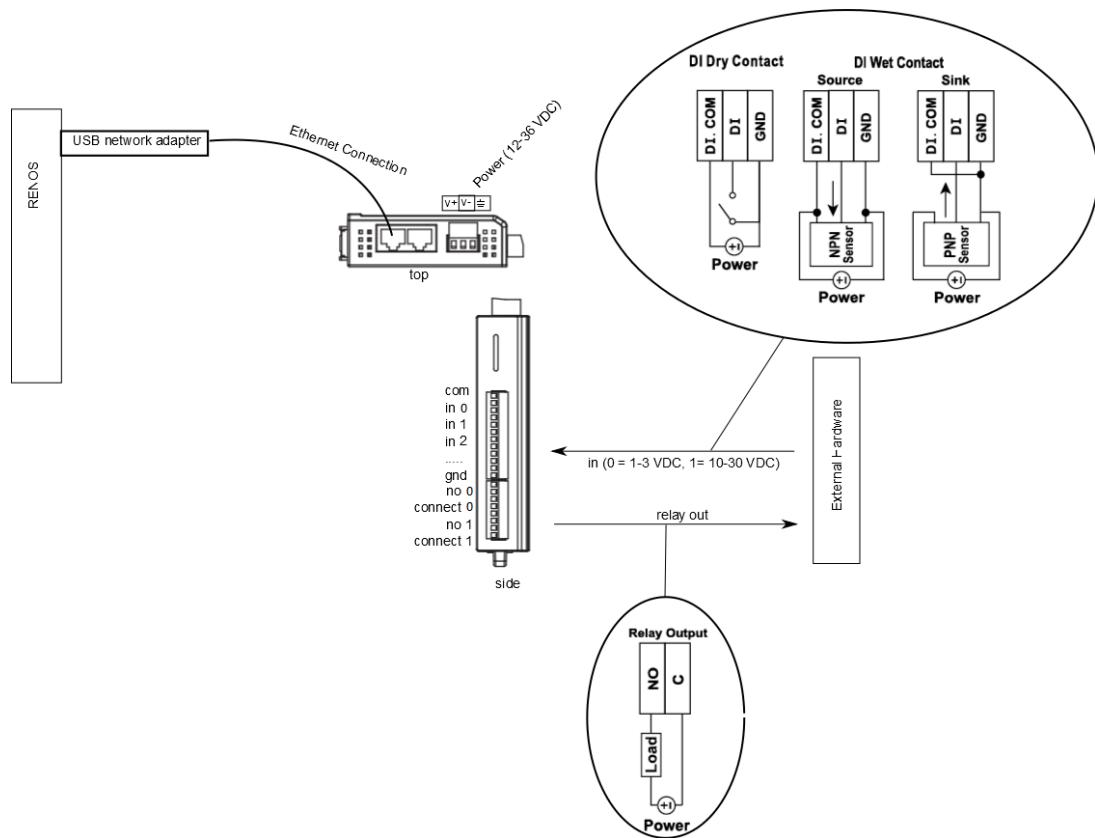
You can **not** connect the IO box to a gate if:

- The internet connection or Pager is already connected with a USB network adapter to that gate
- There is an internet connection to the output of the Renos in that gate.
- The gate is directly connected to the power inserter which is connected to the internet.
- There should be **NO** unused USB network adapters in the system.

See also installation examples below for when the system is also connected to a network.



Connecting the IO box



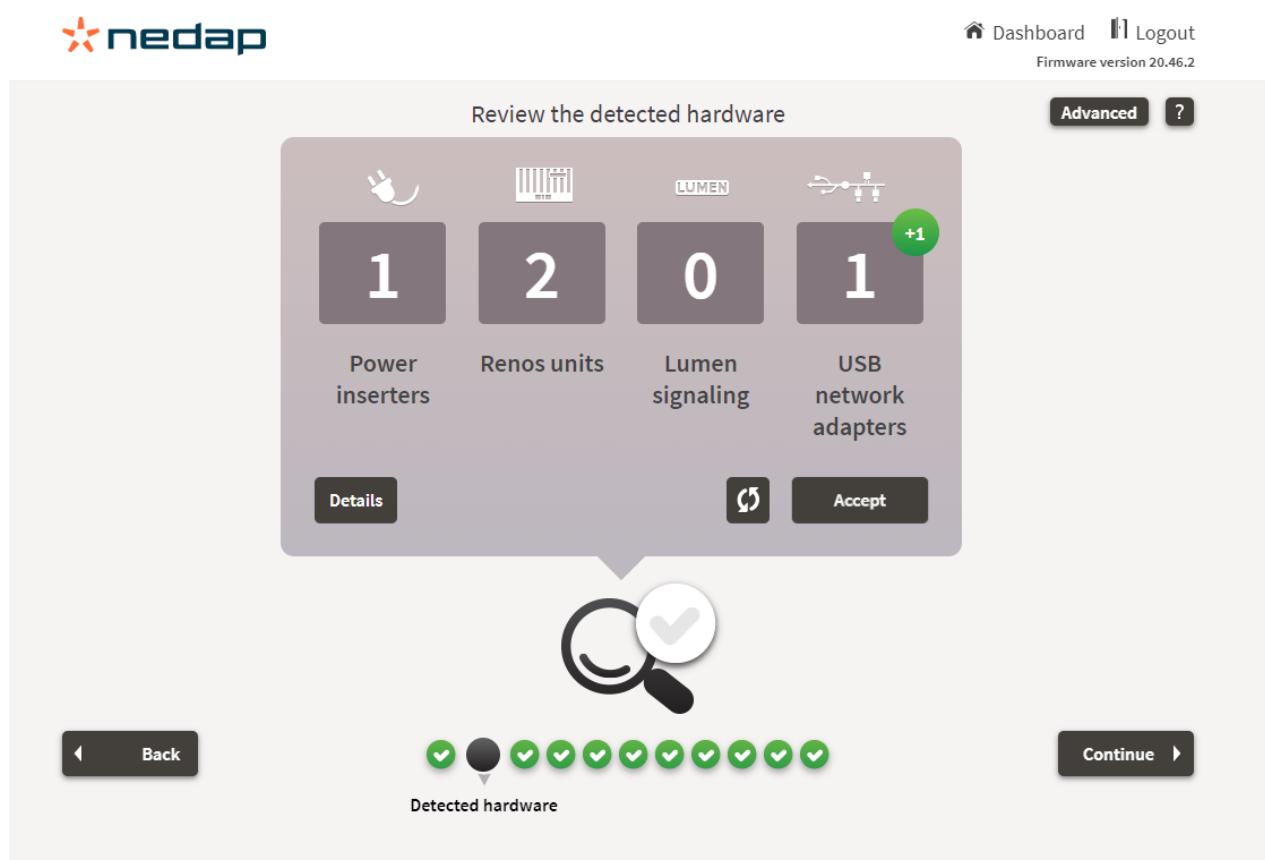
Configuration

The example configuration we are going to create, will demonstrate an input and an output.

- Input 0 - Connected to the "roller-shutter down switch".
- Output 0 - Connected to an external buzzer.

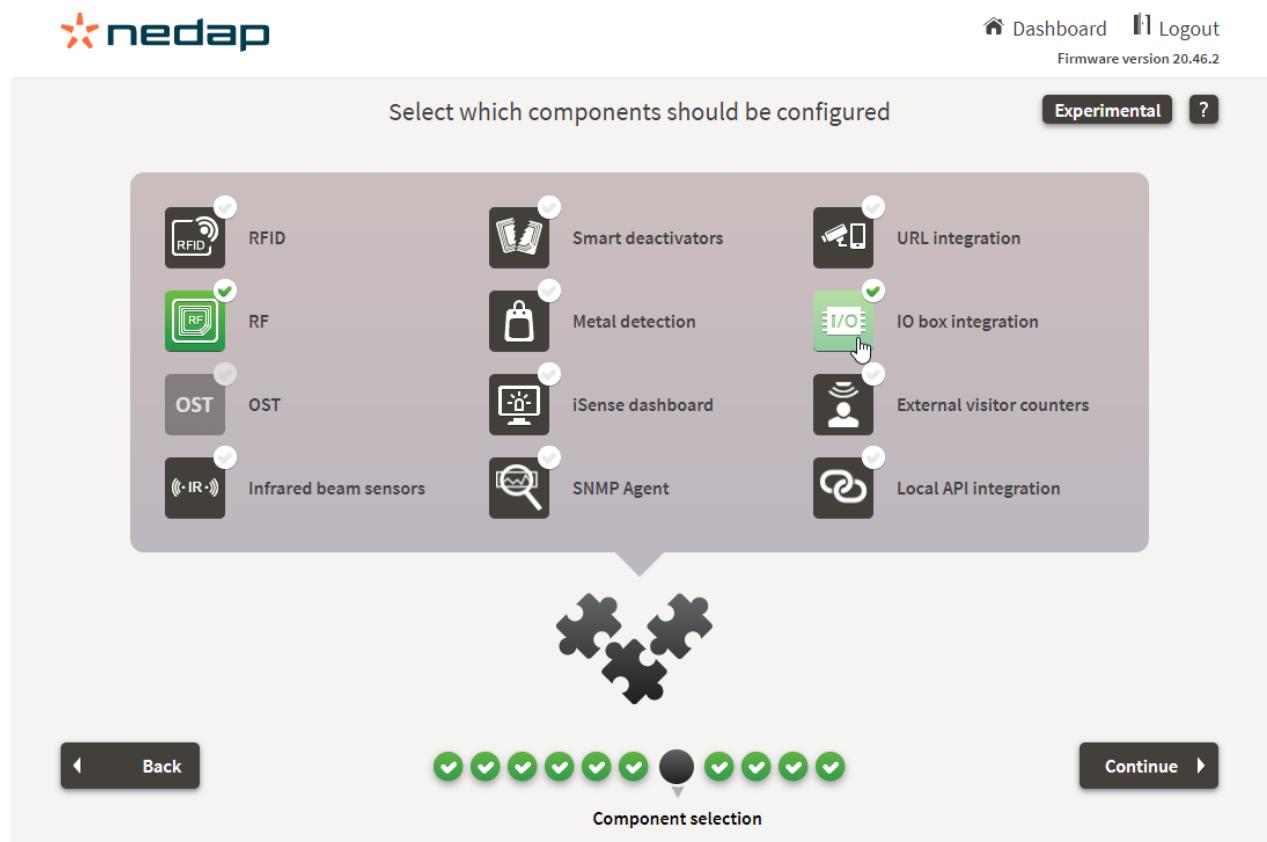
After installing the hardware, enter the Installation Wizard by connecting your computer to the iSense USB device port. In the browser's address-bar type **http://192.168.133.1** to access the installation Wizard.

The first step is to accept the changed hardware as you have added a new USB network adapter.



The screenshot shows the 'Review the detected hardware' step of the Nedap Installation Wizard. At the top right are links for 'Dashboard', 'Logout', and 'Firmware version 20.46.2'. Below that is a summary card with icons and counts: 1 Power inserter, 2 Reno units, 0 Lumen signaling, and 1 USB network adapter (+1). Buttons for 'Details' and 'Accept' are at the bottom of the card. A magnifying glass icon with a checkmark is centered below the card. At the bottom, a 'Back' button with a left arrow, a 'Continue' button with a right arrow, and a 'Detected hardware' status bar with a black dot indicating the current step.

Arrived on the "Components selection" page choose for RF and/or RFID - and the "IO box integration". Click the Continue button.

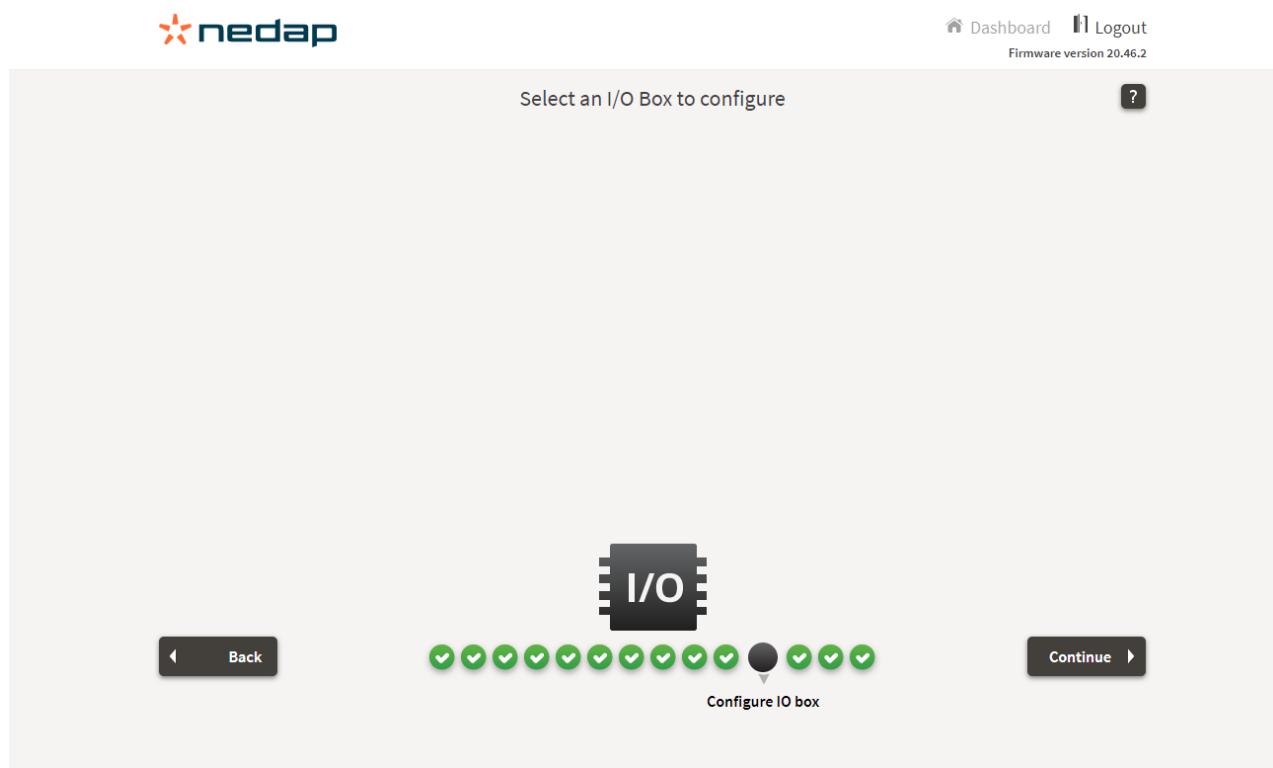


The screenshot shows the 'Select which components should be configured' page. At the top right are links for 'Dashboard', 'Logout', and 'Firmware version 20.46.2'. Below that is a 'Experimental' button and a help icon. The main area displays ten component options in a grid:

Icon	Component Name
RFID icon	RFID
RF icon with a green checkmark	RF
OST icon	OST
Infrared beam sensors icon	Infrared beam sensors
Smart deactivators icon	Smart deactivators
Metal detection icon	Metal detection
iSense dashboard icon	iSense dashboard
SNMP Agent icon	SNMP Agent
URL integration icon	URL integration
IO box integration icon with a cursor over it	IO box integration
External visitor counters icon	External visitor counters
Local API integration icon	Local API integration

Below the grid is a graphic of four interlocking puzzle pieces. At the bottom are navigation buttons: 'Back' with a left arrow, a series of green circular progress indicators, and 'Continue' with a right arrow. A central arrow points downwards from the progress indicators towards the text 'Component selection'.

Continue to the "Configure IO box" page. If the IO box (or IO boxes) is powered and connected properly to the iSense unit, it will be detected and shown on this page. Select the correct IO box to configure by clicking it, after that the inputs and output configuration will be shown.

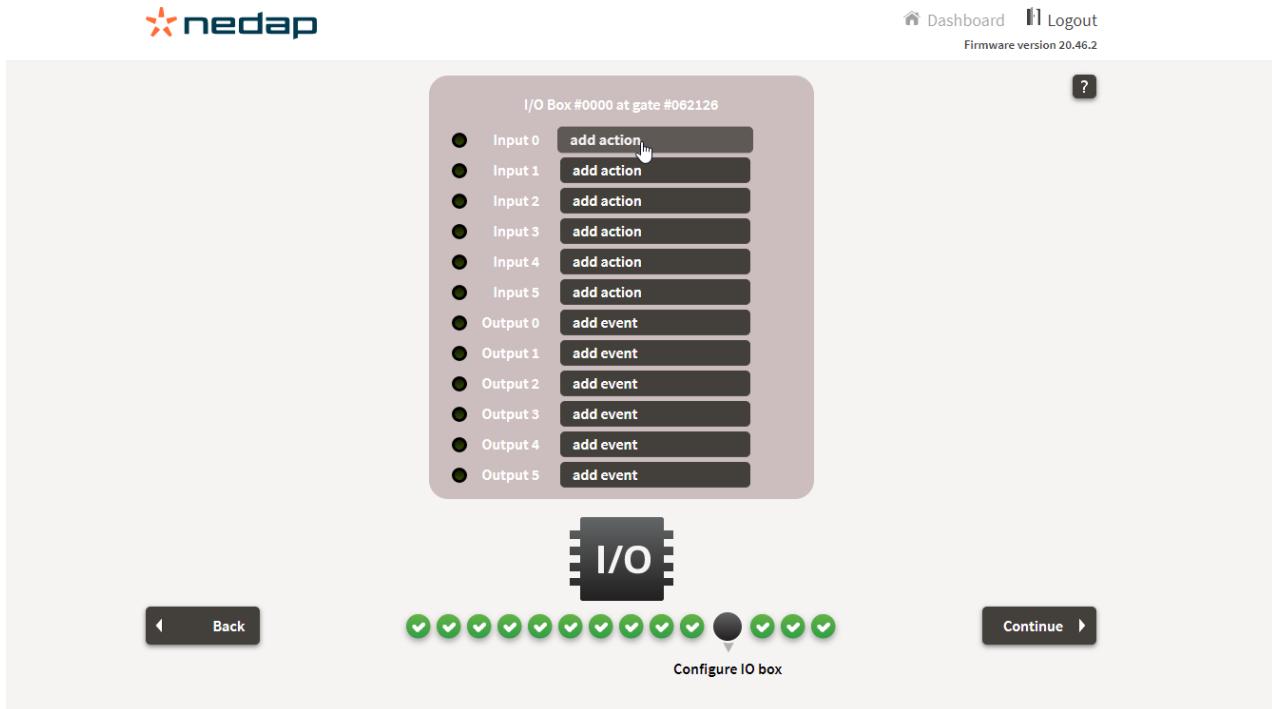


In case no IO box is shown, please check cables and power. Check if the USB network-adapter is added to the hardware layout. Maybe the IO box was configured differently from what iSense expects, if you suspect this, please factory reset the IO box.

Factory Reset IO box

The RESET button (find it on one of the sides of the IO box) restarts the server and resets all settings to factory defaults. Use a pointed object such as a straightened paper clip to hold down the RESET button for 5 seconds. The factory defaults will be loaded once the READY LED turns green again. You may then release the RESET button.

Input Event



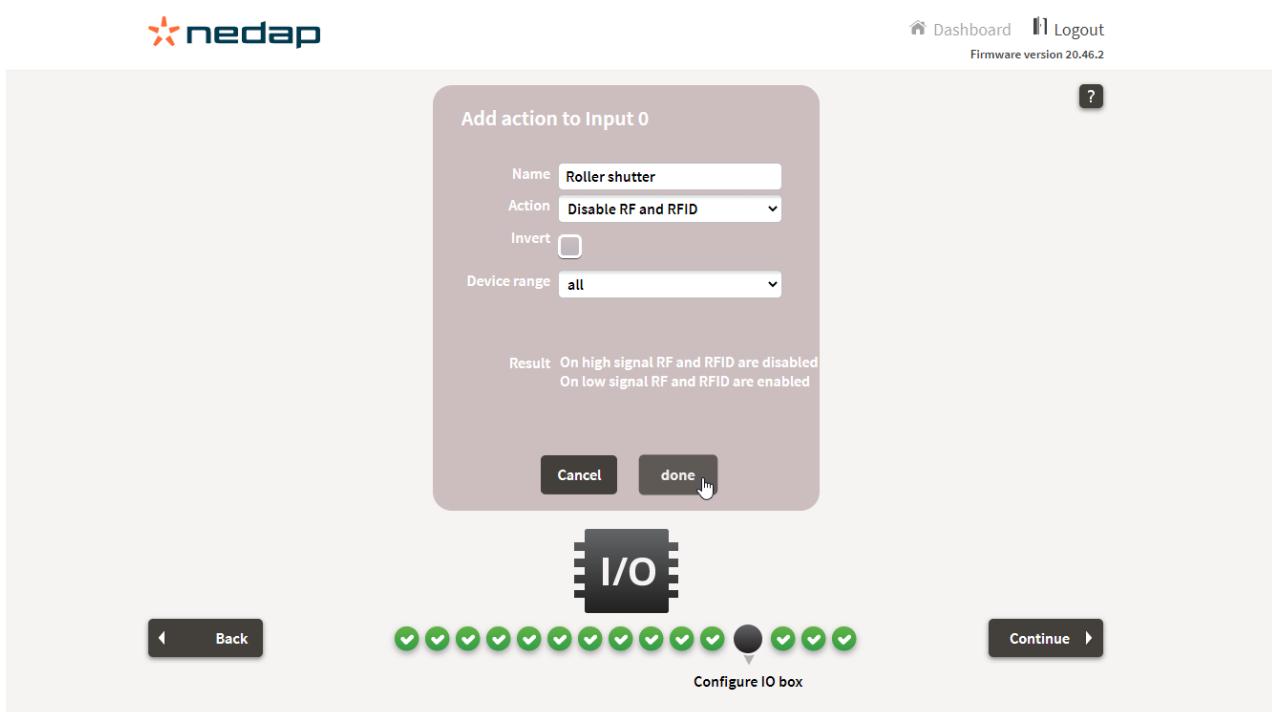
I/O Box #0000 at gate #062126

- Input 0 [add action](#)
- Input 1 [add action](#)
- Input 2 [add action](#)
- Input 3 [add action](#)
- Input 4 [add action](#)
- Input 5 [add action](#)
- Output 0 [add event](#)
- Output 1 [add event](#)
- Output 2 [add event](#)
- Output 3 [add event](#)
- Output 4 [add event](#)
- Output 5 [add event](#)

I/O

Configure IO box

Now we will create an action for the Roller-Shutter. Click on the Add Action button for Input 0.



Add action to Input 0

Name	<input type="text" value="Rollershutter"/>
Action	<input type="button" value="Disable RF and RFID"/>
Invert	<input type="checkbox"/>
Device range	<input type="button" value="all"/>

Result On high signal RF and RFID are disabled
On low signal RF and RFID are enabled

[Cancel](#) [done](#)

I/O

Configure IO box

Fill in the fields according to the image above and click the Done button.

Name

A logical name for the action. In this case "Roller Shutter".

Action

What action should be taken when the input is active? Six Options:

Disable RF	No RF events anymore and no alarms
Disable RFID	No RFID events anymore and no alarms
Disable RF and RFID	No RF and RFID events anymore and no alarms
Mute RF	Mute RF Alarms, evens are still generated
Mute RFID	Mute RFID Alarms, evens are still generated
Mute RF and RFID	Mute RF and RFID Alarms, evens are still generated

Invert

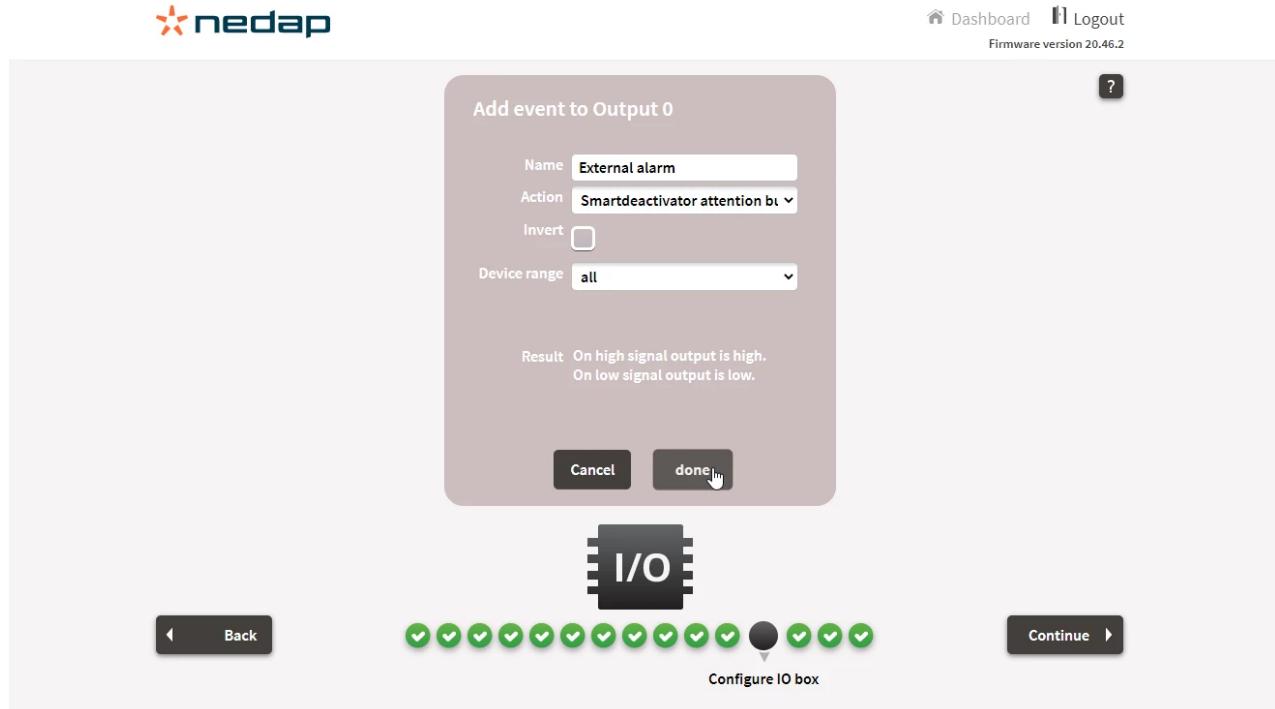
If not checked the action is triggered on an open switch (Active High), if checked the action is triggered on a closed switch (Active Low).

Gate Range

Select which gates should be monitored for this action. There are three options:

All	All gates in the system
Group	A predefined group, defined in the wizard in an earlier stage. An extra combo-box for selecting these groups becomes available
Specified Range	With this you will be able to select a specific range of gates that was not earlier specified as a group

Output Event



Add event to Output 0

Name: External alarm

Action: Smartdeactivator attention button

Invert:

Device range: all

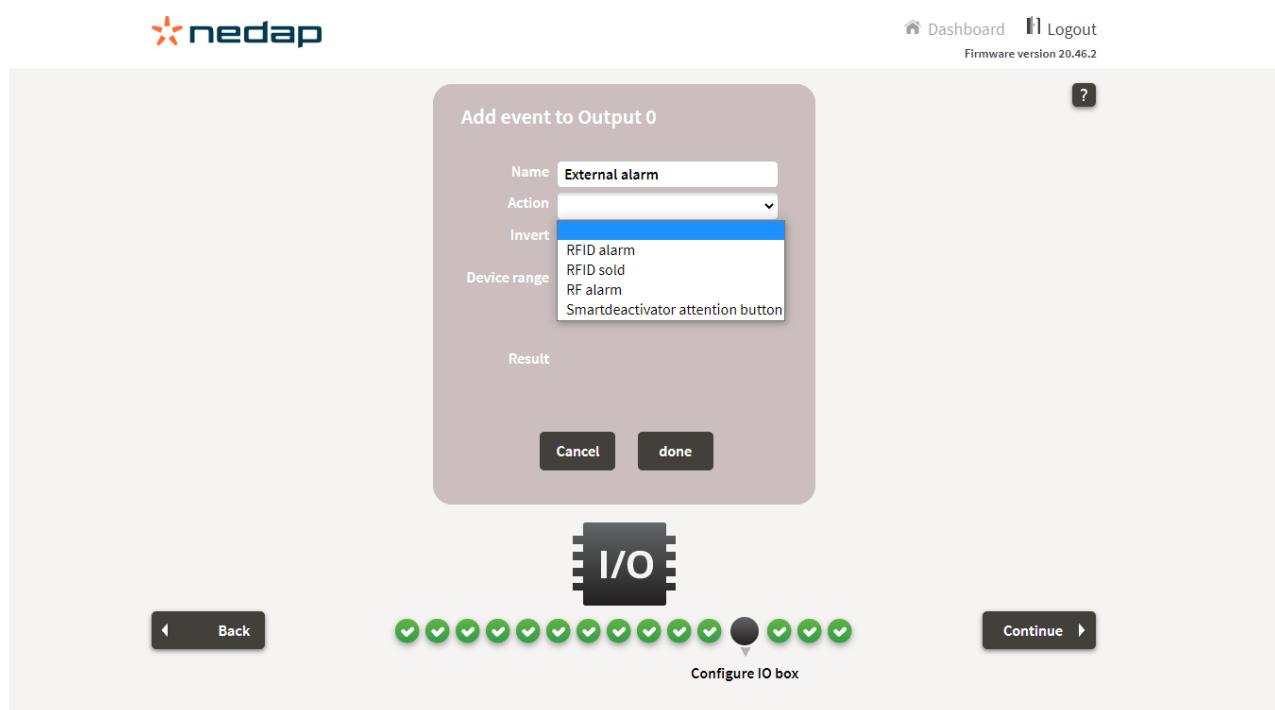
Result: On high signal output is high.
On low signal output is low.

Cancel done

I/O

Configure IO box

For adding an action to trigger and the output click the "Action" button:



Add event to Output 0

Name: External alarm

Action: **Smartdeactivator attention button**

Invert:

Device range: all

Result

Cancel done

I/O

Configure IO box

Fill in the fields according to the image above and click the Done button.

Name

A logical name for the output action. In this case "External Alarm".

Event

On what event should the output be activated?

Seven Options:

RFID Alarm
RFID Sold
RF Alarm
Customer IN
Customer OUT
Smart Deactivator attention button
Metal detection alarm

Invert

If not checked the output is triggered when the selected action is true. In case of an "RF Alarm" the output is triggered, if checked the output is triggered when the selected action is false. So when no "RF Alarm" available.

Gate Range

Select which gates should be monitored for this action.

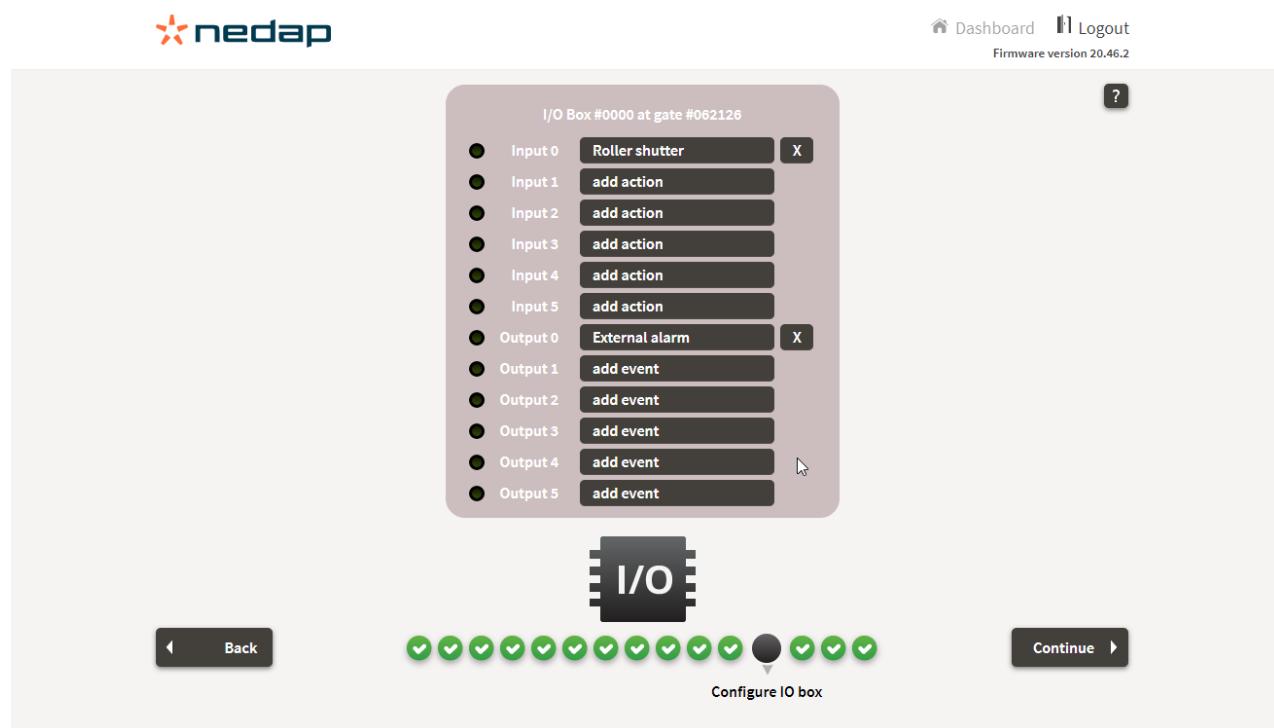
There are three options:

All	All gates in the system
Group	A predefined group, defined in the wizard in an earlier stage. An extra combo-box for selecting these groups becomes available
Specified range	With this you will be able to select a specific range of gates that was not earlier specified as a group

Delivery test

Now you have configured an input action and an output event. On the overview screen of the IO box you can also test/verify the current status for each input/output.

Test your integration and check if it works as expected.



The screenshot shows a configuration interface for an IO Box. At the top, there's a navigation bar with the nedap logo, a Dashboard link, a Logout link, and a Firmware version 20.46.2 notice. Below the navigation is a large central panel titled "I/O Box #0000 at gate #062126". This panel contains a list of 12 items, each consisting of a circular icon and a text label: Input 0 (Roller shutter), Input 1 (add action), Input 2 (add action), Input 3 (add action), Input 4 (add action), Input 5 (add action), Output 0 (External alarm), Output 1 (add event), Output 2 (add event), Output 3 (add event), Output 4 (add event), and Output 5 (add event). To the right of the "External alarm" entry is a small "X" button. Below this list is a large "I/O" icon. At the bottom of the page are navigation buttons for "Back" and "Continue", and a "Configure IO box" button.

Appendix Moxa ioLogik E1214

Specifications

Input/Output Interface	
Digital Input Channels	6
Relay Channels	6
Isolation	3k VDC or 2k Vrms
Buttons	Reset button
Digital Inputs	
Connector	Screw-fastened Euroblock terminal
Sensor Type	Dry contact Wet contact (NPN or PNP)
I/O Mode	DI or event counter
Dry Contact	On: short to GND Off: open
Wet Contact (DI to COM)	On: 10 to 30 VDC Off: 0 to 3 VDC
Counter Frequency	250 Hz
Digital Filtering Time Interval	Software configurable
Points per COM	6 channels
Relays	
Connector	Screw-fastened Euroblock terminal
Type	Form A (N.O.) power relay
I/O Mode	Relay or pulse output

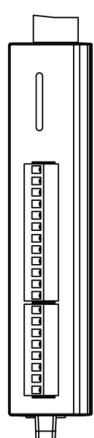
Relays	
Pulse Output Frequency	0.3 Hz at rated load (max.)
Contact Current Rating	Resistive load: 5 A @ 30 VDC, 250 VAC, 110 VAC
Contact Resistance	100 milli-ohms (max.)
Mechanical Endurance	5,000,000 operations
Electrical Endurance	100,000 operations @ 5 A resistive load
Breakdown Voltage	500 VAC
Initial Insulation Resistance	1,000 mega-ohms (min.) @ 500 VDC
Note	Ambient humidity must be non-condensing and remain between 5 and 95%. The relays may malfunction when operating in high condensation environments below 0°C.
LED Interface	
LED Indicators	Power, Ready, Port 1, Port 2
Power Parameters	
Power Connector	Screw-fastened Euroblock terminal
No. of Power Inputs	1
Input Voltage	12 to 36 VDC
Power Consumption	188 mA @ 24 VDC
Physical Characteristics	
Housing	Plastic
Dimensions	27.8 x 124 x 84 mm (1.09 x 4.88 x 3.31 in)
Weight	200 g (0.44 lb)
Installation	DIN-rail mounting, Wall mounting

Physical Characteristics	
Wiring	I/O cable, 16 to 26 AWG Power cable, 12 to 24 AWG
Environmental Limits	
Operating Temperature	-10 to 60°C (14 to 140°F)
Storage Temperature (package included)	-40 to 85°C (-40 to 185°F)
Ambient Relative Humidity	5 to 95% (non-condensing)
Altitude	4000 m
Standards And Certifications	
EMC	EN 55032/24, EN 61000-6-2/-6-4
EMI	CISPR 32, FCC Part 15B Class A
EMS	IEC 61000-4-2 ESD: Contact: 4 kV; Air: 8 kV IEC 61000-4-3 RS: 80 MHz to 1 GHz: 10 V/m IEC 61000-4-4 EFT: Power: 2 kV; Signal: 1 kV IEC 61000-4-5 Surge: Power: 2 kV; Signal: 1 kV IEC 61000-4-6 CS: 10 V IEC 61000-4-8 PFMF
Hazardous Locations	ATEX, Class I Division 2
Safety	UL 508
Shock	IEC 60068-2-27
Freefall	IEC 60068-2-32
Vibration	IEC 60068-2-6
Declaration	
Green Product	RoHS, CRoHS, WEEE
MTBF	
Time	808,744 hrs

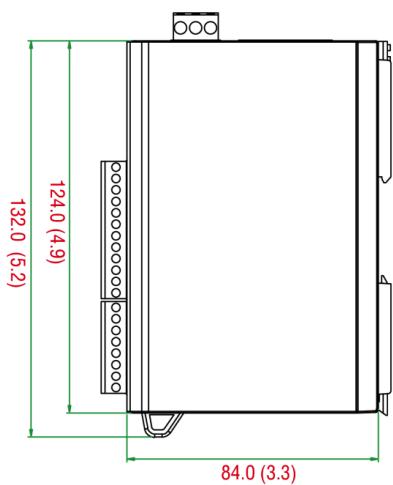
MTBF	
Standards	Telcordia SR332
Warranty	
Warranty Period	2 years
Details	See www.moxa.com/warranty

Dimensions

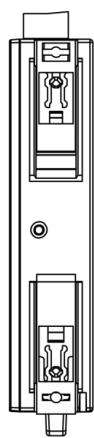
Unit: mm (inch)



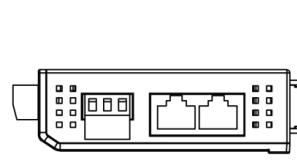
Front View



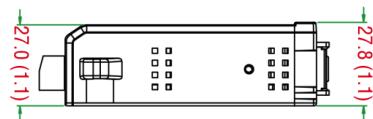
Side View



Rear View



Top View



Bottom View

Used abbreviations

Standard terms may be abbreviated in this document. The following table shows the descriptions of the abbreviations used. RFID-specific abbreviations are highlighted.

Abbreviation	Description
API	Application Programming Interface - is a way for two or more apps to communicate with each other.
CC	Customer Counting
DM	Device Management
EAS	Electronic Article Surveillance
EPC (RFID)	The Electronic Product Code is one of the available formats for encoding identifiers on RFID tags. The EPC is a globally unique number that identifies a specific item in the supply chain.
External CC	External Customer Counting (e.g., Brickstream)
FRS	Fast Remote Service
GS1 (RFID)	(Global Standards 1) An international standards organization with member bodies in more than 100 countries worldwide. Nedap Retail follows the GS1 and RainRFID standards.
GTIN (RFID)	A Global Trade Item Number (GTIN) is a number that uniquely identifies a product. It can be found beneath the barcode of a product.
IO Box	Input/Output Electronics device
IR	Infra Red
MD	Metal Detection
RF	Radio Frequency
RFID	Radio Frequency Identification

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 135

Document Last modification date 16 February 2024

Document PDF Exported 16 February 2024 by Nedap Retail | Operations



support-retail@nedap.com



Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com

Connected Devices Guideline

iSense Metal Detection Pager

version 86, February 2024



Introduction	3
Preparation	4
Required products	5
Installation.....	6
USB options	7
Network options	9
Configuration.....	10
Name	11
Event	11
Gate Range	11
URL	12
Customize Pager messages manually	13
Pager.....	14
Delivery test	14
Trouble shooting.....	16
Used abbreviations	17



Introduction

This document describes how to integrate the Nedap Pager with iSense. The pager can be used as an extension to the iSense basic system. This is especially useful with the Metal Detection upgrade where the pager can provide a message to indicate that metal has been detected.

Preparation

Determine (from the store map) where the transmitter module should be installed, make sure that there is a power socket available to power the transmitter. Choose a place so that the transmitter is able to connect to the pager(s).

Required products

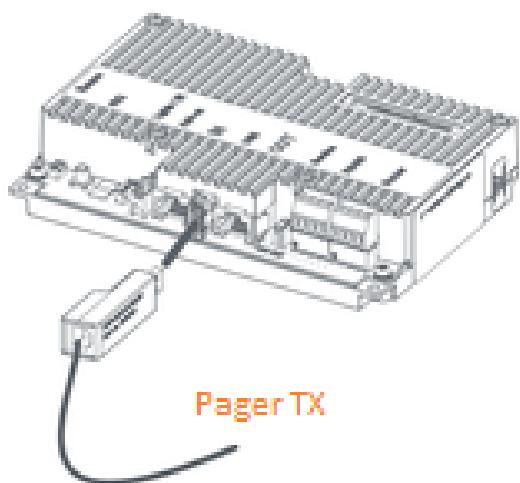
- iSense system
- A map with instructions of the installation layout.
- Transmitter + Power supply
- Pager + Belt clip + 1x AAA battery
- USB network-adapter
- Standard Installation tools and materials to create a network cable (Network cable Cat 5E or better, Filters, UTP connectors, Crimp tool, Cable tester)
- Powered USB hub (in case of an RFID Hybrid system).

Installation

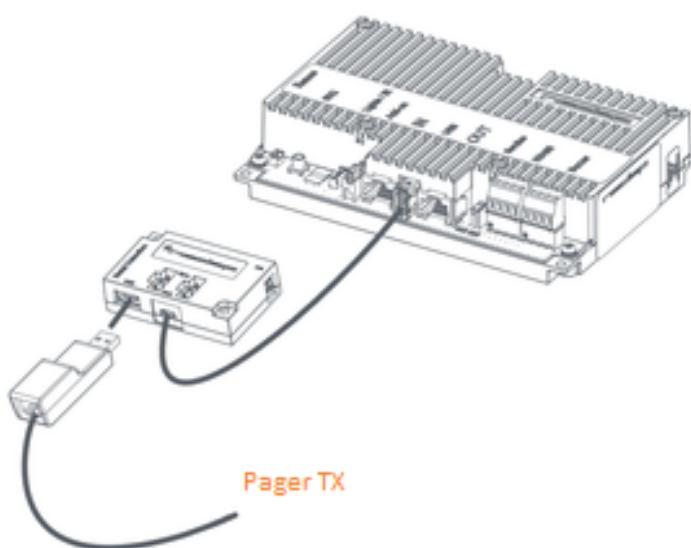
1. Install the transmitter at a convenient location (e.g. on a wall). Make sure that there is a socket available to power the transmitter
2. Create a UTP cable with the correct length based on the position of the transmitter and the position of the nearest available gate (see remark below).
3. Connect the UTP cable to the transmitter
4. Connect the other end of the UTP cable to the USB network-adapter
5. Connect the USB network-adapter to the Renos unit
6. Power the transmitter
7. Add the battery to the pager

USB options

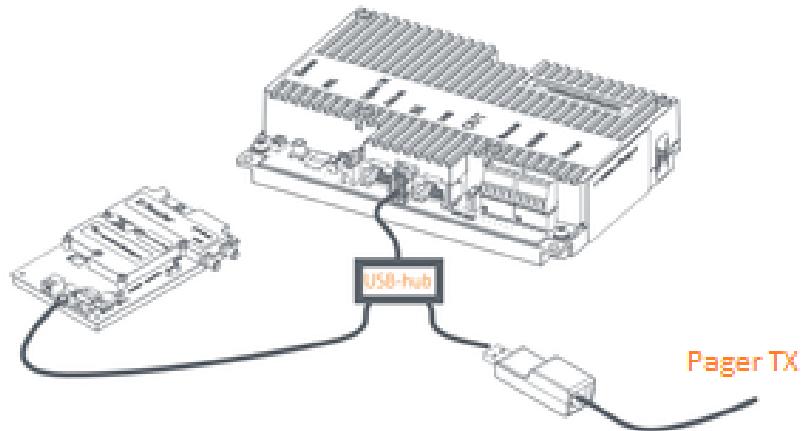
If there is no RFID reader and no Metal Detection unit installed, use the USB Host port on the iSense unit to connect the USB network-adapter:



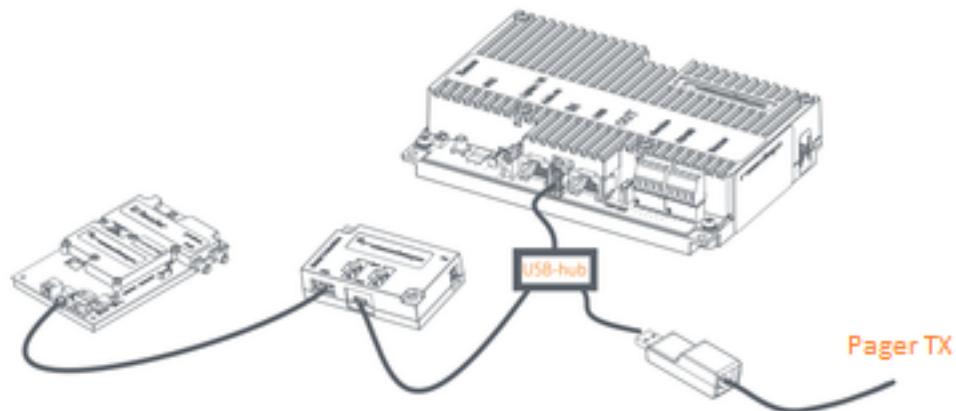
In combination with a Metal Detection unit, use the USB Host port on the Metal Detection unit to connect the USB network-adapter:



In combination with an RFID reader, add a powered USB hub to connect the RFID reader and the USB network-adapter:



And finally, in combination with an RFID reader and a Metal Detection unit, add a powered USB hub to connect the Metal Detection unit with the RFID reader and the USB network-adapter:



- (i)** The powered USB hub does not need to be powered.
Not every USB Hub will work, test before using!

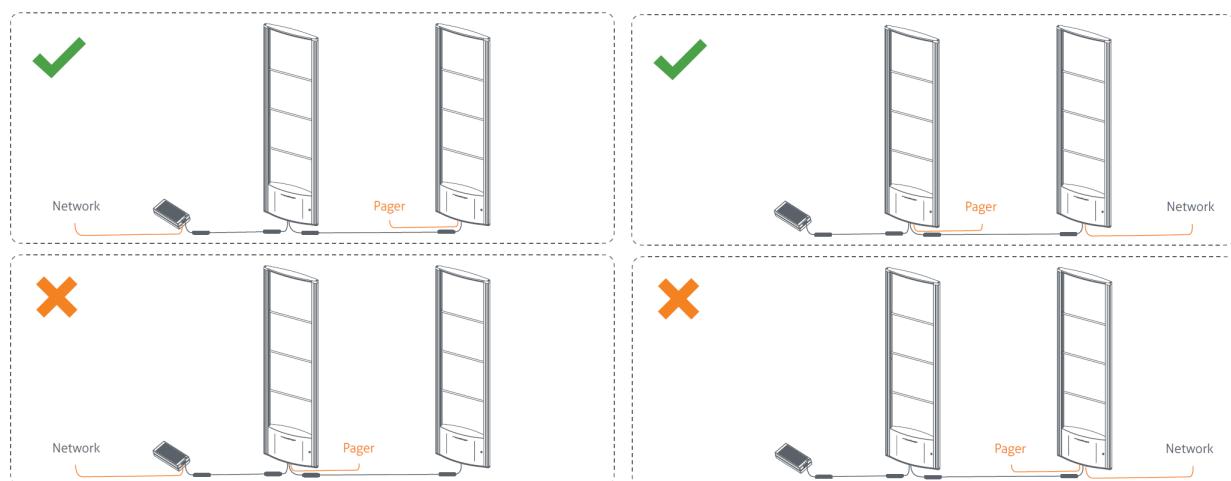
Network options



You can **not** connect the pager to a gate if:

- The internet connection or IO box is already connected with a USB network adapter to that gate
- There is an internet connection to the output of the Renos in that gate.
- The gate is directly connected to the power inserter which is connected to the internet.
- There is already another pager installed in the system.
- There should be **NO** unused USB network adapters in the system.

See also installation examples below for when the system is also connected to a network.



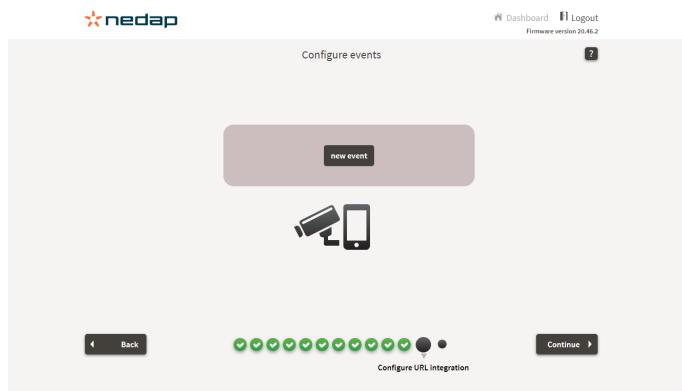
Configuration

After installing the hardware enter the Installation Wizard by connecting your computer to the Renos service-port. In the browser's address-bar type <http://192.168.133.1> to access the installation Wizard.

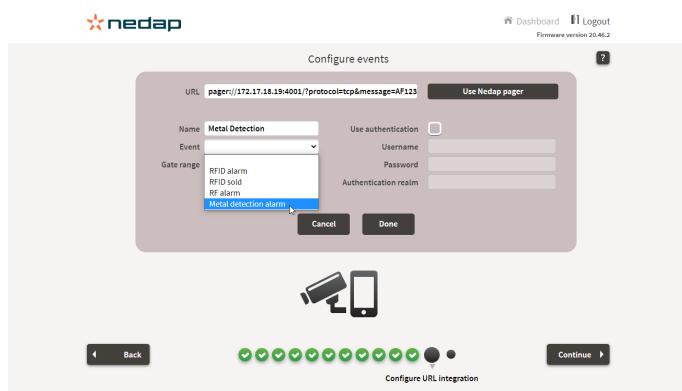
Select the "URL integration" component, in the Component selection step of the wizard.



To activate the pager you will need to use the Configure URL integration page and create a "new event"



The pager system can respond to a Metal Detection alarm, but can also be used to notify on other events (e.g. RF, RFID alarm).



Name

A logical name for the action. In this case "Metal Detection"

Event

On what event should the output be activated?

Seven Options:

RFID Alarm
RFID Sold
RF Alarm
Customer IN
Customer OUT
Smart Deactivator attention button
Metal detection alarm

Gate Range

Select which gates should be monitored for this action.

There are three options:

All	All gates in the system
Group	A predefined group, defined in the wizard in an earlier stage. An extra combo-box for selecting these groups becomes available
Specified range	With this you will be able to select a specific range of gates that was not earlier specified as a group

URL

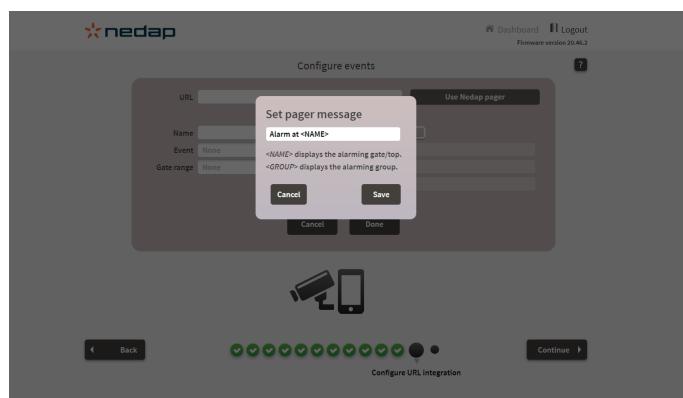
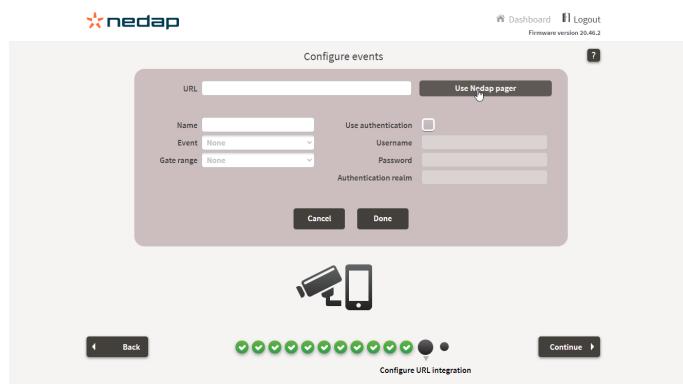
Specific URL that will be triggered based on the settings.

For the pager use the following URL:

```
pager://172.17.18.19:4001/?protocol=tcp&message=AF1234567DAlarm%20at%20<NAME>%0D
```

This URL will automatically generate the correct gate name on the pager.

You can easily select "Use Nedap pager" in the wizard, this way you don't need to type the URL manually, here you also use the option to easily customize the message that will be shown on the pager.



Customize Pager messages manually

If you want to change the message on the pager in case of an event, you can change the following part of the URL manually:

pager://172.17.18.19:4001/?protocol=tcp&message=AF1234567DAlarm%20at%20<NAME>%0D

- The **orange** part of the URL is fixed and should not be changed!
- The **green** part of the URL is the receiver ID of the pager, this is standard **1234567**.
- The **blue** part of the URL can be changed to make a customized message

In the example, the gate name is used: <NAME>, if you want to show the Group name, you can change this to <GROUP> :

- <NAME> = Name of gate (as configured in the Technical Dashboard of the Wizard)
- <GROUP> = Name of the group (as configured in the Technical Dashboard of the Wizard)

The message itself can also be adjusted, %20 can be used as a space between text:

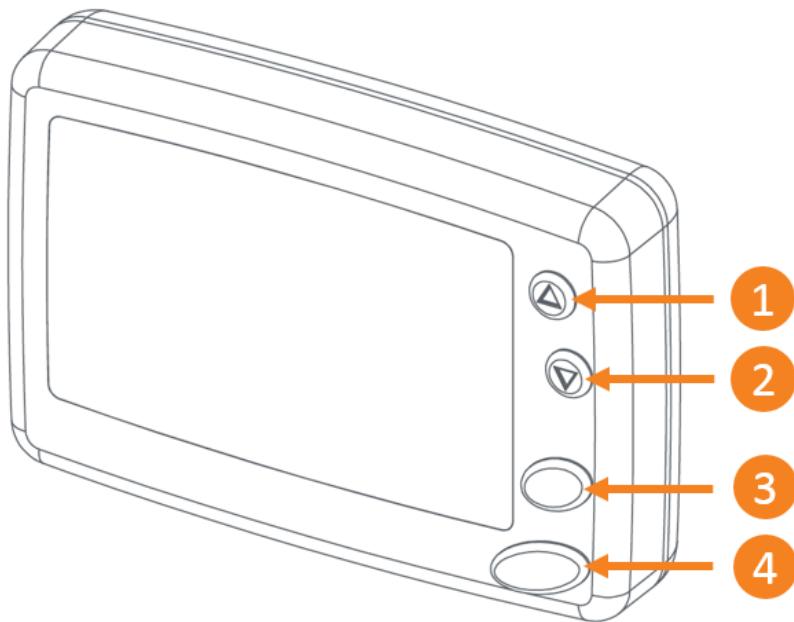
%20 = Space

In case of the example URL you will see the following message on your pager in case of an alarm at gate 1:

Alarm at Gate 1

Pager

The pager needs no configuration before use. Press button 4 for 3 seconds to start-up.



1. “Up” button
2. “Down” button
3. “Function>Select” button
4. “Read/Escape” key

To change the pager address, there is a hidden menu that can be reached by pressing button “1” and “4” simultaneously until you will see a password screen.

The password is “0000”. When you change the address in the pager, you also need to change this in the URL trigger to the same address.

Delivery test

Now you have configured an event and the pager, it is time to test it.

On the overview screen you can also test by pressing the “trigger” button.



When everything is correct the transmitter will beep and send a message to the pager.

Test pager

When you test the pager in the wizard the message on the pager will still show <NAME> or <GROUP> when used. After you deliver the system, this message will change to the correct group name or gate name in the message.

You can create many different URL triggers simultaneously. For example the following combination:

- Trigger a pager using a metal detection event on group 1
- Use another pager trigger for an RF event on group 2

Trouble shooting

Transmitter is not beeping when triggered:

- Check if the power adapter is connected and if the socket is powered
- Check UTP cable to the Renos unit
- Check if the address in the URL corresponds with the address in the pager

Transmitter is beeping but no message to the pager:

- replace battery. When the battery is very low, it is also possible that the pager will not receive a message!

Used abbreviations

Standard terms may be abbreviated in this document. The following table shows the descriptions of the abbreviations used. RFID-specific abbreviations are highlighted.

Abbreviation	Description
API	Application Programming Interface - is a way for two or more apps to communicate with each other.
CC	Customer Counting
DM	Device Management
EAS	Electronic Article Surveillance
EPC (RFID)	The Electronic Product Code is one of the available formats for encoding identifiers on RFID tags. The EPC is a globally unique number that identifies a specific item in the supply chain.
External CC	External Customer Counting (e.g., Brickstream)
FRS	Fast Remote Service
GS1 (RFID)	(Global Standards 1) An international standards organization with member bodies in more than 100 countries worldwide. Nedap Retail follows the GS1 and RainRFID standards.
GTIN (RFID)	A Global Trade Item Number (GTIN) is a number that uniquely identifies a product. It can be found beneath the barcode of a product.
IO Box	Input/Output Electronics device
IR	Infra Red
MD	Metal Detection
RF	Radio Frequency
RFID	Radio Frequency Identification

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 86

Document Last modification date 16 February 2024

Document PDF Exported 16 February 2024 by Nedap Retail | Operations



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com



Connected Devices Guideline

iSense Metal Detection Integration

version 60, February 2024

Introduction	3
Preparation	4
Required products	5
Installation.....	6
Configuration.....	7
Troubleshooting.....	10
RF signal disturbed after installing Metal Detection	10
Possible causes for Metals detection synchronization errors	10
Possible causes for Metals detection coupling errors	10
Used abbreviations	11



Introduction

This document describes how to integrate Metal Detection (MD) with iSense.

Preparation

Read the important notes below to prepare for the installation.

Power inserters

Using Metal Detection has consequences for the required number of Power Inserters (PI)! You can find the power table in the general manual

At least 2 gates

At least 2 gates in one system are required for Metal Detection to work

Metal objects

The distance between large (Metal) doors and the gates with Metal Detection must be at least 1.5 meters.

Doors swinging open to the outside, must be at a distance of at least 1 meter.

Gate distance within groups

The distance between the gates within 1 group should be the same for the system to work well

Metal Detection hardware per group

When using Metal Detection, all gates within 1 group need Metal Detection hardware.

Detection distance

The maximum distance between 2 gates is the same as specified for RF with one exception.

For a Lumen iL33 the maximum distance changes when shielding is used:

- With shielding at one side: the maximum distance between all the gates in this group becomes 1.5m (instead of 1.65m)
- If the group contains 2 gates and both are shielded, the distance becomes 1.25m

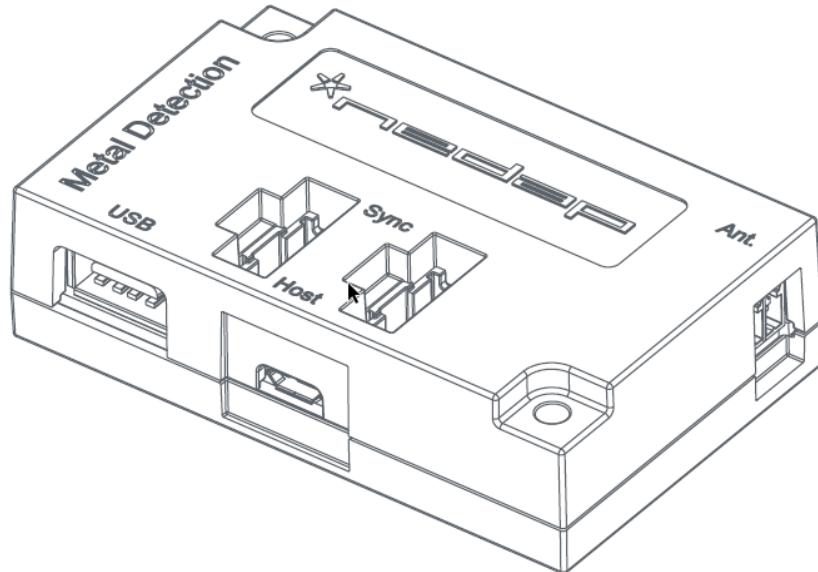
Remember that the shielding also influences the RF performance

i37

Metal detection is not possible for the i37

Required products

- iSense system
- Metal Detection upgrade kit



Installation

Install the Metal Detection units as described in the Quick Reference that is enclosed with the upgrade set.

USB connection

In case of a Hybrid system, always connect the RFID reader to the Metal Detection USB port.

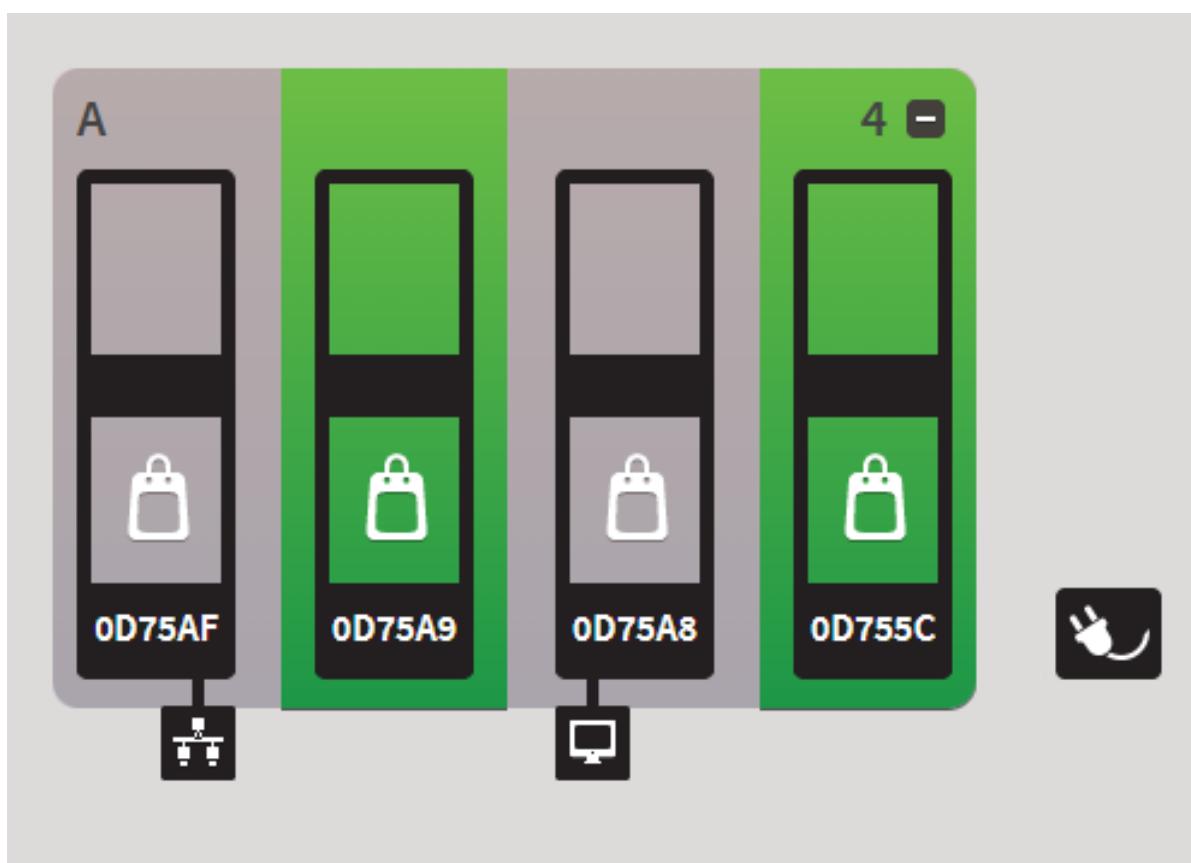
When you also need a Pager or IO box, use a USB hub between the Metal Detection and the Renos USB Host.

When there is no RFID reader present, you can also connect the Pager or IO box to the Metal Detection USB port.

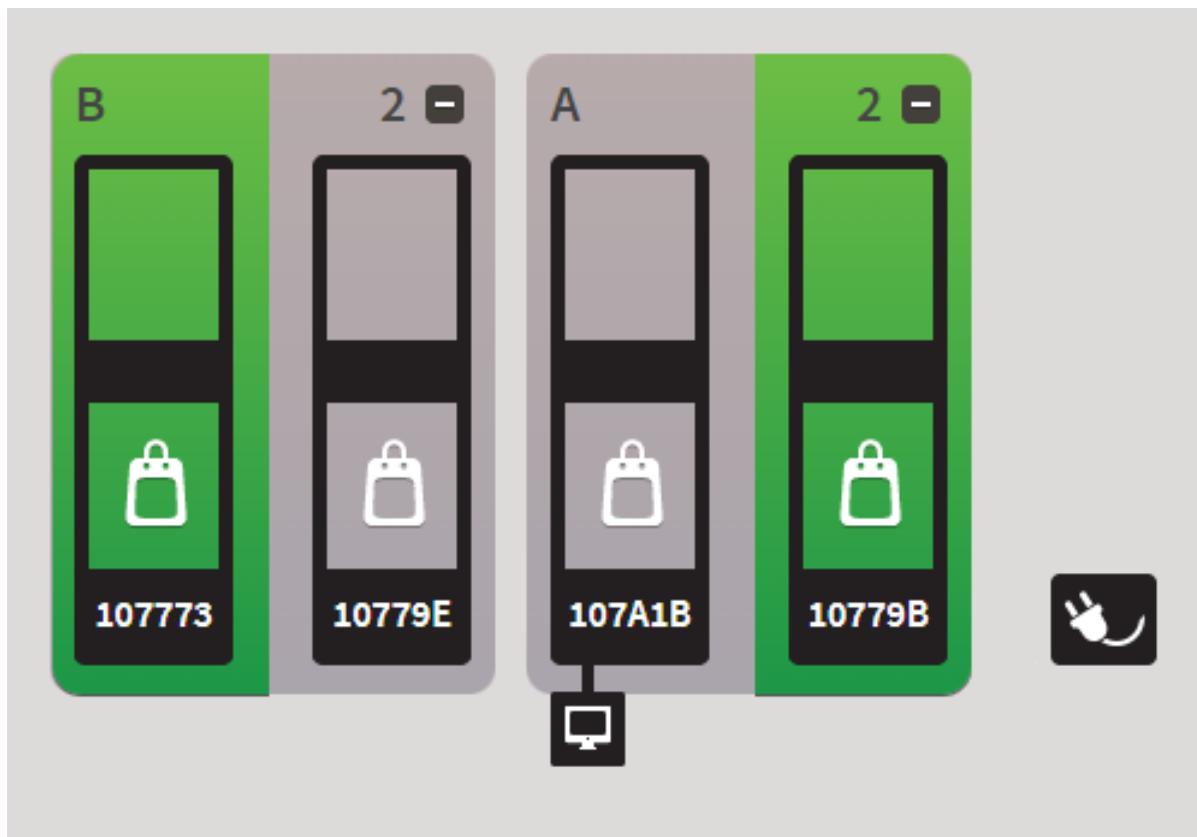
Configuration

Metal Detection (MD) is a transmission technology. During the configuration the transmitter (Tx) and receiver (Rx) of the Metal Detection will be set automatically. The first MD unit of a group will be configured as receiver. The first MD unit of the next group will have the same type (Rx/Tx) as the last MD unit of the previous group, this is to prevent interference. During the configuration you will set the sensitivity of the receiver(s).

Metal detection will be configured automatically. If four gates with Metal Detection are placed in one group, the Metal Detection configuration will look like this (green units are receivers):



If four gates with Metal Detection are configured in two groups, there is no Metal Detection in between the second and third gate. The Metal Detection configuration will look like this (green units are receivers):



After installing the hardware enter the Installation Wizard by connecting your computer to the Renos service-port. In the browser's address-bar type <http://192.168.133.1> to access the installation Wizard.

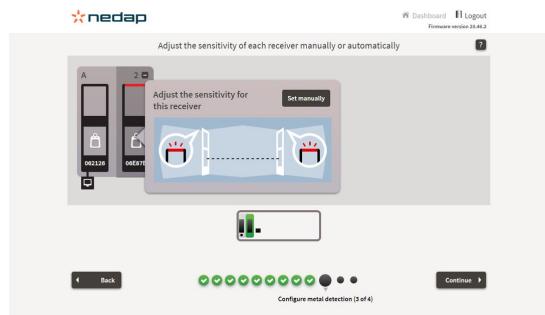
The RF and/or RFID component must be selected to be able to select "Metal Detection" component.



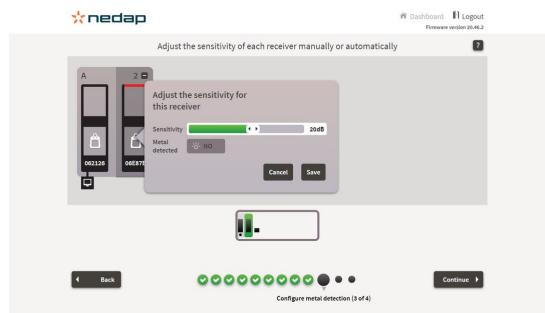
The first 2 steps will automatically detect and set the basic settings based on the environment and hardware.

The 3rd step is to set the sensitivity. There are 2 ways to set the sensitivity:

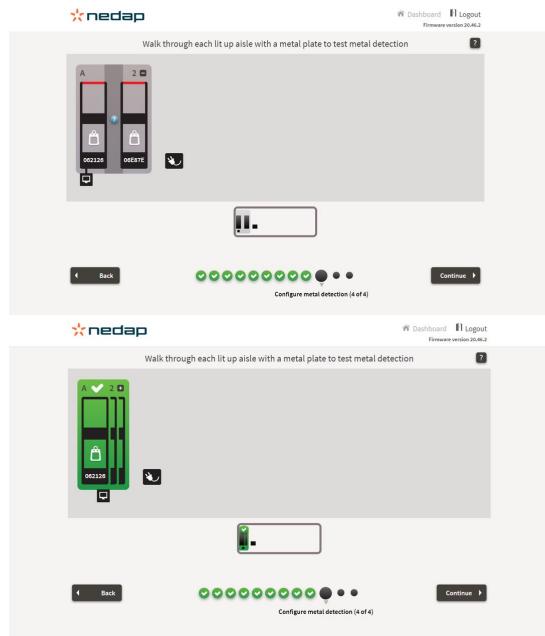
1. Automatically: With a metal plate between the gates as shown below. Turn a metal plate between the gates until the lights go off.



2. Set Manually: Use the slider to set the sensitivity



In the last page a test is required to finalize the configuration.



Troubleshooting

RF signal disturbed after installing Metal Detection

- Do not use a nonstandard antenna cable (red/black cable), always use the enclosed one.
- Make sure that the ferrite core is close to the 50 Ohm PCB

Possible causes for Metals detection synchronization errors

- Problems with the 6-core cable between the Renos unit and the Metal Detection unit
- A defect in the Renos unit and/or the Metal Detection unit (regarding the sync)
- An issue with the LAN cable between Renos units can also cause sync errors with Metal Detection. If the wizard also shows LAN errors, this could be a clue

All these possible causes may not appear until after a reboot.

Possible causes for Metals detection coupling errors

- Too great distance between the antennas
- Shielding (the effect is similar to increasing the distance)
- Issues with the antenna, antenna pcb and/or all cables that go with it

Used abbreviations

Standard terms may be abbreviated in this document. The following table shows the descriptions of the abbreviations used. RFID-specific abbreviations are highlighted.

Abbreviation	Description
API	Application Programming Interface - is a way for two or more apps to communicate with each other.
CC	Customer Counting
DM	Device Management
EAS	Electronic Article Surveillance
EPC (RFID)	The Electronic Product Code is one of the available formats for encoding identifiers on RFID tags. The EPC is a globally unique number that identifies a specific item in the supply chain.
External CC	External Customer Counting (e.g., Brickstream)
FRS	Fast Remote Service
GS1 (RFID)	(Global Standards 1) An international standards organization with member bodies in more than 100 countries worldwide. Nedap Retail follows the GS1 and RainRFID standards.
GTIN (RFID)	A Global Trade Item Number (GTIN) is a number that uniquely identifies a product. It can be found beneath the barcode of a product.
IO Box	Input/Output Electronics device
IR	Infra Red
MD	Metal Detection
RF	Radio Frequency
RFID	Radio Frequency Identification

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 60

Document Last modification date 16 February 2024

Document PDF Exported 16 February 2024 by Nedap Retail | Operations



support-retail@nedap.com



Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com

Connected Devices Guideline

Online Services – Analytics API

version 184, September 2024

Introduction	3
Requesting an access token	5
POST formats	5
Description of elements	5
Returns in the following format	5
Description of elements	6
Return codes	6
Request the organization metadata	7
Returns in the following format	7
Description of elements	7
Return codes	7
Request the stores for organization	8
Returns in the following format	8
Description of elements	8
Return codes	9
Request data for a store	10
You should POST in the following format	10
Description of elements	11
Returns in the following format (bucket is different from RAW)	14
Description of elements	15
Returns in the following format (bucket is RAW)	17
Description of elements (bucket is RAW)	18
Return codes	18
Request real-time occupancy	19
You should POST in the following format	19
Description of elements	19
Returns in the following format	19
Description of elements	19
Return codes	20
Required subscriptions	21
Data completeness	22
Rate limit.....	23

Introduction

Nedap Retail systems collect customer counter, metal detection, deactivation, RF and RFID data. This data can be retrieved through the web interface <https://analytics.nedapretail.com> or through the API at <https://api.nedapretail.com>

This document describes the API.



The Analytics API is intended as a retrieval tool, not as a synchronization tool.

The API offers multiple endpoints for different kinds of information:

Endpoint	Description
<code>https://api.nedapretail.com/analytics/v1/organization</code>	Request the organization metadata for the current <i>client id</i>
<code>https://api.nedapretail.com/analytics/v1/stores</code>	Request the stores for organization
<code>https://api.nedapretail.com/analytics/v2/data</code>	Request data for store
<code>https://api.nedapretail.com/analytics/v1/occupancy</code>	Request real-time occupancy



For all the above endpoints, data will only be returned when the *client id* has access to it and a valid subscription is available for the store

Please note that we version per endpoint, not per product and because of the fact that we are at v2 for some endpoints, does not mean other v1 endpoints are outdated. A version increase merely indicates that we've made breaking changes in the past that required us to increase the version of that single endpoint, while the rest remains unaffected.



To access the data via the API, please contact Nedap Retail support (support-retail@nedap.com):

1. After your request has been processed, you will receive an email from noreply@nedapretail.com with the subject: Nedap Retail OAuth Client Activation.
2. The email contains instructions and an activation button for the next steps. Read the instructions and act accordingly.
3. During activation, a client and secret will be shown in a pop-up only once. Make sure to copy these credentials and store these in a secure way, like a password manager.

Requesting an access token

Before the API can be used, you will need to authenticate. Authentication is done by requesting an OAuth2 token through the endpoint:

```
https://api.nedapretail.com/login/oauth/token
```

POST formats

```
{  
  "grant_type": "client_credentials",  
  "client_id": "{CLIENT_ID}",  
  "client_secret": "{SECRET}"  
}
```

Description of elements

Element	Description
grant_type	Fixed string value: "client_credentials"
client_id	The <i>client id</i> you have received through Nedap
client_secret	The <i>secret</i> you have received through Nedap

Returns in the following format

```
{  
  "access_token": "{ACCESS_TOKEN}",  
  "refresh_token": "{REFRESH_TOKEN}",  
  "expires_in": 3600,  
  "token_type": "Bearer"  
}
```

Description of elements

Element	Description
access_token	The token needed to access the data
refresh_token	Not used
expires_in	Number of seconds the <code>access_token</code> is valid
token_type	Fixed string value: <code>Bearer</code>

Return codes

HTTP Code	Description
200	OK

The call always ends with a 200 HTTP status code, any errors are displayed in a json message.

For example:

```
{  
  "realm": "Device Management",  
  "error": "invalid_client",  
  "error_description": "Supplied credentials are incorrect, or cannot find client  
with supplied client ID."  
}
```

Request the organization metadata

You can request basic information about the organization the provided access token belongs to.

Endpoint	<code>https://api.nedapretail.com/analytics/v1/organization</code>
Method	<code>GET</code>
Headers	<code>Authorization: Bearer {ACCESS_TOKEN}</code>
Parameters	none

Returns in the following format

```
{  
  "id": "{ORGANIZATION_ID}",  
  "name": "{ORGANIZATION_NAME}"  
}
```

Description of elements

Element	Description
<code>id</code>	The identifier of the organization in the Nedap Device Management system
<code>name</code>	The name of the organization as configured in the Nedap Device Management system

Return codes

HTTP Code	Description
<code>200</code>	OK
<code>403</code>	Not authorized. User is not authorized for organization
<code>429</code>	Rate limit was exceeded

Request the stores for organization

To retrieve data for stores, you will need their ID's. You can request a list of stores belonging to the organization the access token belongs to (and have a valid subscription).

Endpoint	<code>https://api.nedapretail.com/analytics/v1/stores</code>
Method	<code>GET</code>
Headers	<code>Authorization: Bearer {ACCESS_TOKEN}</code>
Parameters	none

Returns in the following format

```
{  
  "stores": [  
    {  
      "id": "{STORE_ID}",  
      "name": "{STORE_NAME}",  
      "timezone": "{TIMEZONE}",  
      "customer_organization_id": "{ORGANIZATION_ID}",  
      "branch_id": "{BRANCH_ID}"  
    },  
    {  
      ...  
    }  
  ]  
}
```

Description of elements

Element	Description
<code>id</code>	The identifier of the store in the Nedap Device Management system
<code>name</code>	The name of the store as configured in the Nedap Device Management system
<code>timezone</code>	The name of the timezone of the store as configured in the Nedap Device Management system. e.g. Europe/Amsterdam, America/Los_Angeles, Europe/Moscow

Element	Description
customer_organization_id	The identifier of the organization this store belongs to
branch_id	The configurable, alternative identifier of a store that can be used to correlate the Nedap internal identifiers to identifiers used internally by customer organizations

Return codes

HTTP Code	Description
200	OK
400	Bad request. Client supplied an invalid request and is ignored
403	Not authorized. User is not authorized for organization
429	Rate limit was exceeded
500	Internal server error. Unexpected error occurred

Request data for a store

Endpoint	<code>https://api.nedapretail.com/analytics/v2/data</code>
Method	POST
Headers	<code>Authorization: Bearer {ACCESS_TOKEN}</code>

You should POST in the following format

```
{  
  "store": "{STORE_ID}",  
  "type": "{TYPE}",  
  "from": "{TIMESTAMP}",  
  "until": "{TIMESTAMP}",  
  "bucket": "{BUCKET}"  
}
```

Description of elements

Element	Description
store	<p>Store ID the data is requested for</p> <p>(i) Requires 1 store per request, a batch option is not available.</p>
type	<p>Type of data requested</p> <ul style="list-style-type: none"> • IN : Incoming customers • OUT : Outgoing customers • IN_INTERNAL : Incoming customers for groups marked "internal". Often used near restrooms or escalators (OS/T only, not available for iSense) • OUT_INTERNAL : Outgoing customers for groups marked "internal" (OS/T only, not available for iSense) • RF_ALARM : RF alarms • RF_ALARM_IN : RF alarms with incoming movement detected • RF_ALARM_OUT : RF alarm with outgoing movement detected • RF_ALARM_NON_DIRECTIONAL : RF alarm where no direction was reliably detected • DEACTIVATION : deactivations of tags at the point-of-sale • METAL : large metal bodies detected • RFID_ALARM : RFID alarms • RFID_ALARM_IN : RFID alarms with incoming movement detected • RFID_ALARM_OUT : RFID alarms with outgoing movement detected • RFID_ALARM_NON_DIRECTIONAL : RFID alarms where no direction was reliably detected • RFID SOLD : sold items that passed the system • RFID_UNSOLD : unsold items that passed the system (likely, but not necessarily, also resulted in a RFID_ALARM) • RFID_UNKNOWN : the EAS system did either not receive an EAS response in time OR the tag did not meet GS1 EPC Tag Data Standard. In either case, the status of the tag could not be determined by the EAS system. It is normal to frequently see RFID_UNKNOWN events, because tags carried by people passing an EAS system don't necessarily contain GS1 EPC data.

Element	Description
from	<p>This timestamp defines the start of the period of interest and should reflect the local time of the store requested. Format must conform to ISO 8601 date/time format. To avoid confusion it is best to omit any timezone offsets. This timestamp is inclusive (greater than or equal to this timestamp)</p> <p>Depending on the requested <code>bucket</code>, the timestamp is rounded down to the previous <code>bucket</code> boundary.</p> <p> Data remains available for 2 years</p>
until	<p>This timestamp defines the end of the period of interest and should reflect the local time of the store requested. Format must conform to ISO 8601 date/time format. To avoid confusion it is best to omit any timezone offsets. This timestamp is exclusive (smaller than this timestamp)</p> <p>Depending on the requested <code>bucket</code>, the timestamp is rounded up to the next <code>bucket</code> boundary.</p>

Element	Description
bucket	<p>This determines the time frame the data is grouped by e.g. requesting one day worth of data with bucket <code>HOUR</code> will result in 24 data points</p> <ul style="list-style-type: none"> • <code>MONTH</code> : monthly totals • <code>WEEK</code> : weekly totals. A week starts on Monday and ends on Sunday • <code>USWEEK</code> : weekly totals for US week definition. US weeks start on Sunday and end on Saturday • <code>DAY</code> : daily total • <code>HOUR</code> : hourly total • <code>MIN_30</code> : half-hourly total • <code>MIN_5</code> : five-minute total • <code>RAW</code> : unique events with additional data where available <p>(i) Systems behind a proxy or with a firmware version less than 19.09.1 do not have the ability to provide real-time data and therefore events received using buckets <code>RAW</code> are reported per 5 minutes for such systems instead of per event</p> <p>(i)</p> <ul style="list-style-type: none"> • Buckets <code>YEAR</code> , <code>MONTH</code> , <code>WEEK</code> and <code>USWEEK</code> are limited to 366 days • Buckets <code>DAY</code> and <code>HOUR</code> are limited to 31 days • Buckets <code>MIN_30</code> , <code>MIN_5</code> and <code>RAW</code> are limited to 1 day <p>As defined in the field <code>from</code> . If you set the <code>until</code> field to a value that exceeds the limit, no additional data is returned.</p>

Returns in the following format (bucket is different from RAW)

```
{  
  "store": {STORE_ID},  
  "branch_id": {BRANCH_ID},  
  "type": "{TYPE}",  
  "bucket": "{BUCKET}",  
  "data": [  
    {  
      "system": "{SYSTEM}",  
      "group": "{GROUP}",  
      "aisle": "{AISLE}",  
      "values": {  
        "{LOCAL_TIMESTAMP)": {VALUE},  
        ...  
      }  
    },  
    {  
      ...  
    }  
  ]  
}
```

Example:

```
{  
  "store": 501859,  
  "branch_id": "123",  
  "type": "IN",  
  "bucket": "DAY",  
  "data": [  
    {  
      "system": "1e16107d-225f-49e3-b169-fdbcbdcfb85d",  
      "group": "Foodhall",  
      "aisle": "6",  
      "values": {  
        "2020-02-07T00:00:00.000": 79,  
        "2020-02-08T00:00:00.000": 135  
      }  
    }  
  ]  
}
```

Description of elements

Element	Description
store	The identifier of the store in the Nedap Device Management system
branch_id	The configurable, alternative identifier of a store that can be used to correlate the Nedap internal identifiers to identifiers used internally by customer organizations
type	Type of data that is in the response
bucket	The bucket that was requested
system	The ID of the system that reported the events. A store contains one or more systems, containing one or more groups, each containing one or more aisles
group	The ID of the group that reported the events. A store contains one or more systems, containing one or more groups, each containing one or more aisles i This field is an empty string in the following cases: <ul style="list-style-type: none">• for overhead customer counters, which aren't assigned to groups and aisles like the regular integrated pedestal customer counters• for systems that are behind a proxy• or have a firmware version below 19.09.1

Element	Description
aisle	<p>The ID of the aisle that reported the events. A store contains one or more systems, containing one or more groups, each containing one or more aisles</p> <p>i This field is an empty string in the following cases:</p> <ul style="list-style-type: none"> for overhead customer counters, which aren't assigned to groups and aisles like the regular integrated pedestal customer counters for systems that are behind a proxy or have a firmware version below 19.09.1 <p>i For iDGates, every set of 2 adjacent iDGates count as an aisle, even across groups. In the example below, aisle 3, 5 and 7 will never occur in the results, as it is a non-existing aisle.</p>  <p>i For iTops, the aisle number matches with the unit and as such, there are no invalid aisles.</p> 
values	<p>This contains a map structure with the local timestamp as its key and the value of the requested datatype for the requested bucket. Example: if you would request the HOUR bucket of datatype IN (incoming customers) and from 09:00 AM to 10:00 AM 5 customers entered the store, the first item in this collection will be 09:00 with a value of 5.</p> <p>i It only contains values for buckets that contain data.</p>

Returns in the following format (bucket is RAW)

```
{  
  "store": {STORE_ID},  
  "branch_id": {BRANCH_ID},  
  "type": "{TYPE}",  
  "bucket": "RAW",  
  "data": [  
    {  
      "system": "{SYSTEM}",  
      "group": "{GROUP}",  
      "aisle": "{AISLE}",  
      "events": {  
        "local_timestamp": "{TIMESTAMP}",  
        "value": {VALUE}  
      }  
    },  
    {  
      ...  
    }  
  ]  
}
```

Example:

```
{  
  "store": 501859,  
  "branch_id": "123",  
  "type": "RFID_ALARM",  
  "bucket": "RAW",  
  "data": [  
    {  
      "system": "1e16107d-225f-49e3-b169-fdbcbdcfb85d",  
      "group": "Foodhall",  
      "aisle": "6",  
      "events": {  
        "local_timestamp": "2020-07-03T09:01:51.932",  
        "value": 1  
      }  
    }  
  ]  
}
```

Description of elements (bucket is RAW)

Element	Description
events	Contains information of a unique event with the local timestamp and a value .

Return codes

HTTP Code	Description
200	OK
400	Bad request. Client supplied an invalid request and is ignored
403	Not authorized. User is not authorized for organization or the store does not have the correct subscription for the requested type
429	Rate limit was exceeded
500	Internal server error. Unexpected error occurred

Request real-time occupancy

Endpoint	<code>https://api.nedapretail.com/analytics/v1/occupancy</code>
Method	POST
Headers	<code>Authorization: Bearer {ACCESS_TOKEN}</code>

You should POST in the following format

```
{  
  "store": {STORE_ID}  
}
```

Description of elements

Element	Description
store	Store ID the data is requested for

Returns in the following format

```
{  
  "store": {STORE_ID},  
  "value": {VALUE}  
}
```

Description of elements

Element	Description
store	Store ID the data is requested for
value	The current number of customers in the store

Return codes

HTTP Code	Description
200	OK
400	Bad request. Client supplied an invalid request and is ignored
403	Not authorized. User is not authorized for organization or the store does not have the correct subscription
429	Rate limit was exceeded
500	Internal server error. Unexpected error occurred

Required subscriptions

Depending on the endpoint and the type of data requested, a different subscription is required. This table lists the required subscriptions per `endpoint` and `type`:

Endpoint	Type	Required Subscription
<code>https://api.nedapretail.com/analytics/v1/organization</code>		none
<code>https://api.nedapretail.com/analytics/v1/stores</code>		“Analytics Visitor” and/or “Analytics Theft”
<code>https://api.nedapretail.com/analytics/v2/data</code>	<code>IN</code> , <code>OUT</code> , <code>IN_INTERNAL</code> and <code>OUT_INTERNAL</code>	“Analytics Visitor”
	<code>RF_*</code> , <code>DEACTIVATION</code> , <code>METAL</code> and <code>RFID_*</code>	“Analytics Theft”
<code>https://api.nedapretail.com/analytics/v1/occupancy</code>		“Analytics Visitor”



It may take up to 24 hours for the details of a newly added store or subscription to be available in the Analytics API

Data completeness

It is not possible to guarantee that the requested data is complete. It is always possible that there are some 'late data deliveries' due to network interruptions, for example.

There are a few ways to correct the data collected through the API afterwards.

- One could run the same query for the same time span at a later time.
- Provide scheduled (s)ftp reports with the same data every day to correct the data already collected. The (s)ftp report must contain the data of at least 2 or 3 days. In this way, the originally collected data can be corrected.
- You can request an (s)ftp report from Nedap Retail Support: support-retail@nedap.com

Rate limit

When more than a certain number of requests are received per minute, it is possible to receive a 429
Rate limit was exceeded

There is no back-off time defined, but the client is expected to wait before sending a new request.

Examples of how to deal with this:

- Use an exponential back-off when receiving a 429, so for example first wait 1 second, then 3, then 9, up to a max of 81 seconds and a reset of the back-off when things go well again.
- Wait a fixed time, for example wait 60 seconds

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Document Version 184

Document Last modification date 9 September 2024

Document PDF Exported 2 October 2024 **by** Nedap Retail | Operations

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com



Guideline 2024

Online Services - Nedap Retail Analytics

version 50, November 2023

Introduction	3
iSenseGo Analytics Subscriptions	3
Technical specifications	6
Available data	6
Remarks regarding the use of Nedap Retail Analytics	7
Login	7
Add data in Analytics	7
Overview page	9
Overview - Division	9
Overview - Store	10
System Status page	11
System status - Division	11
System status - Store	12
Date picker & comparison	13
Date picker - Division	13
Comparison - Division	14
Date picker - Store	15
Comparison - Store	15
Dwell and Visiting time	16
Dwell time	16
Visiting time	17
Weather widget	17
Detailed data	18
Data exports / integration	19
Store Occupancy	20
Tips & Tricks	21
Install iSenseGo Analytics Starter	21

Introduction

The data captured by our iSenseGo solutions is crucial for retailers. Data on their EAS estate, such as system health, visitor information and alarm data, is the backbone of a data driven loss prevention strategy to secure every checkout.

This document describes the most important features and options of the Nedap Retail Analytics platform. Retail Analytics is our real-time analytics platform. All the data collected by your EAS systems is send to Retail Analytics. This means that you always have insights in to your EAS estate and how well they are performing. Next to the previous text, it is also possible to send this data through your systems with our API.

iSenseGo Analytics Subscriptions

We recognize three types of subscriptions:

1. iSenseGo Analytics Starter
2. iSenseGo Analytics Visitor
3. iSenseGo Analytics Theft

iSenseGo Analytics Starter

iSenseGo Analytics Starter services offer data & insights, generated from your Nedap EAS system and your EAS estate. In international retail organizations, management is becoming increasingly complex and time consuming. To help retailers with this challenge, Nedap has developed iSenseGo Analytics Starter, which makes sure that you know precisely which stores need your attention.

iSenseGo Analytics Starter gives detailed insight in alarm data and the system status. This helps you to permanently reduce losses and increase the performance of individual stores.

iSenseGo Analytics Visitor

The iSenseGo Analytics Visitor service allows the information from customer counters to show in the Retail Analytics web interface. The customer counting information comes from Nedap connected systems.

View the number of visitors per hour and day, the visitors per m², the dwell time and the visiting time of the customers in the Visitor Intelligence widget.

Store occupancy help retailers manage the maximum visitor capacity in their stores. It shows warnings when occupancy limits are approached or exceeded, on any device which is connected to the internet and is able to run a web browser.

iSenseGo Analytics Visitor Service is also needed to report the alarm to visitor ratio in the EAS Monitor widget in Retail Analytics.



iSenseGo Analytics Theft

The iSenseGo Analytics Theft service will enable alarm information to be seen in the Retail Analytics web interface. The information will be shown in the EAS Monitor widget in Retail Analytics.

The alarm information comes from Nedap connected systems. The alarm information will include alarm directionality, Metal Detection¹ and deactivation¹ and is accessible in the Retail Analytics web interface. Data is also available via export and reports.

¹ if hardware is installed and connected

Features per subscription

iSenseGo service	Analytics Starter	Analytics Theft	Analytics Visitor
Article number	6670164	6669514	6669549
	See alarm data in Analytics Web. Downloads and integrations are not possible (read-only).	Access to alarms, metal detection and deactivations via web dashboard and integrations.	Access to visitor counting via web dashboard and integrations.
Estate overview	✓	✓	✓
System Health	✓	✓	✓
Theft Insights Web <i>Alarms, Metal and Deactivations</i>	✓	✓	-
Download Theft data	-	✓	-
Automated Theft reporting	-	✓	-
Realtime Theft Analytics API	-	✓	-
Visitor Insights Web	-	-	✓
Download Visitor data	-	-	✓
Automated Visitor reporting	-	-	✓
Realtime Visitor Analytics API	-	-	✓
Realtime Occupancy Monitor	-	-	✓

Technical specifications

Web interface

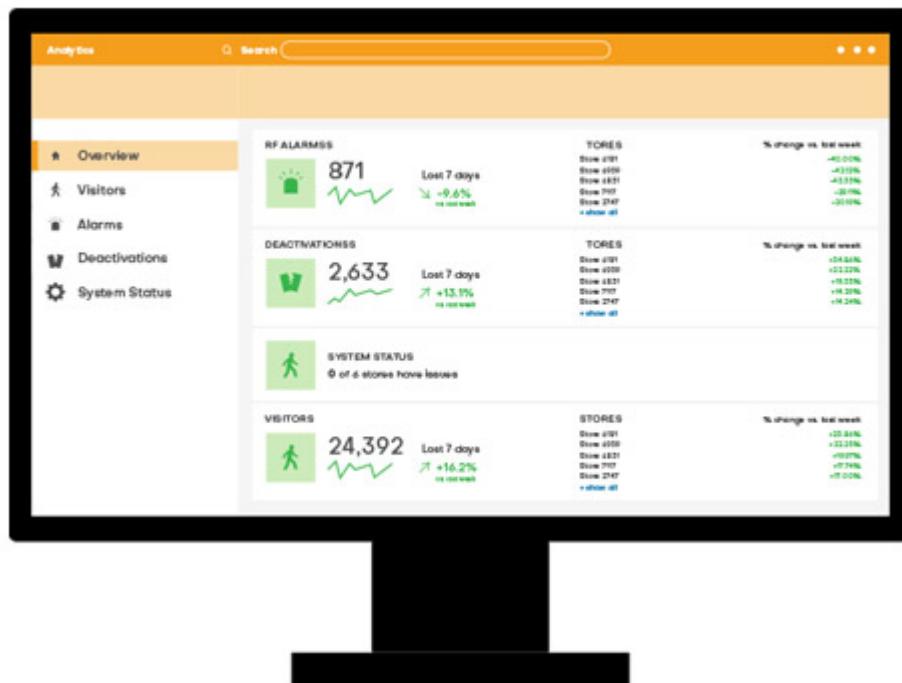
iSenseGo Analytics services has a clear, responsive web interface to view data.

Hosting

Nedap Retail's services run in multiple co-located data centers, on multiple servers. Servers are owned and managed by Nedap.

Security

We hold your data behind a secure firewall system. We regularly upgrade equipment, software and policies to provide you with the highest levels of availability, performance, and disaster-recovery.



Available data

Data that can be available in Analytics:

- Customer counting data (Incoming and Outgoing)
- RF alarm data
- RFID alarm data
- Metal Detection alarms
- Number of deactivations
- System status

Remarks regarding the use of Nedap Retail Analytics

The following remarks apply when using Analytics of Nedap Retail:

- Analytics has a 2-year data retention period
- Available data in Analytics is depending on installed hardware and activated subscriptions
- Real time data : As of firmware version 19.09 , real time data delivery is added, which means that alarm- and customer events per aisle are stored.”

Login

To login to Nedap Retail Analytics, go to:

- <https://login.nedapretail.com/roadsign> or directly to:
- <https://analytics.nedapretail.com/>



A Nedap Retail account is required to login with the correct permissions. The local installation partner can arrange an account.

Add data in Analytics

To make Analytics data visible at store level, subscriptions need to be added to that store in Device Management.

[Click here](#) for an overview of the features per subscription.



For more information, please consult the **Online Services - Analytics API** documentation at the Partner Portal.

Required subscriptions

Depending on the type of data requested, a different subscription is required. This table lists the required subscriptions per type :

Type	Required Subscription
IN , OUT , IN_INTERNAL , OUT_INTERNAL	“Analytics Visitor”
RF_* , DEACTIVATION	“Analytics Theft”
METAL	
RFID_*	

Overview page

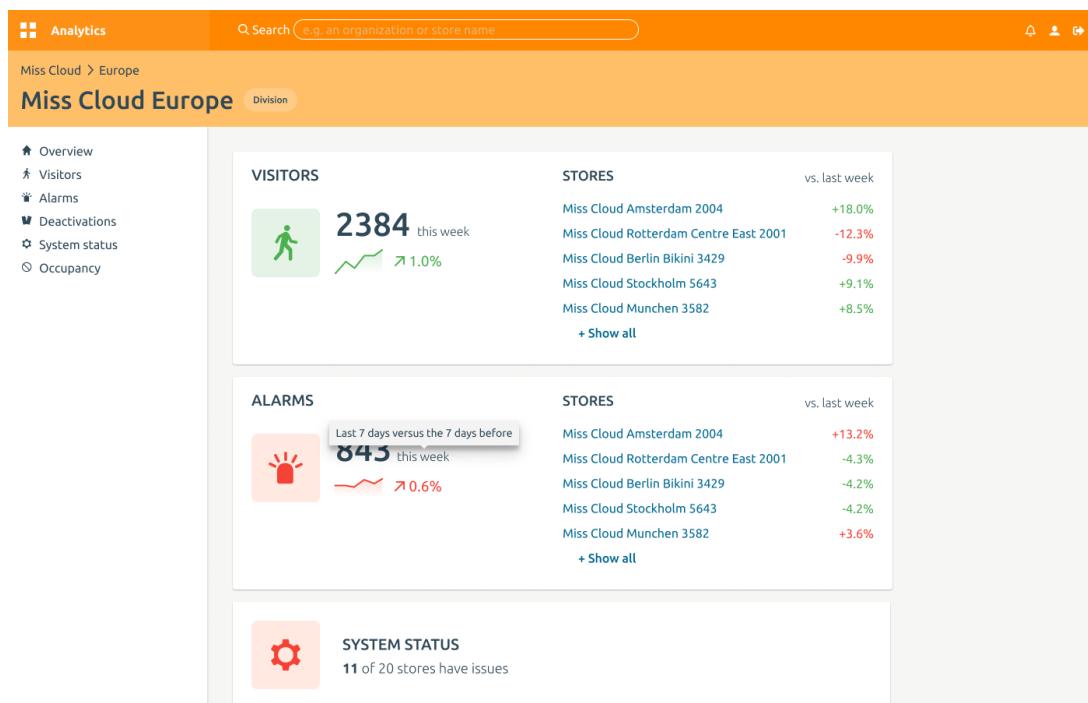
When logged in, the first page is the overview page of the organization/division or store (depending on access rights).

Overview - Division

The division overview shows the top 5 stores with the largest growth/decrease. The percentage on which the stores are sorted is based on the last 7 days, compared to the 7 days prior.

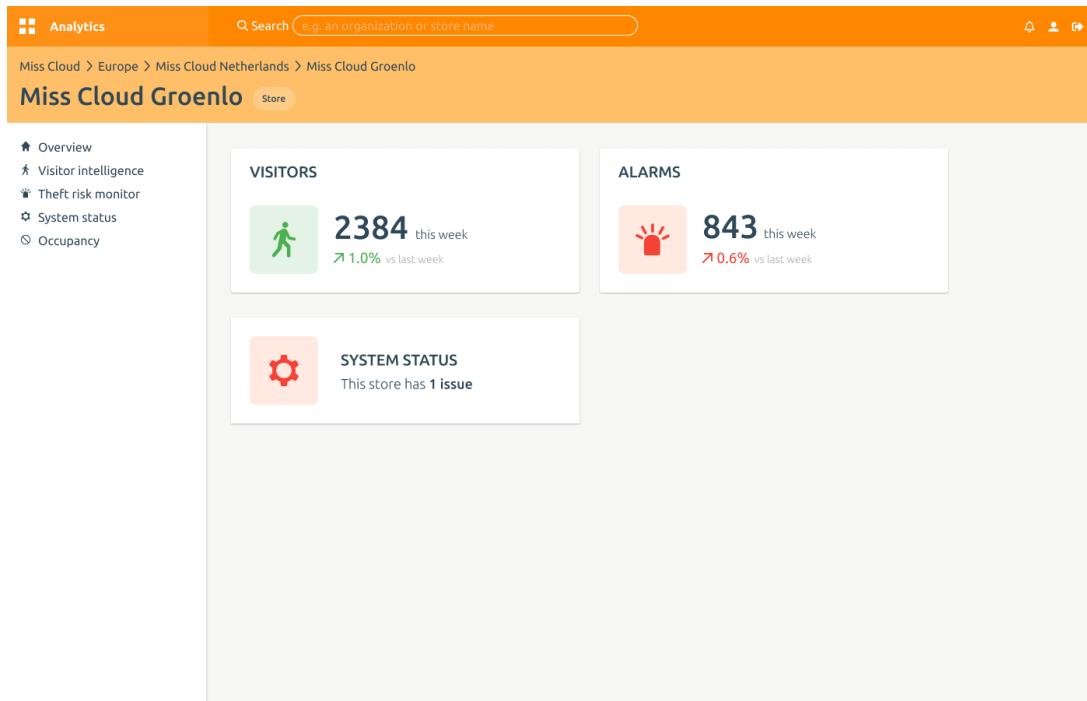
These lists only show the store, and the value. For more details, click on the store

 By clicking 'show all', the list becomes scrollable.



Overview - Store

The store overview contains a similar overview as the Division overview, but for the store.



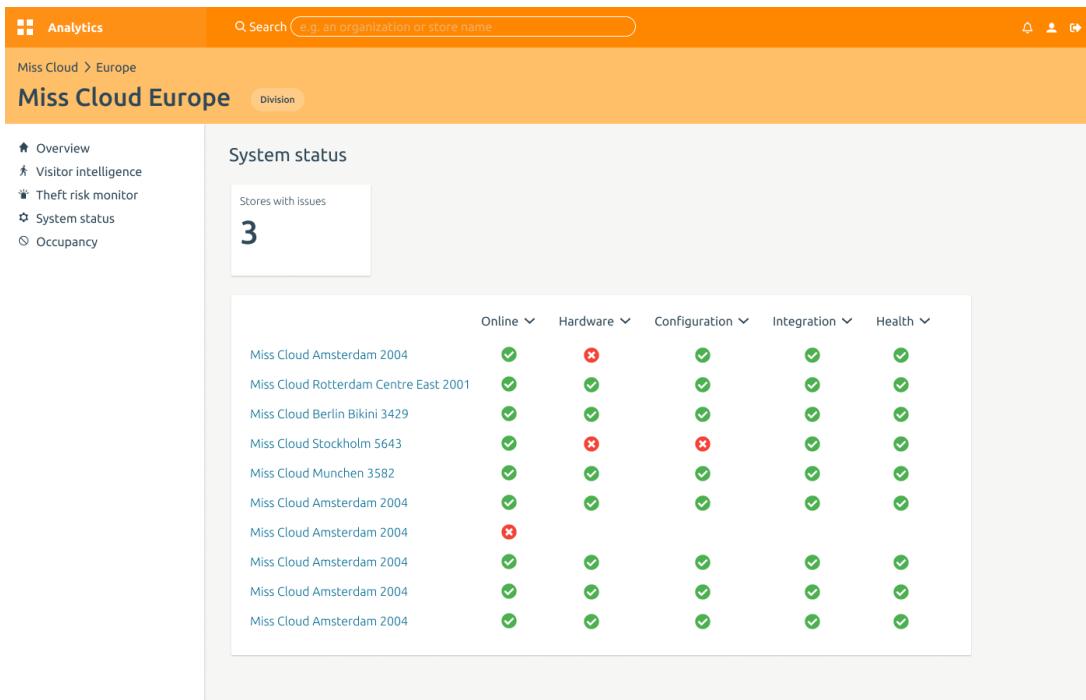
System Status page

System status - Division

The system status shows issue per store and per category:

- Online
- Hardware
- Configuration
- Integration
- Health

It also shows how many stores have issues (e.g.: '7 out of 154' stores have issues).

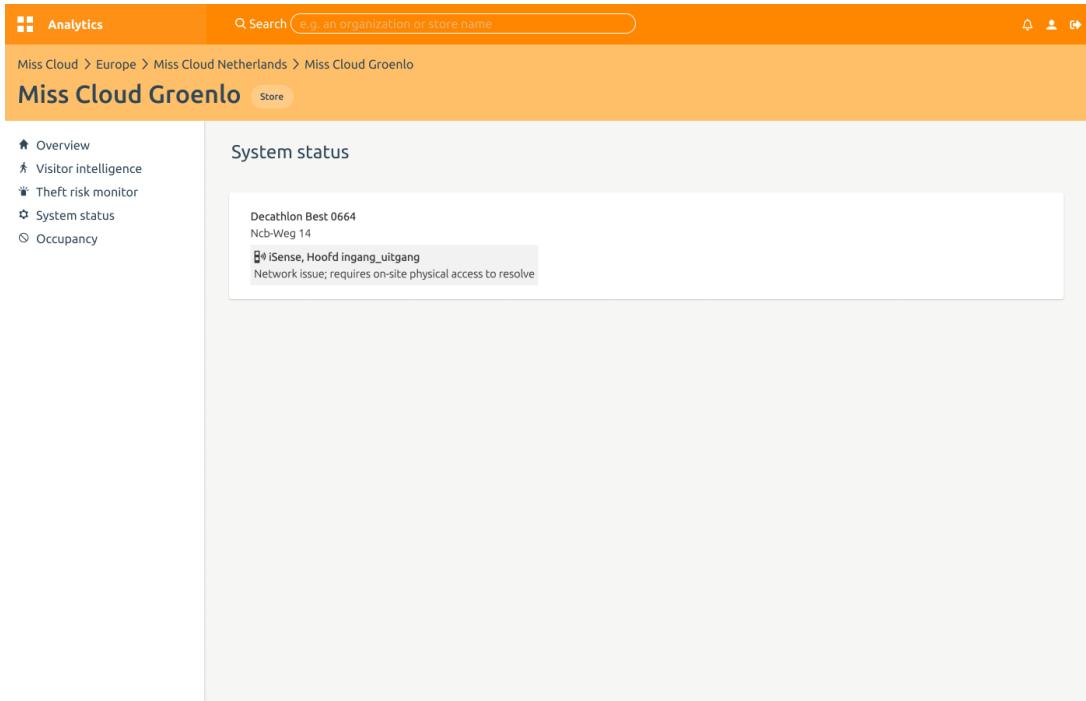


The screenshot shows the 'System status' section of the Miss Cloud Europe dashboard. It displays a summary of 3 stores with issues across five categories: Online, Hardware, Configuration, Integration, and Health. The categories are listed at the top with dropdown arrows, and each store row has a status icon (green checkmark or red X) for each category.

Store	Online	Hardware	Configuration	Integration	Health
Miss Cloud Amsterdam 2004	✓	✗	✓	✓	✓
Miss Cloud Rotterdam Centre East 2001	✓	✓	✓	✓	✓
Miss Cloud Berlin Bikini 3429	✓	✓	✓	✓	✓
Miss Cloud Stockholm 5643	✓	✗	✗	✓	✓
Miss Cloud Munchen 3582	✓	✓	✓	✓	✓
Miss Cloud Amsterdam 2004	✓	✓	✓	✓	✓
Miss Cloud Amsterdam 2004	✗				
Miss Cloud Amsterdam 2004	✓	✓	✓	✓	✓
Miss Cloud Amsterdam 2004	✓	✓	✓	✓	✓
Miss Cloud Amsterdam 2004	✓	✓	✓	✓	✓

System status - Store

On store level it is also possible to see open issues in more detail.



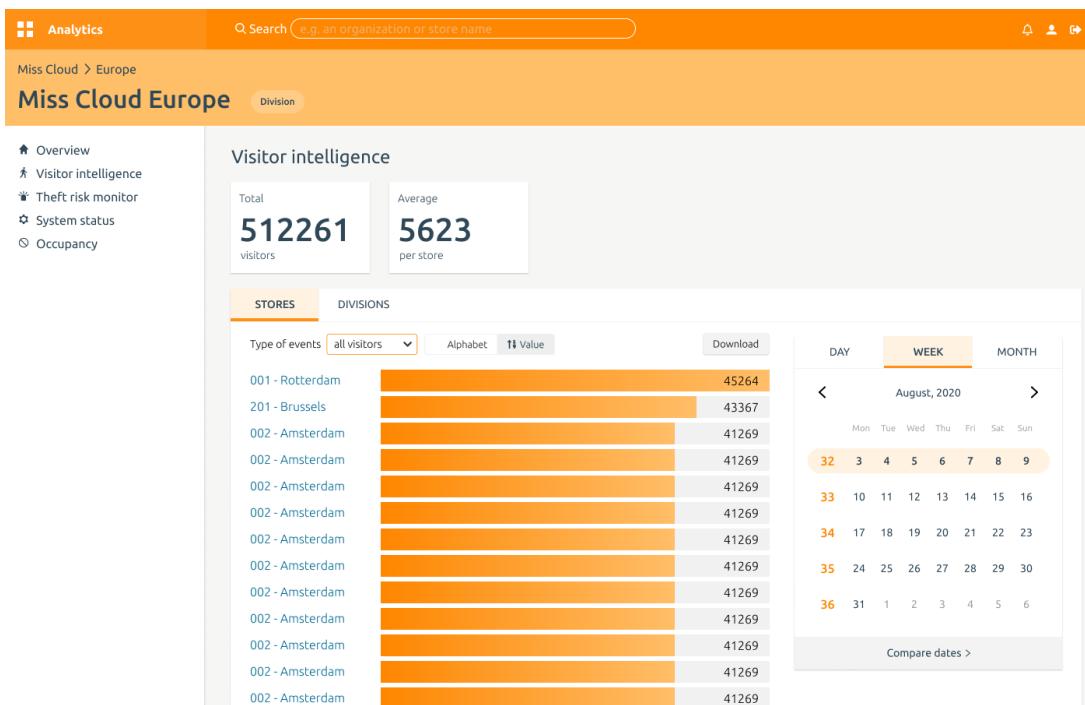
The screenshot shows a web-based system status interface for a store. At the top, there's a navigation bar with a search bar containing "Search e.g. an organization or store name". Below the search bar, the breadcrumb navigation shows "Miss Cloud > Europe > Miss Cloud Netherlands > Miss Cloud Groenlo". The main title "Miss Cloud Groenlo" is displayed next to a "Store" link. On the left, a sidebar menu includes "Analytics", "Overview", "Visitor intelligence", "Theft risk monitor", "System status" (which is selected), and "Occupancy". The main content area is titled "System status" and lists a single item: "Decathlon Best 0664 Ncb-Weg 14". Below this item is a callout box containing the text "iSense, Hoofdingang_uitgang Network issue; requires on-site physical access to resolve".

Date picker & comparison

With the date picker and comparison it is easy to dive into historical data and/or compare data.

Date picker - Division

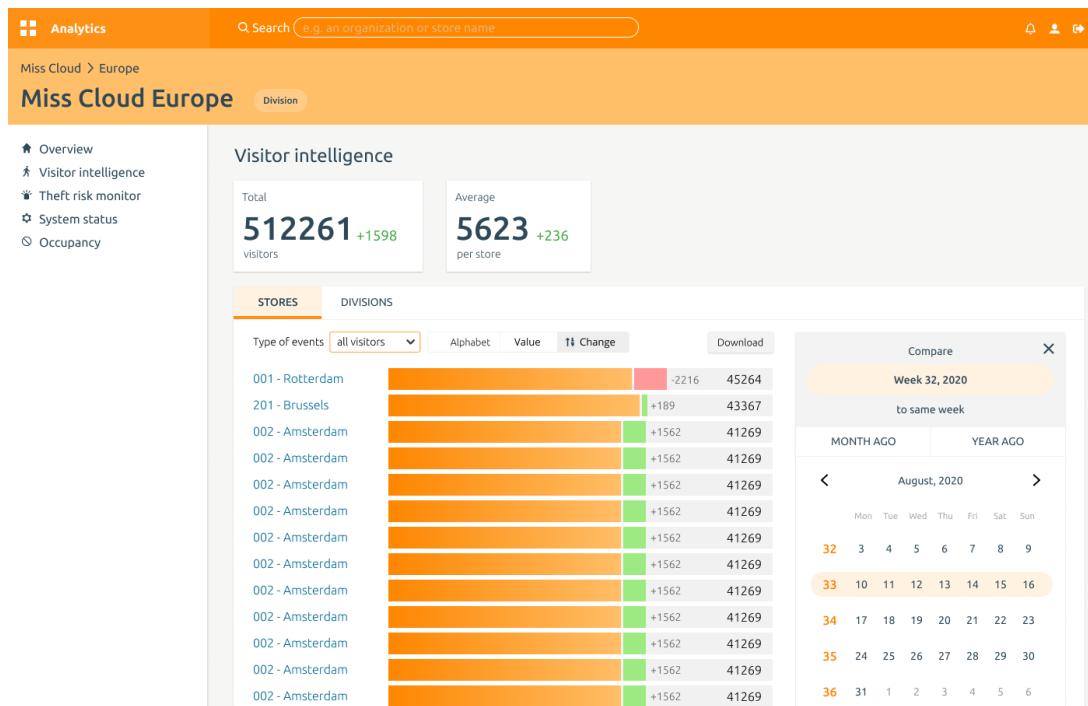
The date picker allows users to view a specific day/week/month



Comparison - Division

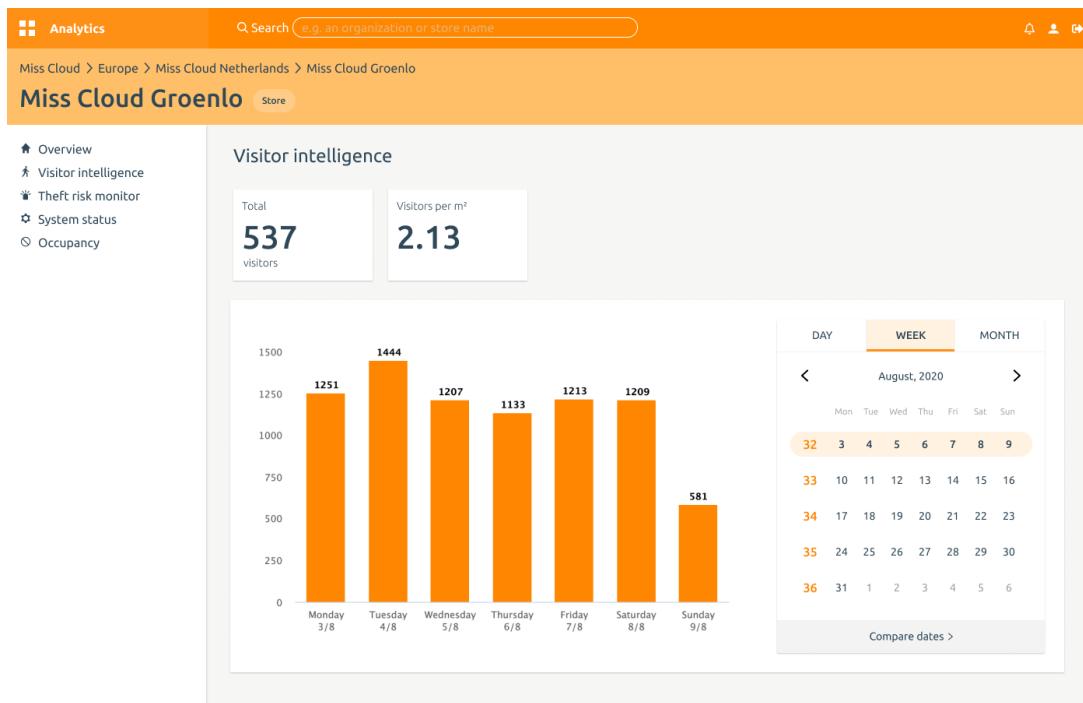
The comparison tool allows users to compare the currently selected day/week/month to any other day/week/month in order to find largest changes.

Shortcuts enable easily selected the same period a week, month or year ago.



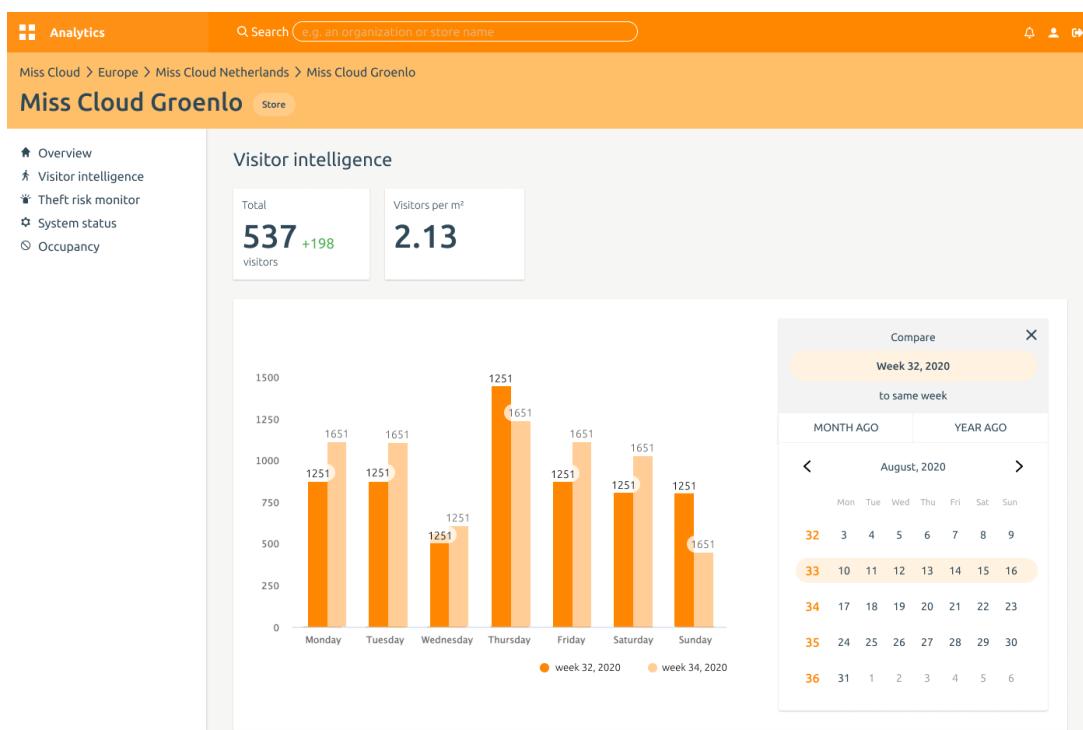
Date picker - Store

The date picker on store level:



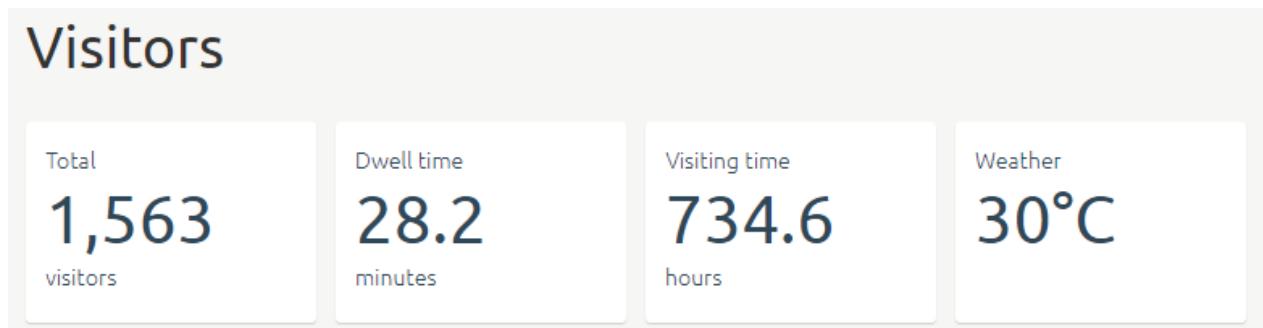
Comparison - Store

The comparison tool on store level:



Dwell and Visiting time

For customer counting data is also possible to see the Dwell time and the Visiting time.



- (i)** The **Weather** shows local weather information (from *openweathermap*) which is the average weather during the day (not night)

Dwell time

Dwell time is the average time spend in the store.

- ⚠** Dwell time will not be shown:
- On the current day
 - If the deviation is too high (5%)

Deviation Calculation

```
difference = abs(Cin - Cout) / max(Cin, Cout);
if (difference < 0.06) {
    show dwell time in Analytics
} else {
    hide dwell time in Analytics
}
```

Visiting time

Visiting time is the total time that all people together have spent in the store.

Calculation

Visiting time = (dwell time * amount of visitors) / 60

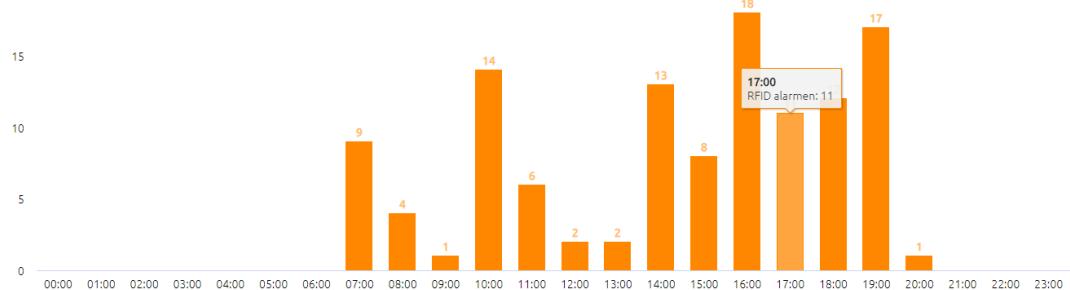
Weather widget

The Weather shows local weather information (from *openweathermap*) which is the average weather during the day (not night).

Detailed data

In the web dashboard it is possible to dig deeper into the data per store-, system-, group-, and aisle level.

Example:



		▼ More detailed info																							
groep	00:00	01:00	02:00	03:00	04:00	05:00	06:00	07:00	08:00	09:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00	
Spogliatoi	0	0	0	0	0	0	0	9	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0
Bagni	0	0	0	0	0	0	0	0	0	2	0	0	0	0	1	0	1	0	1	0	1	0	0	0	0
Ingresso clienti	0	0	0	0	0	0	0	0	0	2	1	0	4	0	0	0	0	1	0	1	0	0	0	0	0
Uffici	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0
Uscita clienti	0	0	0	0	0	0	0	0	0	0	13	2	2	1	13	7	16	10	11	15	0	0	0	0	0

Data exports / integration

Customer Counting data (in .csv or .xlsx format) can be downloaded in the web interface on store-, system-, group-, and aisle level.

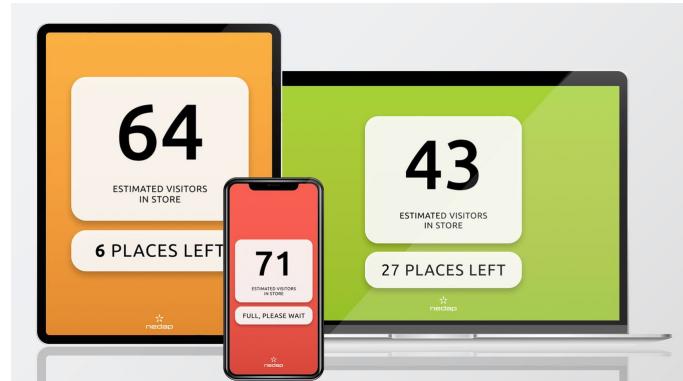
Download



-  Automated reports need to be set up in Device Management, by the business partner.

Store Occupancy

This feature allows the user to monitor the occupancy level in the store.



Tips & Tricks

Install iSenseGo Analytics Starter

When installing iSense Lumen, turn on customer counting and use it in combination with iSenseGo Analytics Starter (free of charge).

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright Nedap Retail 2023

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 50

Document Last modification date 29 November 2023

Document PDF Exported 29 November 2023 **by** Nedap Retail | Operations



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com



Connected Devices Guideline

iSense Online Services Issue Solving

version 182, September 2024

Introduction	4
Device Management - Store Assist	4
Device Management - History Page	5
Device Management - E-mail notifications	6
Analytics System Status Page	7
iSense Technical Dashboard System Overview	8
Modules	9
RF Issues.....	12
RF Extreme Alarms	12
High RF pulse interference	15
Units in RF maintenance mode	17
RF units are muted	19
RFID Issues	25
RFID EAS database error	25
RFID EAS database is slow	27
RFID reader power error	30
RFID antenna is not working properly	32
RFID synchronization failed	34
RFID reader connection problem	36
RFID false alarms suspected	38
RFID reader disabled	41
RFID units are muted	43
Units in RFID maintenance mode	49
Customer Counting Issues.....	51
Infrared beam sensors blocked	51
Infrared beam sensors not connected	53
Signaling hardware issue	55
External Customer Counting Issues	57
No data from external customer counter	57
Metal Detection Issues.....	59
Metal detectors disconnected	59
Metal detection coupling issues	60
IO Box Issues	62



IO box disconnected	62
OST Integration Issues.....	64
OST not connected	64
System Issues	66
Units inactive	66
Not connected to Device Management	68
Key switch active	70
Status.....	72
iSense system is in sleep mode	72

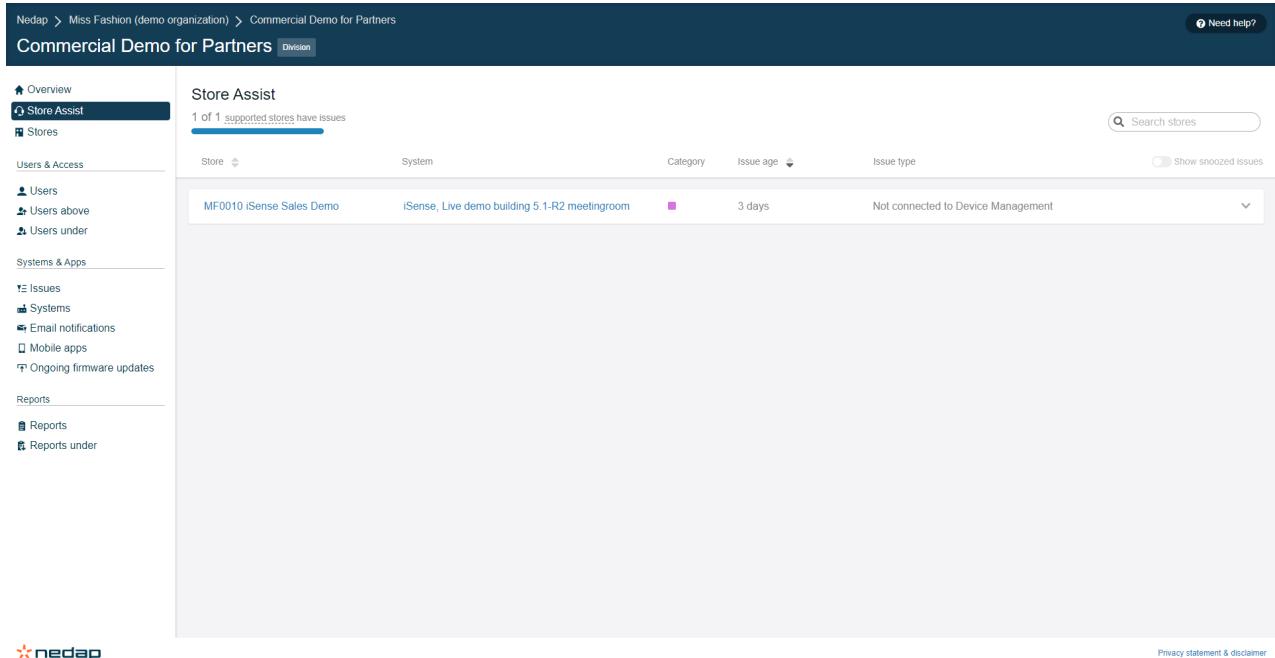
Introduction

This document describes the messages, interpretation, and resolution of issues that can occur in Device Management (Store Assist and System Issues), Analytics and iSense systems

 In this document, Device Management is abbreviated to DM.

Device Management - Store Assist

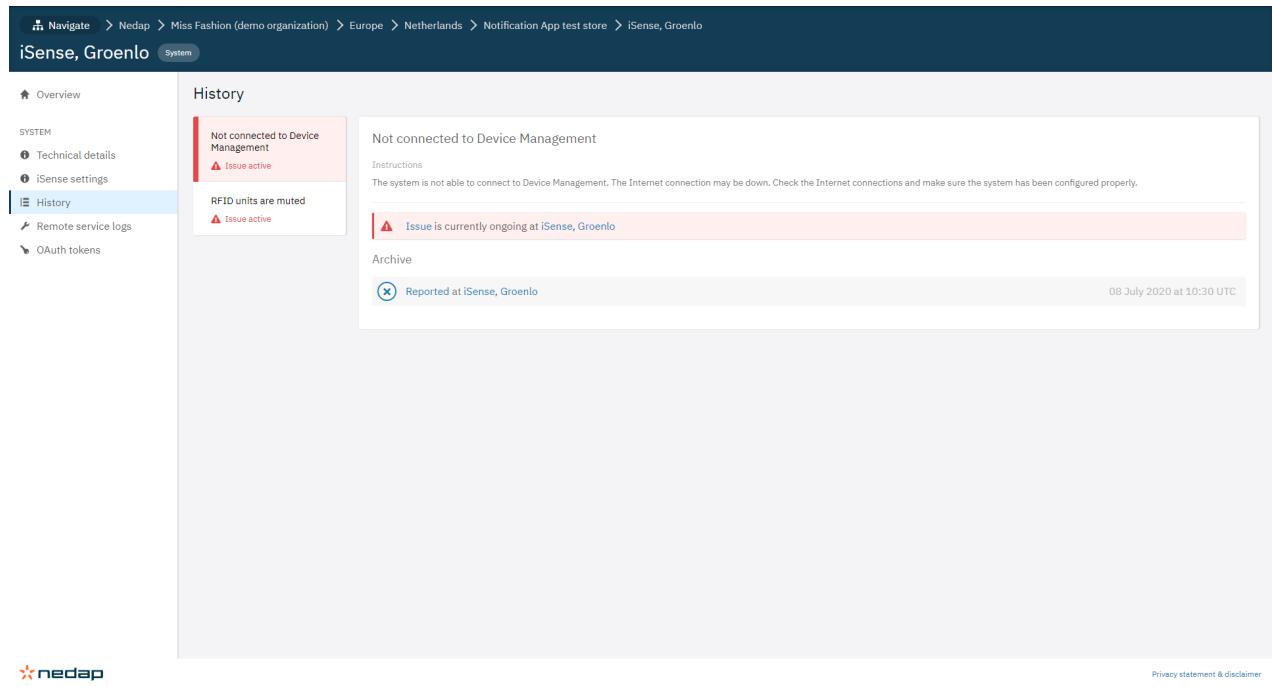
Store Assist shows the issues found for all systems in a division or at a certain level. It is a powerful tool to manage systems.



The screenshot shows the Nedap Device Management interface. The left sidebar has a dark blue header with 'Commercial Demo for Partners' and a 'Division' dropdown set to 'Division'. The sidebar includes links for Overview, Store Assist (which is highlighted in yellow), Stores, Users & Access, Users, Users above, Users under, Systems & Apps, Issues, Systems, Email notifications, Mobile apps, Ongoing firmware updates, Reports, and Reports under. The main content area is titled 'Store Assist' and shows a summary: '1 of 1 supported stores have issues'. Below this, there's a table with columns: Store, System, Category, Issue age, and Issue type. One row is visible: 'MF0010 iSense Sales Demo' (System), 'iSense, Live demo building 5.1-R2 meetingroom' (Category), '3 days' (Issue age), and 'Not connected to Device Management' (Issue type). There are also filters for 'Category', 'Issue age', and 'Issue type', and a search bar 'Search stores' with a magnifying glass icon. At the bottom right of the content area, there are links for 'Privacy statement & disclaimer' and 'Need help?'. The nedap logo is at the bottom left of the page.

Device Management - History Page

The History Page shows the same information as the Store Assist page, and adds a few details.



The screenshot shows the Device Management - History Page. At the top, there is a breadcrumb navigation: "Navigate > Nedap > Miss Fashion (demo organization) > Europe > Netherlands > Notification App test store > iSense, Groenlo". Below the breadcrumb is a header bar with the text "iSense, Groenlo" and a "System" button. On the left, a sidebar menu includes "Overview", "SYSTEM" (with "Technical details", "iSense settings", and "History" selected), "Remote service logs", and "OAuth tokens". The main content area is titled "History" and displays two sections: "Not connected to Device Management" (status: "Issue active") and "RFID units are muted" (status: "Issue active"). Both sections include instructions and a link to "Reported at iSense, Groenlo". A timestamp "08 July 2020 at 10:30 UTC" is shown at the bottom right. The footer contains the nedap logo and a link to "Privacy statement & disclaimer".

Device Management - E-mail notifications

It is possible to send automatic e-mail notifications for issues

Navigate > Nedap Business Partner Demo > Netherlands

Netherlands Division

- [Overview](#)
- [Store Assist](#)
- [Stores](#)

- SYSTEMS & APPS**
- [Issues](#)
- [Systems](#)
- [RFID EAS performance](#)

- [Email notifications](#)
- [Mobile apps](#)
- [Ongoing firmware updates](#)

- REPORTS**
- [Reports](#)
- [Reports under](#)

Notifications (beta)

Add Notification

Show notifications: Under Netherlands Above Netherlands

Search notifications

Recipient	Send delay	Issue type	Location	Creation date	Set by
Business Partner	30 minutes	Units inactive	Netherlands	Today at 12:28 PM	Business Partner X
Business Partner	30 minutes	Not connected to Device Management	Netherlands	Today at 12:28 PM	Business Partner X

nedap

Navigate > Nedap Business Partner Demo > Netherlands

Netherlands Division

[Privacy statement & disclaimer](#)

- [Overview](#)
- [Store Assist](#)
- [Stores](#)

- SYSTEMS & APPS**
- [Issues](#)
- [Systems](#)
- [RFID EAS performance](#)
- [Email notifications](#)
- [Mobile apps](#)
- [Ongoing firmware updates](#)

- REPORTS**
- [Reports](#)
- [Reports under](#)

Set new email notification

Set for a different location? Use the [overview](#) to go to another location.

Which issue type(s) do you want to subscribe to?

<input type="checkbox"/> Not connected to Device Management
<input type="checkbox"/> Units inactive
<input type="checkbox"/> Units in RF maintenance mode
<input type="checkbox"/> RF extreme alarms
<input type="checkbox"/> High RF pulse interference
<input type="checkbox"/> RFID units are muted
<input type="checkbox"/> Units in RFID maintenance mode
<input type="checkbox"/> RFID false alarms suspected
<input type="checkbox"/> RFID EAS database error
<input type="checkbox"/> Key switch active
<input type="checkbox"/> Infrared beam sensors blocked
<input type="checkbox"/> IO box disconnected

After how long should the notification be sent?

Direct	30 minutes	1 hour	1.5 hours	2 hours	4 hours	12 hours	24 hours	48 hours
--------	------------	--------	-----------	---------	---------	----------	----------	----------



Analytics System Status Page

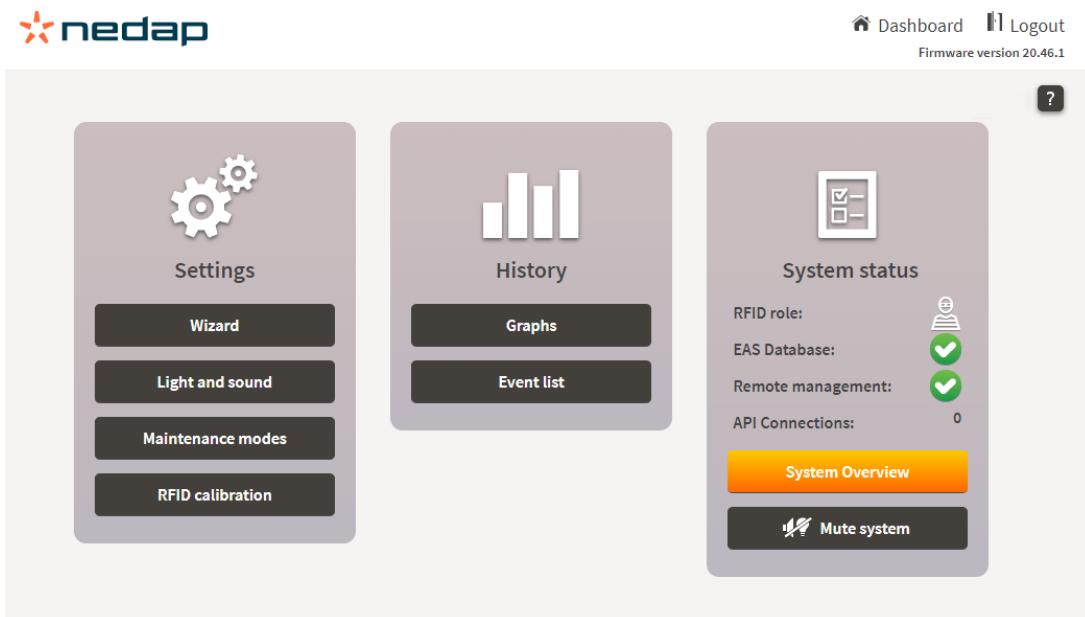
Analytics only shows generic messages of the issue. They have been added in this document to have everything together. The issue itself is derived from the issue in Device Management. No interpretation or timing differences.

The screenshot shows the Analytics System Status Page for the MF0010 New York store. The top navigation bar includes links for Analytics, Search, and various user icons. The main content area displays the System status, showing 1 system with issues, specifically the iSense device in the meetingroom, which has a network issue requiring on-site physical access to resolve.

OVERVIEW	System status
VISITORS	Systems with issues 1 of 1 systems
ALARMS	
SYSTEM STATUS	iSense, Live demo building 5.1-R2 meetingroom Network issue; requires on-site physical access to resolve

iSense Technical Dashboard System Overview

Most issues are visible in the specific wizard steps per module, however, this document only describes how they appear on the **System Overview** page. The button is colored **orange** if items are available.



The page shows the layout of the system and the issues found. Reports of issues are combined where possible and displayed per unit. Where Device Management only indicates an issue, the iSense system can show more detailed information about the problem.

Some issues do not appear on the **System Overview** page; in such cases, the page that provides information is added to the issue description.

For most issues, the Device Management 'Description' and 'Instruction' should give you enough information about the issue to take action. Additional comments are added where necessary.

Modules

In this document the issues are categorized per module:

- RF
- RFID
- Customer Counting
- External Customer Counting
- Smart Deactivator
- Metal Detection
- IO Box
- OST Integration
- System

Issue classification

Issues are classified in degrees / types of effort / action.

Category	Analytics Issue	Issues In This Category
Health	System health issues, which may be resolved by store staff	<ul style="list-style-type: none"> RF Extreme Alarms
	Customer Counting system (partially) interrupted, remove blocking objects, otherwise contact the local Business Partner (installer)	<ul style="list-style-type: none"> Infrared beam sensors blocked
Integration	Integration related issues, to be investigated by the local Business Partner (installer)	<ul style="list-style-type: none"> RFID EAS database error RFID EAS database is slow No data from external customer counter
Hardware	Hardware related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff	<ul style="list-style-type: none"> High RF pulse interference RFID reader power error RFID antenna is not working properly RFID synchronization failed RFID reader connection problem Infrared beam sensors not connected Signaling hardware issue Metal detectors disconnected Metal detection coupling issues IO box disconnected
	System (partially) interrupted, check all power cables, otherwise contact the local Business Partner (installer)	<ul style="list-style-type: none"> Units inactive
Network	Network related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff	<ul style="list-style-type: none"> OST not connected
	System is offline since {date} (UTC), check power cables and network connection, otherwise contact the local Business Partner (installer)	<ul style="list-style-type: none"> Not connected to Device Management

Category	Analytics Issue	Issues In This Category
Configuration	Configuration related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff	<ul style="list-style-type: none"> • Units in RF maintenance mode • RFID false alarms suspected • RFID reader disabled • Units in RFID maintenance mode • Key switch active
	System (partially) muted, contact the local Business Partner (installer)	<ul style="list-style-type: none"> • RF units are muted • RFID units are muted
No category	Not really an issue → A status	<ul style="list-style-type: none"> • iSense system is in sleep mode

Timing

iSense and Device Management use different ways and timing for showing and removing issues.

The difference in timing sometimes lead to confusion. "Device Management says the system is offline, but I'm not having any trouble connecting" or worse, "Device Management says the system is online, but I can't connect".

Most issues are visible in Device Management within 0 to 5 minutes, except;

- **RF Extreme Alarms**, which is visible after 10 to 15 minutes (Firmware versions before 22.31: 90 to 95 minutes)
- **Not connected to Device Management**, which is visible after 30 minutes in Device Management (before Februari 2023: 60 minutes), while an iSense system will show this immediately.

Level of detail

iSense and Device Management also have a different level of detail of an issue.

Device Management only indicates that a particular issue has occurred, it has no indication which unit, or units are involved in an issue, it only indicates that there is an issue, details can be found in the iSense system.

RF Issues

RF Extreme Alarms

Category

Health

Device Management Description

One or more gates are automatically muted because of too many RF alarms.

Device Management Instruction

After removing the alarm source, the sound will be re-enabled automatically.

Device Management Notification

yes

Timing

Issue is shown after 10 to 15 minutes (< 22.31 → 90 to 95 minutes)

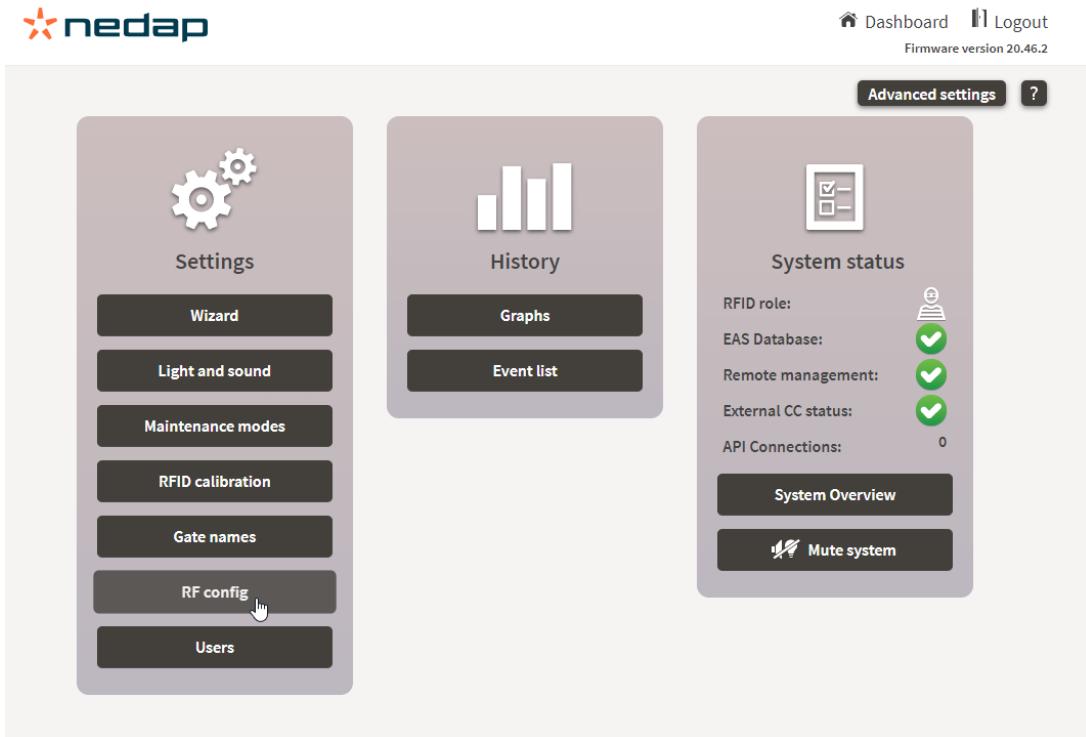
Analytics Issue

System health issues, which may be resolved by the store staff.

Nedap Internal Label

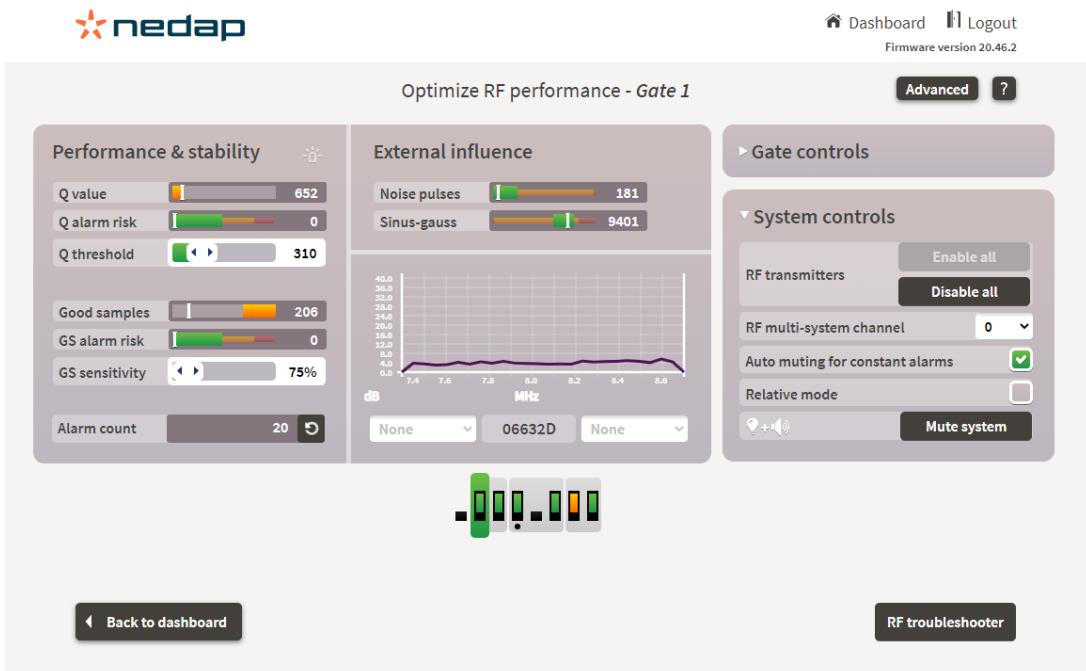
EXTREME_ALARMS

iSense Wizard



The screenshot shows the Nedap iSense Wizard interface. At the top right, there are links for 'Dashboard' (with a house icon), 'Logout' (with a user icon), and 'Firmware version 20.46.2'. Below these are three main cards: 'Settings' (with icons for gears and a list of options like 'Wizard', 'Light and sound', 'Maintenance modes', 'RFID calibration', 'Gate names', 'RF config', and 'Users'), 'History' (with icons for bars and a list of 'Graphs' and 'Event list'), and 'System status' (with icons for a checklist and a system status summary). A 'System Overview' button and a 'Mute system' button are also present. In the 'RF config' section of the Settings card, a cursor is hovering over the 'RF config' button.

This issue is only shown when configured in the **RF config** page.



The screenshot shows the 'Optimize RF performance - Gate 1' page. At the top right are 'Advanced' and '?' buttons. The page is divided into several sections: 'Performance & stability' (showing Q value: 652, Q alarm risk: 0, Q threshold: 310, Good samples: 206, GS alarm risk: 0, GS sensitivity: 75%, Alarm count: 20), 'External influence' (showing Noise pulses: 181 and Sinus-gauss: 9401 with a graph from 7.4 to 8.6 MHz), 'Gate controls' (with a 'Enable all' and 'Disable all' button), and 'System controls' (with RF transmitters, RF multi-system channel set to 0, Auto muting for constant alarms checked, Relative mode unchecked, and a 'Mute system' button). At the bottom center is a graphic of four vertical bars with different patterns. Navigation buttons at the bottom include 'Back to dashboard' and 'RF troubleshooter'.

When 'Auto muting for constant alarms' is configured on the **RF config** page, the system will mute a unit when a label is in the field for at least 1 minute in a 2 minute period. The sound will be muted, but the light will continue to flash. 1 Minute after the tag is removed from the field, the lights will turn off and the mute will stop.

Hardware status

?



(())

[Back to dashboard](#)



High RF pulse interference

Category

Hardware

Device Management Description

One or more units have an RF pulse count greater than 14.500, which means there is a hardware problem or high level of interference.

Device Management Instruction

Check RF hardware and/or store environment.

Device Management Notification

yes

Timing

Issue is shown after 0 to 5 minutes

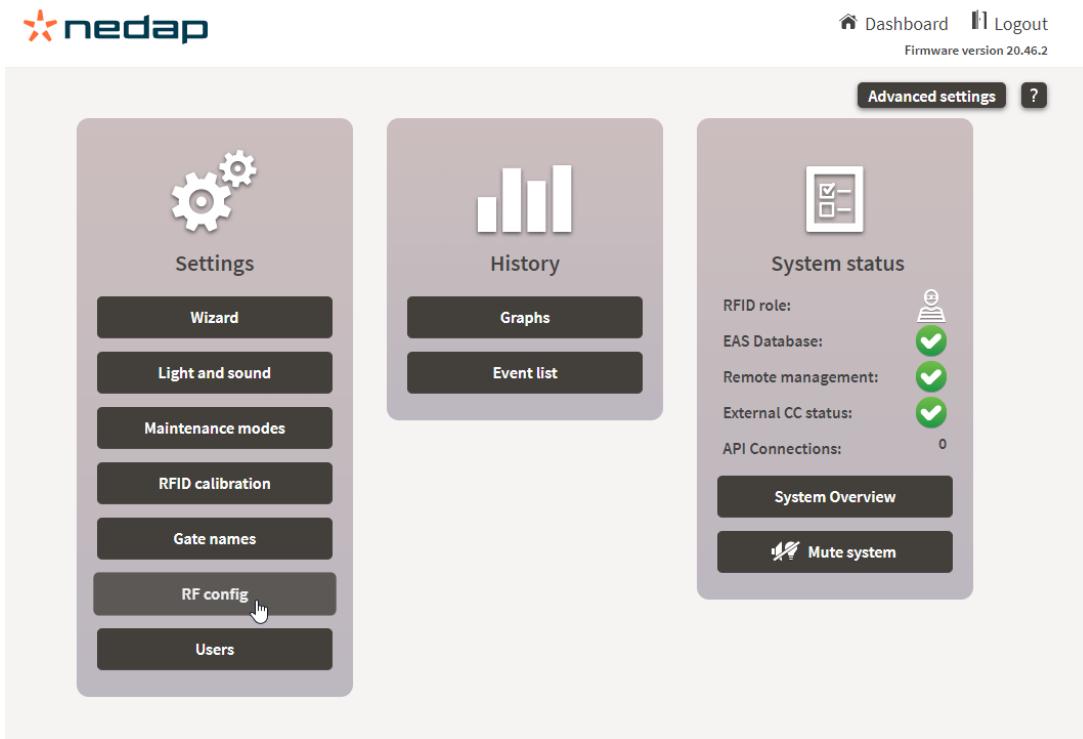
Analytics Issue

Hardware related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff

Nedap Internal Label

RF_NOISE_PULSES

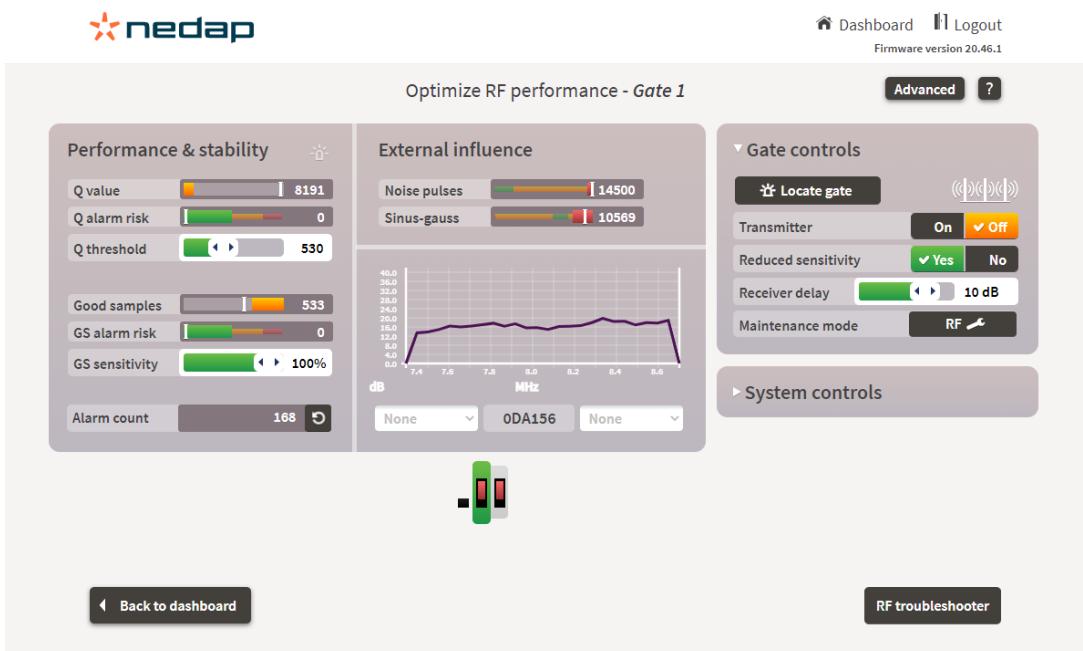
iSense Wizard



The screenshot shows the iSense Wizard dashboard. On the left, there's a sidebar with 'Settings' and several buttons: 'Wizard', 'Light and sound', 'Maintenance modes', 'RFID calibration', 'Gate names', 'RF config' (which has a mouse cursor hovering over it), and 'Users'. In the center, there are two cards: 'History' with 'Graphs' and 'Event list' buttons, and 'System status' with sections for 'RFID role', 'EAS Database', 'Remote management', 'External CC status', and 'API Connections'. At the top right, there are 'Dashboard', 'Logout', 'Firmware version 20.46.2', 'Advanced settings', and a help icon.

This issue is visible by going to the **RF config** page. A few possible causes:

- Bad connection from the Renos unit to the antenna PCB
- Defect antenna PCB
- Strong external interference



The screenshot shows the 'Optimize RF performance - Gate 1' page. It includes three main sections: 'Performance & stability' (with Q value, Q alarm risk, Q threshold, Good samples, GS alarm risk, GS sensitivity, and Alarm count), 'External influence' (with Noise pulses and Sinus-gauss levels, and a graph of dB vs MHz), and 'Gate controls' (with Locate gate, Transmitter On/Off, Reduced sensitivity Yes/No, Receiver delay, and Maintenance mode). At the bottom, there are 'Back to dashboard' and 'RF troubleshooter' buttons, along with a small antenna icon.



Units in RF maintenance mode

Category

Configuration

Device Management Description

One or more units have been disabled by a technician or by the retailer because of RF issues.

Device Management Instruction

Investigate and solve the RF issues and undo Maintenance Mode to re-enable RF functionality.

Device Management Notification

yes

Timing

Issue is shown after 0 to 5 minutes

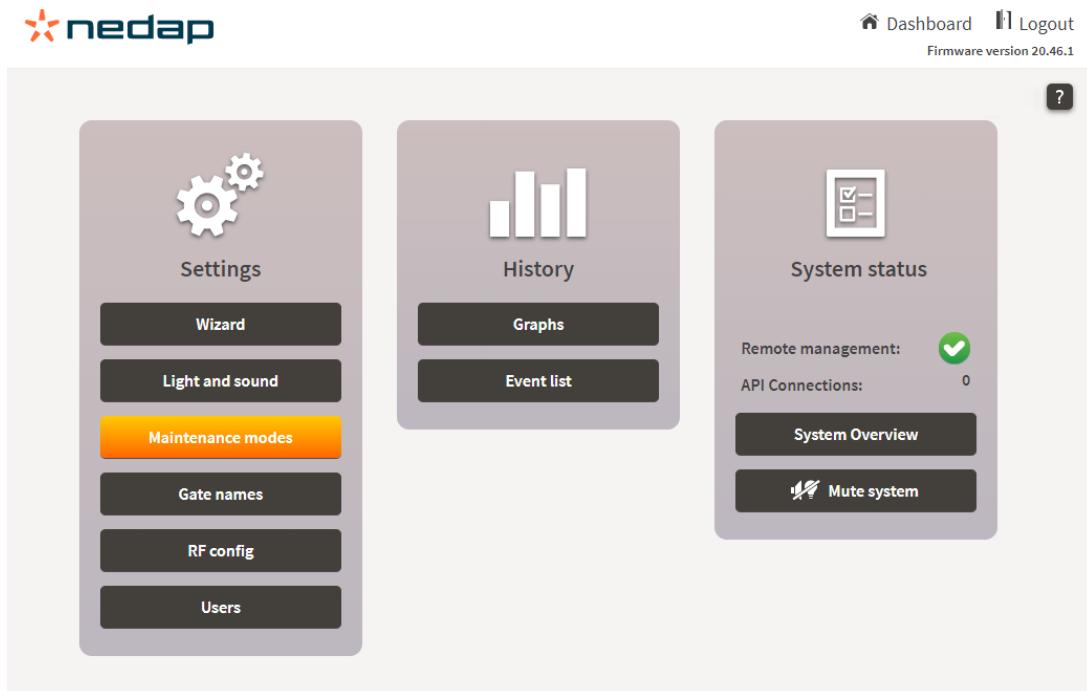
Analytics Issue

Configuration related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff

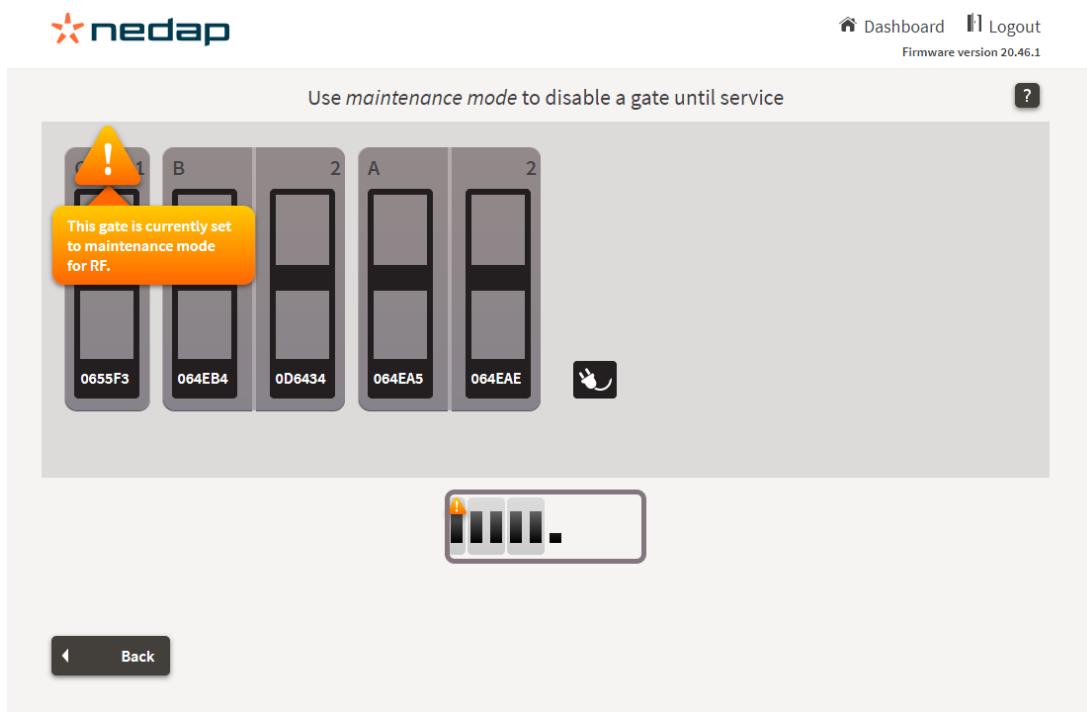
Nedap Internal Label

RF_MAINTENANCE_MODE

iSense Wizard



This issue is visible by going to the **Maintenance modes** page, where you also can turn off the maintenance mode. It is important to check why this mode was added and to fix the underlying issue.



RF units are muted

Category

Configuration

Device Management Description

One or more RF units have been muted and will be operating quietly.

Device Management Instruction

Unmute the RF units.

Device Management Notification

no

Analytics Issue

System (partially) muted, contact the local Business Partner (installer)

Nedap Internal Label

RF_MUTING_STATUS

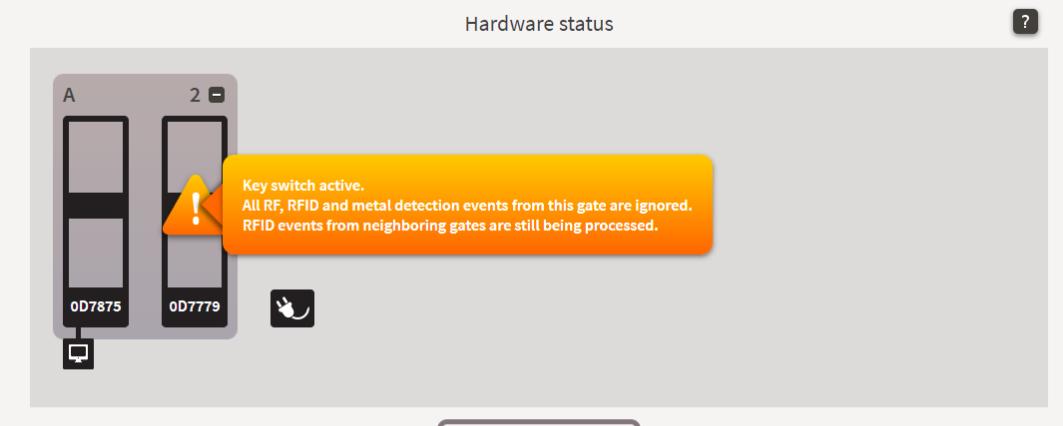
iSense Wizard

This issue can have several causes, to be more precise, 7 different reason for this issue, but not all are visible in DM:

- disabled by a key switch
- disabled by an IO box
- disabled by an API integration
- muted manually through the Technical Dashboard (not shown in DM)
- muted by an IO box (not shown in DM)
- muted by an API integration (not shown in DM)
- muted through the iSense Dashboard (aka snoozing; not shown in DM)

The first 3 will be shown in the **System Overview** page, the last 4 in the **Light and Sound** page.

The first option is by having a key switch placed in the active position.

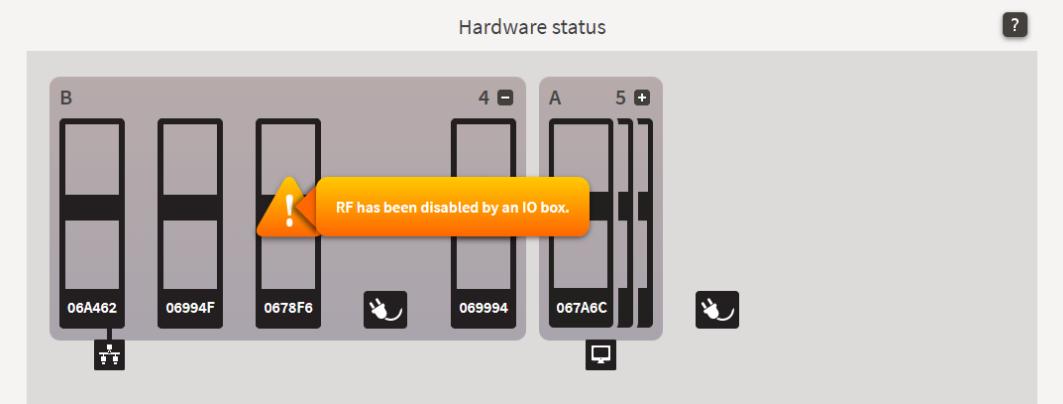


Hardware status

Key switch active.
All RF, RFID and metal detection events from this gate are ignored.
RFID events from neighboring gates are still being processed.

Back to dashboard

The second option is when an IO box has disabled the RF functionality.



Hardware status

RF has been disabled by an IO box.

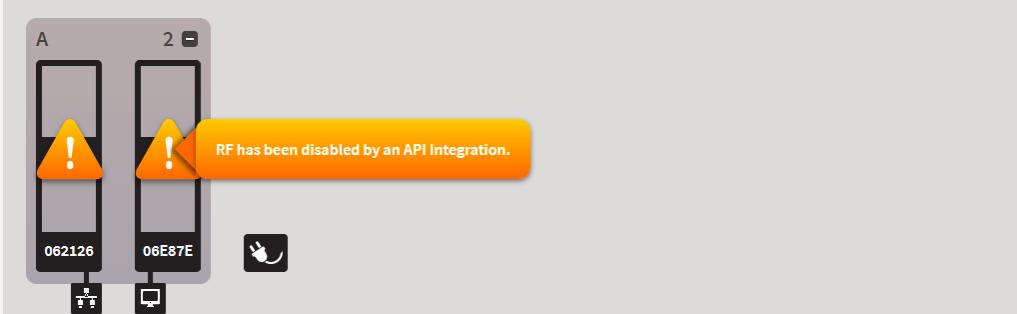
Back to dashboard

The third option is when the RF functionality is disabled by an API integration.

nedap

Dashboard Logout
Firmware version 20.46.2

Hardware status



RF has been disabled by an API Integration.

Do RFID cable detection

Back to dashboard

This next 3 issues are visible by going to the **Light and sound** page.

nedap

Dashboard Logout
Firmware version 20.46.2

Advanced settings ?


Settings

- Wizard
- Light and sound**
- Maintenance modes
- RFID calibration
- Gate names
- RF config


History

- Graphs
- Event list


System status

RFID role:

EAS Database:

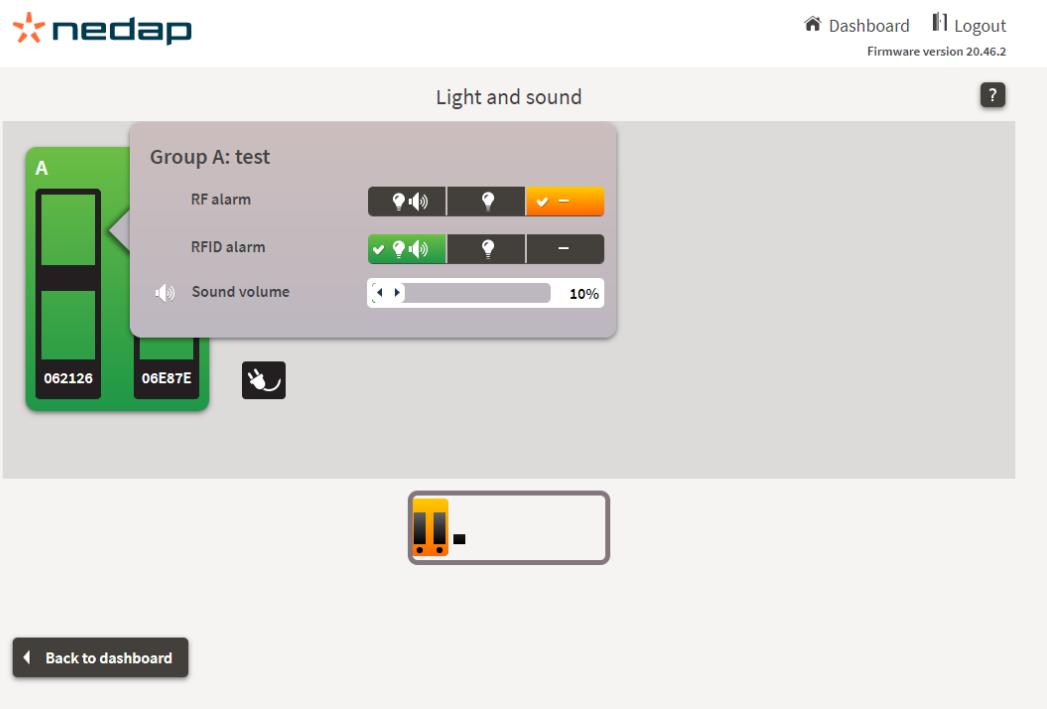
Remote management:

External CC status:

API Connections: 0

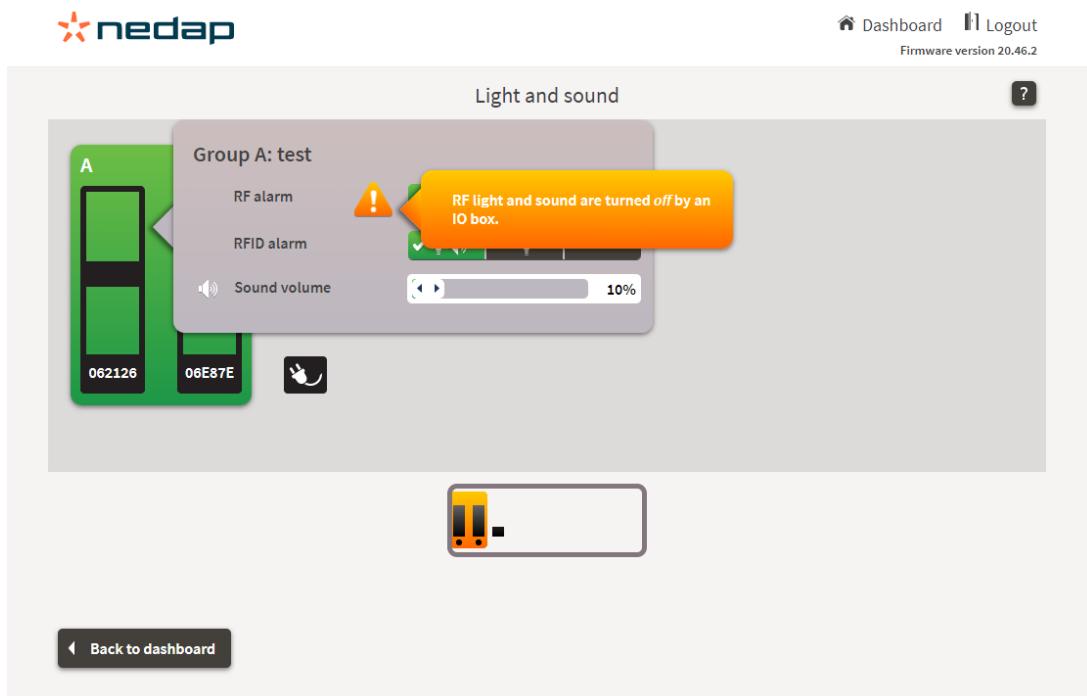
- System Overview
- Mute system

The fourth option is when the light and sound are muted manually (not shown in DM).



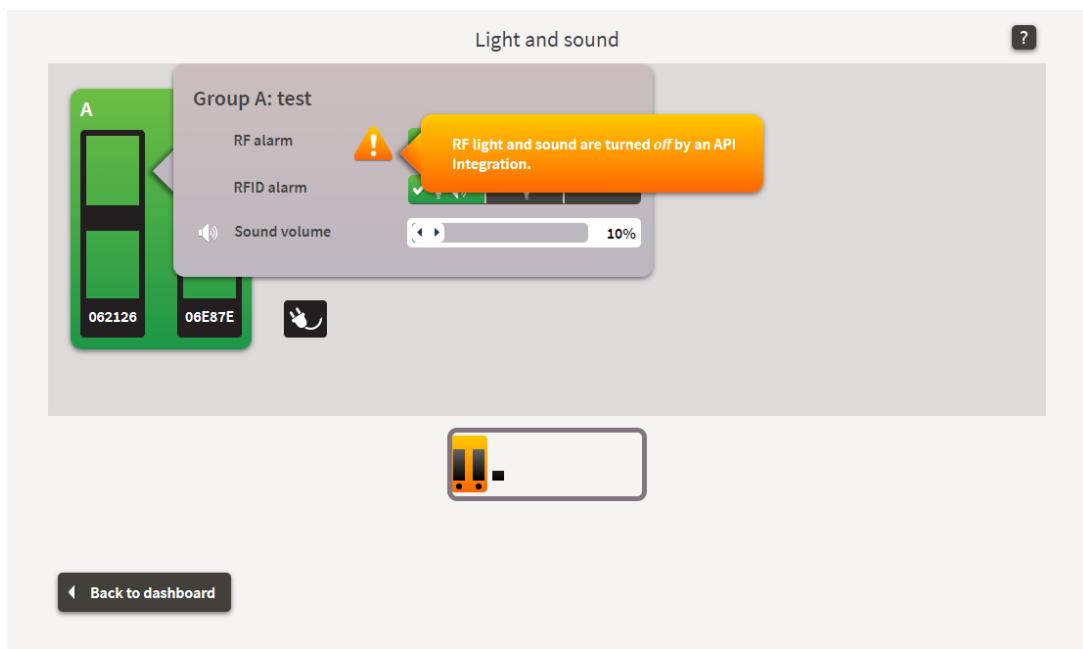
The screenshot shows the 'Light and sound' configuration for 'Group A: test'. On the left, there's a green panel labeled 'A' containing two items: '062126' and '06E87E'. To the right is a control panel with three sections: 'RF alarm' (green button), 'RFID alarm' (green button), and 'Sound volume' (a slider set at 10%). Below these are two small icons: a hand cursor and a speaker. At the bottom center is a yellow status indicator showing a vertical bar with a dot. At the very bottom is a 'Back to dashboard' button.

The fifth option is when the light and sound are turned off by an IO box (not shown in DM).

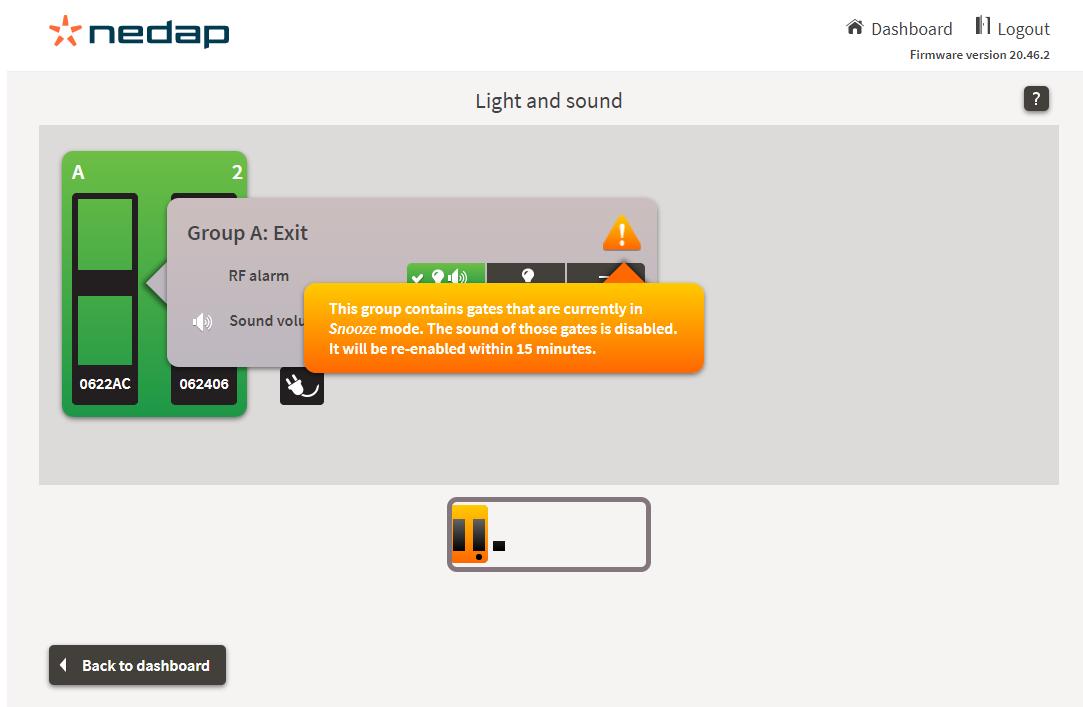


This screenshot is identical to the one above, but it includes a prominent orange warning message box in the center-right area. The message box contains the text 'RF light and sound are turned off by an IO box.' and has an exclamation mark icon. The rest of the interface elements are the same as in the previous screenshot.

The sixth option is when the light and sound are turned off by an API integration (not shown in DM).



And, finally the seventh option is when the retailer snoozes a unit from within the iSense Dashboard (not shown in DM).



When a system is muted from within DM, it will be shown in the wizard as an API mute option.

e2690a60-a6fc-4d38-84ce-be9c438dc4f0 renos

beta Change muting status for e2690a60-a6fc-4d38-84ce-be9c438dc4f0

System mute setting  

System RF mute setting   

! Muting depends on a stable internet connection of the iSense system. Not every mute type can be disabled remotely via Device Management.

! RF and RFID muting are shown as muted through API integration in the iSense dashboard.

[Cancel](#)

<input checked="" type="checkbox"/> RF	<input checked="" type="checkbox"/> enabled	EAS Protocol	
<input type="checkbox"/> RFID	<input type="checkbox"/> disabled	MAC Address	00:0D:A0:06:73:BD

! [\(Un\)mute system](#)

RFID Issues

RFID EAS database error

Category

Integration

Device Management Description

The communication between the system and the RFID EAS database is interrupted.

Device Management Instruction

Check whether the system is connected to the local network. Check with the customer or integrator whether the RFID EAS database is up and running.

Device Management Notification

yes

Timing

Issue is shown after 0 to 35 minutes

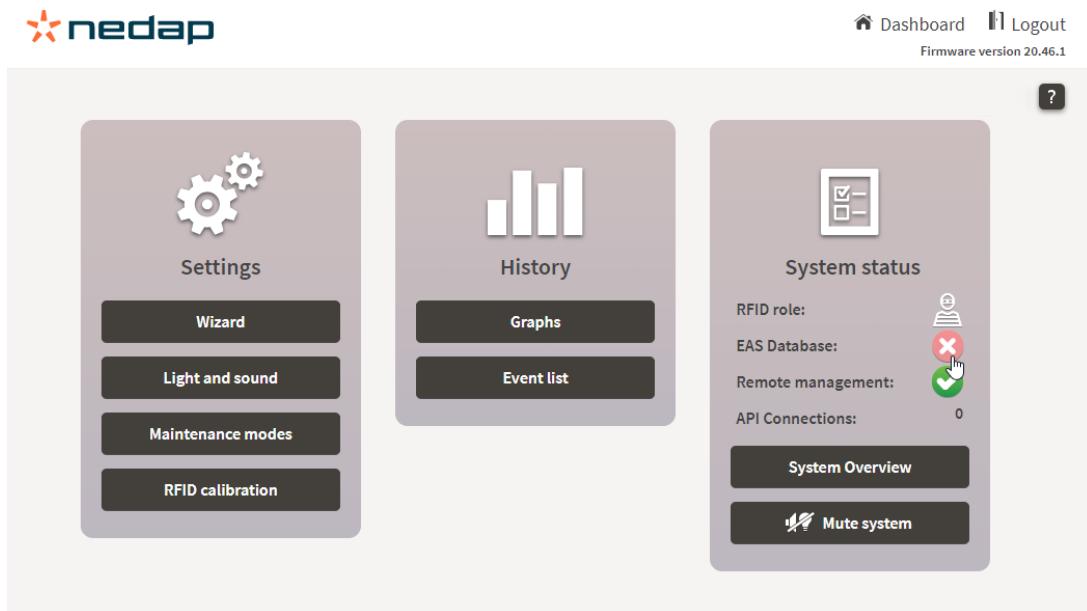
Analytics Issue

Integration related issues, to be investigated by the local Business Partner (installer)

Nedap Internal Label

EAS_PROTOCOL_ERROR

iSense Wizard



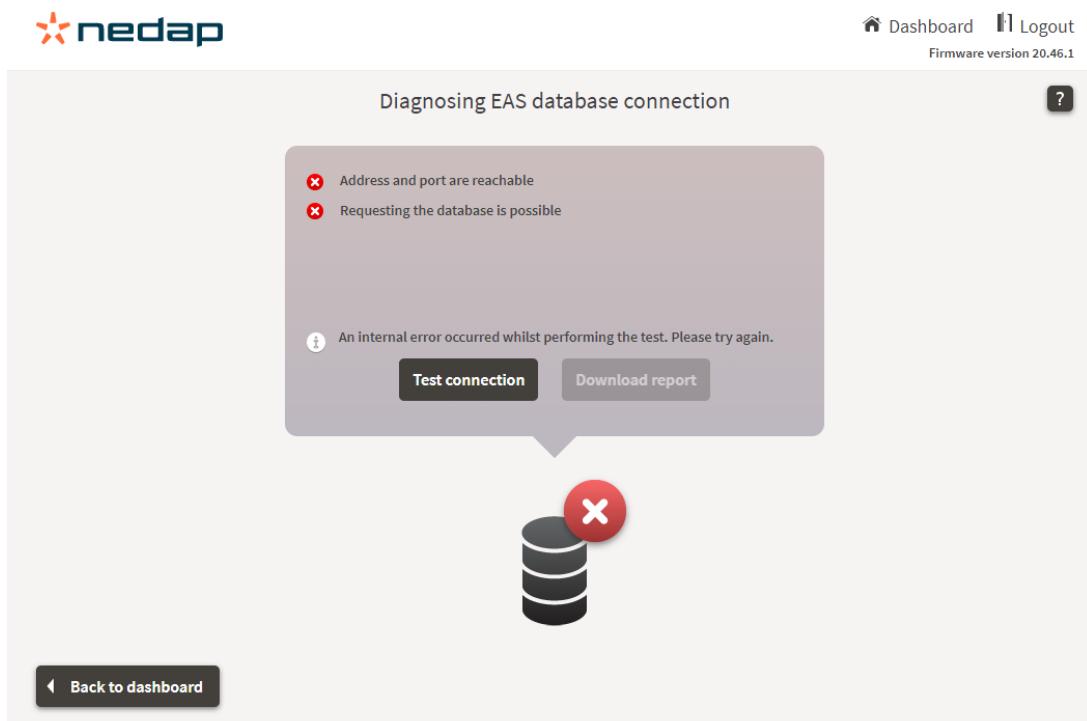
The screenshot shows the iSense Wizard dashboard. At the top right, there are links for 'Dashboard', 'Logout', and 'Firmware version 20.46.1'. A question mark icon is in the top right corner. The main area has three cards:

- Settings** card (left):
 - Icon: gear
 - Text: Settings
 - Buttons: Wizard, Light and sound, Maintenance modes, RFID calibration
- History** card (middle):
 - Icon: bar chart
 - Text: History
 - Buttons: Graphs, Event list
- System status** card (right):
 - Icon: monitor with checkmarks
 - Text: System status
 - Details:
 - RFID role: (green)
 - EAS Database: (red cross)
 - Remote management: (green checkmark)
 - API Connections: 0
 - Buttons: System Overview, Mute system

Press the **red cross** icon to get details of this issue.

In general this is an IT issue in the store.

The consequence of this issue is that all products, sold and unsold can leave the store unnoticed. The system is not able to alarm as long as the connection with the EAS database is lost.



The screenshot shows the 'Diagnosing EAS database connection' page. At the top right, there are links for 'Dashboard', 'Logout', and 'Firmware version 20.46.1'. A question mark icon is in the top right corner. The main area has a central message box:

Diagnosing EAS database connection

✗ Address and port are reachable
 ✗ Requesting the database is possible

An internal error occurred whilst performing the test. Please try again.

Test connection Download report

A large red 'X' is overlaid on a database icon at the bottom center.

Back to dashboard

RFID EAS database is slow

Category

Integration

Device Management Description

The RFID EAS database did not respond within the timeout limit.

Device Management Instruction

Check with the customer or integrator whether the RFID EAS database is up and running correctly.

Device Management Notification

Yes

Analytics Issue

Integration related issues, to be investigated by the local Business Partner (installer)

Nedap Internal Label

EAS_PROTOCOL_RESPONSIVENESS

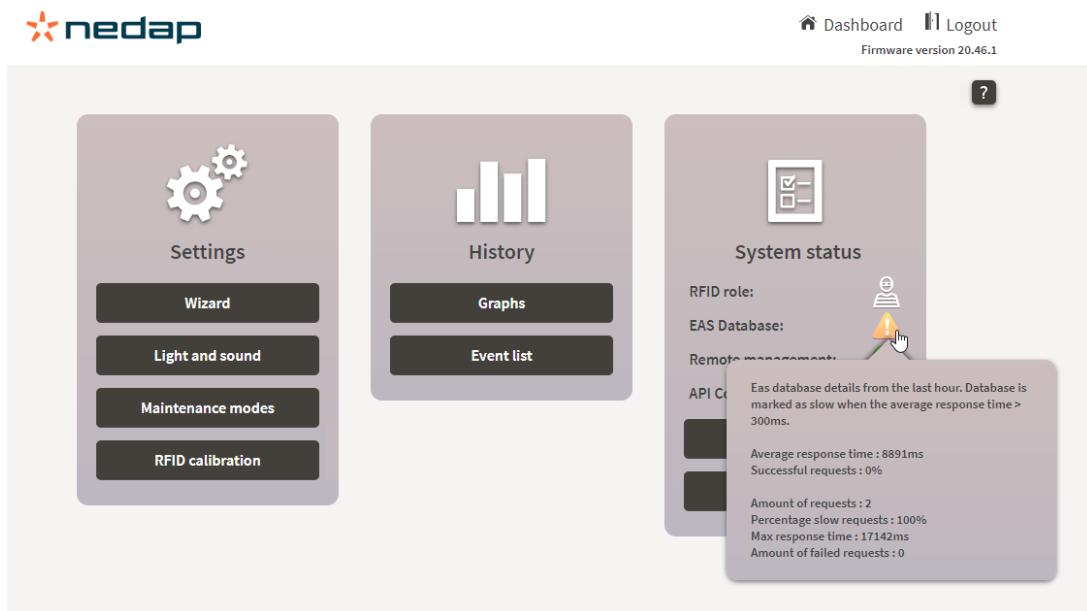
iSense Wizard



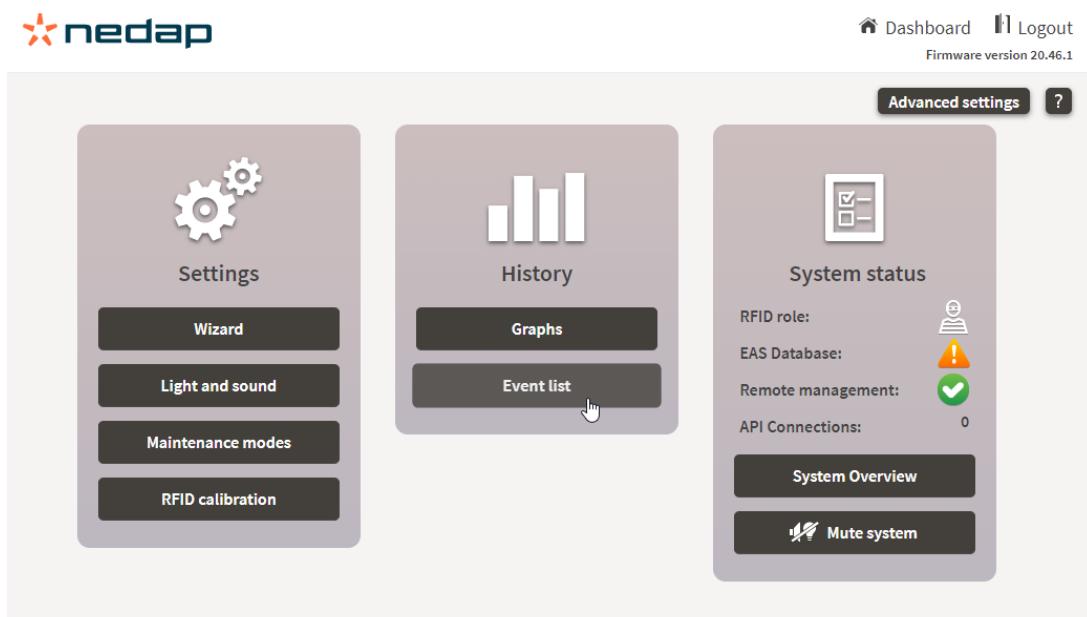
Press the **orange exclamation** icon to get details of this issue.

In general this is an IT issue in the store.

The consequence of this issue is that all products, sold and unsold can leave the store unnoticed. The system is not able to alarm as long as the connection with the EAS database is too slow.



The event list that you can download from the **Event list** page or the **Graphs** page will show you the response times per RFID event. This can be very helpful in the search for a solution. Again, most of the time this is an IT issue in the store.



Event history

[Download events](#)

- Visible events:
- Sold EPCs
 - RFID alarms
 - Foreign EPCs
 - Unknown EPCs
 - Config changes

Type	Dir	Time	Description	Group
System		6 minutes ago	User 'jaap.dejong' has logged in	
System		8 minutes ago	Remote connection started	
Image	Out	1 hour ago	00B07A14701F279010003BE4	B
Image	Out	1 hour ago	00B07A14701F279010004B32	B
Image	Out	1 hour ago	00B07A14703B2410100070B2	B
Image	Out	1 hour ago	00B07A146C4724924C396511	A
Image	Out	1 hour ago	00B07A14646054970BD5BAF4	A
Image	Out	1 hour ago	00B07A146C2F575040007B2C	A
Image	Out	1 hour ago	00E0864808345A080800025A	A
Image	Out	1 hour ago	00E08648083519D048001318	A
Image	In	1 hour ago	00E08648083519D048001318	A

[Back to dashboard](#)

Database response time (ms)									
A	B	C	D	E	F	G	H	I	J
ID	Type	Time	Timezone	Message	Group code	Details	Database response time (ms)		
3bf6d461-aea-4ad4-8cf-78cc4d88851	SYSTEM_LOG	2021-08-25 12:43:33	GMT	User 'jaap.dejong' has logged in					
958fe55-b38e-4ed7-bce1-76537fd5d508	SYSTEM_LOG	2021-08-25 12:41:28	GMT	Remote connection started					
c16db82d-8f8d-4c2a-9966-63174d02340	RFID SOLD	2021-08-25 11:02:36	GMT	3408328061240104032758A	B	Direction OUT	1423		
f06fb8ab-262d-456e-9506-5e0327477f7	RFID SOLD	2021-08-25 11:02:36	GMT	3408328061240104032758A	B	Direction OUT	1193		
f262b007-bbf4-4087-9002-2794e08f64c	RFID SOLD	2021-08-25 11:02:36	GMT	3408328061240104032758A	B	Direction OUT	1439		
443944ec-63d5-4981-b593-74a5521795f	RFID SOLD	2021-08-25 10:50:00	GMT	7EDA919221100433900003D8	A	Direction OUT	1321		
143f1b30-400d-479c-9b78-1075d477684	RFID SOLD	2021-08-25 10:53:33	GMT	7EDA919221100433900003D8	A	Direction OUT	115		
1523ffef-3-4f1c-4900-ab0b-5f898bb1c08	RFID SOLD	2021-08-25 10:53:33	GMT	7EDA919221100433900003D8	A	Direction OUT	337		
42524048-bd16-4298-a9ea-1ddca1f89896	RFID SOLD	2021-08-25 10:51:15	GMT	7EDA919221100433900003D8	A	Direction OUT	187		
4ef0f054-e-418c-4972-bbf5-70893d60984	RFID UNKNOWN	2021-08-25 10:51:09	GMT	7EDA919221100433900003D8	A	Direction OUT	246		
27a39893-a-2e7a-4f09-8f60-51309e10745	RFID SOLD	2021-08-25 10:48:33	GMT	3408328061240104032758A	A	Direction OUT	279		
27366116-0c73-48bf-3278-7fbfe128776	RFID SOLD	2021-08-25 10:48:33	GMT	3408328061240104032758A	A	Direction OUT	710		
c35acee0-5390-4023-a2a2-fcb273309880	RFID UNKNOWN	2021-08-25 10:48:32	GMT	3408328061240104032758A	A	Direction IN			
2b90fd01d-4567-4e98-9e2a-d0f7c15d596	RFID UNKNOWN	2021-08-25 10:48:32	GMT	3408328061240104032758A	A	Direction IN			
f1219065-8d8e-4c0a-477f-842dc3d9e090	RFID SOLD	2021-08-25 10:45:00	GMT	3408328061240104032758A	B	Direction OUT	1277		
c0046590-7475-4b87-b1f6-9c3468623618	RFID SOLD	2021-08-25 10:42:50	GMT	3408328061240104032758A	B	Direction OUT			
f13af50c-f408-4413-8f26-525524fa373	RFID SOLD	2021-08-25 10:42:47	GMT	3408328061240104032758A	B	Direction OUT			
c9d-7779-d4e-4004-bf0b-181b54d00acbf	RFID SOLD	2021-08-25 10:39:44	GMT	3408328061240104032758A	B	Direction IN	1393		
f7350183-ba02-4003-91ab-2b2cedee76484	RFID SOLD	2021-08-25 10:39:39	GMT	7EDA919221100433900003D8	A	Direction OUT	1313		
b2220f8e-c684-404b-a11a-c330d63c111	RFID SOLD	2021-08-25 10:38:47	GMT	7EDA919221100433900003D8	A	Direction OUT	326		
7049348d-1ed4-4e5a-97a0-477973431ed	RFID SOLD	2021-08-25 10:36:30	GMT	7EDA919221100433900003D8	A	Direction OUT	39		
d342f206-40f1-4e84-bc10-42c76915681	RFID SOLD	2021-08-25 10:36:30	GMT	7EDA919221100433900003D8	A	Direction OUT	100		
5d3da1b9-16dc-49de-943f-7949650d2c70	RFID SOLD	2021-08-25 10:36:30	GMT	3408328061240104032758A	A	Direction OUT	221		
112a1e77-9b54-451b-ba10-e929c9c03b4	RFID SOLD	2021-08-25 10:33:28	GMT	7EDA919221100433900003D8	A	Direction OUT	1478		
72554b19-94b6-4e09-b95f-faa0bcbb4cd4d	RFID SOLD	2021-08-25 10:33:28	GMT	7EDA919221100433900003D8	A	Direction OUT	1020		
886eb550-0d8f-415d-8fe1-b51dcb261f	RFID SOLD	2021-08-25 10:31:38	GMT	7EDA919221100433900003D8	A	Direction OUT	339		
2209f134-4351-41e8-8105-1ab6d820ab	RFID SOLD	2021-08-25 10:31:28	GMT	3408328061240104032758A	A	Direction OUT	213		



RFID reader power error

Category

Hardware

Device Management Description

One or more RFID readers cannot reach the set output power.

Device Management Instruction

Replace the RFID reader.

Device Management Notification

no

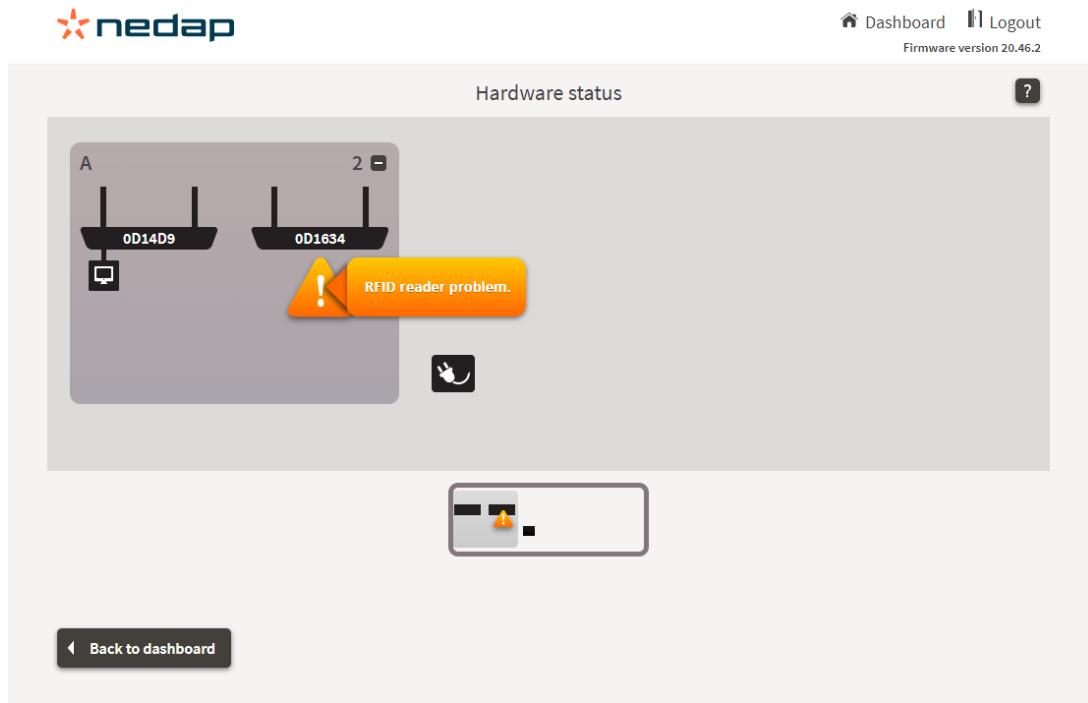
Analytics Issue

Hardware related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff

Nedap Internal Label

RFID_READER_POWER_ERROR

iSense Wizard



The screenshot shows the 'Hardware status' section of the iSense Wizard interface. At the top right are links to 'Dashboard' and 'Logout', and a note about 'Firmware version 20.46.2'. Below this is a title 'Hardware status' and a help icon. The main area displays two reader units labeled 'A' and '2'. Reader 'A' has two ports labeled '0D14D9' and '0D1634', each with a small monitor icon below it. A yellow warning bubble with an exclamation mark is positioned between the two ports, containing the text 'RFID reader problem.' To the right of the ports is a mouse cursor icon. Below the main panel is a smaller summary box with a single port icon and a warning symbol. At the bottom left is a 'Back to dashboard' button.

Hardware status

?

A

0D14D9

0D1634

RFID reader problem.

2

!

Back to dashboard



RFID antenna is not working properly

Category

Hardware

Device Management Description

One or more of the RFID antennas are not working properly.

Device Management Instruction

Make sure all antennas are connected properly and are not damaged.

Device Management Notification

no

Analytics Issue

Hardware related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff

Nedap Internal Label

RFID_ANTEENNA_ERROR

iSense Wizard



The screenshot shows the 'Hardware status' section of the iSense Wizard interface. It displays four antenna units labeled A, B, C, and D, each with a unique identifier below it: 0D60C9, 0D61F0, 0D62CA, and 0D6022 respectively. Unit B has a small monitor icon next to it. A prominent orange warning bubble is centered over unit A, containing the text 'No RFID antenna detected. Please check the cables.' with an exclamation mark icon. Below the main status area is a small navigation bar with a back arrow and the text 'Back to dashboard'.

Hardware status

D 1

C 1

B 1

A 1

0D60C9

0D61F0

0D62CA

0D6022

No RFID antenna detected. Please check the cables.

! 

Back to dashboard



RFID synchronization failed

Category

Hardware

Device Management Description

One or more readers do not receive a synchronization signal.

Device Management Instruction

Check all ethernet cables between the Renos units with an Ethernet cable tester. Check if the Ethernet connectors on the Renos units are loose or damaged. Check the power and sync cable between RFID reader and Renos. If the problem persists, contact Nedap Retail support to help you solve this problem.

Device Management Notification

no

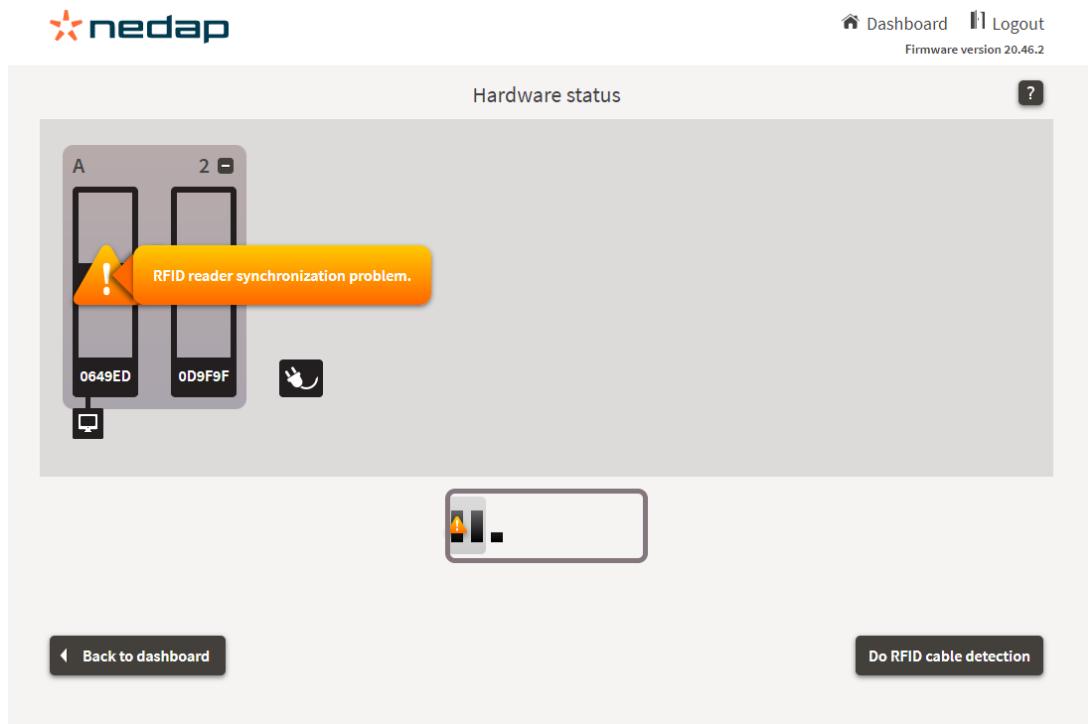
Analytics Issue

Hardware related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff

Nedap Internal Label

RFID_READER_SYNC_ERROR

iSense Wizard



The screenshot shows the 'Hardware status' section of the iSense Wizard interface. At the top right are links for 'Dashboard', 'Logout', and 'Firmware version 20.46.2'. Below that is a 'Hardware status' header with a question mark icon. The main area displays two reader units labeled 'A' and '2'. Reader 'A' has an orange warning icon and the message 'RFID reader synchronization problem.' It also shows the MAC addresses '0649ED' and '0D9F9F'. A small mouse cursor icon is positioned next to the second reader. At the bottom are two buttons: 'Back to dashboard' and 'Do RFID cable detection'.



RFID reader connection problem

Category

Hardware

Device Management Description

Not all RFID readers are connected properly.

Device Management Instruction

Make sure all RFID readers are connected properly to the system, with both power and USB. Check lights on the RFID reader. If this does not resolve the issue, replace and RMA.

Device Management Notification

no

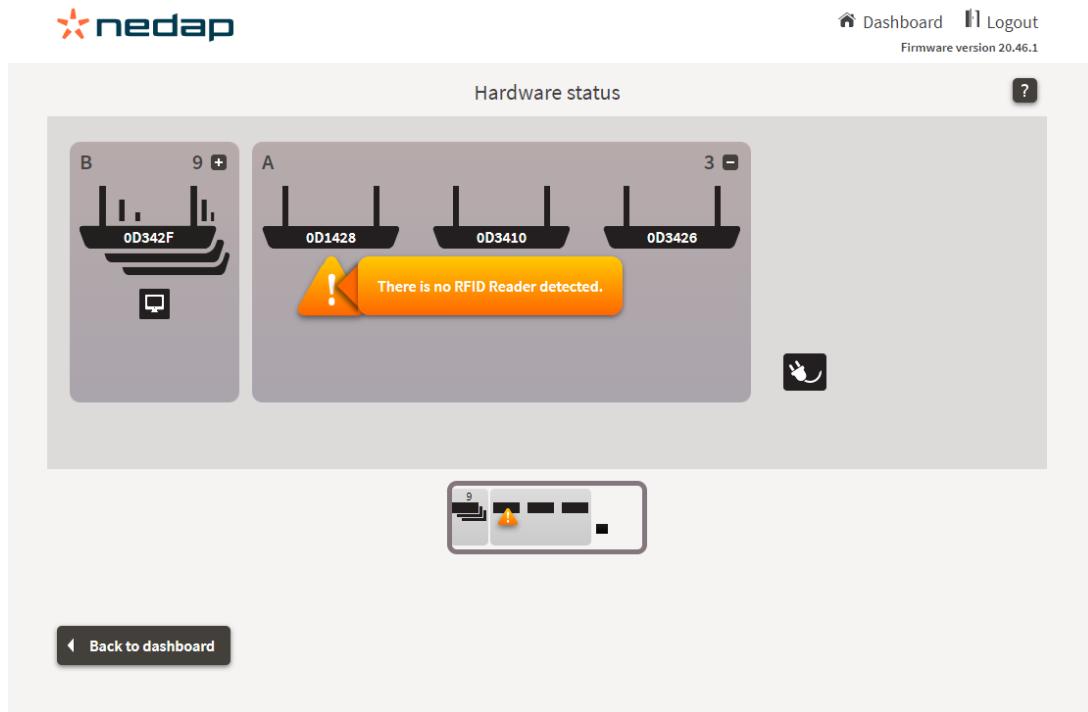
Analytics Issue

Hardware related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff

Nedap Internal Label

RFID_READER_CONNECTED

iSense Wizard



The screenshot shows the 'Hardware status' section of the iSense Wizard interface. At the top right are links for 'Dashboard' and 'Logout', and a note about 'Firmware version 20.46.1'. Below this is a question mark icon.

The main area displays two sections: 'B' and 'A'. Section 'B' contains a single device labeled '0D342F'. Section 'A' contains three devices labeled '0D1428', '0D3410', and '0D3426'. A yellow warning box with an exclamation mark is centered over section 'A', stating 'There is no RFID Reader detected.' To the right of section 'A' is a small mouse icon.

At the bottom left is a 'Back to dashboard' button with a back arrow icon. In the center is a small summary icon showing a 9-reader setup with one reader highlighted in orange.



RFID false alarms suspected

Category

Configuration

Device Management Description

The same RFID label is generating multiple alarms over a long stretch of time.

Device Management Instruction

Remove RFID labels too close to the system. Change the power and filtering settings of the system.

Device Management Notification

yes

Timing

Issue is shown after 0 to 180 minutes

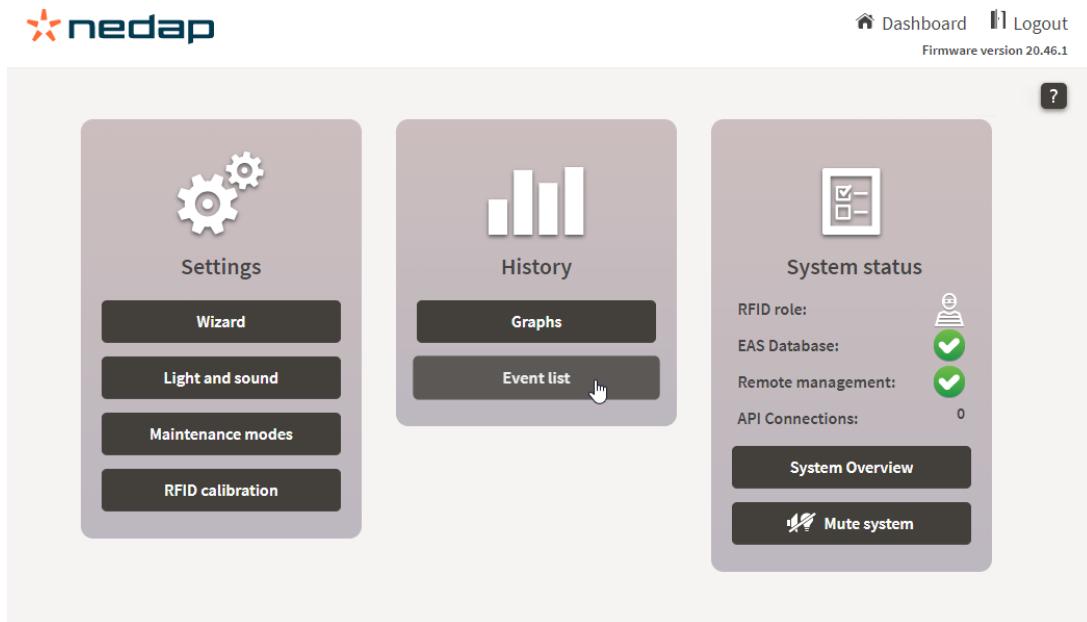
Analytics Issue

Configuration related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff

Nedap Internal Label

SUSPECTED_FALSE_ALARMS

iSense Wizard



This issue is raised whenever tags seen in the past 24 hours have given more than 50 alarms in the past 3 hours. So this can be 1 tag seen 50 times or 25 tags each seen 2 times in this time window.

This issue can be examined by entering the **Event list** page. Try to find what tags are causing this issue, like tags in the shop window or otherwise nearby the installation and hotspots.

Downloading the event list and loading it into Excel can help the debugging process also.

Event history

?

[Download events](#)

Type	Dir	Time	Description	Group
?		1 minute ago	30340BB6403CE390E4ACE801	B
?		1 minute ago	30340BB6403CE390E4ACE801	B
?		1 minute ago	30340BB6403CE390E4ACE801	B
?		1 minute ago	30340BB6403CE390E4ACE801	B
?		1 minute ago	30340BB6403CE390E4ACE801	B
?		1 minute ago	30395DFA82F8E440001D413B	B
?		1 minute ago	3039606203C6964000085793	A
?		1 minute ago	30340BB6403CE390E4ACE801	B
?		1 minute ago	30396062436847800019941C	B
?		1 minute ago	30396062436DB200000A21C4	A
?		1 minute ago	303960624369E9C000094614	A

- Visible events:
- Sold EPCs 
 - RFID alarms 
 - Foreign EPCs 
 - Unknown EPCs 
 - Incoming customers 
 - Outgoing customers 
 - Metal detection 
 - Config changes 

[Back to dashboard](#)



RFID reader disabled

Category

Configuration

Device Management Description

One or more RFID readers are disabled.

Device Management Instruction

Enable the RFID reader through the iSense API or the configuration interface.

Device Management Notification

no

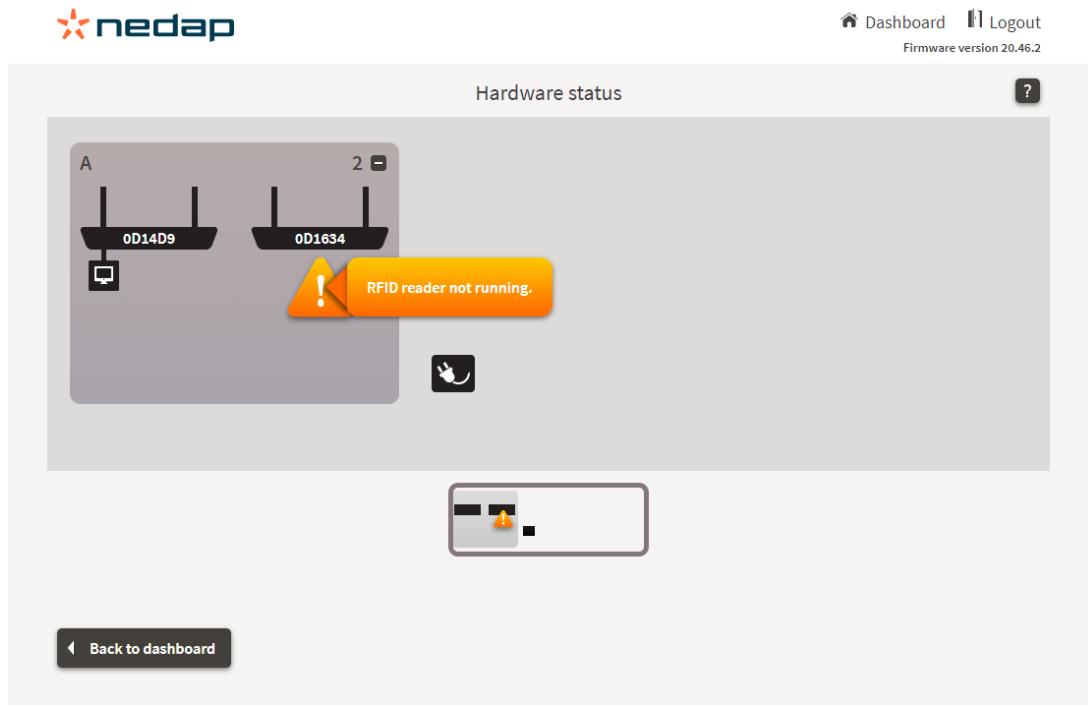
Analytics Issue

Configuration related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff

Nedap Internal Label

RFID_READER_RUNNING

iSense Wizard



The screenshot shows the 'Hardware status' section of the iSense Wizard interface. At the top, there are navigation links: 'Dashboard' (with a house icon), 'Logout' (with a user icon), and 'Firmware version 20.46.2'. Below the navigation is a title 'Hardware status' and a help icon (a question mark in a box).

The main area displays two sensor units labeled 'A' and '2'. Unit 'A' contains two readers labeled '0D14D9' and '0D1634'. A yellow warning box with an exclamation mark is overlaid on the first reader, containing the text 'RFID reader not running.' A small mouse cursor icon is positioned near the bottom right of the warning box.

Below the main area is a summary box with a warning icon, indicating a system issue. At the bottom left is a 'Back to dashboard' button with a back arrow icon.

RFID units are muted

Category

Configuration

Device Management Description

One or more units have been muted and will be operating quietly.

Device Management Instruction

Unmute the units

Device Management Notification

yes

Timing

Issue is shown after 0 to 5 minutes

Analytics Issue

System (partially) muted, contact the local Business Partner (installer)

Nedap Internal Label

MUTING_STATUS

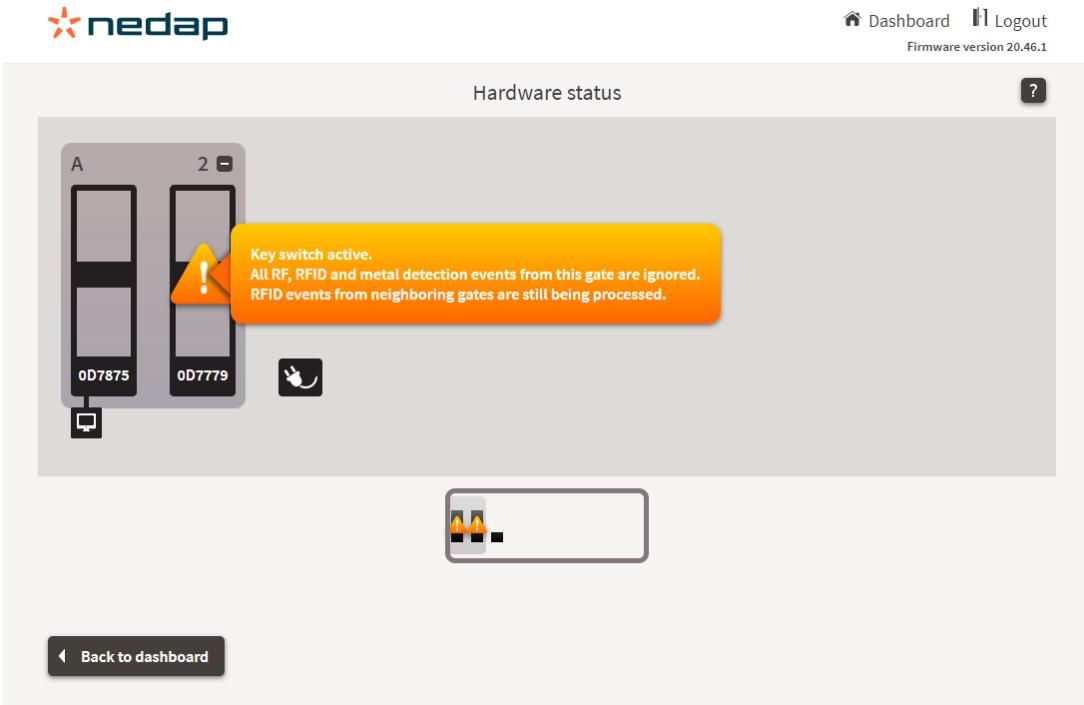
iSense Wizard

This issue can have several causes, to be more precise, 7 different reason for this issue, but not all are visible in DM:

1. disabled by a key switch
2. disabled by an IO box (not shown in DM)
3. disabled by an API integration (not shown in DM)
4. muted manually through the Technical Dashboard
5. muted by an IO box
6. muted by an API integration
7. muted through the iSense Dashboard (aka snoozing)

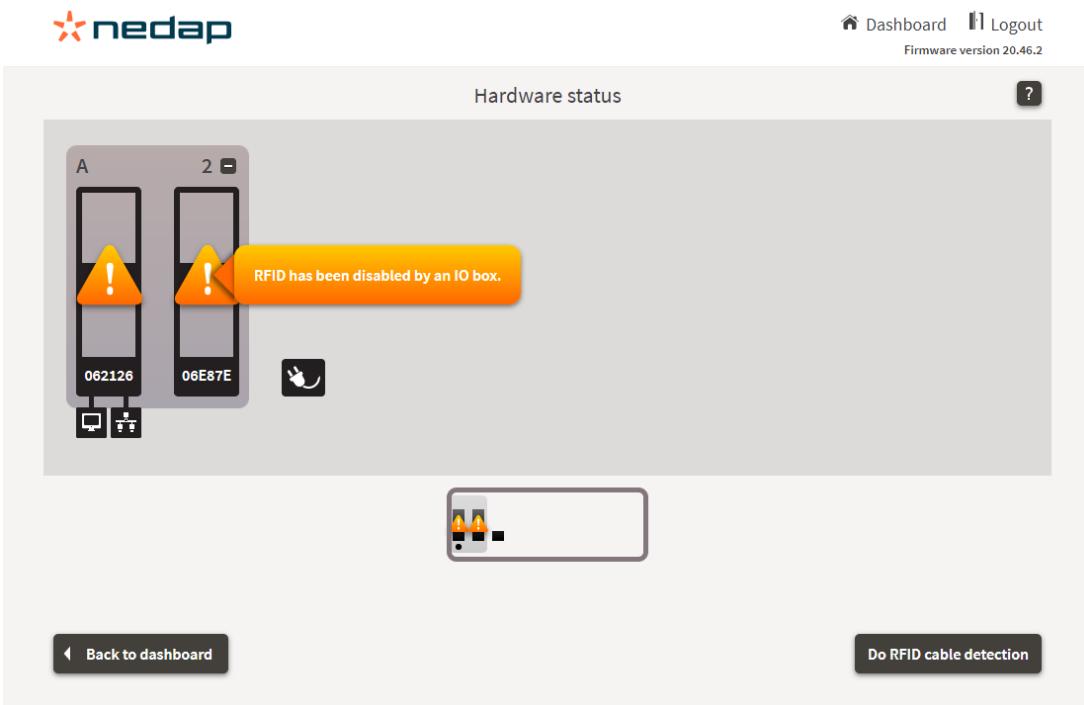
The first 3 will be shown in the **System Overview** page, the last 4 in the **Light and Sound** page.

1. A key switch is placed in the active position.



The screenshot shows the 'Hardware status' section of the nedap software. It displays two gate panels labeled 'A' and '2'. The first panel has a key switch icon with an exclamation mark, indicating it is active. A yellow callout bubble with an exclamation mark says: 'Key switch active. All RF, RFID and metal detection events from this gate are ignored. RFID events from neighboring gates are still being processed.' The second panel shows a standard key switch icon. Below the panels is a small graphic of two doors. At the bottom left is a 'Back to dashboard' button, and at the bottom right is a question mark icon.

2. An IO box has a disabled RFID functionality (not shown in DM).



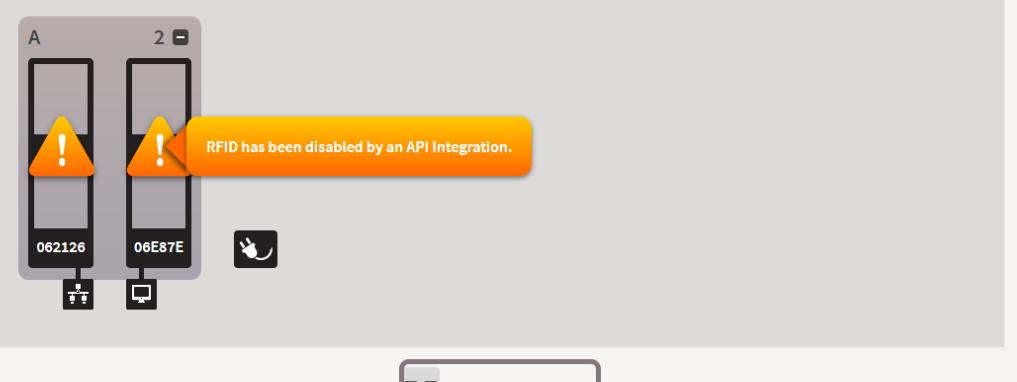
The screenshot shows the 'Hardware status' section of the nedap software. It displays two gate panels labeled 'A' and '2'. Both panels have key switch icons with exclamation marks, indicating they are active. A yellow callout bubble with an exclamation mark says: 'RFID has been disabled by an IO box.' The second panel also has a key switch icon with an exclamation mark. Below the panels is a small graphic of two doors. At the bottom left is a 'Back to dashboard' button, and at the bottom right is a 'Do RFID cable detection' button.

3. The RFID functionality is disabled by an API integration (not shown in DM).

nedap

Dashboard Logout
Firmware version 20.46.2

Hardware status



RFID has been disabled by an API Integration.

Back to dashboard Do RFID cable detection

This next 3 issues are visible by going to the **Light and sound** page.

nedap

Dashboard Logout
Firmware version 20.46.2

Advanced settings ?



Settings

- Wizard
- Light and sound**
- Maintenance modes
- RFID calibration
- Gate names
- RF config



History

- Graphs
- Event list



System status

RFID role:	
EAS Database:	
Remote management:	
External CC status:	
API Connections:	0

System Overview

Mute system

4. Light and sound are muted manually.

Light and sound

?

Group B: SALIDA

B

RF alarm    -

RFID alarm    -

Sound volume  65%

0D99A5 0D99B0

?

Back to dashboard



5. Light and sound are turned off by an IO box.

Light and sound

?

Group A: test

A

RF alarm   -

RFID alarm     RFID light and sound are turned off by an IO box.

Sound volume  65%

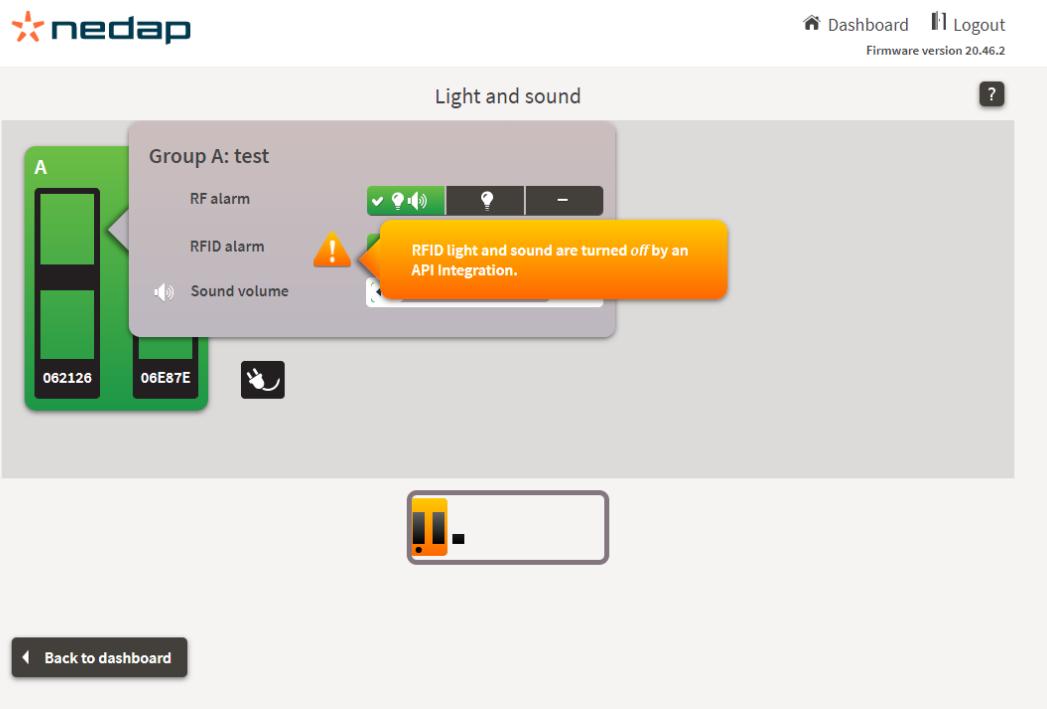
062126 06E87E

?

Back to dashboard



6. Light and sound are turned off by an API integration.



Light and sound

Group A: test

RF alarm

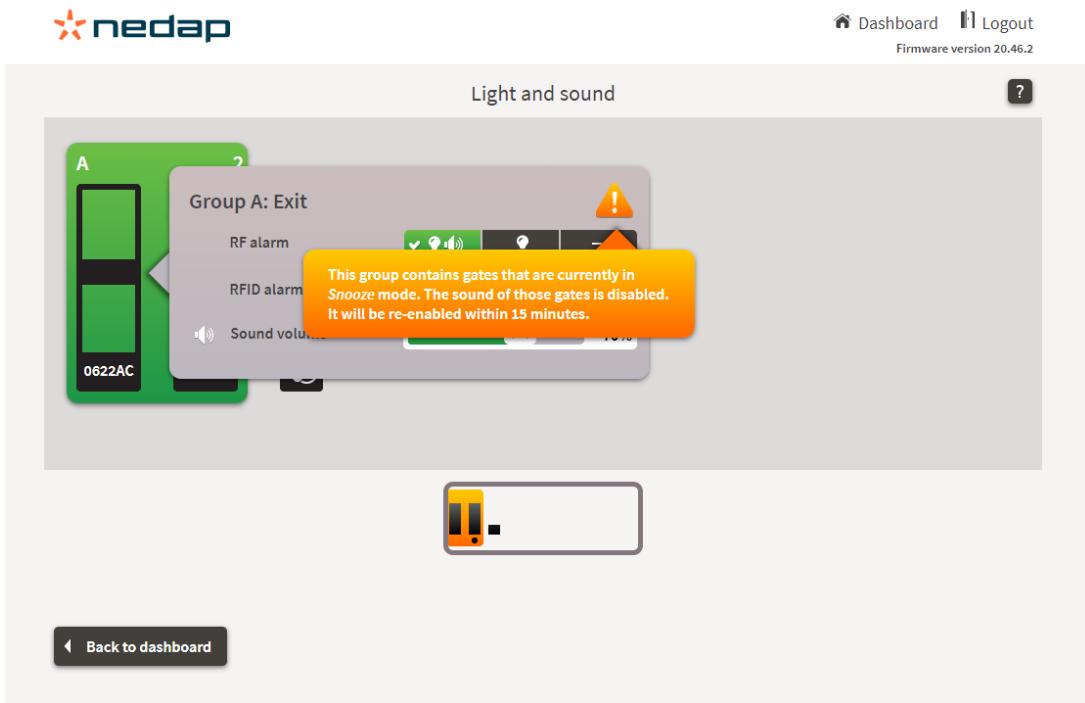
RFID alarm

Sound volume

RFID light and sound are turned off by an API Integration.

Back to dashboard

7. The retailer snoozes a unit from within the iSense Dashboard.



Light and sound

Group A: Exit

RF alarm

RFID alarm

Sound volume

This group contains gates that are currently in Snooze mode. The sound of those gates is disabled. It will be re-enabled within 15 minutes.

Back to dashboard

When a system is muted from within DM, it will be shown in the wizard as an API mute option.

e2690a60-a6fc-4d38-84ce-be9c438dc4f0 renos

beta Change muting status for e2690a60-a6fc-4d38-84ce-be9c438dc4f0

System mute setting  

System RFID mute setting   

Muting depends on a stable internet connection of the iSense system. Not every mute type can be disabled remotely via Device Management.

RF and RFID muting are shown as muted through API integration in the iSense dashboard.

[Cancel](#)

<input type="checkbox"/> RF	<input checked="" type="radio"/> disabled	EAS Protocol	Custom EPC prefixes
<input type="checkbox"/> RFID	<input checked="" type="radio"/> enabled	MAC Address	00:0D:A0:06:73:BD

Remote service  [\(Un\)mute system](#)



Units in RFID maintenance mode

Category

Configuration

Device Management Description

One or more units have been disabled by a technician because of RFID issues.

Device Management Instruction

Investigate and solve the RFID issues and undo Maintenance Mode to re-enable RFID functionality.

Device Management Notification

yes

Timing

Issue is shown after 0 to 5 minutes

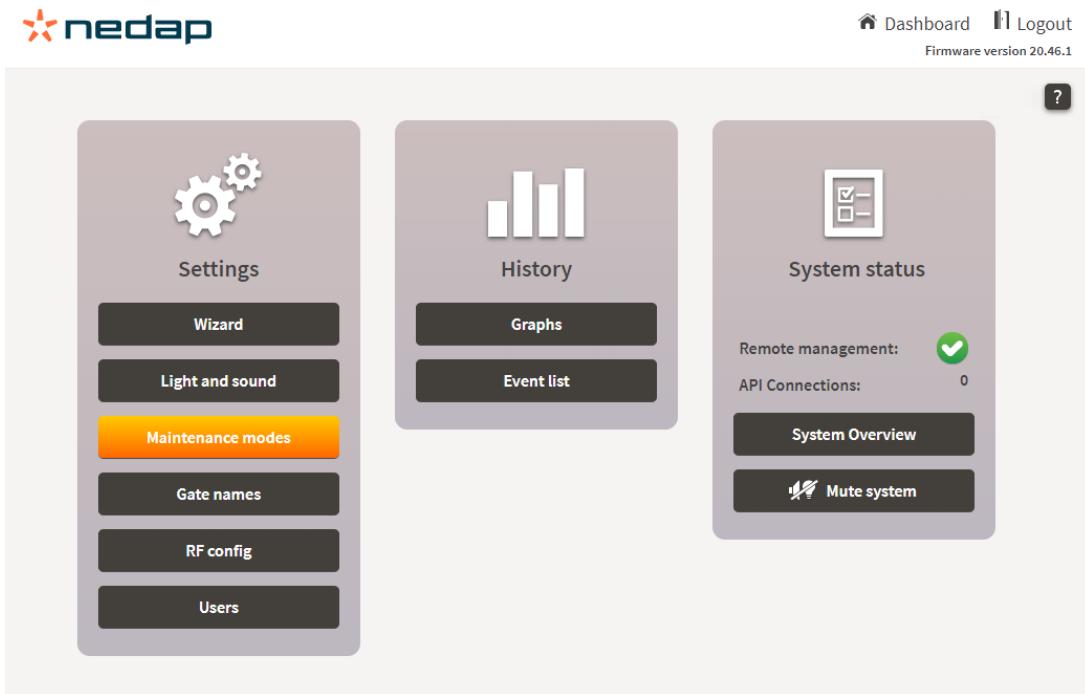
Analytics Issue

Configuration related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff

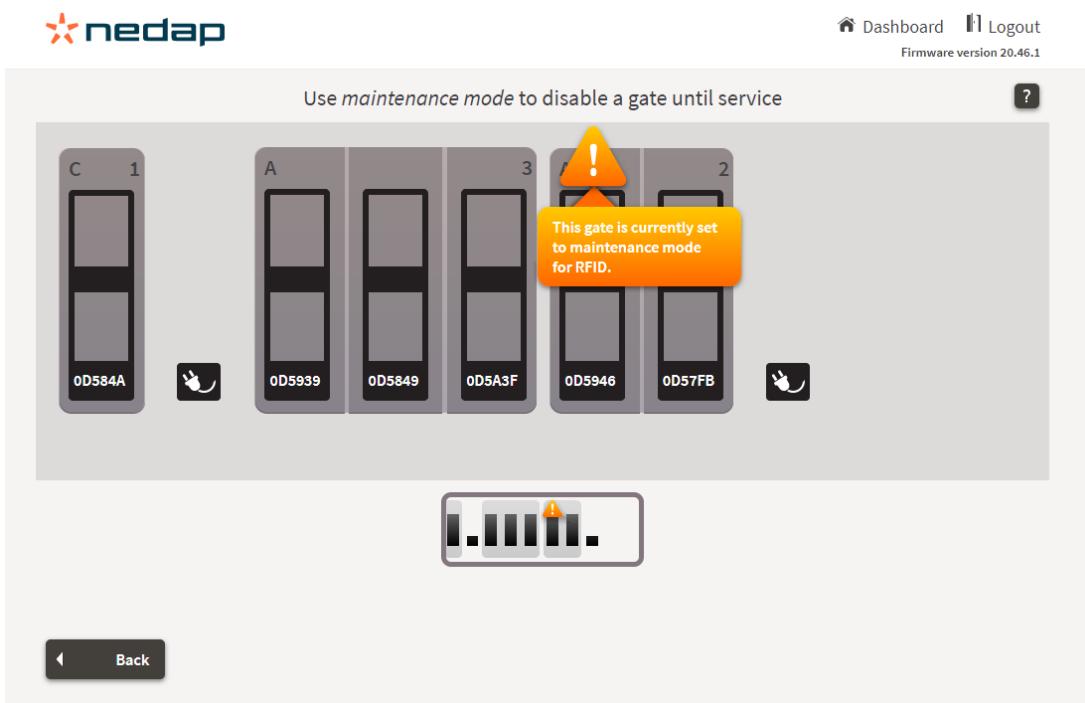
Nedap Internal Label

RFID_MAINTENANCE_MODE

iSense Wizard



This issue is visible by going to the **Maintenance modes** page, where you also can turn off the maintenance mode. It is important to check why this mode was added and to fix the underlying issue.



Customer Counting Issues

Infrared beam sensors blocked

Category

Health

Device Management Description

One or more of the infrared beam sensors are blocked by an object.

Device Management Instruction

Remove the object between the sensors.

Device Management Notification

yes

Timing

Issue is shown after 0 to 5 minutes

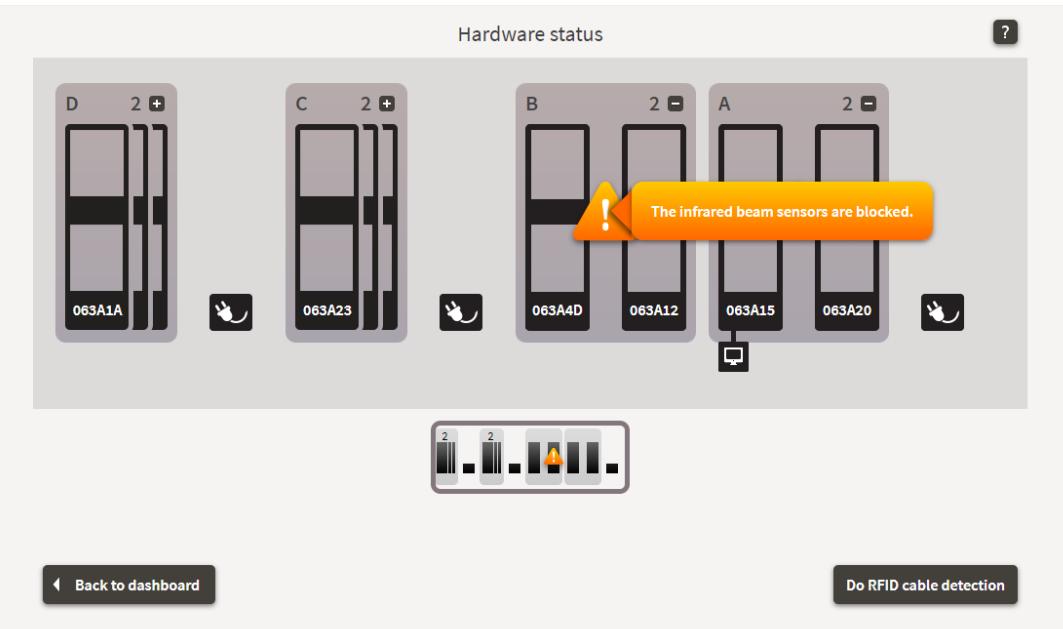
Analytics Issue

Customer Counting System (partially) interrupted, remove blocking objects, otherwise contact the local Business Partner (installer)

Nedap Internal Label

DIRECTION_SENSORS_BLOCKED

iSense Wizard



The screenshot shows the iSense Wizard interface. At the top right are links for "Dashboard", "Logout", and "Firmware version 20.46.2". Below that is a section titled "Hardware status" with four groups labeled D, C, B, and A. Each group contains two antenna icons. Group B has a yellow warning box with an exclamation mark and the text "The infrared beam sensors are blocked.". At the bottom are buttons for "Back to dashboard" and "Do RFID cable detection".

Lumen systems will remove this warning once the block is removed. Non-Lumen systems must see a customer's movement before detecting that the block has been removed.

Blocking can occur due to garments placed between two adjacent antennas, a misaligned advertising panel, or misaligned antennas.



Infrared beam sensors not connected

Category

Hardware

Device Management Description

One or more of the infrared beam sensors are not connected properly.

Device Management Instruction

Make sure that the cables connecting the direction sensors to the system are not damaged and connected properly.

Device Management Notification

no

Analytics Issue

Hardware related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff

Nedap Internal Label

DIRECTION_SENSORS_CONNECTED

iSense Wizard



The screenshot shows the iSense Wizard interface. At the top right are links for "Dashboard" and "Logout", and a note about "Firmware version 20.46.1". Below this is a "Hardware status" section. It displays two sections, A and B, each with three units labeled 062DC1, 062DC3, and 062DC5. In section A, the middle unit (062DC3) has a yellow warning icon with an exclamation mark and the text "Customer counter connection problem.". There are also small icons for a computer mouse and a monitor next to the units. At the bottom left is a "Back to dashboard" button.

Hardware status

B

062DC7 062DCB

3 062DC3

A 062DC1 062DC5

Customer counter connection problem.

062DC7 062DCB

3 062DC3

2 062DC5

?

Customer counter connection problem.

Back to dashboard

Signaling hardware issue

Category

Hardware

Device Management Description

One or more units have an issue with their signaling hardware. Light, sound and infrared direction detection might not work.

Device Management Instruction

Make sure the signaling hardware is properly connected to Renos in every unit.

Device Management Notification

no

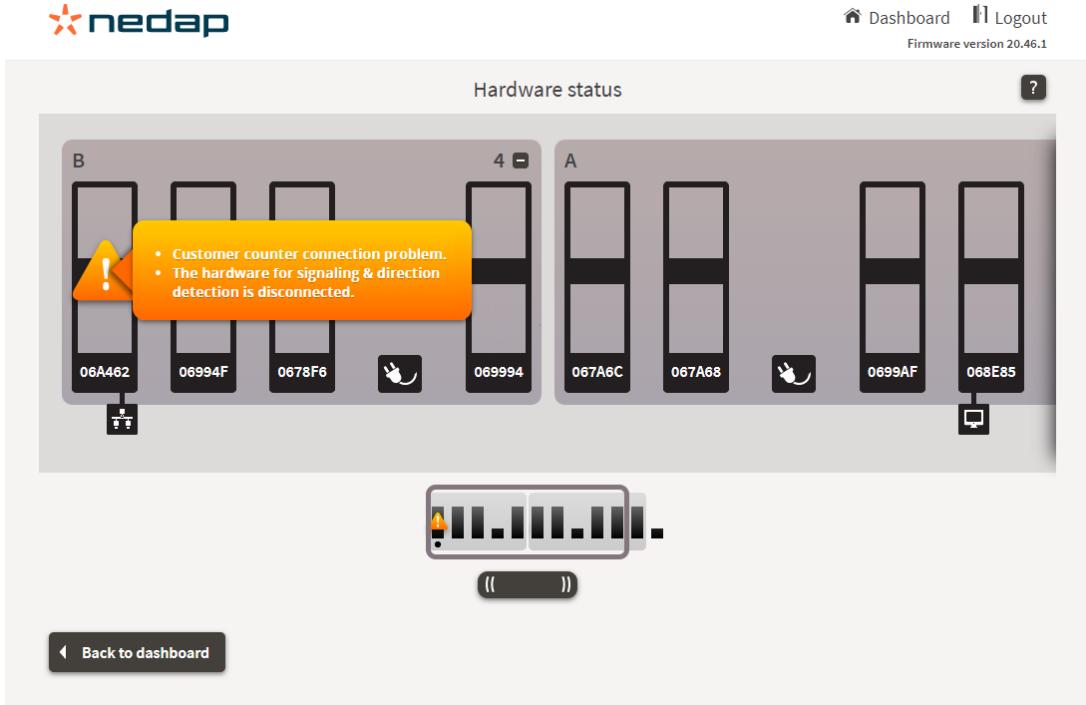
Analytics Issue

Hardware related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff

Nedap Internal Label

AVCC_HARDWARE_ISSUE

iSense Wizard



The screenshot shows the 'Hardware status' section of the iSense Wizard interface. It displays two panels, labeled A and B, each containing four antenna slots. Panel A has slots 067A6C, 067A68, 0699AF, and 068E85. Panel B has slots 06A462, 06994F, 0678F6, and 069994. Each slot is represented by a vertical bar with a small icon at the bottom. A yellow warning box is overlaid on panel B, containing the following text:

- Customer counter connection problem.
- The hardware for signaling & direction detection is disconnected.

At the bottom of the screen, there is a navigation bar with a 'Back to dashboard' button and a set of arrows indicating the ability to switch between different hardware configurations.

This issue is only available for Lumen antennas.

External Customer Counting Issues

No data from external customer counter

Category

Integration

Device Management Description

The system did not receive data from one or more external customer counters.

Device Management Instruction

Access remote service to see which external counter is having issues. Make sure the external counters are powered and can communicate with the Renos system.

Device Management Notification

no

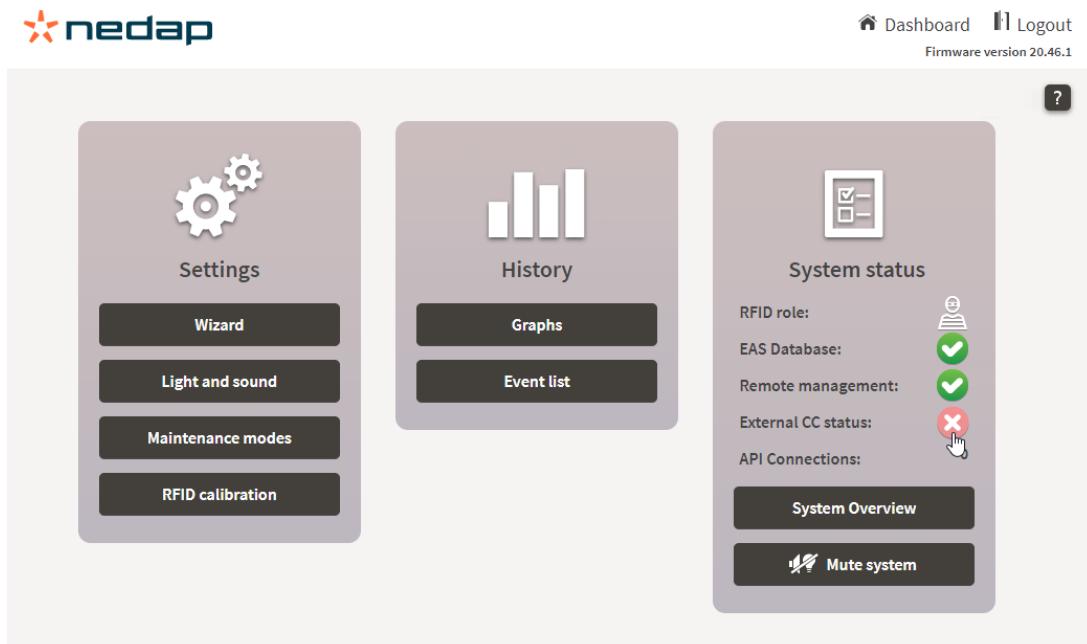
Analytics Issue

Integration related issues, to be investigated by the local Business Partner (installer)

Nedap Internal Label

EXTERNAL_CC_NO_DATA

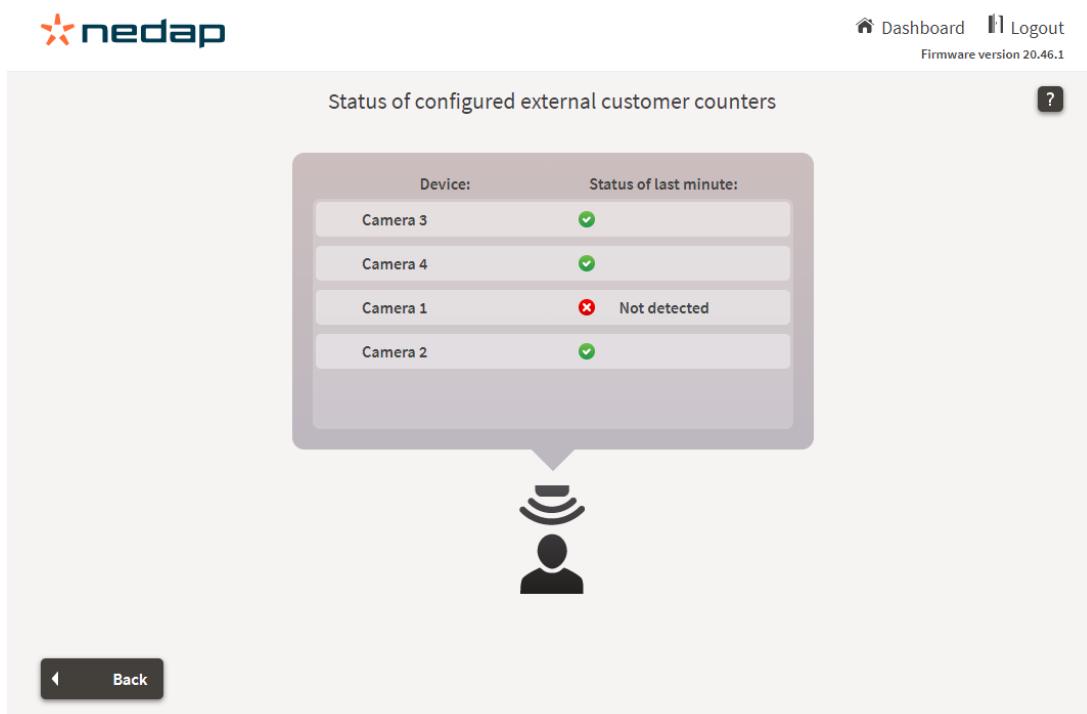
iSense Wizard



The dashboard screen displays three main sections:

- Settings**: Contains buttons for "Wizard", "Light and sound", "Maintenance modes", and "RFID calibration".
- History**: Contains buttons for "Graphs" and "Event list".
- System status**: Shows the following status indicators:
 - RFID role: (green checkmark)
 - EAS Database: (green checkmark)
 - Remote management: (green checkmark)
 - External CC status: (red cross)
 - API Connections: (hand cursor icon over a red circle)Buttons for "System Overview" and "Mute system" are also present.

Press the **red cross** icon to get details of this issue. In general this is an IT issue in the store.



The screen shows the "Status of configured external customer counters" with the following data:

Device:	Status of last minute:
Camera 3	✓
Camera 4	✓
Camera 1	✗ Not detected
Camera 2	✓

A large speech bubble points from the "Not detected" status of Camera 1 towards a camera icon at the bottom center.

At the bottom left, there is a "Back" button.

Metal Detection Issues

Metal detectors disconnected

Category

Hardware

Device Management Description

Not all metal detectors are connected properly.

Device Management Instruction

Make sure the metal detectors are powered and that the USB-cables between the metal detectors and the systems are connected properly.

Device Management Notification

no

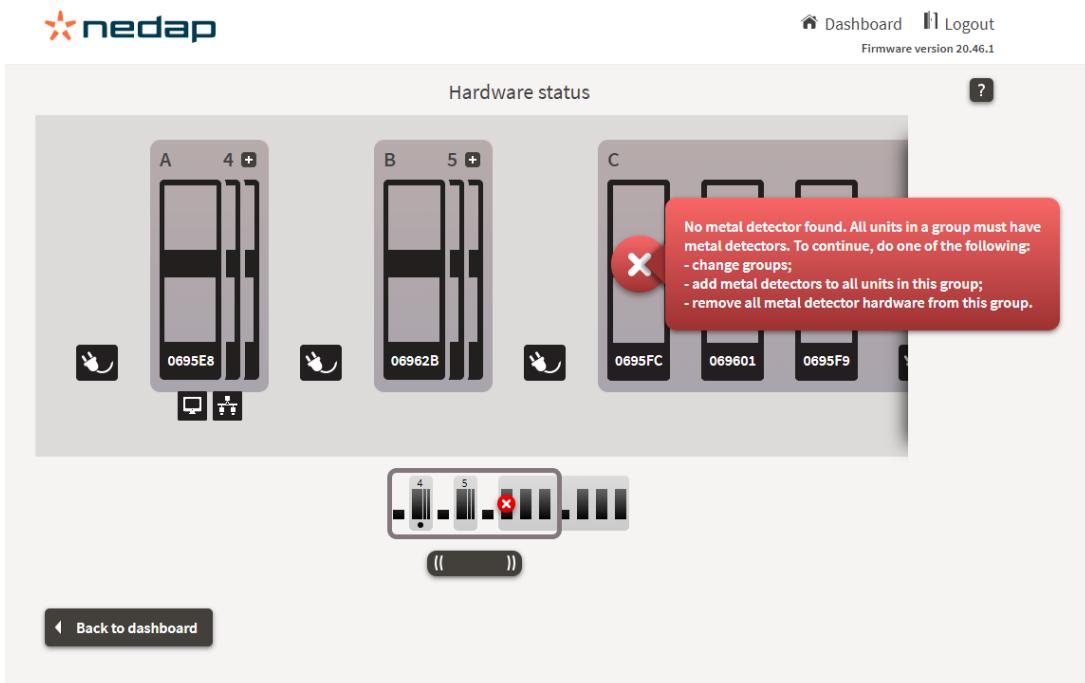
Analytics Issue

Hardware related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff

Nedap Internal Label

METAL_DETECTION_CONNECTED

iSense Wizard



Metal detection coupling issues

Category

Hardware

Device Management Description

One or more metal detectors are experiencing coupling issues and do not function.

Device Management Instruction

Check the cables of both the receiving and the transmitting metal detectors. When large metal objects have been (permanently) moved into, or removed from the environment, reconfigure metal detection.

Device Management Notification

no

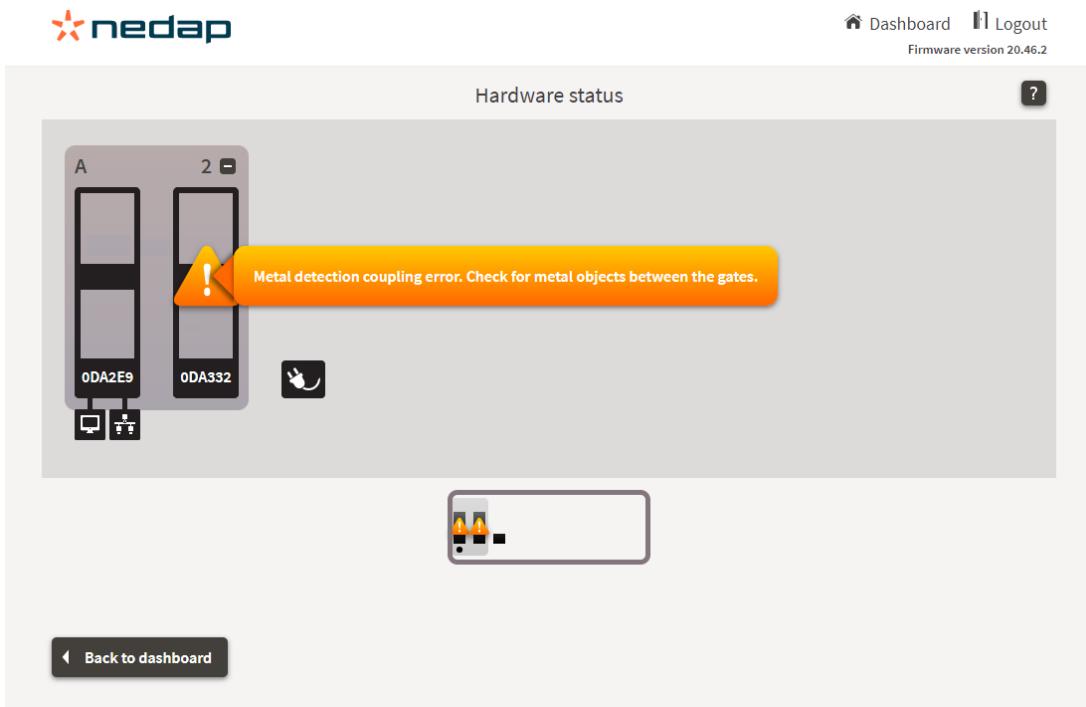
Analytics Issue

Hardware related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff

Nedap Internal Label

METAL_DETECTION_COUPLING

iSense Wizard



The screenshot shows the Nedap iSense Wizard interface. At the top, there's a navigation bar with the nedap logo, a Dashboard link, a Logout link, and a Firmware version 20.46.2 notice. Below the navigation is a section titled "Hardware status". On the left, there's a diagram of two metal detection units labeled "A" and "2" with ports numbered 1 through 4. Unit A has a port labeled "ODA2E9" and unit 2 has a port labeled "ODA332". A yellow warning icon with an exclamation mark is positioned between the two units. An orange callout bubble contains the text: "Metal detection coupling error. Check for metal objects between the gates." To the right of the units is a small hand cursor icon. At the bottom of the "Hardware status" section is a small rectangular icon containing two orange and black symbols. At the very bottom of the screen is a dark button with the text "Back to dashboard" and a left arrow icon.

Metal detection is disturbed when this issue is active. The receiving Metal Detection unit is showing this error. Keep in mind that the issue also might be related to the transmitter Metal Detection unit, so another unit than the unit that is reporting the issue.

IO Box Issues

IO box disconnected

Category

Hardware

Device Management Description

One or more IO boxes are disconnected.

Device Management Instruction

Check if the IO box is connected to Renos and if it is powered.

Device Management Notification

yes

Timing

Issue is shown after 0 to 5 minutes

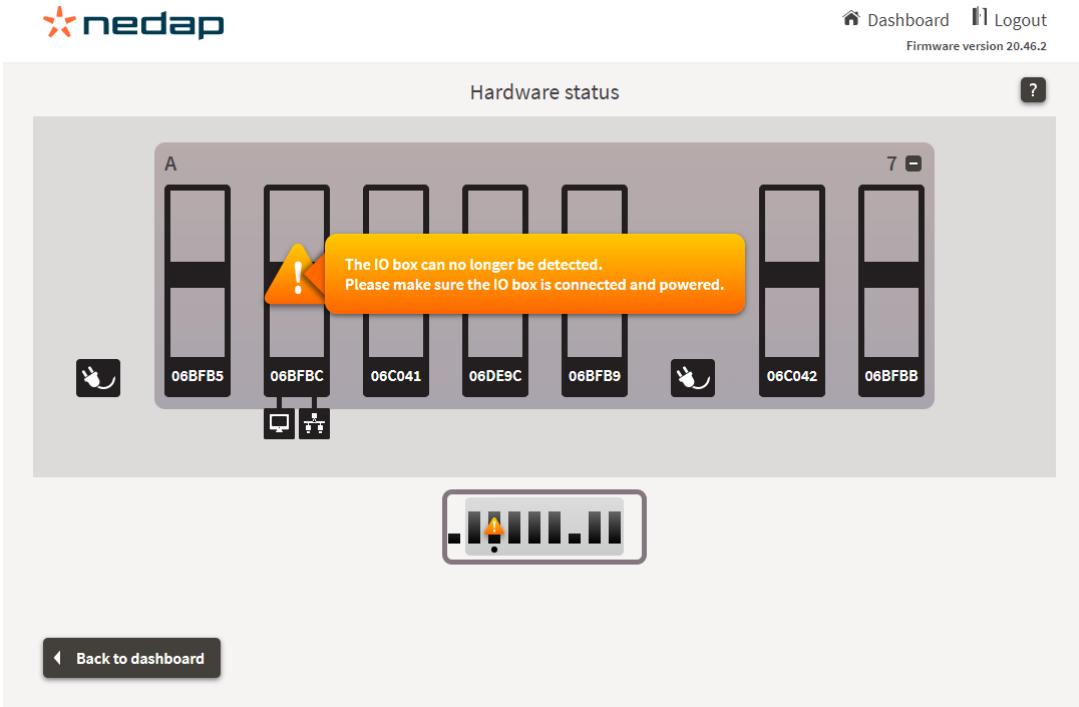
Analytics Issue

Hardware related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff

Nedap Internal Label

IO_BOX_CONNECTED

iSense Wizard



The screenshot shows the 'Hardware status' section of the iSense Wizard interface. It displays a grid of 14 slots labeled A through T. The first slot (A1) contains a warning message: 'The IO box can no longer be detected. Please make sure the IO box is connected and powered.' Below the grid is a small bar chart with an orange flame icon at the top.

Hardware status

A 7

06BF85 06BFBC 06C041 06DE9C 06BF89 06C042 06BFBB

! The IO box can no longer be detected.
Please make sure the IO box is connected and powered.

Back to dashboard

If an IO box is disconnected, the integrations built with it will no longer work and RF, RFID or MD may be muted or disabled until fixed.

OST Integration Issues

OST not connected

Category

Network

Device Management Description

OST is not connected.

Device Management Instruction

Check the cabling between the Renos system and the OST unit.

Device Management Notification

no

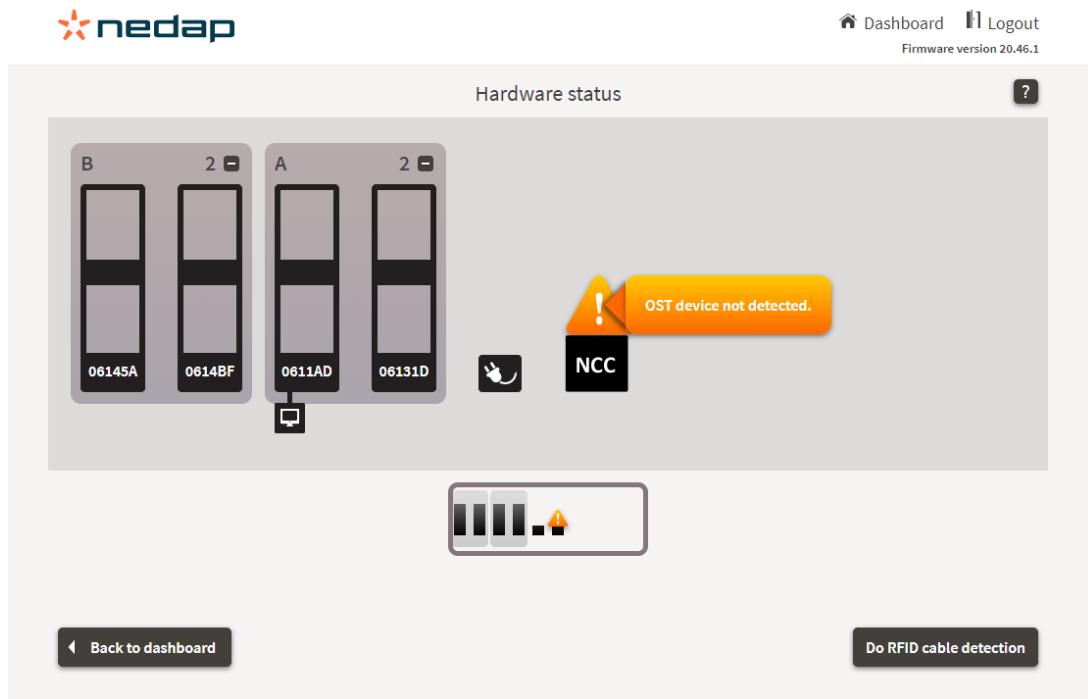
Analytics Issue

Network related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff

Nedap Internal Label

OST_CONNECTED

iSense Wizard



Hardware status

B 2

2

06145A 0614BF

A 2

2

0611AD 06131D

OST device not detected.

NCC

Back to dashboard

Do RFID cable detection

System Issues

Units inactive

Category

Hardware

Device Management Description

One or more units are not active.

Device Management Instruction

Check if all units are properly connected and switched on.

Device Management Notification

yes

Timing

Issue is shown after 0 to 5 minutes

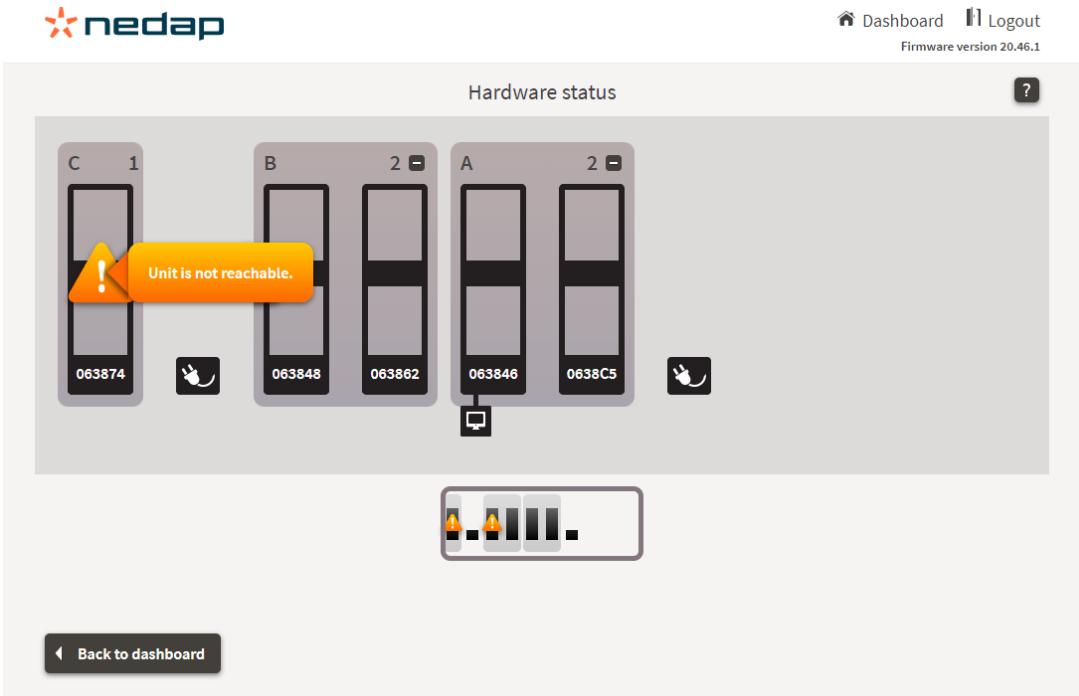
Analytics Issue

System (partially) interrupted, check all power cables, otherwise contact the local Business Partner (installer)

Nedap Internal Label

ALL_UNITS_ACTIVE

iSense Wizard



The screenshot shows the iSense Wizard interface. At the top right, there are links for 'Dashboard', 'Logout', and 'Firmware version 20.46.1'. Below the header is a section titled 'Hardware status' containing three rows of units labeled A, B, and C. Each row has two units. Unit C1 has a yellow warning icon with the text 'Unit is not reachable.' A small mouse cursor icon is positioned next to each unit. Below the hardware status is a bar chart with five segments, where the first two are orange (warning) and the others are grey (normal). At the bottom left is a 'Back to dashboard' button.

The consequence of a system with inactive units is that the behavior of the system is undefined. In the best case scenario, only the device that is inactive cannot work.

If all units following a Power Inserter are not reachable, this Power Inserter may no longer be powered. Perhaps someone from the staff in the store can check this.

The next step could be a power cycle. Maybe someone from the staff in the store can do this.

If that doesn't resolve either, a store visit is inevitable.

Defective cables, Power Inserters or iSense units can cause this issue.



Not connected to Device Management

Category

Network

Device Management Description

The system is not able to connect to Device Management. The Internet connection may be down.

Device Management Instruction

Check the Internet connections and make sure the system has been configured properly.

Device Management Notification

yes

Timing

Issue is shown after 30 minutes

Analytics Issue

System is offline since {timestamp} (UTC), check power cables and network connection, otherwise contact the local Business Partner (installer)

Nedap Internal Label

ONLINE

iSense Wizard



[Dashboard](#) [Logout](#)
Firmware version 20.46.2

No connection to the Nedap server is available, select a device with internet to login with



This laptop



Smartphone
or tablet



Other devices



[Continue](#) ➔



Key switch active

Category

Configuration

Device Management Description

Key switch active on one or more gates. No RF, RFID or MD alarms will be raised.

Device Management Instruction

Toggle the key switch to re-enable alarms.

Device Management Notification

yes

Timing

Issue is shown after 0 to 5 minutes

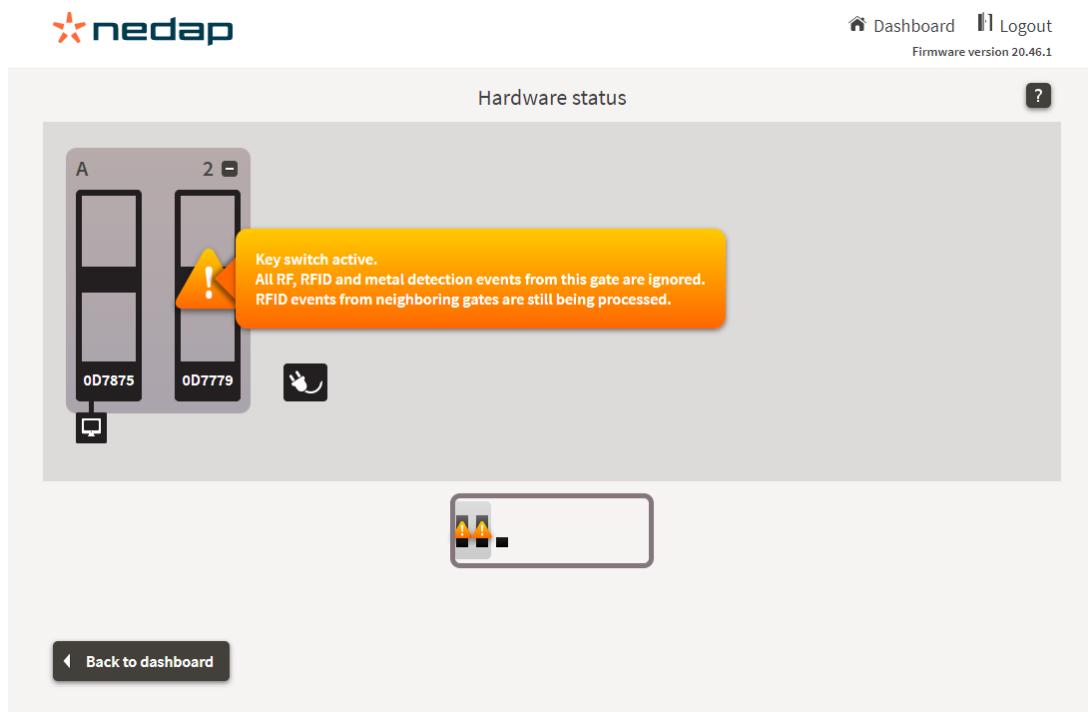
Analytics Issue

Configuration related issues, to be investigated by the local Business Partner (installer), some may be resolved by in-store staff

Nedap Internal Label

KEYSWITCH_ACTIVE

iSense Wizard



The screenshot shows the 'Hardware status' section of the iSense Wizard interface. On the left, there's a diagram of a gate labeled 'A' with two doors, each with an RFID card icon below it: '0D7875' and '0D7779'. To the right of the doors is a yellow warning bubble containing the text: 'Key switch active. All RF, RFID and metal detection events from this gate are ignored. RFID events from neighboring gates are still being processed.' Below the doors is a small hand cursor icon. In the center, there's a small rectangular icon with three orange lights and a black square. At the bottom left, there's a 'Back to dashboard' button with a left arrow icon.

Status

iSense system is in sleep mode

Category

None

Device Management Description

The iSense system has been set to sleep mode, reducing its power consumption by disabling RF/RFID detection.

Device Management Instruction

Check if sleep mode is desired. By default the system will automatically get out of sleep mode on the configured time. Otherwise reboot the system.

Device Management Notification

no

Analytics Issue

None

Nedap Internal Label

SLEEP_MODE_ACTIVE

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Document Version 182

Document Last modification date 9 September 2024

Document PDF Exported 2 October 2024 **by** Nedap Retail | Operations

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.



support-retail@nedap.com



Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com

Nedap Sense Guideline

iSense Online Services Network Information

version 161, October 2024

Introduction	3
Monitoring	4
Remote Service	4
Technical operation	5
iSense System	5
Device Management Servers	5
Using a proxy to access the internet.....	8
Data exchange	9
How to connect the system to the internet	10
Other network connections	11
API	11
SNMP	11
Receiving reports via (S)FTP	11
Security information	13

Introduction

Nedap Retail systems can be connected to the online Device Management platform to ensure they can be managed remotely and work optimally worldwide.

The Nedap Device Management service provides four main functions on system level:

- **Monitoring:** Critical system parameters are monitored 24/7. If a system has issues, an alert is generated and sent to the supporting partner.
- **Remote Service:** Through the Device Management website, an authorized Nedap-certified engineer can access the system's user interface to make changes to the configuration or access system logs.
- **Firmware Update:** The Device Management website allows an authorized Nedap-certified engineer to install new firmware releases remotely.
- **Data Collection:** events per system are collected (e.g., to be displayed in the Analytics platform).

Real-time data

As of firmware version 19.09, real-time data delivery has been added, which means that the alarm and customer events per aisle are stored.

This document describes essential IT information related to the Nedap Retail systems and online environment.



Monitoring

The status of each system is continuously monitored and transmitted to the Device Management server.

The following items are monitored:

- Whether the system is connected to the Device Management server.
- Whether all units in the system are up and running.
- Whether API connections with a system integrator are still present - when applicable.
- Whether all cables between all units are connected properly.
- Complete system status based on several metrics (e.g., False alarms suspected, RFID reader status, etc.)

Remote Service

An authorized Nedap-certified engineer can access a system's configuration interface via the Device Management website/server. This allows the engineer to monitor the system and change settings when needed.

Authorization is only granted to Nedap-certified engineers who can provide service to the system. Authorization can be agreed upon between the Nedap-certified partner and the customer.

Technical operation

iSense System

An iSense system integrates one or more Renos devices. Each iSense system needs **one** physical ethernet socket to connect to the outside world.

The system connects to the Device Management server over a secure HTTPS connection to set up the connection. Due to a technology called 'long polling,' the system waits for commands from the Device Management server. Each 'long poll' takes 5 minutes before the iSense system starts a new one.

To use Device Management, the system must be able to communicate with Nedap servers. Please inform the IT department about the system's specific internet connectivity needs so that they can adapt the firewall **before installation**.

Device Management Servers

Firewall recommended connections, allowing:

- outbound TCP port 443 traffic to *.nedapretail.com

Or more specific as:

- outbound HTTPS port 443 traffic to **api.nedapretail.com** (for Monitoring and Data Collection)
- outbound SSH port 443 traffic to **ssh1.nedapretail.com** (for Remote Service)
- outbound HTTPS port 443 traffic to **renos-updates.nedapretail.com** (for Firmware Update)
- outbound HTTPS port 443 traffic to **eas.nedapretail.com** (when using iD Cloud)

If whitelisting based on hostnames is not possible, please use the following list of ip addresses instead:

- 77.222.68.161 - 77.222.68.190 (77.222.68.160/27)
- 77.222.80.1 - 77.222.80.30 (77.222.80.0/27)
- 77.222.80.33 - 77.222.80.62 (77.222.80.32/27)
- 77.222.80.65 - 77.222.80.94 (77.222.80.64/27)
- 87.249.123.1 - 87.249.123.126 (87.249.123.0/25)
- 144.2.168.1 - 144.2.171.254 (144.2.168.0/22)
- 149.3.168.1 - 149.3.168.254 (149.3.168.0/24)
- 213.126.140.97 - 213.126.140.126 (213.126.140.96/27)

- 213.160.213.81 - 213.160.213.94 (213.160.213.80/28)
 - 217.114.110.33 - 217.114.110.62 (217.114.110.32/27)

IP Addresses

The list is subject to change as it depends on external parties.

DNS

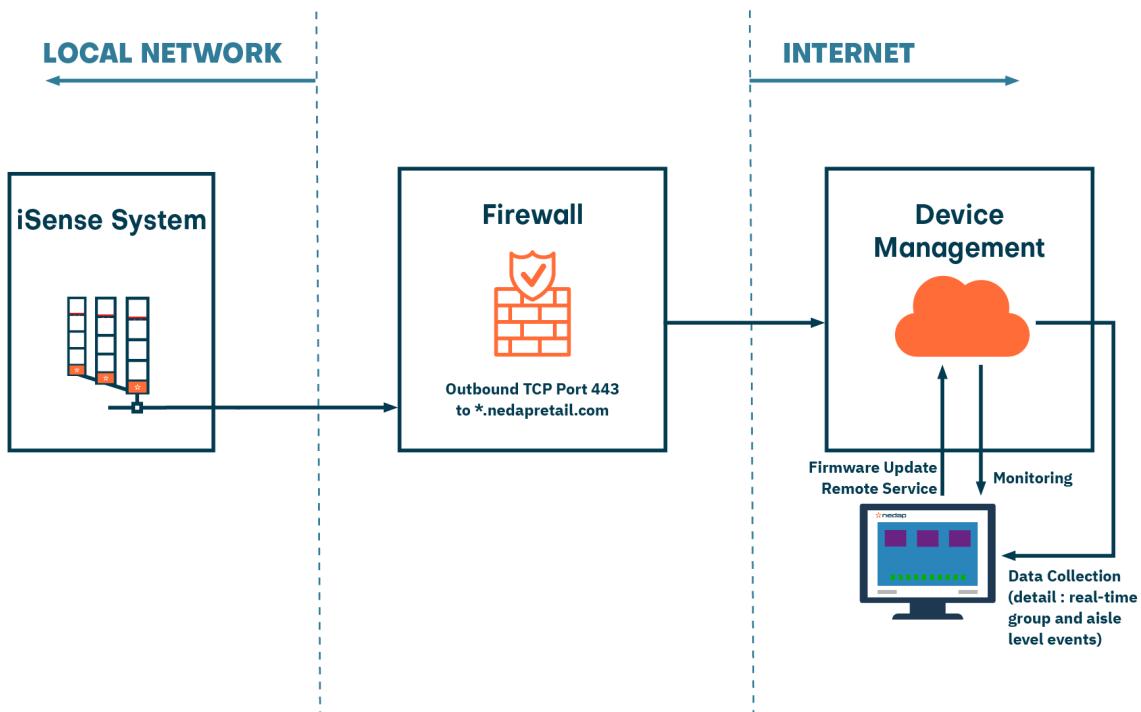
The system needs to resolve the Nedap servers' DNS names, so either a suitable internal DNS server must be present or outbound UDP port 53 traffic to an external DNS server needs to be open.

Remote Service

Remote service uses an SSH outbound connection over TCP port 443 to **ssh1.nedapretail.com**, which is different from port 22, the SSH default.

Transport Layer Security

TLS 1.2 or upwards is required from February 1, 2023. Support for TLS 1.0 and TLS 1.1 is **not** available after that date.

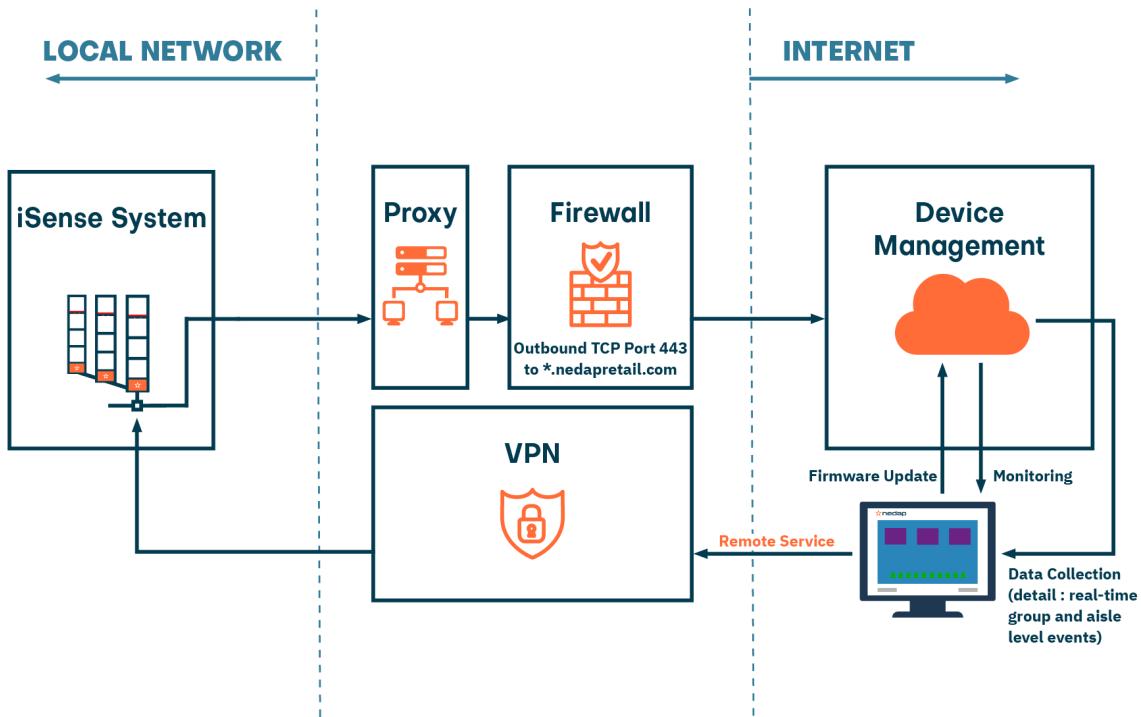




You can **test the firewall and connection** by connecting a PC or laptop to the network and opening <https://api.nedapretail.com> in a browser. If you see the login screen for a Nedap Retail account, the connection was successful. However, remember that this is not a full firewall test, as it only tests the connection to one of all servers.

Using a proxy to access the internet

For environments that dictate the use of a proxy, it is possible to configure the iSense systems accordingly.



When using a proxy server:

- Remote service via Nedap Device Management is **impossible**; a VPN, installed and maintained by the customer, can be used as an alternative.
- Detailed data delivery via Analytics, such as real-time, aisle—and group-related data for systems behind a proxy, has been available since firmware version 22.31. In firmware versions before 22.31, counts aggregated per 5 minutes at the system level are available.
- **ID Cloud** as an EAS database method is **not** possible.

Data exchange

The following information is sent to the Device Management servers:

- Store name and address
- Alarm & customer counts (since firmware version 19.09 events instead of counts)
- Status for monitoring
- Warnings and critical errors in the firmware

The amount of data depends on the type of data. In general, there are three different types of data:

1. Monitoring and Data Collection

- a. Depending on the system configuration, this results in about 10 MB of daily data consumption.
- b. The following information is sent:
 - i. The store name and address,
 - ii. system status for monitoring and warning
 - iii. critical errors in the firmware (some data is sent per 5 minutes, others are sent per heartbeat).

2. Remote Service

The data consumption varies depending on which page in the wizard or dashboard is opened:

- a. A remote access session will consume at least 5 MB (connection, log, etc.)
- b. Be aware that the Advanced Config (with RF spectrum) will consume the most data: 0,5 MB per Minute.
- c. Some other pages that will send continuous data are:
 - i. Automatic sensitivity page (100 KB per minute)
 - ii. final test page (50KB per minute)
 - iii. the iSense Dashboard (50KB per minute)
- d. The other pages will use around 25-50 KB per page.

3. Firmware Update

A firmware update will consume around 30-50 MB per system.



How to connect the system to the internet

An in-store network is the easiest way to connect iSense systems to the Device Management server.

We recommend placing the iSense system in a different firewall-separated VLAN - if available, to enhance security.

If the system cannot be connected to the in-store network or does not provide access to the Internet, it is also possible to connect to the Device Management system via a 3G/4G modem.

Never connect the systems directly to the Internet (e.g., via port forwarding), as this is a severe security risk. Only use Nedap Retail Device Management to make a secure remote connection.

Other network connections

In addition to the firewall configuration to support the iSense systems in the store, a few other network connections need a brief explanation.

API

The iSense systems have an API available that makes it possible, for example, to receive events as they occur in the iSense system. For more details on the API, please contact the Nedap Retail Service Desk.

As of firmware version 20.46.1, authentication is required, and the API is disabled by default and should only be enabled if desired.

SNMP

All iSense systems (with firmware version 14.29 and above) support SNMP to enable integration with local monitoring tools in the retailer's network. The MIB file is included in the iSense system and is available at [http://\(the iSense system's IP address\)/SNMP](http://(the iSense system's IP address)/SNMP). Query the iSense system with SNMP version 2c, community public, and agent nedap.

As of firmware version 20.46.1, SNMP is disabled by default and should only be enabled if desired.

Receiving reports via (S)FTP

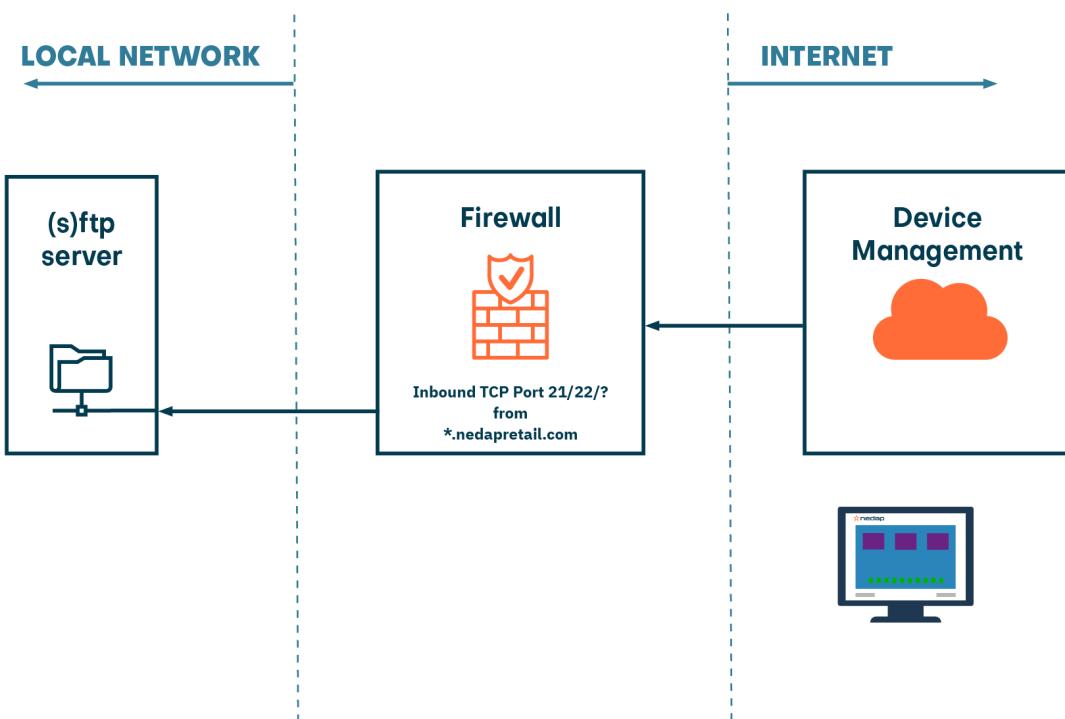
With the correct subscriptions, it is, for example, possible to receive daily Analytics reports from the Nedap Retail Device Management servers.

Delivery options for such reports are (S)FTP and email, with (S)FTP being preferred, especially for more extensive reports.

To deliver a report, our Nedap Retail Device Management servers must be able to store the report on an (S)FTP server of the customer's choice. This means the firewall that protects your (S)FTP server must be adapted to allow the Nedap Retail Device Management servers to connect.

Inbound TCP traffic should be allowed for:

- Port 21 (the default for FTP), port 22 (the default for SFTP), or a port of your choice.
- The same servers are shown in the Device Management Servers paragraph.



Security information

At Nedap (Retail), we understand the importance of protecting the confidentiality, integrity, and availability of systems and data, ensuring business continuity, and maintaining your trust in our products and services. Cybersecurity is one of our top priorities, and we continuously invest in comprehensive measures to protect our systems, the information we process, and the products and services we provide to our clients.

Our commitment to cybersecurity involves a combination of robust technical and organizational measures. We strongly believe cybersecurity is about the right mixture of People, Processes, and Technology (PPT). We employ state-of-the-art security technologies, regularly update our systems, and periodically conduct risk and vulnerability assessments to proactively identify and mitigate potential risks. Third parties and suppliers are included in these risk and vulnerability assessments. We have implemented strict access controls, ensuring only authorized personnel can access our most critical systems or sensitive data. We use MFA and SSO for primary and secondary, as well as facilitating systems and applications. Our employees receive regular training to keep up-to-date and aware of cyber threats. We follow industry best practices and compliance standards to safeguard our products and services.

To ensure resilience against potential vulnerabilities and cyber attacks, we have robust risk management and change management policies and processes in place. These processes enable us to identify, assess, and address security risks promptly and effectively. Moreover, we continuously evaluate our security controls and improve our policies to adapt to evolving cyber threats.

Infrastructure & Hosting

Within Nedap, we use the services of a specialized and dedicated internal hosting team to manage our platform infrastructure. The data centers we use hold various relevant security certifications, such as ISO27001, ISAE3402 type II, and SOC2 type II. Nedap's internal hosting team works closely with Nedap Retail's own DevOps and Development teams to manage and monitor the hosting infrastructures' performance and security continuously. A SIEM and multiple other tools are used for log analysis, monitoring system events, and alerting if thresholds are exceeded or anomalies are detected.

The hosting infrastructure is completely separated from the Nedap office environment and is only accessible by authorized personnel based on their role/function. Access is only possible using non-domain-joined jump hosts and Multi-Factor Authentication (MFA). To ensure secure server configuration at all times, we use Infrastructure-as-Code. Any suggested change is well-documented, goes through a 4-eyes principle (at least), and must be explicitly approved before implementation. Any manual system or configuration change that did not follow this process is automatically being reverted.



Application Security

Multiple software development teams within Nedap Retail develop our applications, such as Device Management, APIs, Loss Prevention, iD Cloud Web, and mobile apps. These teams focus on their specific area and collaborate closely. Our developers all hold higher degrees in software development and share the same robust development principles.

We care a lot about secure and high-quality code. Therefore, we also apply the 4-eyes principle to all changes within our source code. Every Pull Request (PR) must be reviewed and approved by another (senior) developer before being merged. Besides reviewing all code through this 4-eyes principle, we continuously improve our tools and practices to identify and prevent any possible issues as soon as possible in the CI/CD pipeline (shifting security left). We do unit and integration tests, have full traceability of who made what change and why, and use various tooling for Continuous Integration (CI) services so that PRs can only be merged after all tests have passed. We use Software Bill of Materials (SBOM) and Software Composition Analysis (SCA) to gain insight into possible security issues introduced using third-party libraries. Furthermore, we use Dynamic Application Security Testing (DAST) tooling to scan our staging environment for potential vulnerabilities weekly. If any serious security issues are identified, these will be resolved before the code is deployed to production.

Penetration Testing

Besides all the effort we put in ourselves to keep our hosted platform secure, we also engage a reputable cyber security firm to either perform an annual penetration test or to do Agile Security Testing throughout the year (consisting of code reviews and manual hands-on penetration testing, in intervals of several weeks). Our iD Cloud Web environment, Device Management, and our APIs are within the scope of these tests. Resulting reports are assessed and discussed, and any findings are treated following our Information Security Policy, meaning that at least all critical or high-risk findings must be resolved within two weeks.

Certification & Assurance

Our iD Cloud EU platform (including Device Management and our APIs) successfully passed a SOC2 type I attestation, and we are currently in the process of obtaining a SOC2 type II report and a SOC1/ISAE3402 type II report covering our Year-End Count service. In addition to all technical controls, these attestations include relevant organizational aspects assessed by independent external auditors, both in design and effectiveness.

Should you have any questions or concerns regarding our cybersecurity practices, we encourage you to contact your business contact within Nedap (Retail). They will be more than happy to work with you and answer your questions.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Document Version 161

Document Last modification date 31 October 2024

Document PDF Exported 31 October 2024 by Nedap Retail | Operations

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.



support-retail@nedap.com



**Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands**

nedap-retail.com

Connected Devices Guideline

iSense Online Services Setup

version 24, September 2024

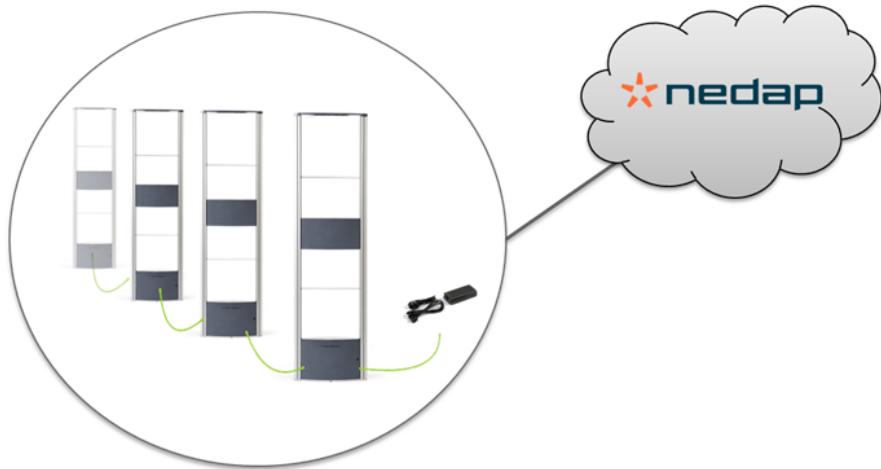
Introduction	3
iSense Online setup	4
1. Preparation	4
2. System installation	4
3. Setup in Device Management	5
4. Add subscriptions to the store	6
5. Add users	9
6. Use the services to its full potential	10



Introduction

The power of iSense is connectivity. In this document we will describe the steps for a complete setup and use of Nedap Retail online services.

iSense Online setup



1. Preparation

In the preparation phase it is already important to think about connectivity.

Discuss with the customer:

- Where the network connection needs to be installed, so the iSense system can be connected
- The iSense network requirements (see document on the Partner Portal)

2. System installation

When installing the system in the store, make sure to connect it to the customer network and test if the system can communicate to the Nedap Servers via the configuration wizard.

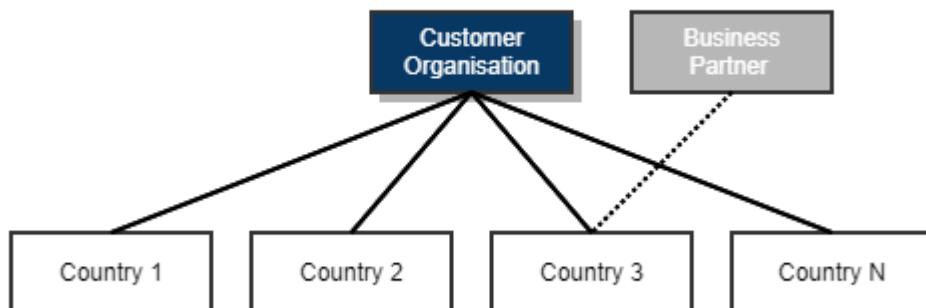
3. Setup in Device Management

After the installation you need to assign the system to the correct store in Device Management (<https://devices.nedapretail.com>)

Organization setup

It is important to create a store in the correct organization within Device Management. If the required organization does not exist in your business partner view, you need to contact Nedap Retail Support:

1. Send an e-mail to **support-retail@nedap.com** with:
 - Organization name
 - Address
 - Country
 - Website (so we easily check the organization)
2. Nedap Retail support will create the organization and connect the country level to your organization.



It is very important to use the correct organization in Device Management! Moving stores to another organization afterwards is not possible!



The structure in Device Management is also used for Analytics

Create store

Now the organization is available, the next step is to create a store within the organization. Make sure to follow the guidelines for the name of the store that are applicable for the organization.

Add system

Now the store is available in Device Management, the next step is to add the system to the store.

This can be done with the System ID from the system. The system ID is available via:

- In the configuration wizard (click on firmware version)
- Via an e-mail that is automatically send to the technician that installed the system
- Via the registrations list in Device Management where new online systems are automatically available for the correct partner that installed the system

4. Add subscriptions to the store

After the store is created it is possible to add services to the store.

Add subscriptions

Add Fast Remote Service

There are two main categories for online services:

- **Device Services**
- **Analytics Services**



Adding a subscription in Device Management is a financial action!

- Creating / Editing a subscription is a contract change with financial consequences!
- Once the end date is set, it cannot be changed!
- Invoices are automatically generated and sent based on the service subscriptions active in Device Management.



Subscriptions are always on store level



Subscriptions are invoiced monthly to the business partner

Device Services

The following options are available:

- Device connectivity
- Fast Remote Service (regular 1 year, or 5 years)
- Support Package

Service	Article Number	Content
Device Connectivity	Free (Active as soon as the system is linked to a store)	<ul style="list-style-type: none">• Basic system connectivity• Status information
Fast Remote Service - Regular (1 Year)	8022313	<ul style="list-style-type: none">• Remote Service• Store and Systems overview• Email notifications• Store assist• Store history• RFID performance monitor
Fast Remote Service - Extended Warranty 5 Years	8028818	Fast Remote Service Regular + Extended warranty 5 years
Support Package	6670075	First line support functionality for Retailers: <ul style="list-style-type: none">• Store and Systems overview• Email notifications• Store assist• Store history• RFID performance monitor

Analytics Services packages

In the table below you'll find the iSenseGo Analytics Packages.

iSenseGo Service	Analytics Starter	Analytics Theft	Analytics Visitor
	See alarm data in Analytics Web. Downloads and integrations are not possible (read-only).	Access to alarms, metal detection and deactivations via web dashboard and integrations.	Access to visitor counting via web dashboard and integrations.
Estate overview	✓	✓	✓
System Health	✓	✓	✓
Theft Insights Web <i>Alarms, Metal and Deactivations</i>	✓	✓	-
Download Theft data	-	✓	-
Automated Theft reporting	-	✓	-
Realtime Theft Analytics API	-	✓	-
Visitor Insights Web	-	-	✓
Download Visitor data	-	-	✓
Automated Visitor reporting	-	-	✓
Realtime Visitor Analytics API	-	-	✓
Realtime Occupancy Monitor	-	-	✓

The packages contain a lot of features. These features include:

Feature	Summary
Estate overview	An overview of stores and divisions within the customer organization. This is shown throughout the application (e.g. navigation screens and division overview pages).
System Health	An overview in of system health in Analytics Web. Summaries shown on division levels and detailed information shown at store level.
Alarm Insights Web	An overview of RF and RFID alarms in Analytics Web Totals can be displayed and compared flexibly on division and store level.
Metal Detections Web	An overview of metal detections alarms in Analytics Web Totals can be displayed and compared flexibly on division and store level.
Deactivation Insights Web	An overview of RF label deactivations in Analytics Web Totals can be displayed and compared flexibly on division and store level.
Customer Counting Web	An overview of customer counting data in Analytics Web Totals can be displayed and compared flexibly on division and store level.
Download Data	Allow users to manually download data, using a 'Download' button in web.
Automated Reporting	Automated sftp and email reporting functionalities. Data depends on package (e.g. theft or visitor)
Realtime Analytics API	Allow user to connect to the realtime Analytics API to automate integrations for alarms, metal detections, deactivations and customer counting data. Data depends on package (e.g. theft or visitor)
Realtime Occupancy Monitor	An overview of occupancy levels in stores, existing of a realtime monitor and historical overviews.

5. Add users

Now the setup is ready in Device Management, it is time to add customer users so they can use Analytics (<https://analytics.nedapretail.com>).

Users have to be added by the business partner on the correct level in Device Management (e.g. country or store level). The users need rights for Analytics.

6. Use the services to its full potential

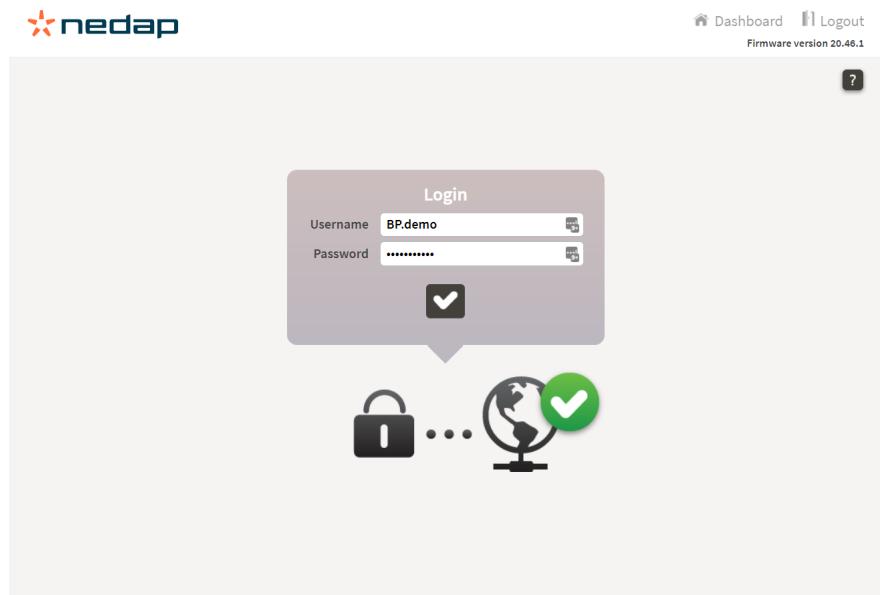
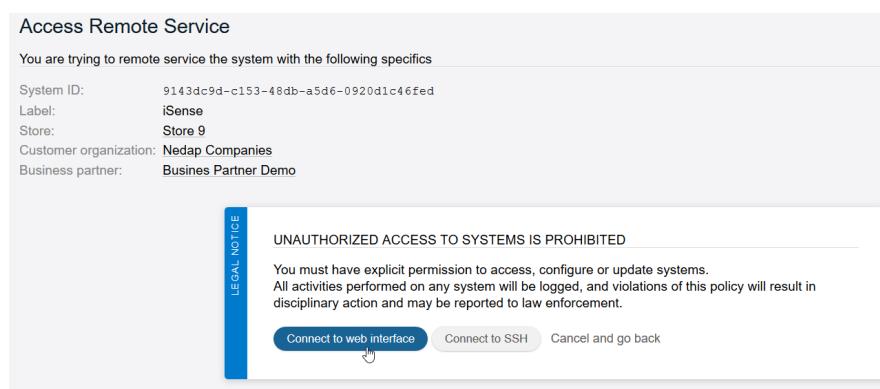
Now all online systems can be monitored in the cloud to make sure that all the iSense systems run optimally all over the world.

Fast Remote service

With Fast Remote Service subscriptions it is possible to pro-actively monitor and control systems remotely. Most important features are described below:

Remote service

Full remote access to the iSense systems



Store Assist

Overview of all open issues on a certain division to easily monitor multiple stores at once

Store Assist [Help](#)
5 of 9 Business Partner have issues
 Search stores
Show filters

Store	System	Category	Issue age	Issue type	Action
Store 5	iSense	■	3 years	Not connected to Device Management	View
Store 4	iSense	■	3 years	Not connected to Device Management	View
Store 2	iSense	■	3 years	Not connected to Device Management	View
Store 1	iSense	■	3 years	Not connected to Device Management	View
Store 9	iSense	■	a year	Not connected to Device Management	View

Seen last month
Actions



Last action
Business Partner snoozed
on 02 April 2020 at 13:42
UTC
"Technician will go onsite"
[View history](#)

[!\[\]\(e8c47d7fc18e08ad73fba4804ae4f2e0_img.jpg\) Snooze issue](#)

[!\[\]\(31d1f05b567a1fe890275fc13d916554_img.jpg\) Remote Service](#)

[!\[\]\(384f5df82aa4553a529684d8595df314_img.jpg\) Create ticket](#)

[!\[\]\(ad499bc3ce6f7294ffdf0dc3f4f86327_img.jpg\) Set notification](#)

E-mail Notifications

Set pro-active notifications by e-mail to enable quick response on open issues

Set new email notification
Set for a different location? Use the [overview](#) to go to another location.

Which issue type(s) do you want to subscribe to?

<input type="checkbox"/> Not connected to Device Management
<input type="checkbox"/> Infrared beam sensors blocked
<input type="checkbox"/> Units inactive
<input type="checkbox"/> Units are muted
<input type="checkbox"/> Units in RF maintenance mode
<input type="checkbox"/> Units in RFID maintenance mode
<input type="checkbox"/> Reno database failing
<input type="checkbox"/> Disk space low

After how long should the notification be sent?

Direct	30 minutes	1 hour	2 hours	4 hours	24 hours	48 hours
--------	------------	--------	---------	---------	----------	----------

Issue history

History of the issues per store in one overview

History

Not connected to Device Management
⚠ Issue active

Not connected to Device Management

Instructions

The system is not able to connect to Device Management. The Internet connection may be down. Check the Internet connections and make sure the system has been configured properly.

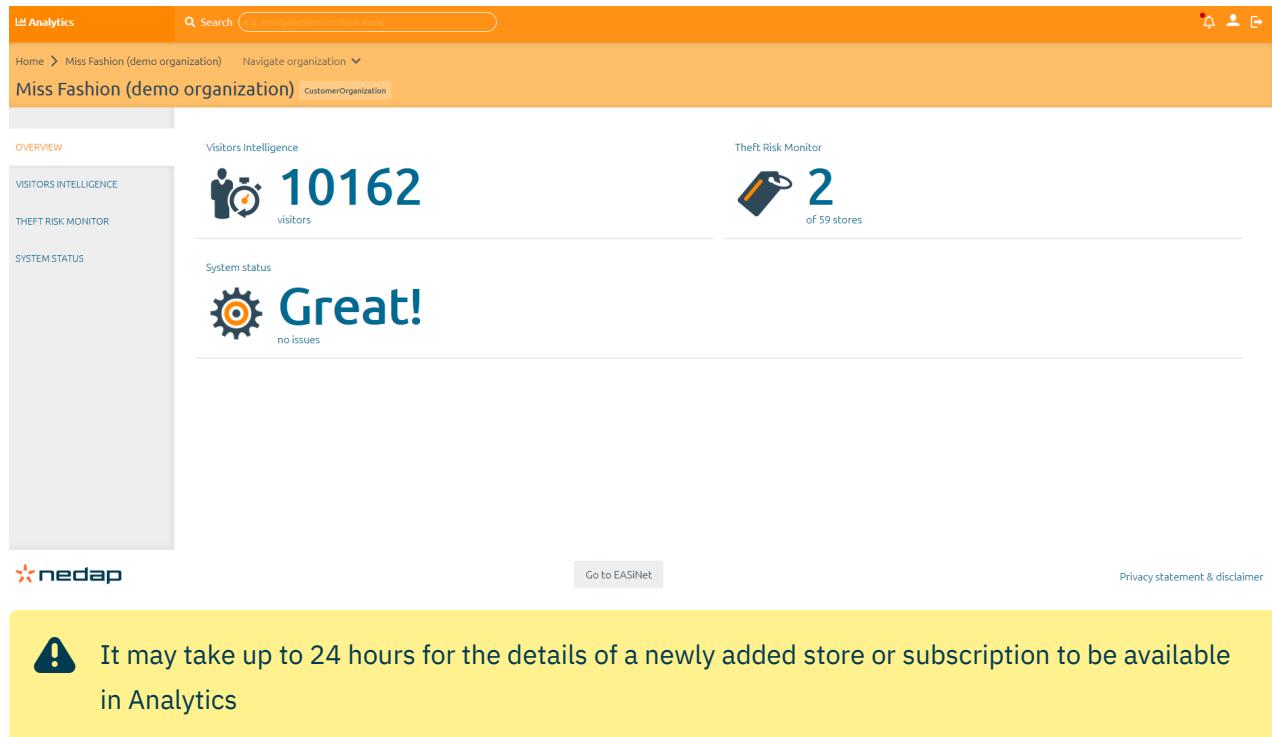
⚠ Issue is currently ongoing at iSense

Archive

Reported at iSense 11 December 2018 at 11:53 UTC

Analytics

With the Analytics subscriptions it is possible for the customers to get more insight in Alarm Data and Customer Counting data depending on the type of subscription.



The screenshot displays the nedap Analytics interface for the organization "Miss Fashion (demo organization)". The top navigation bar includes links for "Analytics", "Search", "Home", "Miss Fashion (demo organization)", "Navigate organization", and user icons. The main content area features three primary metrics:

- Visitors Intelligence:** Shows 10162 visitors.
- Theft Risk Monitor:** Shows 2 stores out of 59.
- System status:** Displays "Great!" with "no issues".

On the left sidebar, there are links for "OVERVIEW", "VISITORS INTELLIGENCE", "THEFT RISK MONITOR", and "SYSTEM STATUS". At the bottom of the page, there are links for "Go to EASiNet", "Privacy statement & disclaimer", and the nedap logo.

Warning message: A yellow callout box contains the text: "⚠️ It may take up to 24 hours for the details of a newly added store or subscription to be available in Analytics".

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Document Version 24

Document Last modification date 9 September 2024

Document PDF Exported 2 October 2024 **by** Nedap Retail | Operations

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.



support-retail@nedap.com



Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com

Nedap Sense Manual

Device Management

version 61, October 2024

Introduction	4
Authentication: Nedap Retail Account	5
Forgot your password?	6
Navigation	7
Search	7
Top menu bar functionalities	8
Organization management	10
Add new organization	11
Add a new division	12
Edit divisions	13
Store management.....	14
Add a new store	14
Add a new system	15
Edit a system	17
Move a system	18
View systems	19
Add subscriptions	20
View and edit services	21
Remote Service	22
Add a report	22
User management.....	24
Invite new users	24
Invitation flow	26
Block a user account	26
Business partners and subcontractors	27
The Partner Address Book on the Portal.....	28
Changes to your Partner Address Book entry	28

Introduction

Using a Nedap Retail product in a retail environment becomes critical to operating your business. Therefore, all units must operate at the optimum performance.

Nedap has developed Device Management, which allows for the management of all organizations, stores, systems, and services. It also allows a Nedap-certified business partner to execute remote service and management. Device Management is offered with all iSense systems.

- **Manage organizations:** an authorized Nedap-certified engineer can access the organizations, stores, and subscriptions and manage, edit, add, or remove stores and systems.
- **Manage users:** Manage users who need access to the Nedap Retail online applications.
- **Remote log-in:** through the Device Management website, an authorized Nedap-certified engineer can remotely access the system's user interface to make changes to the configuration or access system logs.
- **Firmware updates:** an authorized Nedap-certified engineer can install the latest features and security patches remotely utilizing the Device Management website.
- **Remote diagnostics and Monitoring / Proactive status reporting:** Critical system parameters are monitored 24/7. If a system has issues, an alert is generated and sent to the supporting partner.
- **Data Exports and Data Collection:** alarm and customer counts per system are collected to be displayed in our Analytics platform. As of firmware version 19.09, real-time data delivery has been added, which means that alarm and customer events per aisle are stored.
- **Subscriptions:** Add subscriptions to stores and organizations.
- etc

This manual describes how to use the basic functionalities of Device Management.

As Device Management is the leading application for user management for all the Nedap Retail online applications, it is important to add user and contact details correctly.



Authentication: Nedap Retail Account

Owners of a Nedap Retail Account can use Device Management. A technical ambassador employed at a certified business partner will be granted access after completing the Nedap Retail training program. The Nedap Retail Support Desk will provide the Nedap Retail account details.

The certified technical ambassador can invite other employees from his / her organization to create a Nedap Retail Account.

Access to Device Management is only available for certified users.

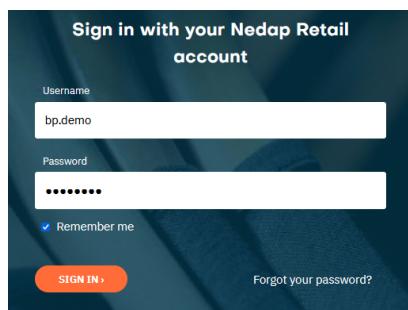
Do not leave your PC / laptop unattended when logged in to Device Management. Lock your screen when moving away from your PC / laptop.

Do not share Nedap Retail login credentials with colleagues or other (third-party) people.

First, open a web browser, enter the URL below, and select Device Management to log in.

<https://login.nedapretail.com>

Direct URL to Device Management: <https://devices.nedapretail.com>



A screenshot of the Nedap Device Management sign-in page. The page has a dark blue background with white text. At the top, it says "Sign in with your Nedap Retail account". Below that is a "Username" field containing "bp.demo". Below the username is a "Password" field with several dots. To the right of the password field is a link "Forgot your password?". At the bottom left is a red "SIGN IN >" button, and next to it is a "Remember me" checkbox which is checked. The overall design is clean and professional.



Forgot your password?

If you have forgotten your password, you can request a new one using the password recovery service.

Click on "Forgot your password?" at the login screen. Fill out your email address or username, and we will send you instructions on resetting your password.

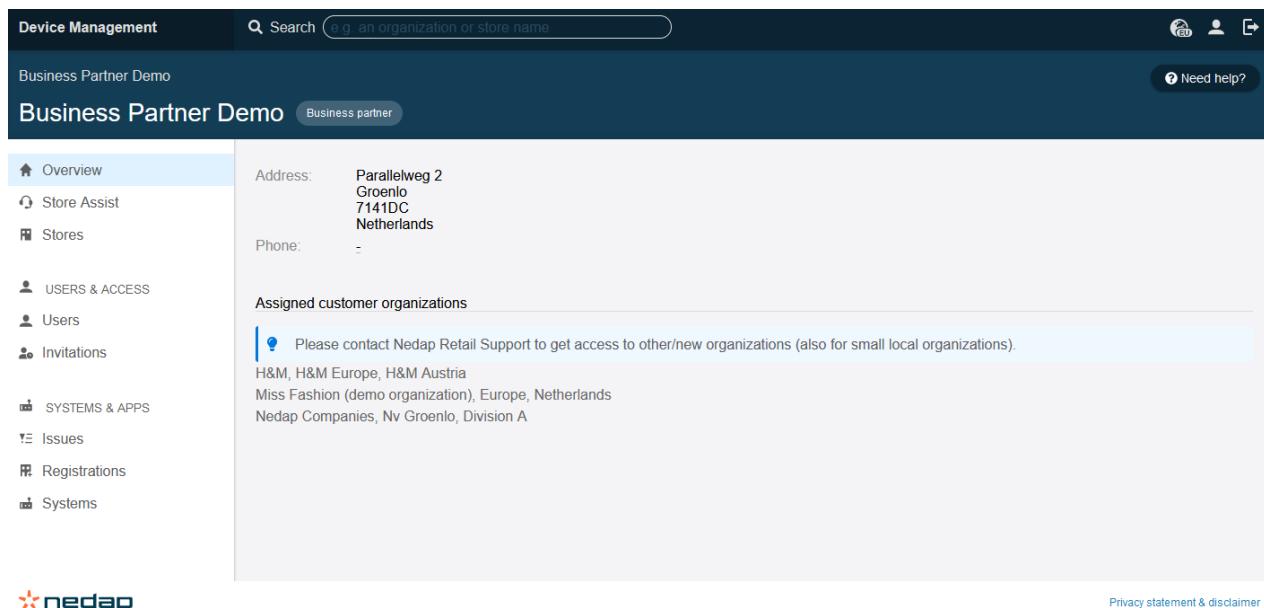


A screenshot of a password recovery form titled "Forgot your password?". The form instructs the user to enter their username or email address to receive password reset instructions. It features a text input field with placeholder text "'john.doe' or 'john.doe@company.com'", an orange "SEND INSTRUCTIONS >" button, and a "Cancel and go back" link.

Navigation

After login, the following aspects are part of the navigation in Device Management:

- Top bar (search, notifications, profile settings, logout)
- Side menu (options depending on user rights)
- Current view (“Assigned customer organizations” in the example below)



The screenshot shows the Device Management interface. At the top, there's a dark header with the "Device Management" logo, a search bar containing "e.g. an organization or store name", and user profile icons. Below the header, the page title is "Business Partner Demo". A sidebar on the left contains links like "Overview", "Store Assist", "Stores", "Users & Access", "Users", "Invitations", "Systems & Apps", "Issues", "Registrations", and "Systems". The main content area displays a store profile for "Business Partner Demo" (Business partner). It shows the address: "Parallelweg 2, Groenlo, 7141DC, Netherlands" and phone: "-". Below this, under "Assigned customer organizations", it says: "Please contact Nedap Retail Support to get access to other/new organizations (also for small local organizations)." followed by a list: "H&M, H&M Europe, H&M Austria", "Miss Fashion (demo organization), Europe, Netherlands", and "Nedap Companies, Nv Groenlo, Division A". At the bottom right, there's a "Privacy statement & disclaimer" link.

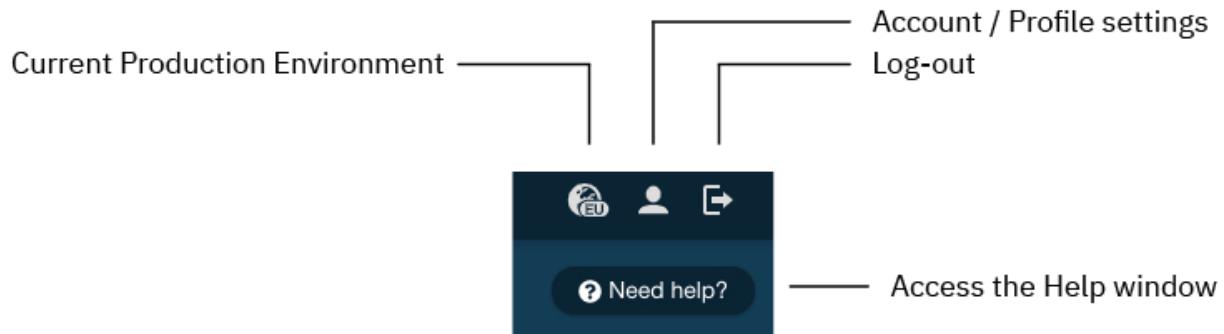
Search

The search function is available on every screen to easily search for your needs.

- Click on the search bar and start typing your search request.
- The search results are listed in a drop-down list while typing and labeled (User, Partner, Org, Store, Device).



Top menu bar functionalities

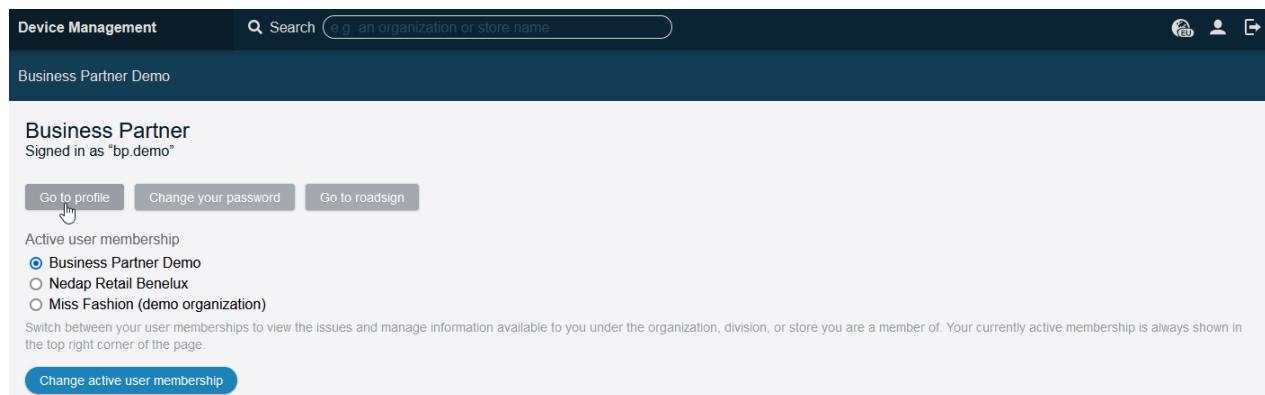


Current Production Environment

The indicator will show which Device Management environment a user is logged in to.

Account / Profile Settings

To change your contact details and password and change between memberships.



Device Management

Search (e.g. an organization or store name)

Business Partner Demo

Business Partner
Signed in as "bp.demo"

Go to profile Change your password Go to roadsign

Active user membership

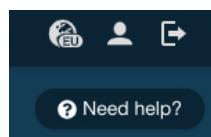
- Business Partner Demo
- Nedap Retail Benelux
- Miss Fashion (demo organization)

Switch between your user memberships to view the issues and manage information available to you under the organization, division, or store you are a member of. Your currently active membership is always shown in the top right corner of the page.

Change active user membership

Need help / first-time introduction window

Each new user entering Device Management for the first time will be introduced to Device Management by a welcome / help screen containing some tips and tricks. On each page of the application, a help function is available. You can access the help function anytime by pressing the "Need help?" button.





Locations

Location name

Overview Store Systems

The header shows the location you are currently at, such as a division or store.

YOU ARE HERE

Using Store Assist

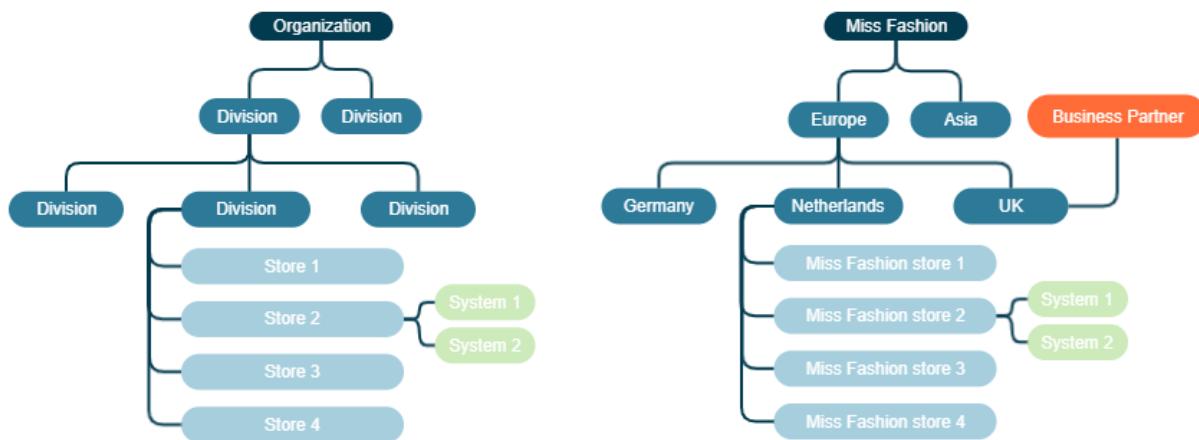
Store Issue

Store

Store Assist is your to-do list of ongoing issues.

Organization management

All organizations, divisions, and stores are provided in a structured overview. It is possible to create new organizations and stores, move stores to another division, or move entire divisions. The organization tree below shows how organizations are listed within Device Management.



A Nedap Business Partner can be found on the country level of the organization tree. Each organization can contain several divisions, which can represent continents, countries, regions, etc.

Multiple divisions are possible, and stores can be added to any level. The devices installed in each store are listed within the information pages of the specific store.

Usually, a retailer has agreed upon an organizational structure and might be part of the signed contract.



Add new organization

Nedap Retail Support will create new organizations. When a new organization needs to be added to Device Management, please contact support-retail@nedap.com. In the mail, provide the following information:

- Organization Name

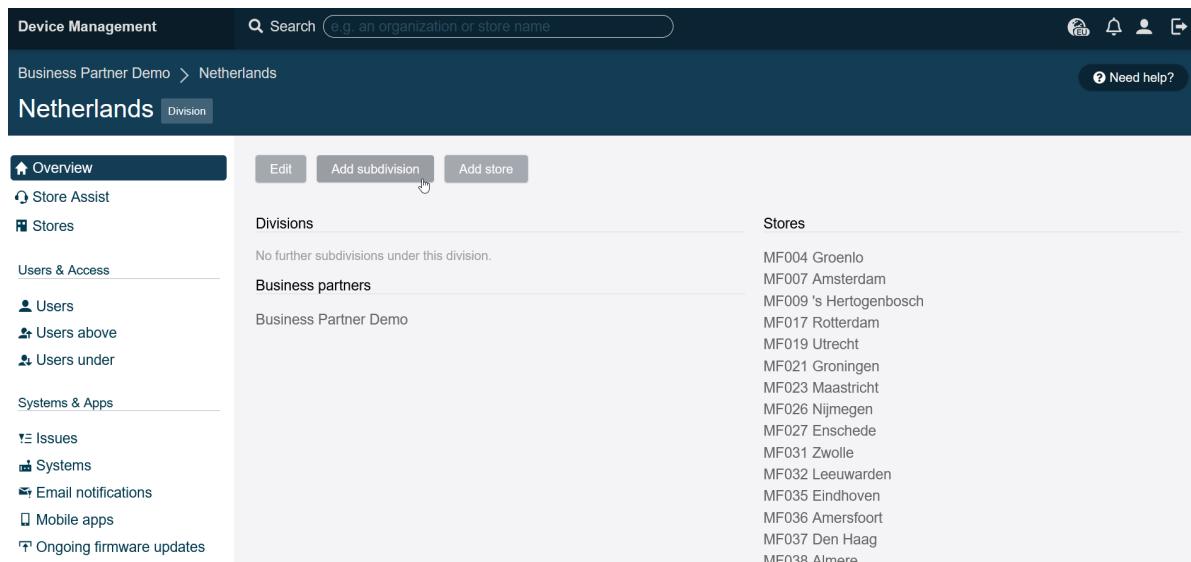
Additional information about the organization's headquarters:

- Street address or P.O. Box
- ZIP code
- City
- Country
- Website URL
- *Optional:* Division list (regions/countries / etc.)

Add a new division

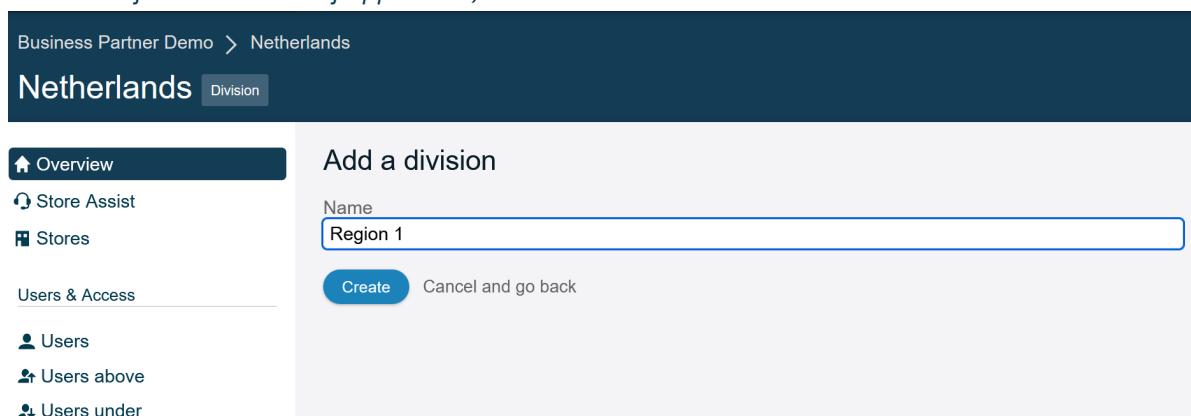
A division is the next level in the organization tree. Nedap Retail Support sets up the country-level division. Business Partners get access to the country-level division. A division can be a region. New divisions can be added to an organization via Device Management following the steps below:

1. Search for the organization where you want to add a division.
2. Click on ‘add subdivision’.



The screenshot shows the Device Management interface for the 'Business Partner Demo > Netherlands' organization. On the left, there's a sidebar with sections like Overview, Store Assist, Stores, Users & Access (with sub-options for Users, Users above, and Users under), Systems & Apps (with sub-options for Issues, Systems, Email notifications, Mobile apps, and Ongoing firmware updates). The main content area has tabs for Overview, Edit, Add subdivision (which is highlighted with a cursor icon), and Add store. Under the 'Divisions' section, it says 'No further subdivisions under this division.' and lists 'Business partners' as 'Business Partner Demo'. Under the 'Stores' section, there's a list of store codes and names: MF004 Groenlo, MF007 Amsterdam, MF009 's Hertogenbosch, MF017 Rotterdam, MF019 Utrecht, MF021 Groningen, MF023 Maastricht, MF026 Nijmegen, MF027 Enschede, MF031 Zwolle, MF032 Leeuwarden, MF035 Eindhoven, MF036 Amersfoort, MF037 Den Haag, and MF038 Almere.

3. Fill out the name of the division you want to add (*please keep in mind the agreed organizational structure of the customer - if applicable*)



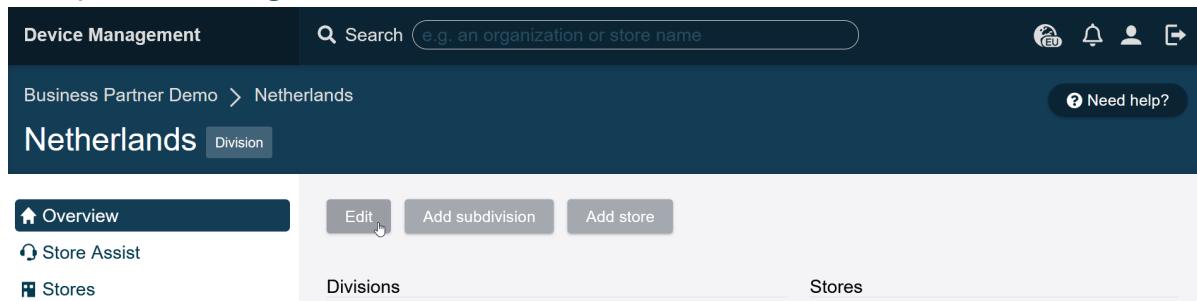
The screenshot shows the 'Add a division' form. It has a sidebar with the same navigation options as the previous screen. The main form area has a title 'Add a division' and a 'Name' input field containing 'Region 1'. Below the input field are two buttons: 'Create' (highlighted with a blue background) and 'Cancel and go back'.

4. After following the steps above, a new division is added to the organization. Within the created divisions, new stores or subdivisions can be added.

Edit divisions

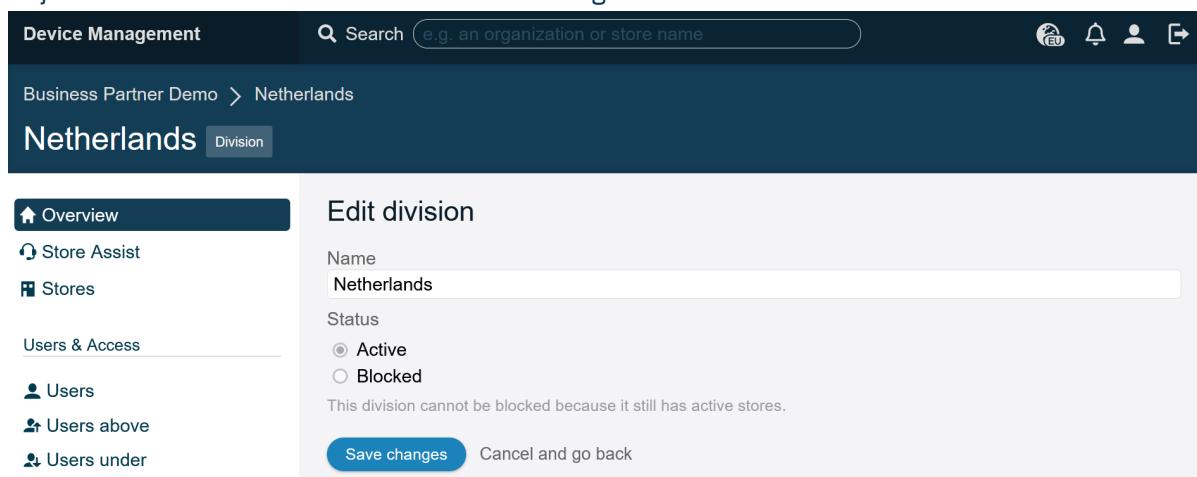
To edit the name of a division or subdivision:

1. Search for the division you want to edit.
2. Once you select the right division, click the “Edit” button.



The screenshot shows the Device Management interface. At the top, there is a search bar with placeholder text "e.g. an organization or store name". To the right of the search bar are icons for EU, notifications, user profile, and a help button. Below the search bar, the breadcrumb navigation shows "Business Partner Demo > Netherlands". On the left, a sidebar menu includes "Overview" (which is highlighted in blue), "Store Assist", and "Stores". In the center, there is a "Division" tab. Below the tabs, there are three buttons: "Edit" (which is highlighted in blue), "Add subdivision", and "Add store". At the bottom of the screen, there are two tabs: "Divisions" and "Stores".

3. Adjust the division name and click on “Save changes”.



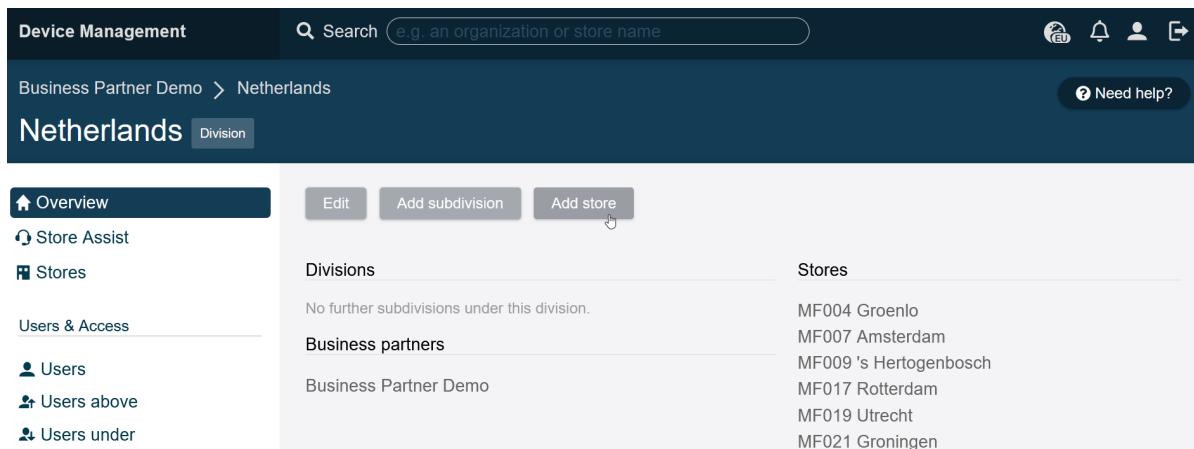
The screenshot shows the "Edit division" form. The title is "Edit division". There are two input fields: "Name" (containing "Netherlands") and "Status" (with radio buttons for "Active" and "Blocked", where "Active" is selected). A note below the status says "This division cannot be blocked because it still has active stores." At the bottom, there are two buttons: "Save changes" (highlighted in blue) and "Cancel and go back".

Store management

Once the organizations and divisions are in place, stores can be added to an organization, and systems (devices) and subscriptions can be added on a store level.

Add a new store

1. Search for the organization where you want to add a new store (make sure you have selected the correct division before you add the store).
2. Click on “Add store.”



The screenshot shows the Nedap Device Management interface. At the top, there's a navigation bar with 'Device Management', a search bar ('e.g. an organization or store name'), and user icons. Below the bar, the path 'Business Partner Demo > Netherlands' is shown. A 'Need help?' link is also present. The main area is titled 'Netherlands' and has a 'Division' button. On the left, a sidebar menu includes 'Overview' (which is active), 'Store Assist', 'Stores' (selected), 'Users & Access', 'Users', 'Users above', and 'Users under'. In the center, there are two sections: 'Divisions' (showing 'No further subdivisions under this division.') and 'Stores' (listing stores with IDs MF004 through MF021 and their locations). At the bottom right of the central area, there's a button labeled 'Add store' with a hand cursor icon.

3. Fill out the required information about the store (*please keep in mind the agreed organizational structure of the customer - if applicable*)
 - a. Add notes if needed.
4. Click on “Create” to add the store.
5. The store is added to the organization and is visible in the organizational structure.

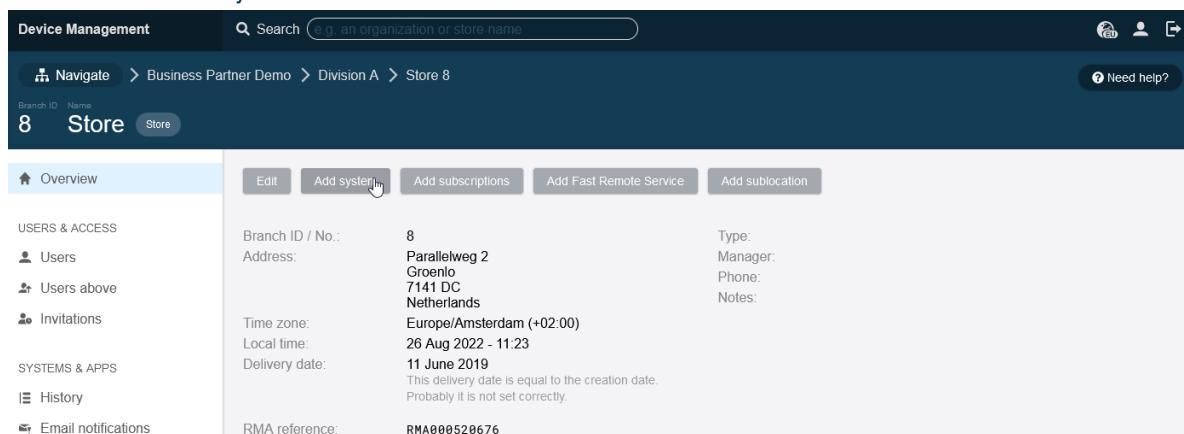
When a country is selected, only the time zones that are valid for that country will be shown in the drop-down

Stores can be added on every level. Please keep in mind the customer's agreed organizational structure.

Add a new system

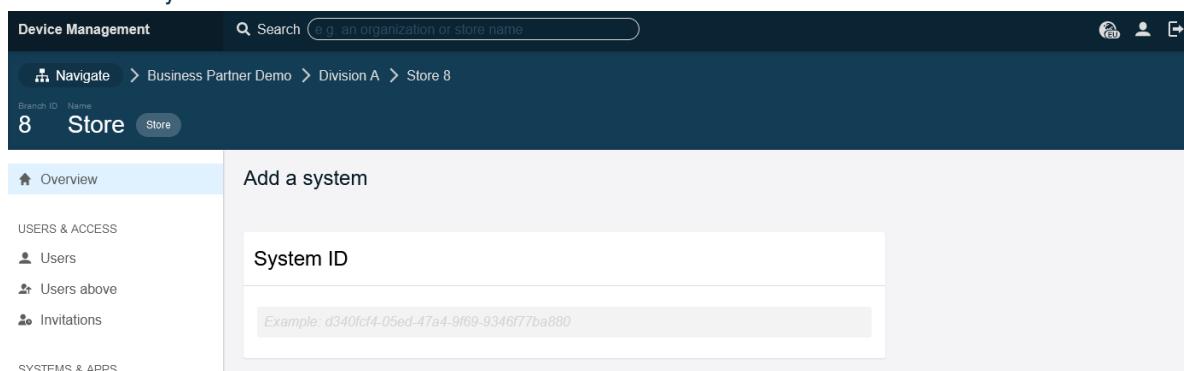
Once a store is created in Device Management, systems (devices) can be added to it.

1. Search for the organization to which a new system needs to be added. Then, navigate to the right division and store to add the device.
2. Click on the “Add system” button.



The screenshot shows the Device Management interface. The top navigation bar includes a search bar, user icons, and a 'Need help?' link. Below the navigation is a breadcrumb trail: 'Business Partner Demo > Division A > Store 8'. The main content area is titled 'Store' with a number '8'. On the left, there's a sidebar with links for Overview, USERS & ACCESS (Users, Users above, Invitations), and SYSTEMS & APPS (History, Email notifications). The main panel has tabs for Edit, Add system (which is highlighted with a mouse cursor), Add subscriptions, Add Fast Remote Service, and Add sublocation. Form fields include Branch ID / No.: 8, Address: Parallelweg 2, Groenlo, 7141 DC Netherlands, Time zone: Europe/Amsterdam (+02:00), Local time: 26 Aug 2022 - 11:23, Delivery date: 11 June 2019, Type: Manager, Phone: Notes: RMA reference: RMA000520676.

3. Fill out the 'System ID'.



The screenshot shows the 'Add a system' page within the Device Management interface. The top navigation bar and breadcrumb trail are identical to the previous screenshot. The main panel is titled 'Add a system'. It features a large input field labeled 'System ID' with the placeholder 'Example: d340fcf4-05ed-47a4-9f69-9346f77ba880'. To the left of the input field is a sidebar with links for Overview, USERS & ACCESS (Users, Users above, Invitations), and SYSTEMS & APPS (History).

The System ID can be obtained in 3 ways:

- a. Copy from the configuration wizard
- b. Copy from the registration e-mail that the installer will receive
- c. Copy from the Registrations list directly from Device Management



4. Optionally, enter the system location and notes.

Location (optional)

Location within the store where the system has been installed. Should make it easy to find the system later, and to differentiate between multiple systems installed in the same store.

Location within the store

Notes (optional)

Share technical details about the system setup.

Technical details

Create

Cancel and go back

5. Click on “Create” to save the settings.

A confirmation or error message, “System ID is not found,” will be shown. In case of an error, ensure that the iSense system is online at least once and connected to Device Management.

After adding the system, its details are accessible in the store overview pages. Click on the system name to enter the detail screen.

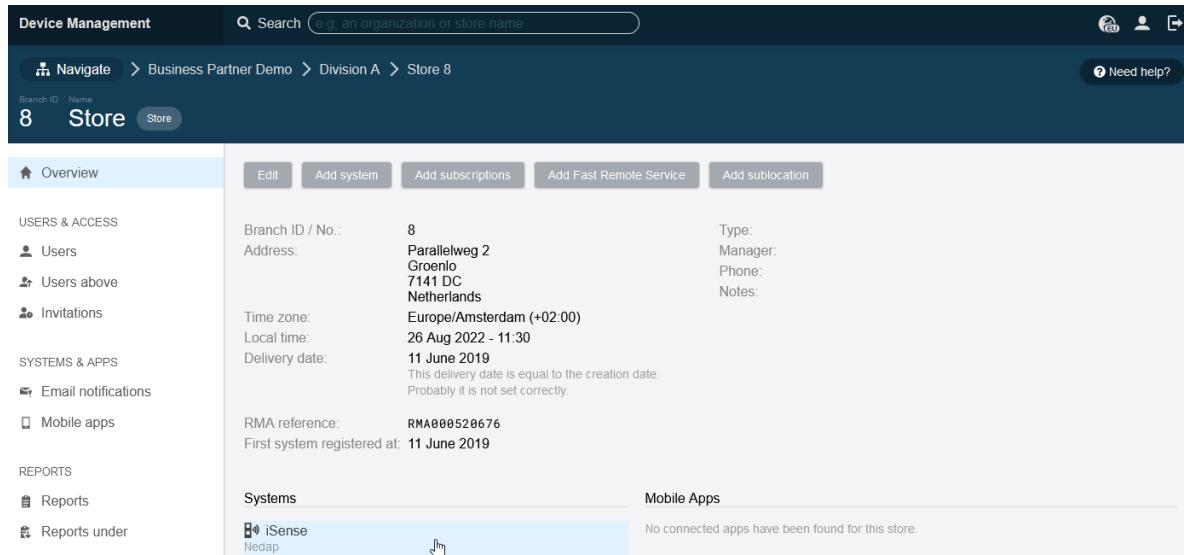
Systems

 iSense, Groenlo
Nedap

Edit a system

To edit the registered systems of a store, please follow these steps:

1. Search for the organization where you want to view or edit a system and navigate to the proper division and store.
2. You will now see the system(s) connected to the store.



The screenshot shows the Device Management interface for a store. The top navigation bar includes a search bar, user icons, and a 'Need help?' button. The main content area shows the store's details: Branch ID: 8, Name: Store, Address: Parallelweg 2, Groenlo, 7141 DC, Netherlands, Time zone: Europe/Amsterdam (+02:00), Local time: 26 Aug 2022 - 11:30, Delivery date: 11 June 2019 (Note: This delivery date is equal to the creation date. Probably it is not set correctly.), RMA reference: RMA000520676, and First system registered at: 11 June 2019. On the left sidebar, there are sections for USERS & ACCESS (Users, Users above, Invitations), SYSTEMS & APPS (Email notifications, Mobile apps), and REPORTS (Reports, Reports under). Below the details, there are two tabs: 'Systems' and 'Mobile Apps'. The 'Systems' tab lists one item: 'iSense Nedap' with a hand cursor icon over it, indicating it is selected or clickable. The 'Mobile Apps' tab displays a message: 'No connected apps have been found for this store.'

3. Click on the device you want to view or edit.

Move a system

Once a system (device) is activated at a store in Device Management, it will be visible at the store level. There is no specific move function for systems, but if a system needs to be transferred to another store, there is a way to do this. Follow the steps below:

1. Search for the organization where the system is currently active.
2. Click through to the store where the system is active.
3. Once you have selected the right store, click on the system you want to move.
4. Now click on the “Edit” button to start the move process.
5. Select “Deactivated” as the state for the system. This system is now available to add to another store.
6. Click on “Save” to confirm the deactivation of this system.
7. Now, follow the steps from the chapter “Add a new system” again at the required store to add the just-deactivated system again.

Please note that data received from a deactivated system will be ignored, and that history data will be lost when activated in another store.

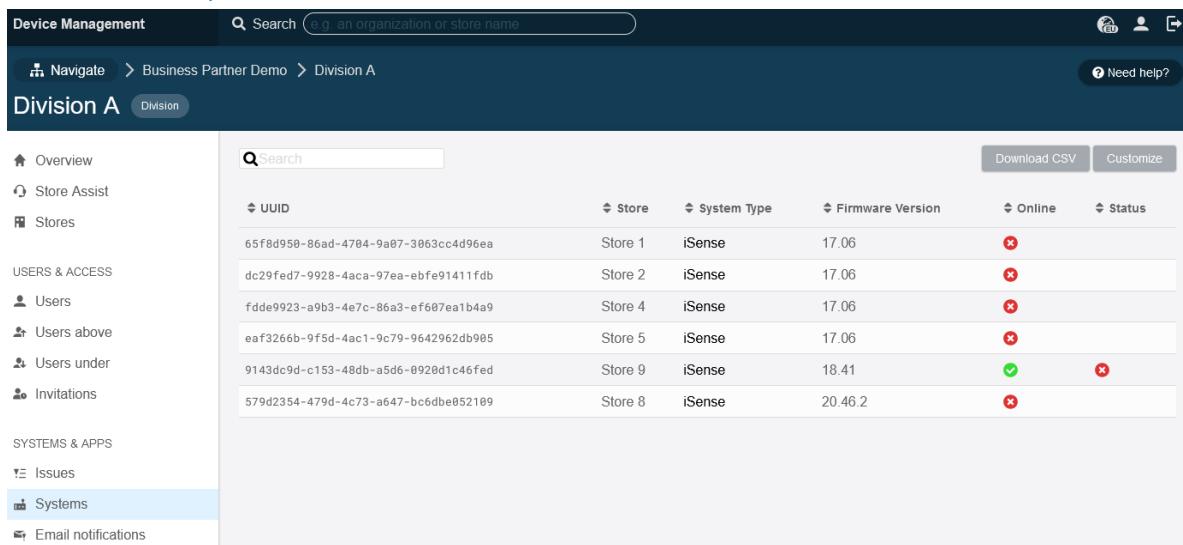
View systems

The systems overview can be opened on each level in the organization tree. This provides a list of all registered systems on that level. Generating this overview on the highest level in an organization may take a while.

1. Search for the organization or division where you want to see the system overview.
2. Click on “Systems” to open the systems overview.



3. An overview of all registered systems will be generated, listing the location, system type, current firmware version, and status.



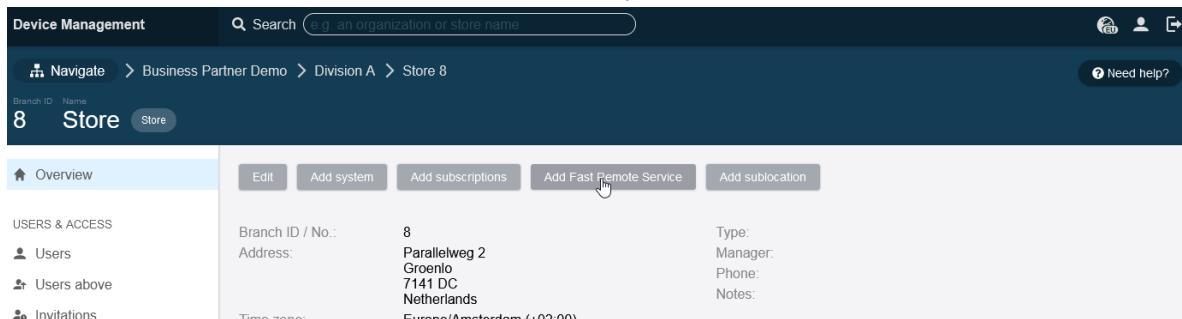
UUID	Store	System Type	Firmware Version	Online	Status
65f8d950-86ad-4704-9a07-3063cc4d96ea	Store 1	iSense	17.06	✖	
dc29fed7-9928-4aca-97ea-ebfe91411fdb	Store 2	iSense	17.06	✖	
fdde9923-a9b3-4e7c-86a3-ef607ea1b4a9	Store 4	iSense	17.06	✖	
eaef3266b-9f5d-4ac1-9c79-9642962db985	Store 5	iSense	17.06	✖	
9143dc9d-c153-48db-a5d6-0920d1c46fed	Store 9	iSense	18.41	✓	✖
579d2354-479d-4c73-a647-bc6dbe052109	Store 8	iSense	20.46.2	✖	

4. Adding additional data fields to the overview page is possible by clicking on “Customize” in the upper right corner.

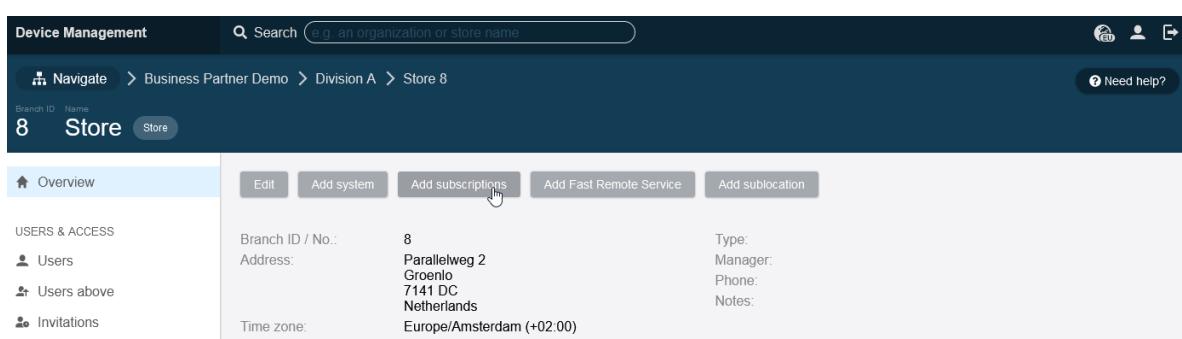
Add subscriptions

At the Store level, it is possible to add services (subscriptions and Fast Remote Service) to the store:

1. Search for the store to add the service.
2. Click on “Add Fast Remote Service” or “Add subscriptions.”



The screenshot shows the 'Device Management' interface with a search bar at the top. Below it, a breadcrumb navigation path: 'Navigate > Business Partner Demo > Division A > Store 8'. The main area is titled 'Store' with a branch ID of '8'. On the left, there's a sidebar with 'OVERVIEW' selected and sections for 'USERS & ACCESS' (Users, Users above, Invitations) and 'Branch ID / No.' (Address: Parallelweg 2, Groenlo, 7141 DC, Netherlands; Time zone: Europe/Amsterdam (+02:00)). At the top right, there are buttons for 'Edit', 'Add system', 'Add subscriptions', 'Add Fast Remote Service', and 'Add sublocation'. The 'Add subscriptions' button is highlighted with a cursor icon.



This screenshot is identical to the one above, showing the 'Device Management' interface for 'Store 8'. The 'Add subscriptions' button is again highlighted with a cursor icon.

3. Follow the instructions on the screen to add the correct subscription(s)
4. Choose the start date for these services and click “Subscribe.”

Once the subscriptions are activated, they are automatically invoiced to the assigned Business Partner.

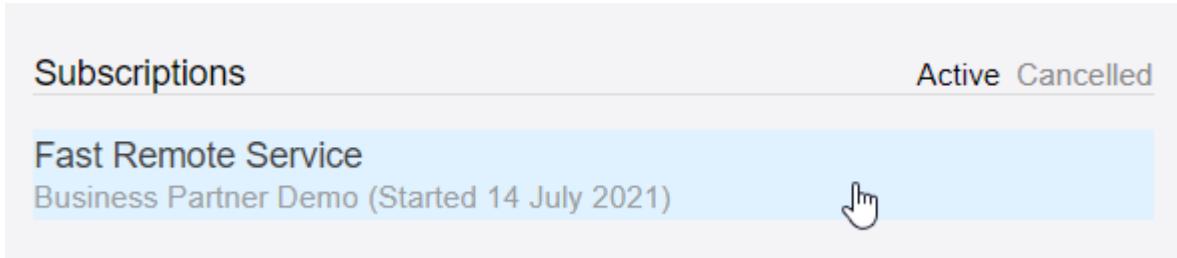
Subscriptions with a specific start or end date cannot be altered until that date is reached.

Do not add iD Cloud subscriptions! This is arranged centrally by Nedap HQ (iD Cloud support)

View and edit services

Once a service is activated at a store, it can be viewed and edited via the store overview page.

1. Search for the store to edit the service.
2. Click on the service you want to view or edit.



The screenshot shows a user interface for managing subscriptions. At the top, there is a header with the word "Subscriptions" and two filter buttons: "Active" and "Cancelled". Below the header, a list item is displayed: "Fast Remote Service" followed by the text "Business Partner Demo (Started 14 July 2021)". To the right of this list item is a blue rectangular button with a white hand cursor icon, indicating it is a clickable element.

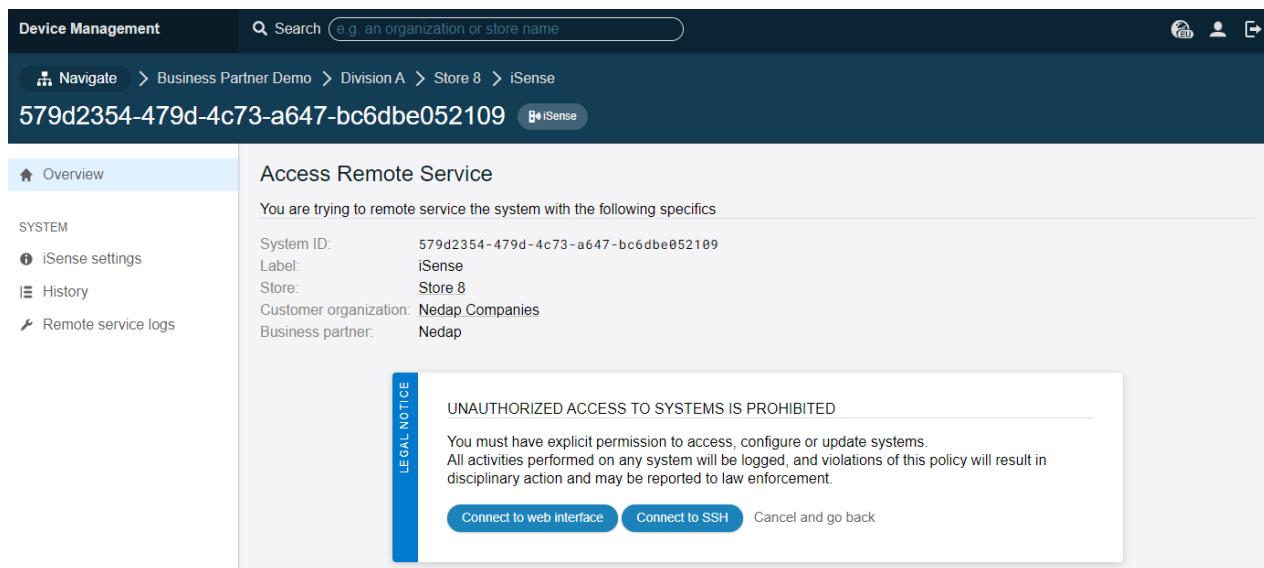
3. In the next screen, click on “Edit”.
4. Now, you can stop or remove a subscription from a store. Once stopped, the invoices will also stop automatically.

Remote Service

For devices where Fast Remote Service is active, the “Remote Service button” will be shown on the system page.

Before access is granted to a specific system, a legal notice is shown, which has to be accepted first.

Only authorized and certified Nedap Retail engineers can access devices (systems) via Fast Remote Service.



The screenshot shows the Nedap Device Management interface. The top navigation bar includes 'Device Management', a search bar ('Search e.g. an organization or store name'), and user icons. Below the navigation is a breadcrumb path: 'Navigate > Business Partner Demo > Division A > Store 8 > iSense'. The main content area displays a system ID: '579d2354-479d-4c73-a647-bc6dbe052109' and a 'iSense' button. On the left, a sidebar menu lists 'Overview', 'SYSTEM', 'iSense settings', 'History', and 'Remote service logs'. The 'Overview' tab is selected. The central panel is titled 'Access Remote Service' and contains a message: 'You are trying to remote service the system with the following specifics'. It lists details: System ID: 579d2354-479d-4c73-a647-bc6dbe052109, Label: iSense, Store: Store 8, Customer organization: Nedap Companies, Business partner: Nedap. A blue vertical bar on the right is labeled 'LEGAL NOTICE'. A box titled 'UNAUTHORIZED ACCESS TO SYSTEMS IS PROHIBITED' contains the text: 'You must have explicit permission to access, configure or update systems. All activities performed on any system will be logged, and violations of this policy will result in disciplinary action and may be reported to law enforcement.' At the bottom of this box are three buttons: 'Connect to web interface', 'Connect to SSH', and 'Cancel and go back'.

Add a report

With the report functionality, it is possible to export relevant system data.

Reports may be configured on different levels of the organization tree. For example, it is possible to generate reports on the organization and store levels and send both reports to different email addresses. To set up multiple reports, follow the steps below for each separate report.

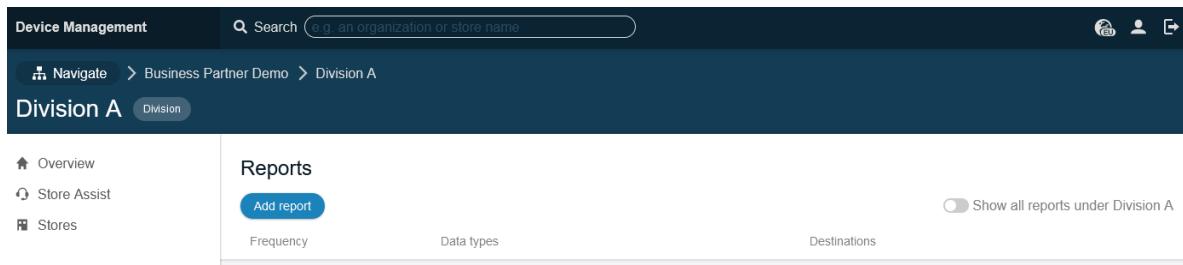
1. Search for the organization, navigate to the level in the organization tree where you want to create the report, and click on “Reports.”

Reports

Reports

Reports under

- Once you are at the level where you want to create a report, click on the “Add report” button.



The screenshot shows the Nedap Device Management interface. At the top, there's a search bar with placeholder text "Search e.g. an organization or store name". Below the search bar, the navigation path is "Device Management > Business Partner Demo > Division A". On the left, there's a sidebar with links for "Overview", "Store Assist", and "Stores". The main content area is titled "Reports" and contains a blue "Add report" button. Below the button are three filter tabs: "Frequency", "Data types", and "Destinations". A toggle switch on the right is labeled "Show all reports under Division A".

- The first screen contains the general settings of the report (what data to include, format, etc.). After selecting these options, click on “Save changes” to proceed to the next step.
- After the general settings, the delivery method must be set. You can add multiple FTP and/or e-mail destinations for the file.

FTP DESTINATIONS

No FTP destinations have been configured.

[Add FTP destination](#)

EMAIL DESTINATIONS

No email destinations have been configured.

[Add email destination](#)

Reports will only include data from stores with the correct subscriptions, as visible during the report setup.

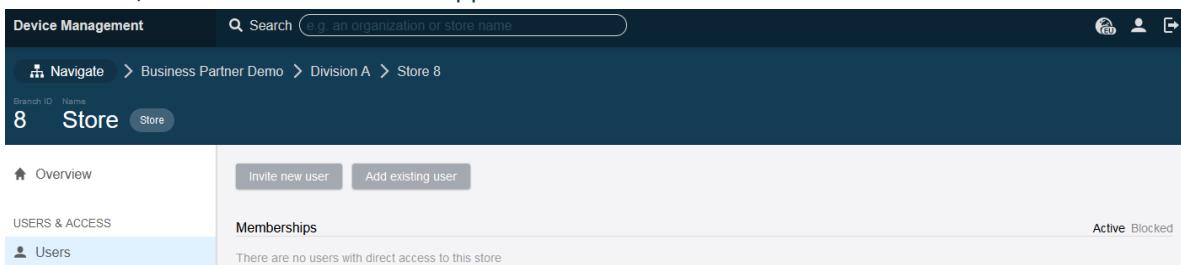
For integrations, always use the CSV column header titles instead of the column number so that integrations will continue working when a column is added in the future.

User management

Invite new users

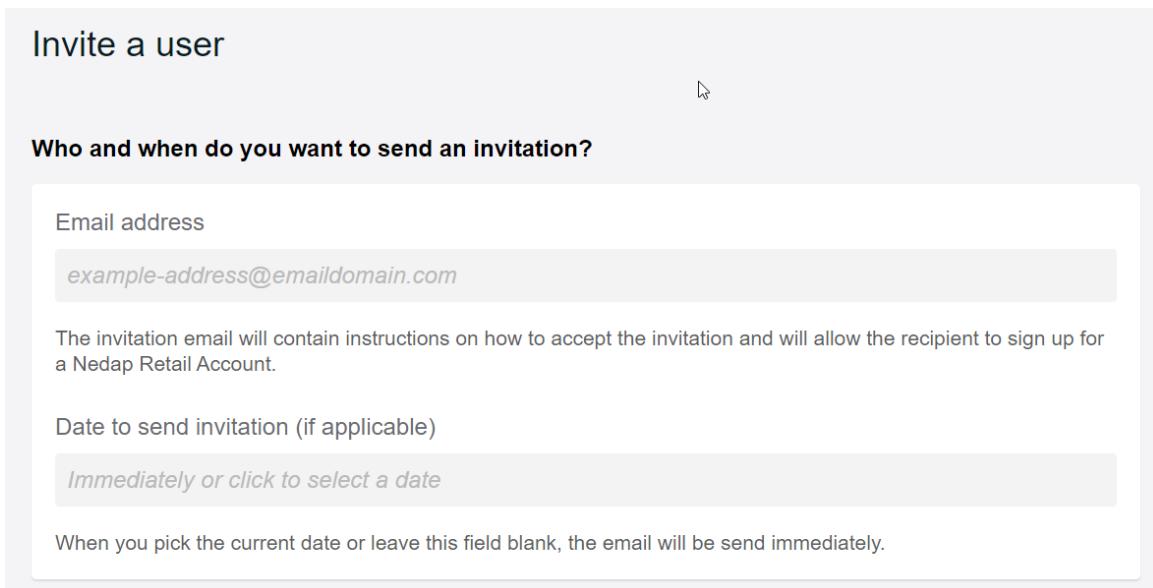
In Device Management, a technical ambassador can invite users to customer organizations, (sub)divisions, or stores. Once a user is invited to a specific level, this user will have access to the data from that level downward in the hierarchy. Follow the steps below to invite a user:

1. Search for the organization, navigate to the proper division, and store where a user needs to be invited.
2. Once you are at the level you want to invite a user to, click on the “Users” button. A list of currently invited and/or added users will then appear.



The screenshot shows the Device Management interface. At the top, there's a search bar with placeholder text "e.g. an organization or store name". Below the search bar, the navigation path is shown as "Navigate > Business Partner Demo > Division A > Store 8". On the left, there's a sidebar with "Branch ID" and "Name" fields, and a "Store" button. The main content area has tabs for "Overview", "Invite new user" (which is highlighted in grey), and "Add existing user". Under "OVERVIEW", it says "There are no users with direct access to this store". On the right, there are "Active" and "Blocked" user counts.

3. Click on “Invite new user” to start the invitation process.
4. a. Enter the email address of the person you want to invite.
b. Select which actions and access apply for this user.
c. Select which “External permissions” apply for this user.
d. Click on 'Send invitation'.



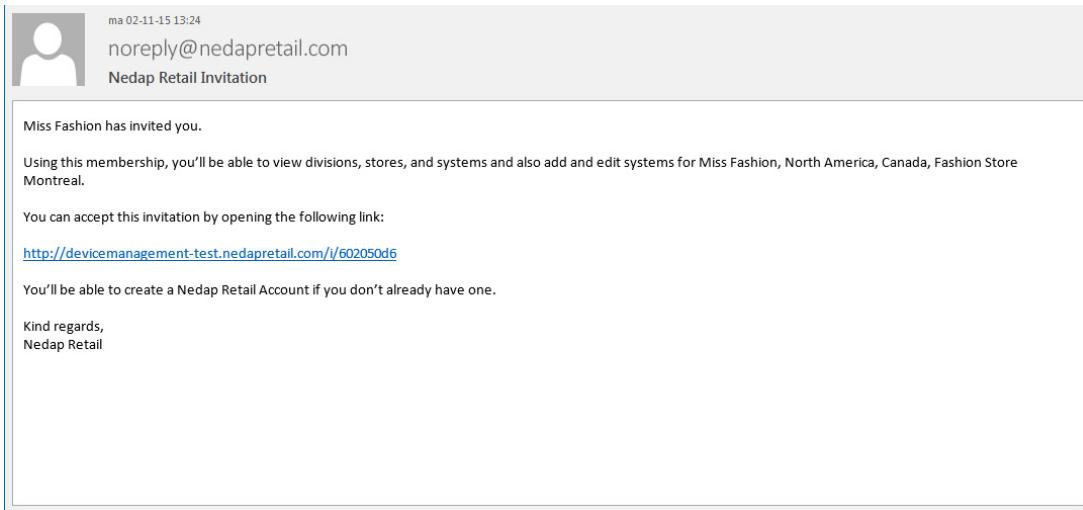
The dialog box is titled "Invite a user". It contains a section for "Who and when do you want to send an invitation?".
Email address: example-address@emaildomain.com
The invitation email will contain instructions on how to accept the invitation and will allow the recipient to sign up for a Nedap Retail Account.
Date to send invitation (if applicable): *Immediately or click to select a date*
When you pick the current date or leave this field blank, the email will be sent immediately.

5. Once the invitation has been sent, the user will receive an email from Nedap Retail explaining how to accept the invitation. The user can use an existing Nedap Retail Account to accept the invitation, or he/she can create a new one.
6. When the user accepts the invitation, he/she will gain access to the organization, division, or store where he/she was invited.

Please make sure you invite the user to the right level within the customer organization; the user will be able to see all stores and divisions on lower levels.

Invitation flow

1. A Nedap Business Partner invites a person to a retail organization, division, or store.
2. This person receives an invitation from Nedap Retail to join the specific customer organization, division or store.



3. The user clicks on the authorization link in the email and is directed to Device Management. If the user is already logged in to Device Management, the user has the choice to accept the invitation with this account to switch to another account or create a new one. For this option, the user must click "Sign in with a different account."
4. Now, the user can log in using another existing account or create a new one.
5. Once this process is finished and the invitation has been accepted, the user has access to the organization, division, or store to which he/she was invited. Click on "Get started..." to proceed.

Please note that if you invite new users using your email address, these invitations will be linked to your account. Use the switch to another account option to link the right user to the organization, division, or store.

Block a user account

In Device Management, it is possible to block a user account.

1. Search for the user you want to block using the search bar.
2. Click on the user name to open the edit screen for the user account.
3. You can block the account by selecting "Block user" and saving the changes.
4. After blocking a user account, the user will be signed out and unable to log in again. The red "Blocked" marking can recognize a blocked account.



Business partners and subcontractors

Suppose subcontractors need access to specific organizations. In that case, it is possible to request a separate Device Management organization managed by the primary Nedap Retail Business partner.

Users from the primary business partner will then get a membership to the subcontractor company.

A subcontractor company can get access to specific customer organizations.

Nedap Retail Support can create subcontractors. When new subcontractors are needed in Device Management, please contact **support-retail@nedap.com**. Supply the following details in the request:

- Reason for the request
- Subcontractor name
- Users that need access from primary business partner organization
- Users (subcontractor)
- Street address or P.O. Box
- ZIP code
- City
- Country



The Partner Address Book on the Portal

The Partner Addressbook on the Portal can be used to find contact information of other partners.

The Partner Addressbook is powered by Device Management, which involves synchronization between Device Management and the Partner Portal.

Changes to your Partner Address Book entry

Changes within the Partner Addressbook can be done in Device Management. A **Partner Admin** within your organization can modify the data.

When a Partner Admin with the correct credentials enters Device Management, the [EDIT] button will be available on the company page to change the settings.

Should you encounter any problems while modifying, please contact the support team.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Document Version 61

Document Last modification date 31 October 2024

Document PDF Exported 31 October 2024 **by** Nedap Retail | Operations

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

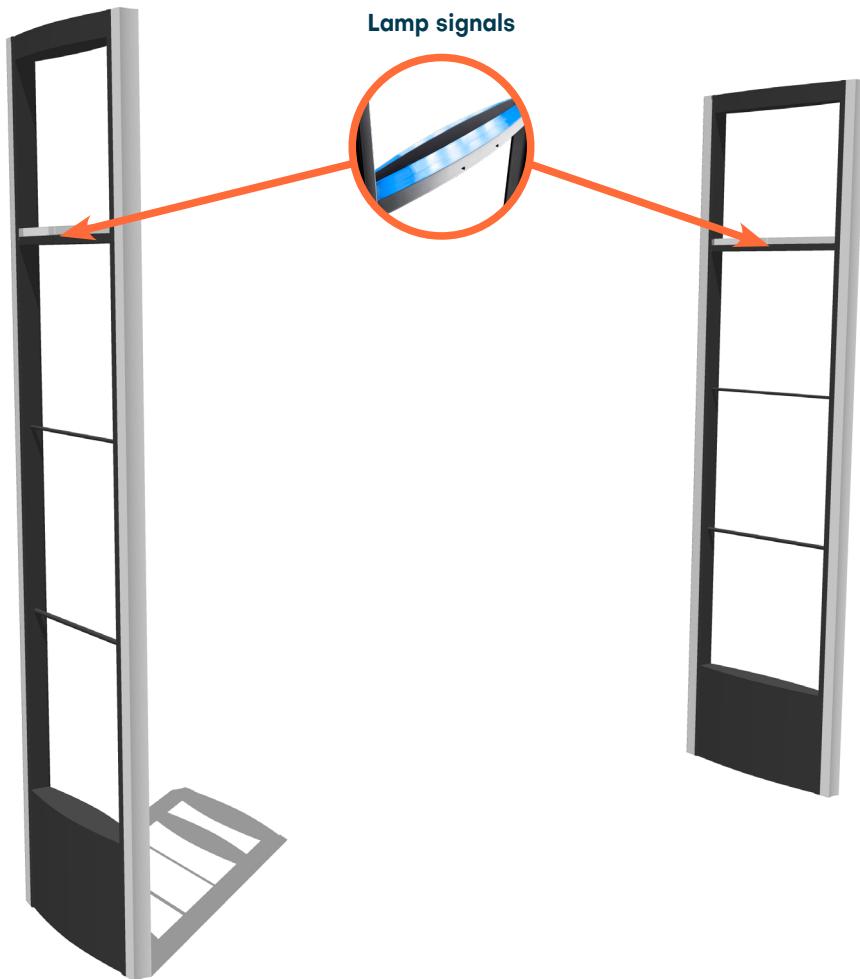


support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com





NEDAP ELECTRONIC ARTICLE SURVEILLANCE SYSTEM

Explanation of Nedap's article surveillance gates: signalling of secured articles and metal foiled items (prepared coats/bags).

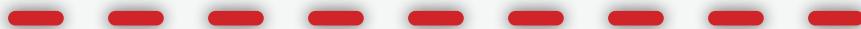
Antennas (article surveillance gates)

The antennas at the passageways for visitors can detect four things:

1. Secured items
2. Outgoing secured items
3. Incoming secured items
4. RFID detection and
5. Detection of metal foiled items (f.i. coats or bags prepared with metal foil)

Secured items

Are optically and acoustically indicated by the antennas by means of a red flashing light; an article, which is still secured, leaves the store.



Outgoing secured items

Are optically and acoustically indicated by the antennas by means of purple flashing light; an article, which is still secured, enters or leaves the store.



Incoming secured items

Are optically and acoustically indicated by the antennas by means of white flashing light; an article, provided with an 'active' label, enters the store.



RFID detection

RFID Secured items are optically indicated by an orange flashing light; an article, which is still protected with an RFID label, leaves the store.



Metal detection

Items are optically marked by the antennas by means of blue light; a large amount of metal is entering the store, which may indicate foil line prepared bags and / or coats.



Nedap Sense Guideline

iSense Basic System

Requirements

version 27, February 2025

About this document	3
System Orientation	4
Cable specifications	5
Cable length	6
Remarks	7
Power consumption iSense	8
Power Inserter	8
Power consumption iSense Lumen	10
Power Inserter	10
Maximum system size	12
Defining the system	12

About this document

To create a successful first-time-right iSense installation, execute this document's basic iSense system requirements.

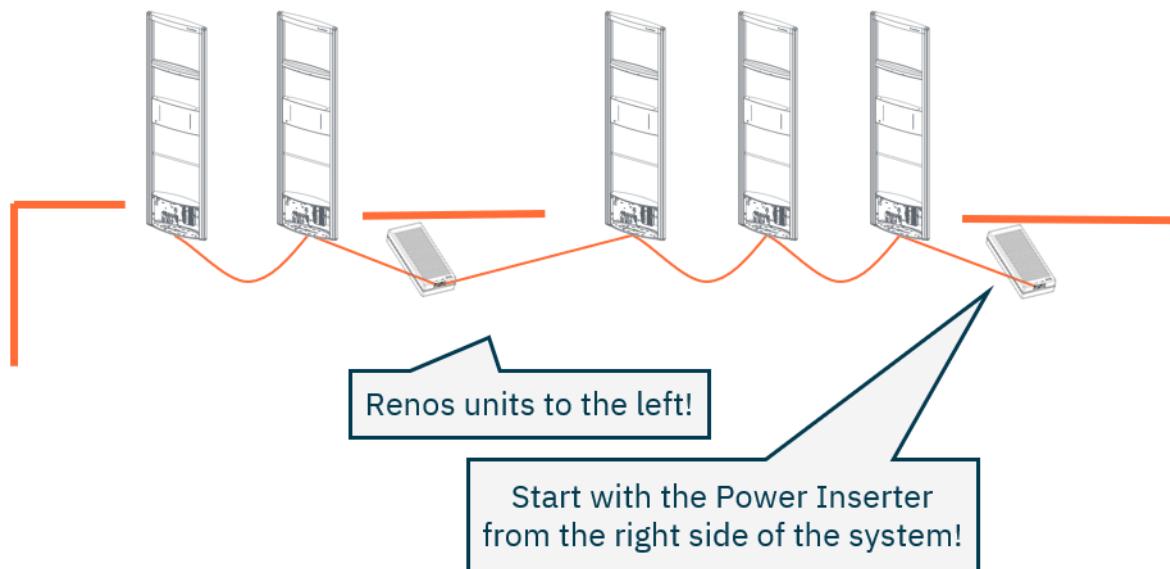
- i For more information on installing the Nedap products mentioned in this document, consult the product manuals at the Nedap Retail Portal.
- i Quick reference documents are available for almost all Nedap Retail hardware products. They are included in the product package and can be downloaded from the Product Catalog at the Nedap Retail Portal.
- i Please visit the **Partnership Downloads & Tools** portal page for information on project planning and all the steps to do a first-time-right installation.

System Orientation

For the functionality of the iSense system, all gates need to be orientated in the same way, and the 1st Power Inserter should be connected to the correct gate. The orientation and gate 1 (the first gate to receive power from the first Power Inserter) should be as follows:

EAS Role – Determine gate 1 by standing inside the store and looking out towards the exit

- The Power Inserter is on the right side of the first gate.
- The Renos electronics unit should be on the left side of the gate.



Cable specifications

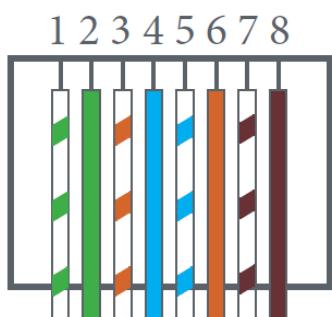
The following cable specifications are recommended for the iSense system:

- Use UTP Cat5e with a stranded copper core, with 24 AWG (0,51mm) core diameter.

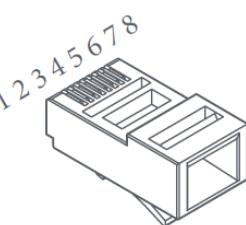
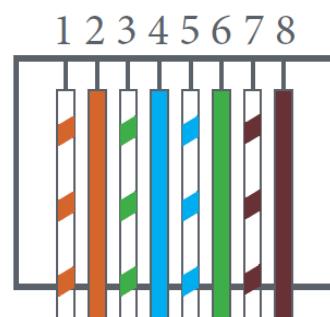
⚠️ Always connect **all four pairs** using the **T568B** termination standard or T568A if specifically required!

⚠️ Never use CCA (copper cladding aluminum) or CCS/CCF (copper cladding steel) cable!

T568A



T568B



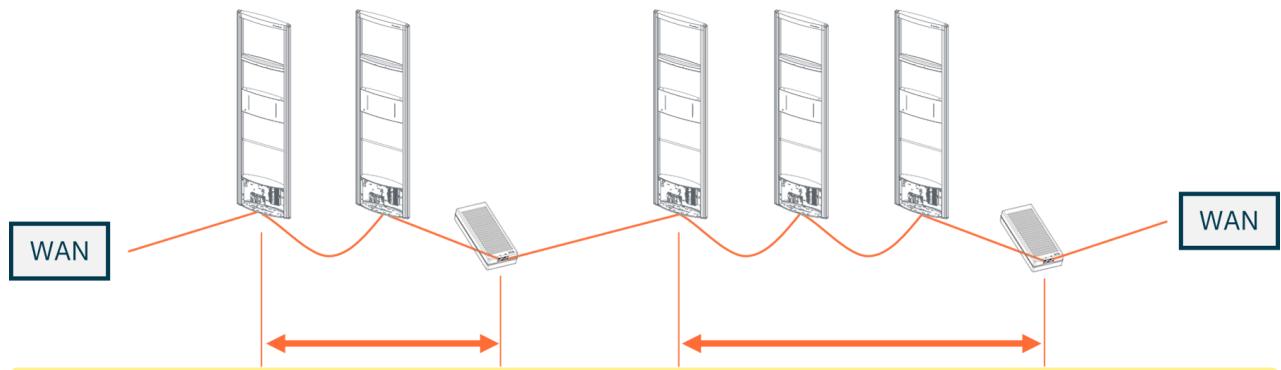
8P8C (RJ45)

Pin	T568A	T568B (Preferred)
1	Green + White	Orange + White
2	Green	Orange
3	Orange + White	Green + White
4	Blue	Blue
5	Blue + White	Blue + White
6	Orange	Green
7	Brown + White	Brown + White
8	Brown	Brown

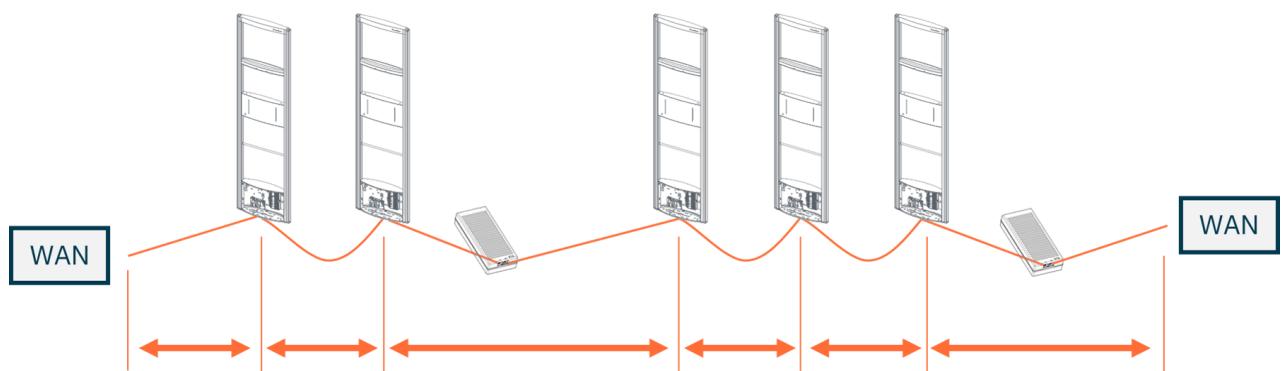
Cable length



Maximum cable length of **80 meters / 250 ft** between a Power Inserter and the last Renos unit that receives the power from this Power Inserter:



Maximum cable length of **80 meters / 250 ft** between Renos units (excluding Power Inserters) and between the first (or last) Renos unit and the WAN connection in the store:



Remarks

- It is possible to use your own preferred connectors.
- Make sure that the connectors are suitable for the cable and that the correct crimping tool is used for the connector.
- Follow the recommendations of the cable manufacturer.
- Local regulations may dictate using a specific cable type or rating.



We recommend placing the Power Inserter in the switch room (near a power socket) when the ethernet cable lengths allow. This way, the customer only has to arrange an ethernet outlet near the system.



If the cable lengths between two groups exceed approximately 50 meters / 164 ft, consider splitting a system into two.

Power consumption iSense

Power Inserter

Once the position of the gates is established, the location of the Power Inserters can be determined. A maximum number of Renos units can be connected to one Power Inserter, depending on which technologies are used and the number of add-ons in use. The table shows the number of Power Inserters needed for each hardware configuration.

Cable conditions: a CAT5E cable with a recommended maximum length of 80 meters / 250ft.

Technologies In Use	#Units / PI 230V	#Units / PI 115V
RF	6	5
RFID	5	5
RF + RFID	3	3
RF + MD	5	5
RF + 2 SD's	5	4
RF + MD + 2 SD's	4	4
RF + RFID + MD	3	3
RFID + MD	5	5
RF + RFID + MD + 2 SD's	3	3

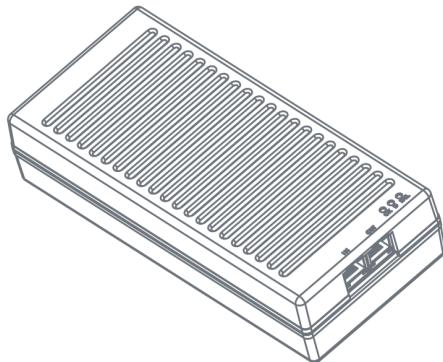
Index:

- RF = Radio Frequency 8.2 MHz
- RFID = RAIN Radio Frequency Identification (~900 MHz)
- MD = Metal Detection
- 2 SD's = 2 connected smart deactivators

- In all situations, it is possible to place Infrared beam sensors for, i.e., customer counting



Please note: Always use a Nedap Power Inserter (Power-over-Ethernet) to power Renos systems. It is not possible to use generic Power-over-Ethernet switches or stand-alone inserters.



If the retailer wants to upgrade an 8.2 MHz RF system to RFID later on, please consider the power requirements for RFID.



Make sure that the Power Inserter is connected to an always-on power socket! This is better for the firmware/hardware, continuous system monitoring, and remote firmware updates during the night.



Ensure the Power Inserter is placed at least 1 m (3.3 ft.) from the gates. When placed closer to the gate, it might cause interference with the RF technology.



Do not disconnect network cables in the system when still powered! First, disconnect the power cable from the power inserter(s).

Power consumption iSense Lumen

Power Inserter

Once the position of the gates is established, the location of the Power Inserters can be determined. A maximum number of Renos units can be connected to one Power Inserter, depending on which technologies are used and the number of add-ons in use. The table shows the number of power inserters needed for each hardware configuration.

Cable conditions: a CAT5E cable with a recommended maximum length of 80 meters / 250ft.

Technologies In Use	#Units / PI 230V	#Units / PI 115V
RF	5	5
RFID	5	5*
RF + RFID	3	3
RF + MD	5	4
RF + 2 SD's	4	4
RF + MD + 2 SD's	4	3
RF + RFID + MD	3	3
RF + RFID + MD + 2 SD's	Three**	Three**

Index:

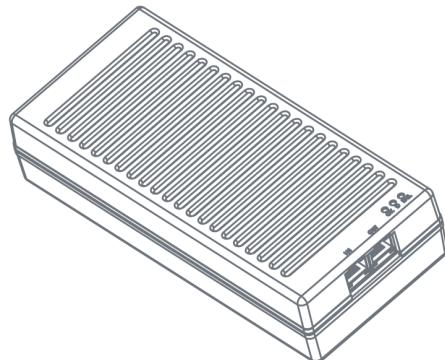
- RF = Radio Frequency 8.2 MHz
- RFID = RAIN Radio Frequency Identification (~900 MHz)
- MD = Metal Detection
- 2 SD's = 2 connected smart deactivators

* if the RFID units are operated monostatically, only four gates can be connected to a single power inserter.

** If the RFID units are operated monostatically, only two gates can be connected to a single power inserter.



Please note: Always use a Nedap Power Inserter (Power-over-Ethernet) to power Renos systems. It is not possible to use generic Power-over-Ethernet switches or stand-alone inserters.



If the retailer wants to upgrade an 8.2 MHz RF system to RFID later on, please consider the power requirements for RFID.



Make sure that the Power Inserter is connected to an always-on power socket! This is better for the firmware/hardware, continuous system monitoring, and remote firmware updates during the night.



Ensure the Power Inserter is placed at least 1 m (3.3 ft.) from the gates. When placed closer to the gate, it might cause interference with the RF technology.



Do not disconnect network cables in the system when still powered! First, disconnect the power cable from the power inserter(s).

Maximum system size

Defining the system

When a store requires gates to be placed at several locations, there needs to be a decision on how to combine these gates into one or multiple systems. The following rules need to be taken into account:

- 1. A different role is a separate system.** Combining gates for Electronic Article Surveillance (EAS) with gates from the stockroom to the sales floor is impossible in one system. Both roles need different systems with their own Power Inserter and customer network connection.
- 2. Within the EAS role, all gates are combined into one system.** To minimize interference between gates, the Renos platform has a built-in synchronization mechanism for both RF and RFID technology. The gates must be connected to one system for this synchronization mechanism.
- 3. However, the maximum cable length requirements must be considered.** If it is impossible to put all the gates within a role in one system due to the maximum cable length requirements, you can split the installation into two or more systems. In this case, assign each system a different *multi-system channel* during the RF configuration.



Build a separate system for the stockroom to the sales floor and goods receiving roles when there is a different door or entrance.

Role/Store Position	Product	Max. System Size (Gates)
EAS	RF Gates	100
	Hybrid RF/RFID	30
	RFID gates	30
Stockroom / Salesfloor	RFID gates	2
Goods receiving	RFID gates	2



It is not possible to combine gates with RFID and without RFID in one system. Either all gates should have RFID or no gates should have RFID.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2025

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 27

Document Last modification date 17 February 2025

Document PDF Exported 17 February 2025 by Nedap Retail | Operations



support-retail@nedap.com



Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com

Nedap Sense Guideline

iSense Firmware Versions

version 79, February 2025

Introduction	3
Situation to overwrite the firmware:	3
Firmware change	4
1. Firmware overwrite - single unit overwrite.....	5
2. Firmware overwrite - complete system overwrite.....	9
Progress indication system firmware over-write	11
Firmware overwrite - Equalizing a system with a mix of firmware versions	12
Upgrade a system where the current firmware version is older than 14.35	13
3. Firmware update - complete system update	14
4. Firmware update - via Device Management	15

Introduction

Nedap Retail frequently releases new firmware versions. They contain new functionalities, improved performance, security updates, bug fixes, and stability improvements.

It is recommended that the firmware version be updated to the latest during installation. When using Nedap Device Management, systems can be updated remotely to the newest firmware version even after installation.



Find firmware version

The installed firmware version of an iSense product can be found on a sticker on the box.

All Renos units in an installation must have the same firmware version installed to ensure the system functions correctly. This document describes the various ways to change the firmware of a Renos unit using the firmware-overwrite and firmware-update mechanisms.



The firmware-overwrite procedure removes all changed settings from the unit and sets it back to factory defaults. To keep the system settings, you should update the system firmware instead.

All over-write and local update methods require a software image. You can download the software images from the Nedap Retail portal at "**iSense - Firmware & Drivers**." Before proceeding with these steps, ensure your laptop has the correct image (IMG) files.

Situation to overwrite the firmware:

- Old hardware with old firmware is still in stock, which you would like to upgrade when installing.
 - The preferred method is to bring the system online and use the updating mechanism through Device Management.
 - If the system cannot be brought online -> see “2. Firmware overwrite - complete system overwrite.”
- If an installation mixes old and new firmware (e.g., gates from two shipments), see “Equalizing a system with a mix of firmware versions.”
- If you wish to downgrade a unit to replace one in an existing installation with older firmware, see “1. Firmware overwrite—single unit overwrite.”



The system must remain powered during overwriting, especially during the critical flash phase. However, if power is lost and a unit becomes unresponsive, it can always be recovered using the single-unit overwrite mechanism..

Firmware change

There are five ways to change the firmware version on an iSense system:

1. Firmware overwrites: Single unit overwrites. The overwrite can be executed by inserting a USB flash drive with the correct firmware into the USB port.
2. Firmware overwrite: This is a Complete system overwrite. You can execute the overwrite with files on your laptop during the configuration wizard.
3. Firmware overwrite: Equalizing a system with a mix of firmware versions.
4. Firmware update: This is a Complete system update. You can execute the update using files on your laptop during the configuration wizard.
5. Firmware update: Via Device Management. The update can be executed via the Device Management service.

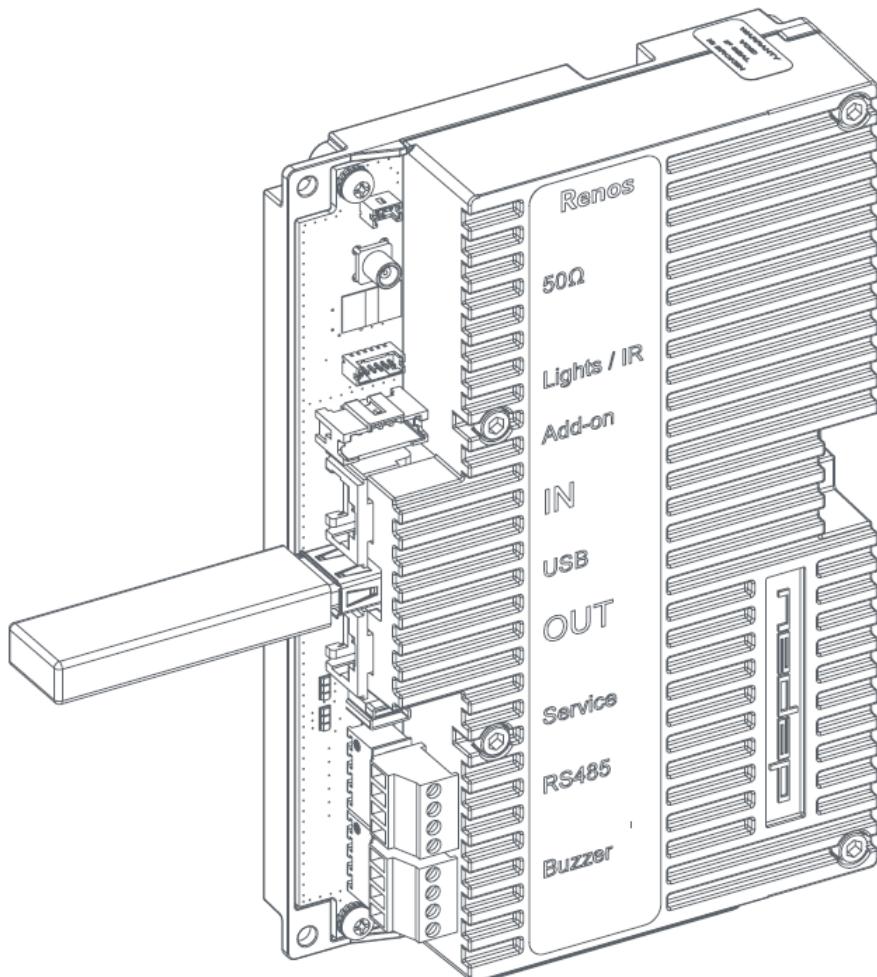


If the system is integrated with a third-party system, please confirm the firmware version with that third party before installing it.

1. Firmware overwrite - single unit overwrite

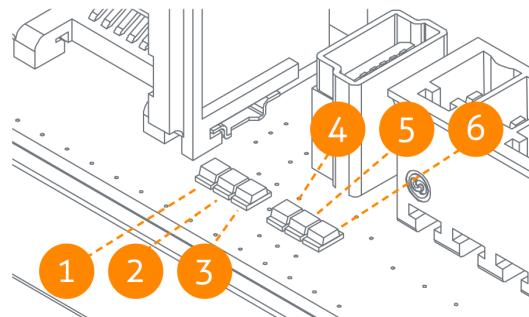
To overwrite the system on a single unit, follow the next steps:

1. Download the correct overwrite firmware image file from the Nedap Retail portal.
2. Open the `zip` file and extract the `img` file to a USB flash drive (see explanation in the chapter below).
3. Turn off the power of the system.
4. Disconnect all the cables except the ethernet cable from the IN port.
5. Insert the USB flash drive in the USB port of a Renos unit (it is possible to use multiple USB flash drives at the same for a system with numerous Renos units)



6. Power the system while the USB flash drive is still connected.

7. Wait until LEDs 4, 5, and 6 are off again. This can take around ten minutes.



Led 4 - Yellow	Led 5 - Green	Led 6 - Green	Phase	Duration
off	off	off	boot	~ 6 seconds
on	off	off	flashing preparation	~ 7 to 8 minutes
on	off	on	critical flashing	~ 1 minute
off	off	off	flashing done	until power is cycled

8. Turn off the power again and remove the USB flash drive.

9. Turn on the power.

Led 4 - Yellow	Led 5 - Green	Led 6 - Green	Phase	Duration
off	off	off	boot	~ 20 seconds
heartbeat	off or blinking for shorter and longer periods	off	finalizing flashing	~ 4 minutes
heartbeat	off or blinking for shorter and longer periods	on	iSense up and running	until power is cycled

10. Connect all cables back into the Renos Unit.

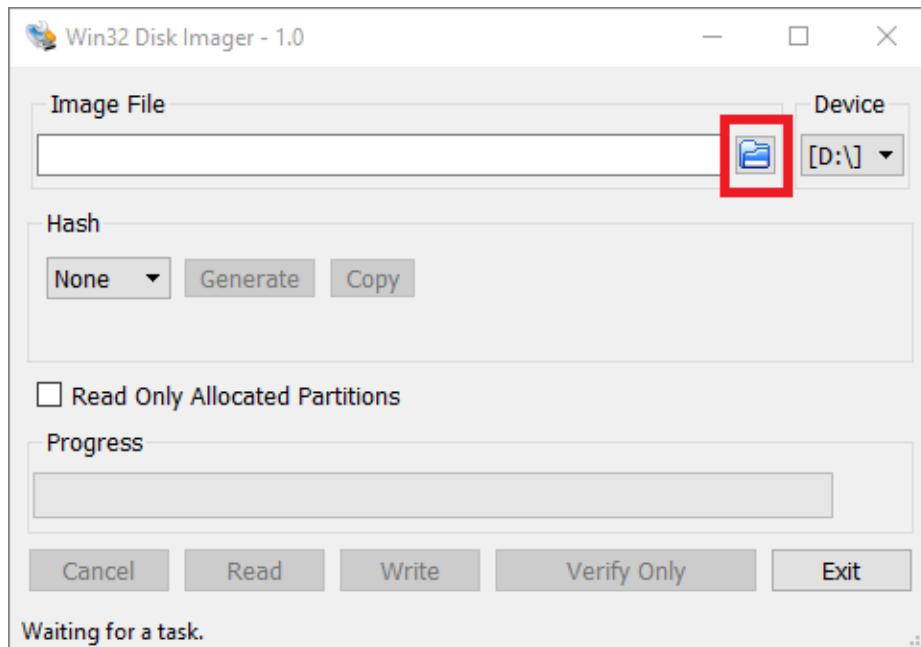


Please note that when using the 'local - single unit flash' firmware change, all settings and configurations of the unit are lost. It's only possible to execute this on-site and not remotely, as the system must be re-configured before it is usable.

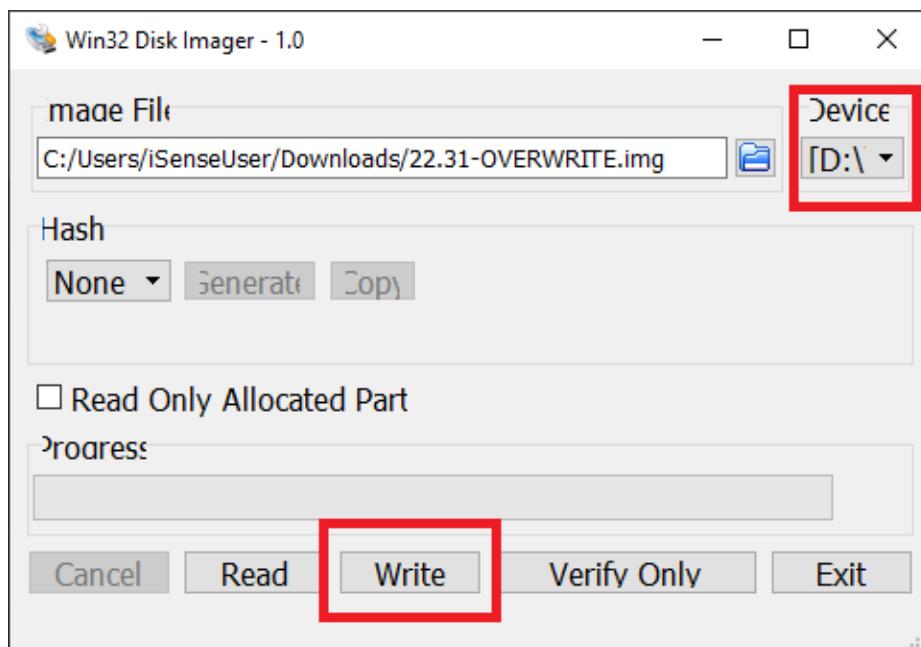
Extract file to USB flash drive

Supported from version 13.39 and higher requires the `.img` file of the desired firmware and a tool to extract the image onto a USB flash drive, for example Win32DiskImager. This can be found at: <http://sourceforge.net/projects/win32diskimager>

Open Win32DiskImager and select the downloaded firmware image.



Select the USB flash drive to which you would like to extract the image and press write. The firmware image will now be written to the USB flash drive.



2. Firmware overwrite - complete system overwrite

Download the correct firmware image file from the Nedap Retail portal (**overwrite version**). Enter the configuration wizard and accept all Renos units in the system that should be updated. Press the “Advanced” button and follow the steps to change the firmware. One of these steps is to upload the firmware image file.



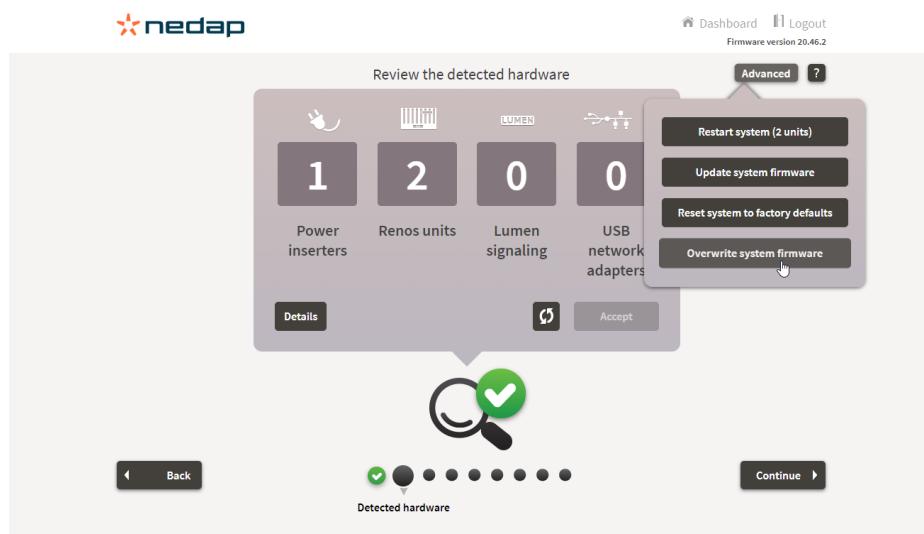
Please note that all system settings and configurations are lost. It's only possible to execute this on-site and not remotely, as the system must be re-configured before it is usable.

The system will overwrite the firmware in 3 steps:

1. The firmware image will be uploaded from your laptop to the Renos unit you are connected to.
2. The firmware will be distributed to all the units in the system.
3. The firmware will be installed on all the units.

To upgrade a system, proceed to the detected hardware section of the wizard and press the “Accept” button to accept the detected hardware.

After pressing the “Advanced” button, the firmware overwrite is possible. Select the desired firmware (**overwrite image**) by pressing the “Browse” button and follow the on-screen instructions to complete the firmware overwrite.





[Dashboard](#) [Logout](#)
Firmware version 20.46.2



Provide a Renos firmware image file to overwrite the system version

Overwrite system firmware

Click Browse and select your Renos firmware image (.img) file:

[Browse](#)

Overwriting system firmware will delete all data and settings!

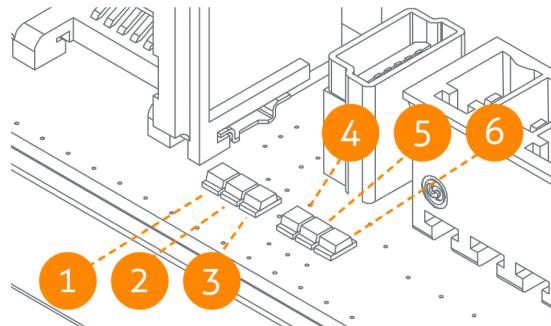
I accept that all data and settings will be lost.



[Cancel](#)

[Overwrite system firmware](#)

Progress indication system firmware over-write



Led 4 - Yellow	Led 5 - Green	Led 6 - Green	Phase	Duration
heartbeat	off or blinking for shorter and longer periods	on	iSense up and running	until the 'Overwrite firmware' button is pressed
heartbeat	off or blinking for shorter and longer periods	off	restarting	~25 seconds
off	off	off	boot	~ 6 seconds
on	off	off	flashing preparation	~ 40 seconds
on	off	on	critical flashing	~ 1 minute
off	off	off	boot	~ 20 seconds
heartbeat	off or blinking for shorter and longer periods	off	finalizing flashing	~ 4 minutes
heartbeat	off or blinking for shorter and longer periods	on	iSense is up and running	until power is cycled

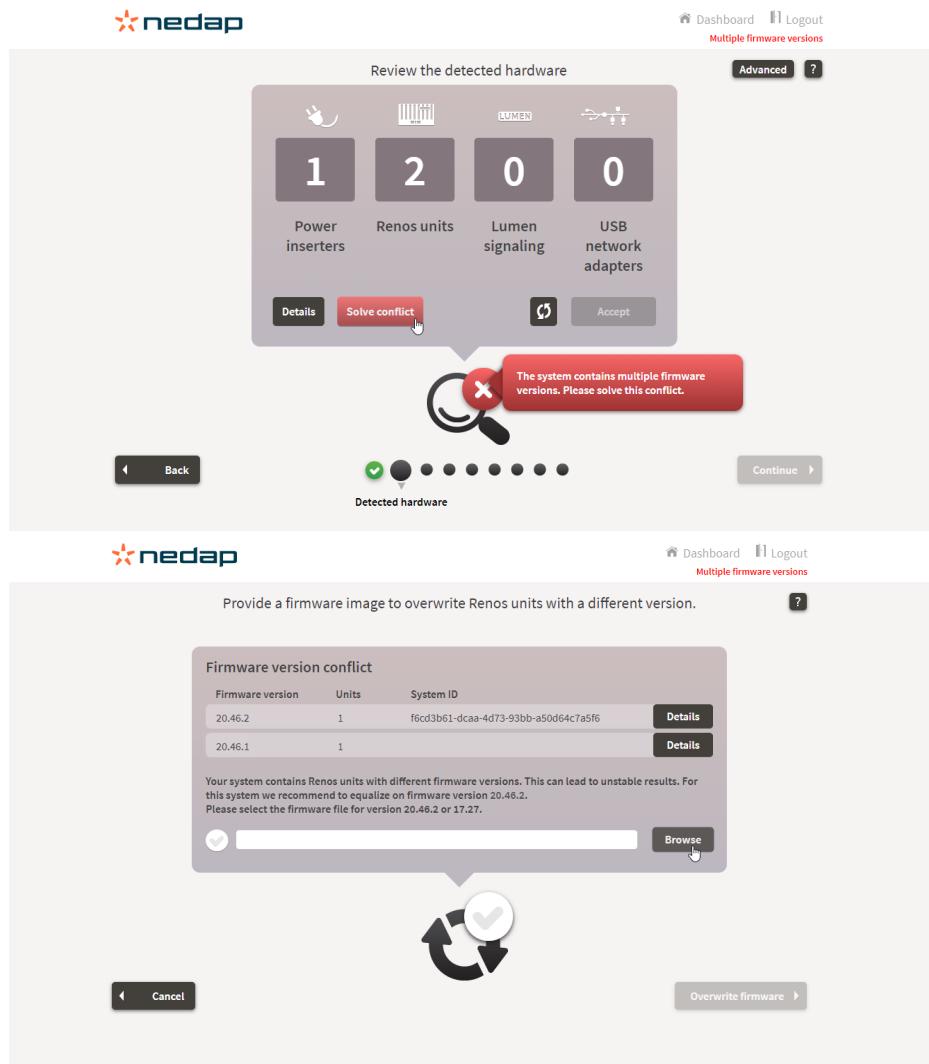
In total, approximately 7 minutes

Firmware overwrite - Equalizing a system with a mix of firmware versions

The steps listed below must be taken if you are connected through a unit with firmware 14.35 or higher.

A firmware conflict is automatically detected, and you are requested to press the "Solve conflict" button to resolve this issue.

Select the desired firmware (**overwrite image**) by pressing the “Browse” button and follow the on-screen instructions to complete the firmware overwrite.



The screenshot shows two consecutive pages from the nedap software:

Page 1: Review the detected hardware

- Header: Dashboard, Logout, Multiple firmware versions
- Section: Review the detected hardware
 - Icons: Power inserters, Renos units, Lumen signaling, USB network adapters
 - Data: 1 Power inserter, 2 Renos units, 0 Lumen signaling, 0 USB network adapters
 - Buttons: Details, Solve conflict (highlighted), Accept
- Message: The system contains multiple firmware versions. Please solve this conflict.
- Footer: Back, Continue, Detected hardware

Page 2: Provide a firmware image to overwrite Renos units with a different version

- Header: Dashboard, Logout, Multiple firmware versions
- Section: Firmware version conflict

Firmware version	Units	System ID
20.46.2	1	f6cd3b61-dcaa-4d73-93bb-a50d64c7a5f6
20.46.1	1	

Your system contains Renos units with different firmware versions. This can lead to unstable results. For this system we recommend to equalize on firmware version 20.46.2. Please select the firmware file for version 20.46.2 or 17.27.

- Input: Browse (highlighted)
- Icon: Refresh with checkmark
- Buttons: Cancel, Overwrite firmware



Upgrade a system where the current firmware version is older than 14.35

In firmware versions before firmware version 14.35, the wizard cannot be used for firmware upgrading. However, two alternative methods are available.

1. Use the single-unit overwrite method on all units. See “1. Firmware overwrites Local - single unit overwrites” for this.
2. You can overwrite a single unit with firmware version 14.35 and use the wizard from that unit to overwrite the system firmware.

3. Firmware update - complete system update

To update a system with firmware version 16.30 or higher, proceed to the detected hardware section of the wizard and press the “Accept” button to accept the detected hardware.

After pressing the “Advanced” button, the firmware update is possible. Select the desired firmware (**update image**) by pressing the “Browse” button and follow the on-screen instructions to complete the update.





4. Firmware update - via Device Management

To update the firmware via Device Management, please ensure the system is configured, delivered, and connected to the Device Management service. Then, navigate to the Device Management website and use the functionality there to initiate the firmware update.

The available updates are shown on the main page of the system.

Press the “Schedule” button for the desired update.



Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2025

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 79

Document Last modification date 11 February 2025

Document PDF Exported 11 February 2025 by Nedap Retail | Operations



support-retail@nedap.com



Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com

Connected Device Guideline

Renos Windows Driver Installation

version 12, January 2024



Introduction	3
Windows	4
Install driver first, connect USB afterwards	5
Connect USB first, update driver afterwards	7
Used abbreviations	14

Introduction

When working with a Windows device, you need to install a driver to communicate with the service port of the Renos unit.

Linux and Apple computers do not need a driver.



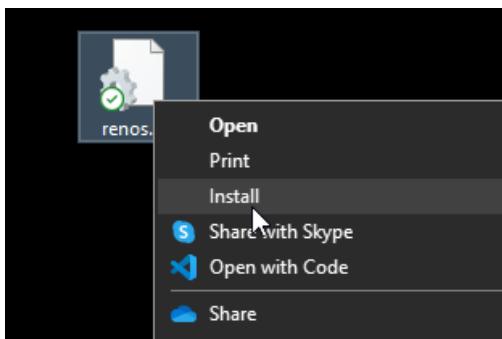
Windows

There are two options to get the driver installed.

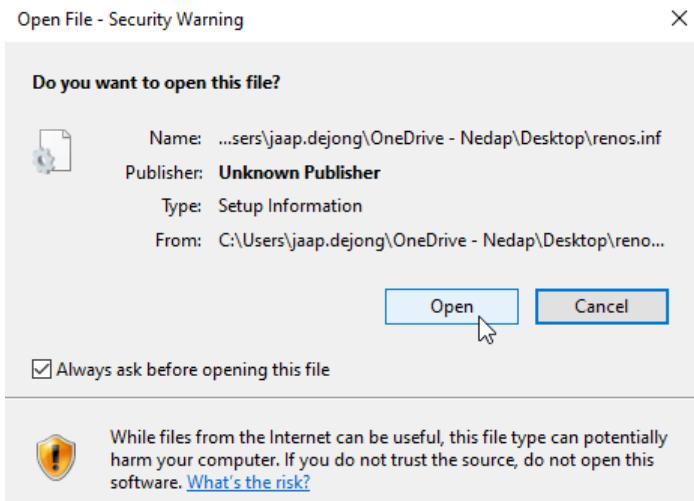
- The first option is installing the driver and then connecting the USB cable.
- The second option is the other way around: connect the USB cable and then update Windows's chosen driver.

Install driver first, connect USB afterwards

- Download the driver from the Nedap Retail Partner portal: <http://portal.nedapretail.com>
- Open the file and save `renos.inf` and `renos.cat` where you can find them when needed
- Unplug your USB device cable (with the other end connected to the Renos unit)
- Right click the `renos.inf` file (make sure the corresponding `renos.cat` file is in the same directory)



- Press `Install`



- Press `Open`

Windows Security

X

Would you like to install this device software?



Name: Renos Network adapters
Publisher: N.V. Nederlandse Apparatenfabriek "Ned..."

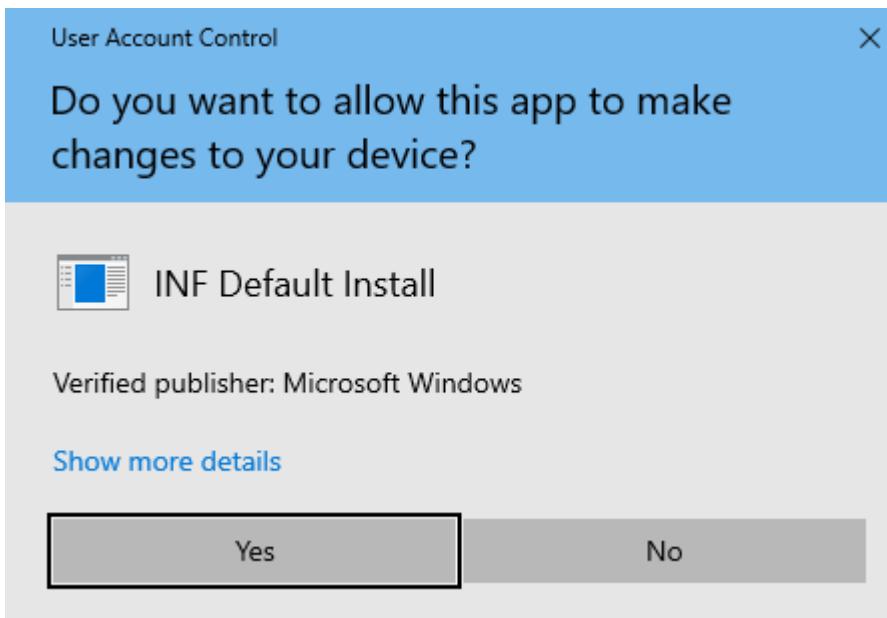
- Always trust software from "N.V. Nederlandse Apparatenfabriek "Ned...".

Install

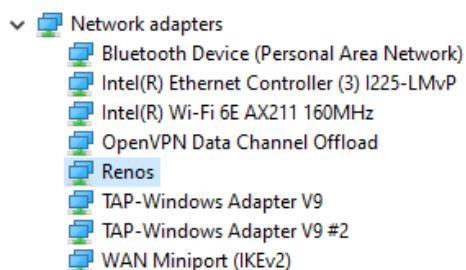
Don't Install

⚠ You should only install driver software from publishers you trust. [How can I decide which device software is safe to install?](#)

- Press Install



- Press Yes
- Wait until done
- Restore the connection to the Renos unit
- In the Device Manager you should see the Renos driver



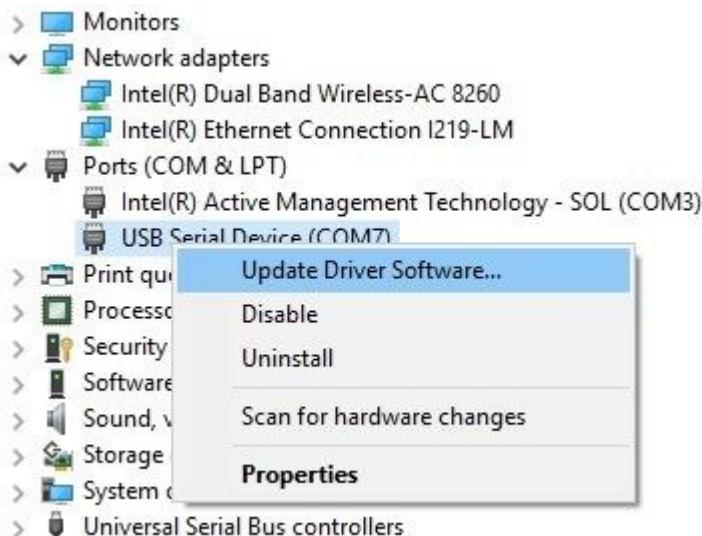
- In some situations, this will not be the case. Windows probably already assigned a driver. In this case, continue with the second option. Right below...

Connect USB first, update driver afterwards

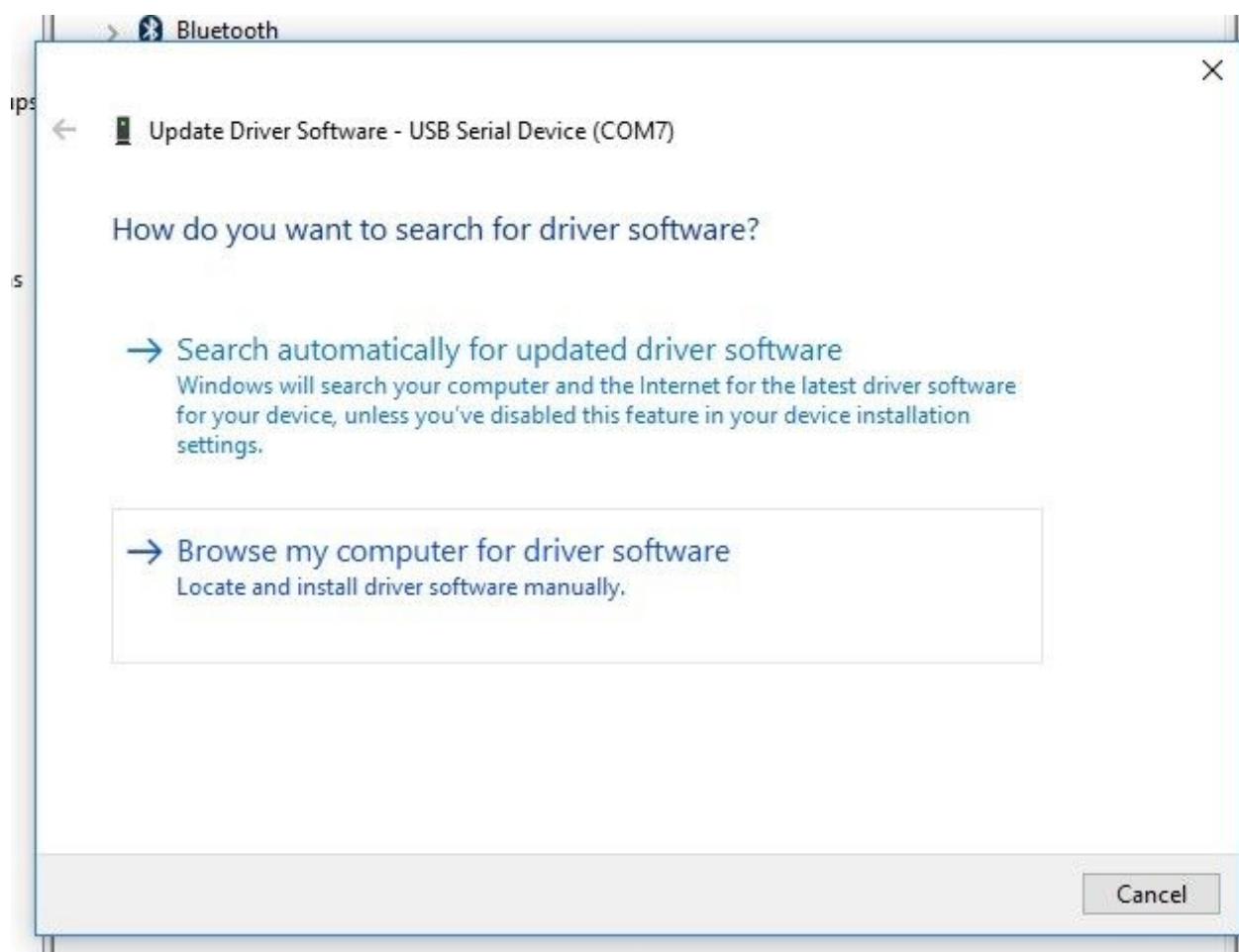
- Download the driver from the Nedap Retail Partner portal: <http://portal.nedapretail.com>
- Open the file and save `renos.inf` and `renos.cat` where you can find them when needed
- Plug-in your USB device cable (with the other end connected to the Renos unit). Once the driver has loaded, you might see a pop-up saying that Windows has found a new hardware device
- Start the Device Manager
- Open Network adapters and search for RNDIS/Ethernet Gadget or USB Serial Device (COMx)
- If not found, try to open Other devices or Ports (COM & LPT) and search for RNDIS/Ethernet Gadget or USB Serial Device (COMx)



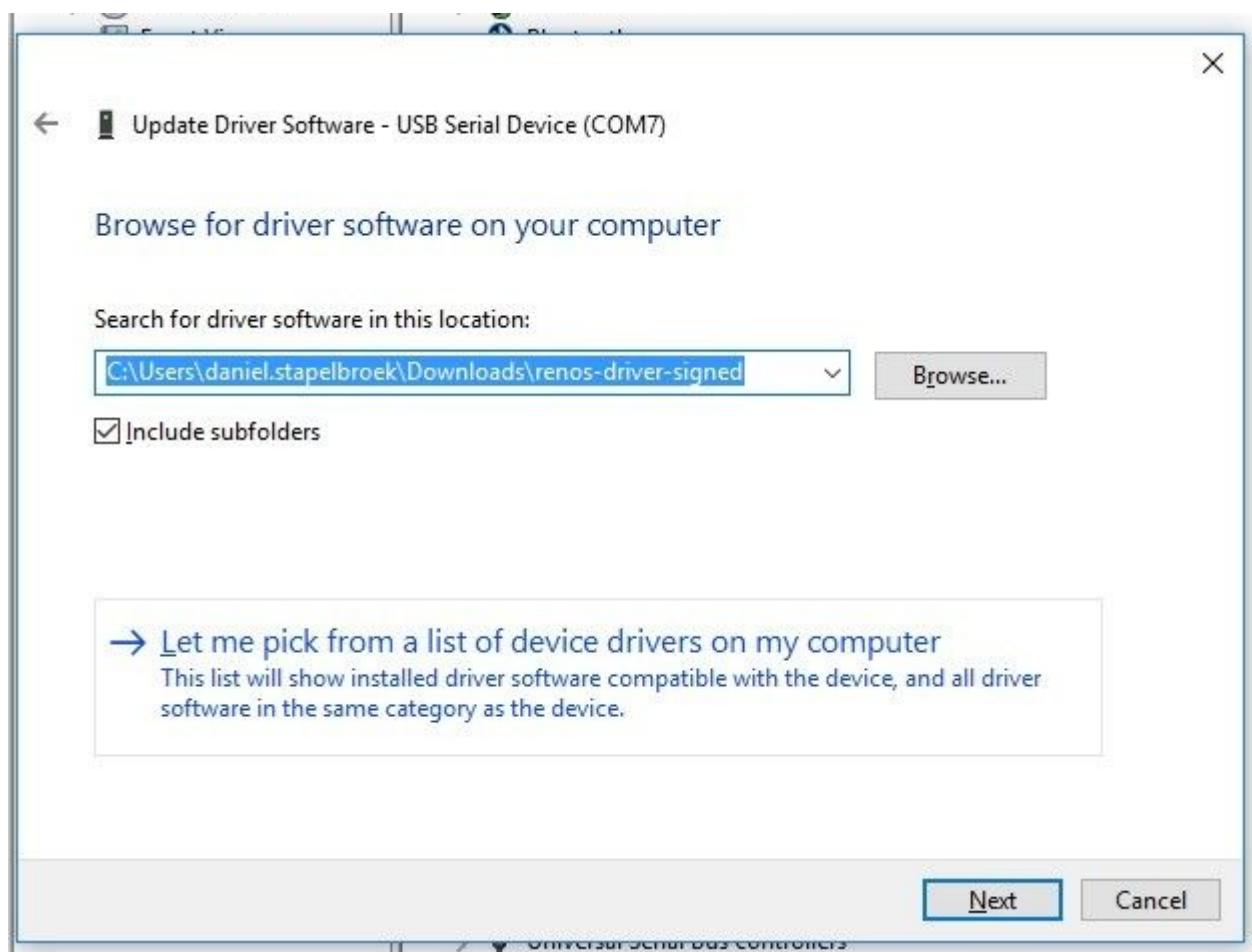
- To be sure that you are going to update the correct device, unplug the USB cable and verify that this device is removed from the list
- Restore the connection to the Renos unit
- Right-click RNDIS/Ethernet Gadget or USB Serial Device (COMx)



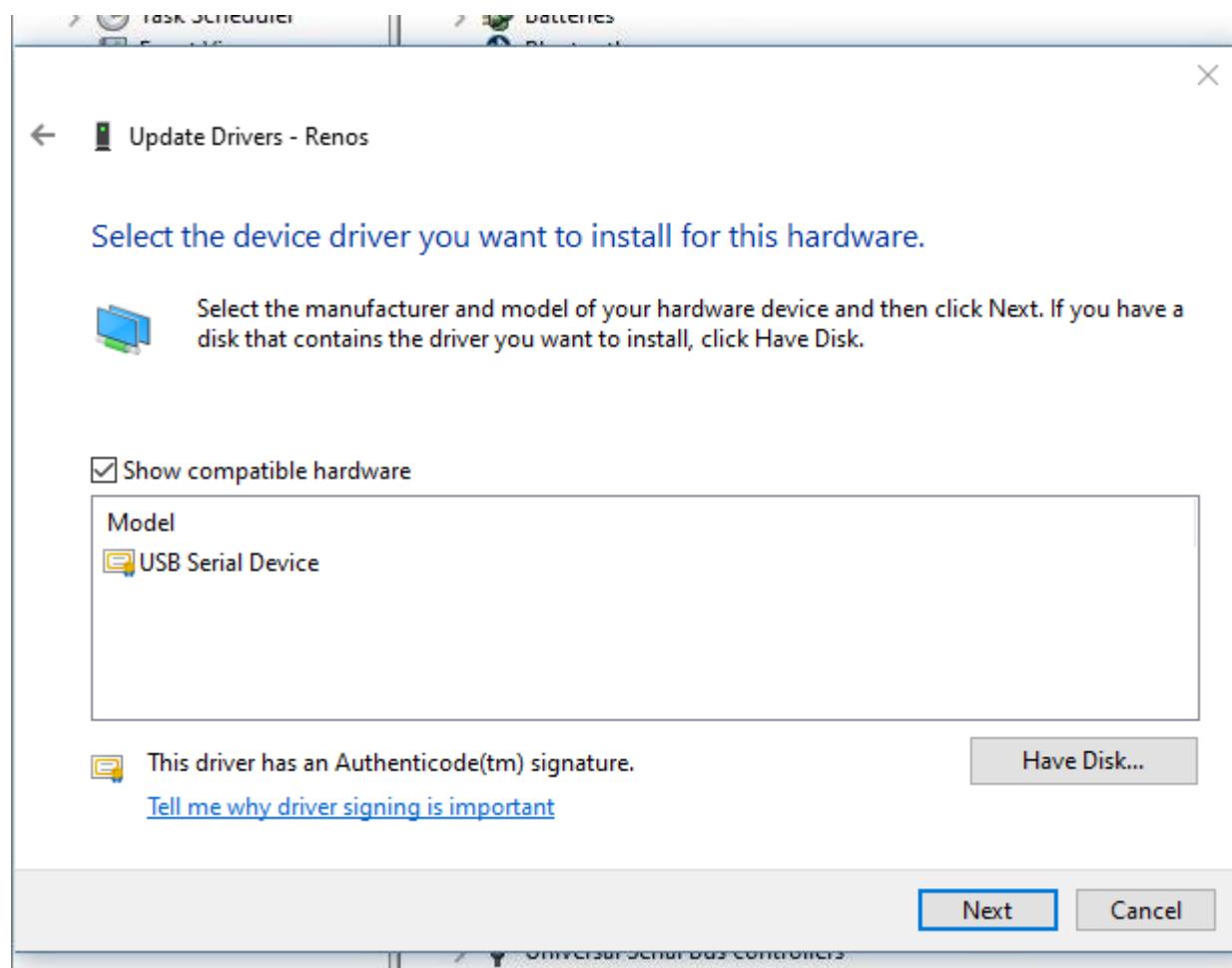
- Select Update Driver Software...



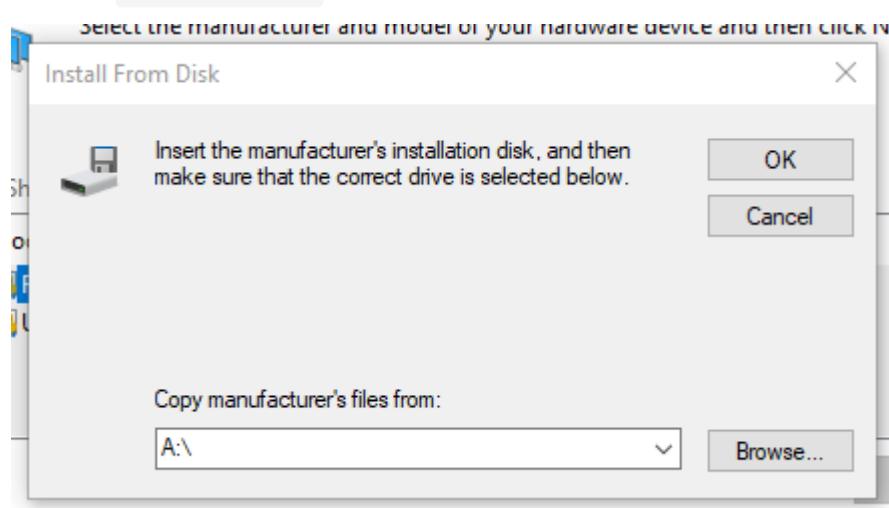
- Select **Browse my computer for driver software**



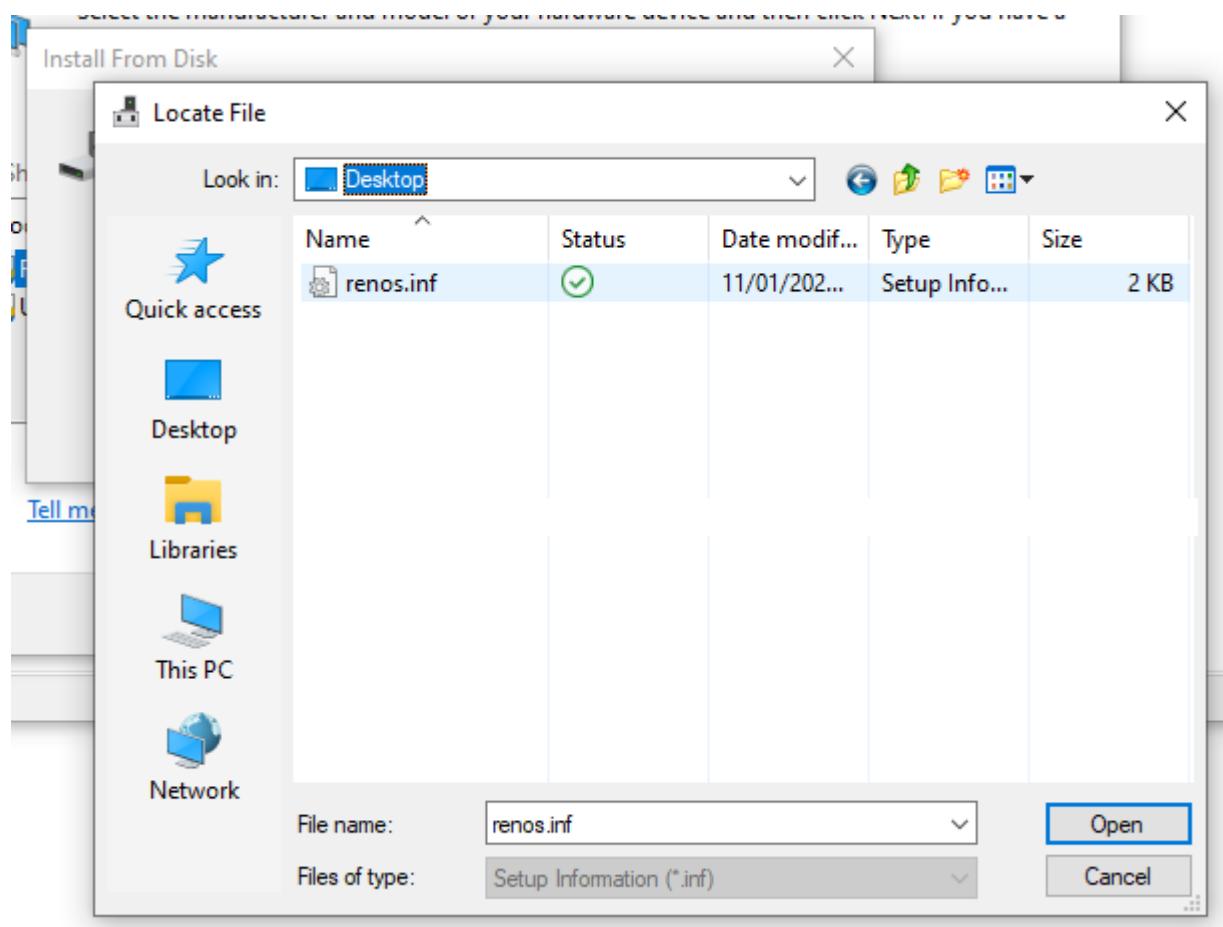
- Select Let me pick from a list of device drivers on my computer



- Click **Have Disk...**

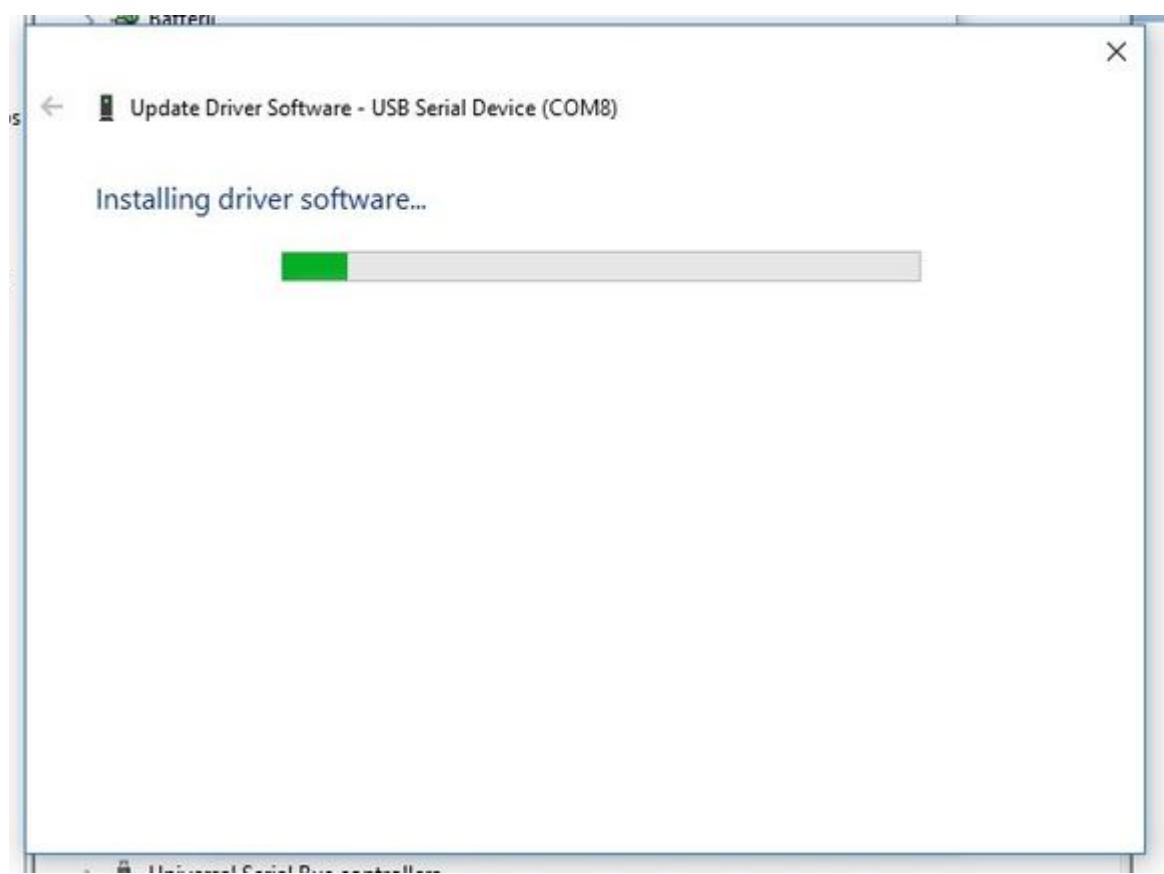


- Select the location where you saved the `renos.inf` file

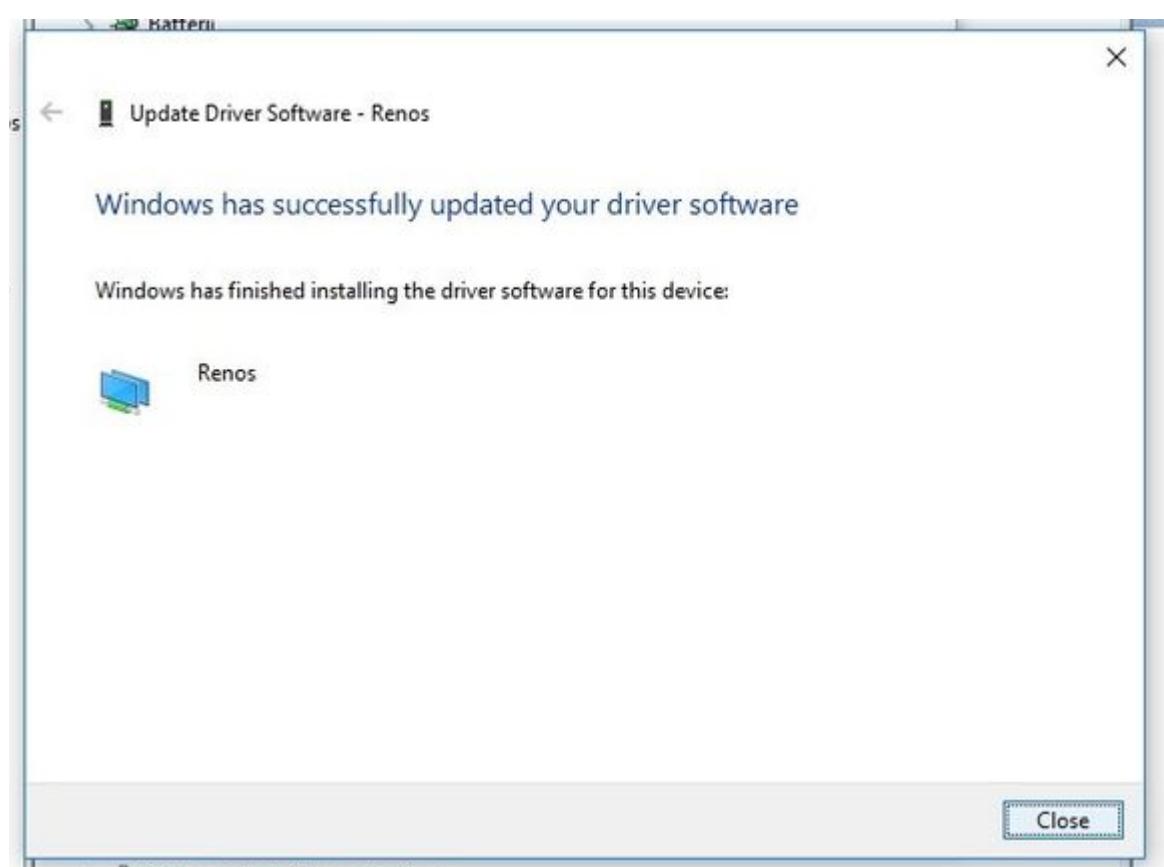


- Click Open
- Click OK
- Click Next

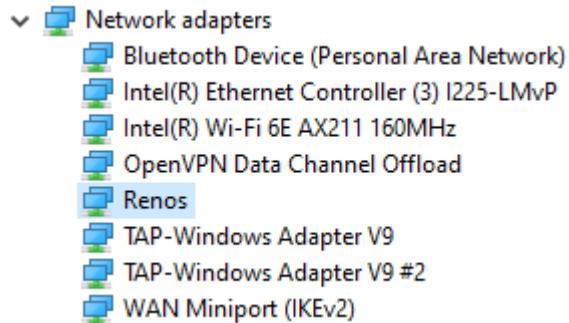
Installing starts:



And when done:



- Click Close
- In the Device Manager you should see the Renos driver



Used abbreviations

Standard terms may be abbreviated in this document. The following table shows the descriptions of the abbreviations used. RFID-specific abbreviations are highlighted.

Abbreviation	Description
API	Application Programming Interface - is a way for two or more apps to communicate with each other.
CC	Customer Counting
DM	Device Management
EAS	Electronic Article Surveillance
EPC (RFID)	The Electronic Product Code is one of the available formats for encoding identifiers on RFID tags. The EPC is a globally unique number that identifies a specific item in the supply chain.
External CC	External Customer Counting (e.g., Brickstream)
FRS	Fast Remote Service
GS1 (RFID)	(Global Standards 1) An international standards organization with member bodies in more than 100 countries worldwide. Nedap Retail follows the GS1 and RainRFID standards.
GTIN (RFID)	A Global Trade Item Number (GTIN) is a number that uniquely identifies a product. It can be found beneath the barcode of a product.
IO Box	Input/Output Electronics device
IR	Infra Red
MD	Metal Detection
RF	Radio Frequency
RFID	Radio Frequency Identification

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 12

Document Last modification date 31 January 2024

Document PDF Exported 31 January 2024 **by** Nedap Retail | Operations



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com



Connected Devices Guideline

iSense Factory Reset Procedure

version 43, February 2024

Introduction	3
Materials needed	4
Procedure.....	5
Step 1: Disconnect	5
Step 2: Connect USB cable	5
Step 3: Connect power	5
Step 4: Wait while the unit is being reset	6
Step 5: Disconnect all cables	6
Step 6: Connect all cables again	7
Step 7: Check the unit	7
Factory reset for the whole system from user interface	8
Used abbreviations	9

Introduction

When a completely configured Renos unit is removed from a system, and added into a new system, it is necessary to execute the factory reset procedure. This might also be the case when an unrecoverable configuration failure has occurred.

It is also possible to reset the whole system back to factory defaults within the configuration Wizard.



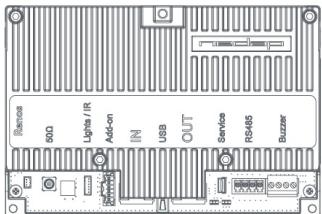
Materials needed

1. Renos unit running firmware version 17.07 or newer
2. USB to mini-USB cable
3. Nedap Power Inserter
4. Network cable

Procedure

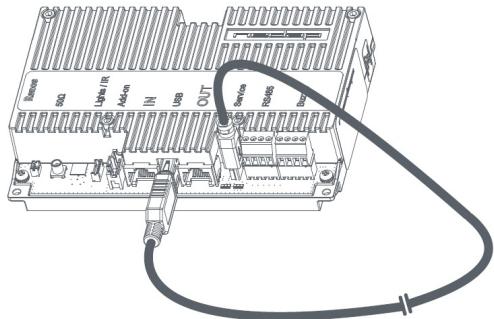
Step 1: Disconnect

Disconnect all cables from the Renos unit. Remember how they were connected.



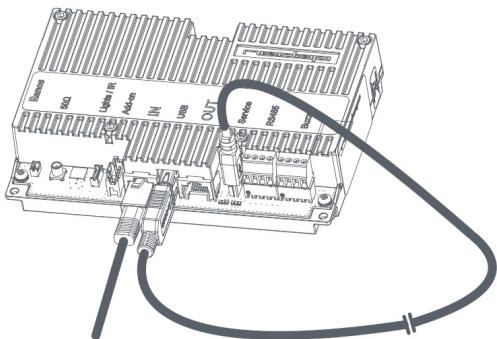
Step 2: Connect USB cable

Connect one end of the USB cable to the USB connector between the network connectors and the other end to the USB service port. Both ends of the same USB cable are now connected to the Renos unit.



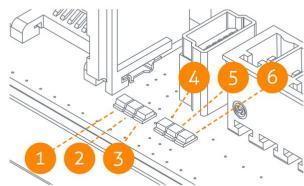
Step 3: Connect power

Connect the network cable to the Out port of the Power Inserter and to the IN port of the Renos unit. After that connect the the Power Inserter to a power outlet.



Step 4: Wait while the unit is being reset

The LEDs will show the following behavior.



Led 4 - Yellow	Led 5 - Green	Led 6 - Green	Phase	Duration
off	off	off	boot	~ 20 seconds
heartbeat	off or blinking for shorter and longer periods	off	starting	~ 25 seconds
heartbeat	off or blinking for shorter and longer periods	blink a couple of times		~ 3 seconds
heartbeat	off or blinking for shorter and longer periods	on	erasing the settings	~ 9 seconds
heartbeat	off or blinking for shorter and longer periods	blink a couple of times		~ 3 seconds
heartbeat	off or blinking for shorter and longer periods	off	shutting down	~ 25 seconds
heartbeat	off	off	ready	until power switched off

Step 5: Disconnect all cables

Remove the USB cable and switch off the power supply to the Renos unit.

Step 6: Connect all cables again

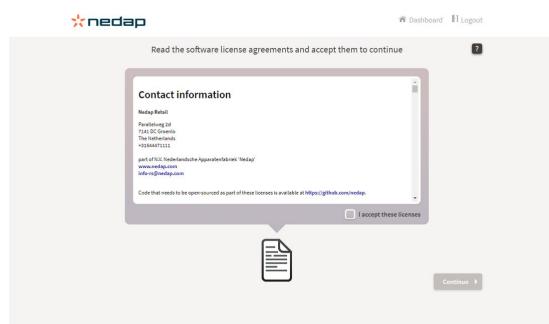
Connect the network cables to the Renos unit and power the system.

Step 7: Check the unit

Now you can connect the Renos unit again.

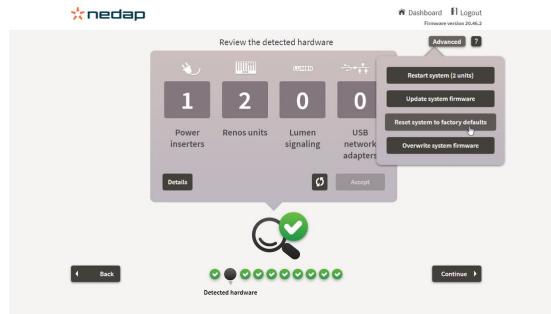
You can check if the reset was successful as follows:

1. Make sure the unit is connected and the firmware is running (the right green LED is on).
2. Connect your computer to the USB service port and open <http://192.168.133.1> in your browser.
3. If you see the license screen the reset was successful:



Factory reset for the whole system from user interface

It is also possible to perform a factory reset for the whole system at ones. This can be done in the hardware detect page under "Advanced" in the configuration wizard.



Used abbreviations

Standard terms may be abbreviated in this document. The following table shows the descriptions of the abbreviations used. RFID-specific abbreviations are highlighted.

Abbreviation	Description
API	Application Programming Interface - is a way for two or more apps to communicate with each other.
CC	Customer Counting
DM	Device Management
EAS	Electronic Article Surveillance
EPC (RFID)	The Electronic Product Code is one of the available formats for encoding identifiers on RFID tags. The EPC is a globally unique number that identifies a specific item in the supply chain.
External CC	External Customer Counting (e.g., Brickstream)
FRS	Fast Remote Service
GS1 (RFID)	(Global Standards 1) An international standards organization with member bodies in more than 100 countries worldwide. Nedap Retail follows the GS1 and RainRFID standards.
GTIN (RFID)	A Global Trade Item Number (GTIN) is a number that uniquely identifies a product. It can be found beneath the barcode of a product.
IO Box	Input/Output Electronics device
IR	Infra Red
MD	Metal Detection
RF	Radio Frequency
RFID	Radio Frequency Identification

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 43

Document Last modification date 16 February 2024

Document PDF Exported 16 February 2024 by Nedap Retail | Operations



support-retail@nedap.com



**Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands**

nedap-retail.com

Connected Devices Guideline

iSense Dashboard

version 62, February 2024

Introduction	3
Information and options	3
Preparation	4
What is needed	4
Installation.....	5
Configuration.....	6
Delivery test	9
Used abbreviations	10

Introduction

This document describes how to configure the iSense Dashboard. The iSense Dashboard is already available on the iSense system and only needs to be activated by entering a valid Dashboard License Key in the Wizard.

Information and options

The iSense Dashboard gives insights in the system events, hardware status and enables several basic actions

Events

- RFID events (including hexadecimal EPC overview)
- RF events
- Metal Detection Events
- Customer counting events
- Smart deactivator events

Actions

- Test RF alarm
- Snooze 15 minutes
- Maintenance mode
- Alarm volume setting per group
- Download events

Preparation

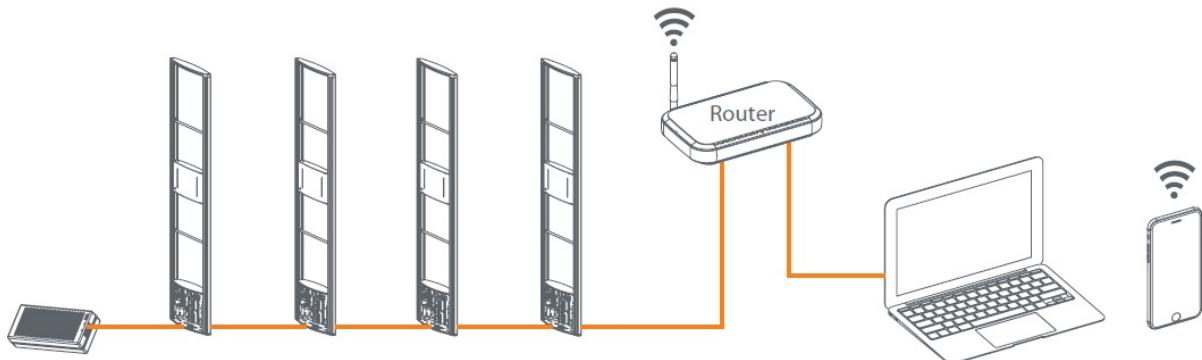
- Make sure you know how the network is setup in which the iSense system is connected.
- Check which device the customer will use to connect with the iSense dashboard and if the IP address of the iSense system is accessible in that way.

What is needed

- An installed iSense system
- Standard Installation tools and materials:
 - A laptop to access the Installation Wizard
 - Nedap Retail account to login
 - A USB to mini-USB cable with ferrite filter
- A valid iSense Dashboard License Key. When the iSense Dashboard is purchased, the the Dashboard License Key will be printed on the order confirmation, the packing list and the invoice.
- A device from which the manager or security guard will access the iSense Dashboard.

Installation

A router is necessary between the system and the iSense Dashboard. This could be an existing router within the store, or a standalone router.



1. Connect the iSense system to the router. There are several possibilities:
 - a. Network cable connected to the IN-port of the first power inserter.
 - b. Network cable connected to the OUT-port of the last Renos unit (inside the last gate).
 - c. Network cable is connected to the USB port of one of the Renos units, using a USB-network adapter.
2. Connect the dashboard-computer with a network cable to the router.
3. Start the configuration by connecting your laptop to a Renos unit

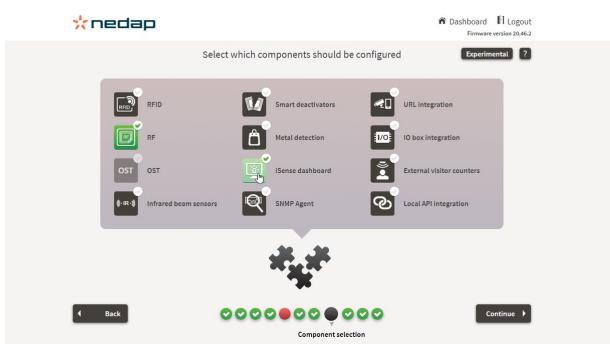
Configuration

- Connect to the iSense installation wizard: Open the web-browser and type "192.168.133.1" into the address bar.
- In the wizard, configure the network settings with a Static IP or via DHCP and write down the IP-address for future use.

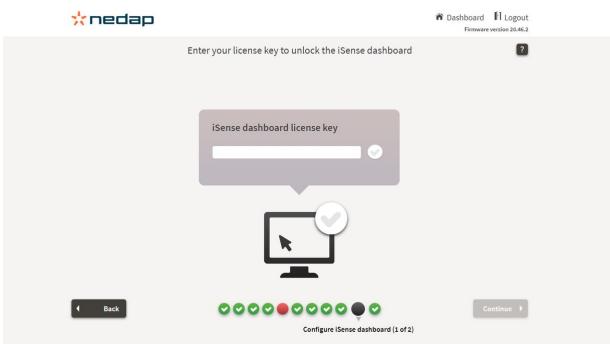


When using DHCP make sure that the IP address will remain the same, because the IP address is needed to access the iSense dashboard

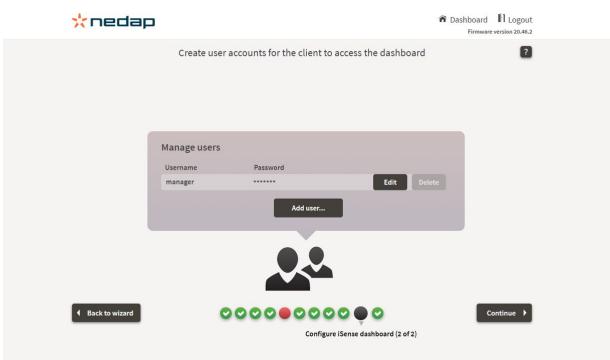
- On the 'Component selection' page, select the iSense dashboard:



- On the page 'configure iSense dashboard', fill in the Dashboard License Key (that you will find on the order confirmation, on the packing list and on the invoice):



- In the next page you can create a custom username and password for the manager or security guard to login with.



- Finish the wizard and deliver the system
- In the dashboard-computer, open an up-to-date web browser (Google Chrome is recommended).
- In the address bar, type in the system's IP-address (which you wrote down earlier).
- You will see the login page of the iSense dashboard:



- At this place the user can login with the created username and password (the default login credentials are 'manager' (username) and 'retailer' (password)). The iSense dashboard will be shown. Examples:

iSense dashboard

System status: ok

RF alarms: 98 today

Download data | Settings | Logout

Gate 1: 18 minutes ago
 Gate 1: 24 minutes ago
 Gate 1: 35 minutes ago
 Gate 1: 42 minutes ago
 Gate 1: 46 minutes ago
 Gate 1: 48 minutes ago
 Gate 1: 49 minutes ago
 Gate 1: 52 minutes ago

nedap

iSense dashboard

System status: ok

RFID alarms: ok today

Download data | Settings | Logout

Gate 1: 17 hours ago
 Gate 1: 4 days ago
 Gate 1: 4 days ago
 Gate 1: 5 days ago
 Gate 1: 6 days ago
 Gate 1: 10 days ago

nedap

iSense dashboard

Download data | Settings | Logout

Event Type	Event ID	Timestamp
Gate 1	YED4038051002710000D1AA	17 hours ago
Gate 1	YED4038051002710000HDC0C	4 days ago
Gate 1	YED4038051002710000HDC10	4 days ago
Gate 1	YED4038051002710000HDE8E	5 days ago
Gate 1	YED4038051002710000HDE9A	5 days ago
Gate 1	YED4038051002710000H724C	5 days ago
Gate 1	YED4038051002710000H8098	5 days ago
Gate 1	YED4038051002710000H724C	5 days ago
Gate 1	YED4038051002710000HDA0A	6 days ago
Gate 1	YED4038051002710000H0223	10 days ago
Gate 1	YED4038051002710000H0784	10 days ago
Gate 1	YED4038051002710000H080A	11 days ago
Gate 1	YED4038051002710000H081E	11 days ago
Gate 1	YED4038051002710000H081E	11 days ago

nedap

- Create a shortcut/bookmark (e.g. on the desktop or inside the web browser) to the iSense Dashboard, so that the user can access the dashboard.

Delivery test

1. Use a test label to raise an alarm, and check whether this event shows up in the dashboard.
2. Show the store manager how to reach the dashboard, and provide him/her with the created (or default) login credentials.
3. Demonstrate the different functions of the iSense Dashboard to the retailer and/or security employees.

You have now successfully configured the iSense Dashboard.

Used abbreviations

Standard terms may be abbreviated in this document. The following table shows the descriptions of the abbreviations used. RFID-specific abbreviations are highlighted.

Abbreviation	Description
API	Application Programming Interface - is a way for two or more apps to communicate with each other.
CC	Customer Counting
DM	Device Management
EAS	Electronic Article Surveillance
EPC (RFID)	The Electronic Product Code is one of the available formats for encoding identifiers on RFID tags. The EPC is a globally unique number that identifies a specific item in the supply chain.
External CC	External Customer Counting (e.g., Brickstream)
FRS	Fast Remote Service
GS1 (RFID)	(Global Standards 1) An international standards organization with member bodies in more than 100 countries worldwide. Nedap Retail follows the GS1 and RainRFID standards.
GTIN (RFID)	A Global Trade Item Number (GTIN) is a number that uniquely identifies a product. It can be found beneath the barcode of a product.
IO Box	Input/Output Electronics device
IR	Infra Red
MD	Metal Detection
RF	Radio Frequency
RFID	Radio Frequency Identification

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 62

Document Last modification date 16 February 2024

Document PDF Exported 16 February 2024 by Nedap Retail | Operations



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com



Nedap Sense Guideline

iSense Sleep Mode

version 31, April 2025

Introduction	3
Requirements	4
Set a Sleep Mode schedule	5
Exclude a store	7
System Overview	7
System page	8
Entering Sleep Mode	9
Leaving Sleep Mode	10

Introduction

Nedap iSense RF and RFID systems are engineered for superior energy efficiency and reliable detection and deactivation, making them a smart choice for environmentally and sustainability-conscious retailers.

A Nedap iSense system can be programmed with the times when the store is closed. In these time slots, the systems will run in a Sleep Mode, consuming 30% less energy than the standard “Store open” times.

The iSense Sleep Mode feature enables retailers to reduce the power consumption of iSense gates by switching off system functionalities outside of the store's opening hours.



The energy consumption is 12W to 16W per gate, depending on the modules (RF, RFID, MD, CC). While sleeping, energy savings are between 25% and 40% (depending on the modules used).



During Sleep Mode, the EAS functionality (RF and RFID), Metal Detection, and (External) Customer Counting do not work! It is crucial to make the customer aware of this fact before activating Sleep Mode.

Requirements

To use iSense Sleep Mode, two things are required:

- Firmware version 24.16.5 or higher
- Online iSense system connected to Device Management



No subscription is needed!

Set a Sleep Mode schedule

Sleep Mode can be activated in Device Management. A schedule can be set for a complete organization, at a division, or on a store level.

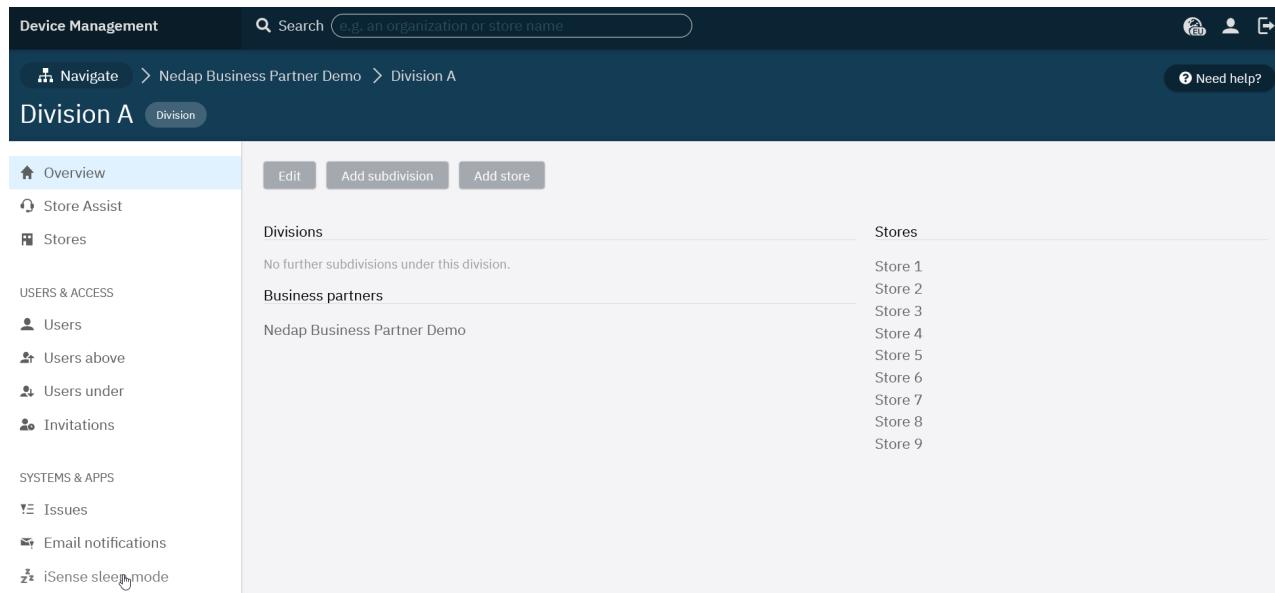


A store can be excluded from Sleep Mode if required, for example, if it is open 24/7.



The closest schedule is always leading, meaning a schedule on the division level is leading over a schedule on the organization level.

To set up Sleep Mode, first, navigate to the desired organization or division to set a schedule and click on **iSense Sleep Mode**:



The screenshot shows the Device Management interface. At the top, there's a navigation bar with 'Device Management' on the left, a search bar in the center containing 'e.g. an organization or store name', and user icons on the right. Below the navigation bar, the breadcrumb path shows 'Navigate > Nedap Business Partner Demo > Division A'. On the far right of this bar is a 'Need help?' link. The main content area is titled 'Division A' and has a 'Division' tab selected. On the left, there's a sidebar with several sections: 'Overview' (selected), 'Store Assist', 'Stores', 'USERS & ACCESS' (with sub-options 'Users', 'Users above', 'Users under', and 'Invitations'), 'SYSTEMS & APPS' (with sub-options 'Issues', 'Email notifications', and 'iSense sleep mode'). In the center, there are three main sections: 'Divisions' (which says 'No further subdivisions under this division.'), 'Business partners' (listing 'Nedap Business Partner Demo'), and 'Stores' (listing 'Store 1' through 'Store 9').

Now it is possible to set a ‘Start time’ and an ‘End time’:

- Start time can be selected between 18:00 - 23:30 (Local store time)
- End time can be chosen between 00:00 - 08:30 (Local store time)

Edit iSense sleep mode

Start time

Please give the time of the day (local time) on which the iSense systems should enter sleep mode.

23:00

End time

Please give the time of the day (local time) on which the iSense systems should awake from sleep mode.

06:00

Schedule

- Enabled
 Disabled

Created by

Michel Florijn

Save

Cancel and go back

Delete sleep mode

The schedule can be ‘Enabled’ or ‘Disabled.’ When set to ‘Enabled’ and saved by clicking on ‘Save,’ the schedule is activated.



The current Sleep Mode schedule is visible when navigating to a store page under the division with the Sleep Mode active.

Systems

The iSense systems in this store are using iSense sleep mode as declared on the division 'Division A' and sleep from 23:00 till 06:00 local time

Disable sleep mode

System	Category	Issue age	Issue type
iSense			No issues
Add system		Add Fast Remote Service	
Access EASiNet...			

Exclude a store

To exclude a store from the Sleep Mode in a specific division or organization, navigate to the store and click on **Disable Sleep Mode**:

Systems

The iSense systems in this store are using iSense sleep mode as declared on the division 'Division A' and sleep from **23:00** till **06:00** local time

Disable sleep mode

This will directly disable Sleep Mode for the specific store. This will remain disabled until it is activated again by clicking **Enable Sleep Mode**.

Systems

The iSense systems are excluded from using iSense sleep mode and will not save energy

Enable sleep mode

System Overview

The 'Systems' overview can be used to have a quick overview of all systems under a specific organization or division, showing the current status for Sleep Mode:

- Sleep Mode active
 - Enabled, not in sleep 
 - Enabled in sleep 
- Sleep Mode possible but disabled (store excluded or not scheduled) 
- Sleep Mode not possible (older firmware) 

Systems

Firmware updates available. [View updates.](#)

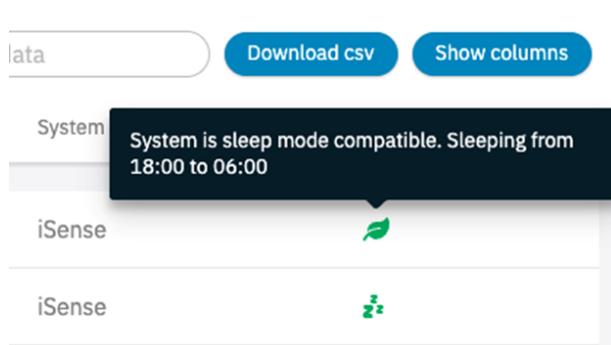
Search data **Download csv** **Show columns**

System ID	Name	Store	Online	Status	System type	Sleep mode
7e96be75-6355-410e-8f09-a01d7c1ac668	10 Corso Como NY City Fulton	10 Corso Como NY City Fulton	✓	✓	iSense	
bb65d115-b8db-4e03-a973-8130c58c62c6	10 Corso Como NY City Fulton	10 Corso Como NY City Fulton	✓	✓	iSense	
aba4abc7-9223-4926-b4b8-7d73723812c5	10 Corso Como NY City Fulton	10 Corso Como NY City Fulton	✓	✓	iSense	
13402c0b-9823-4b7f-ac32-2d114acfb3a5	10 Corso Como NY City Fulton	10 Corso Como NY City Fulton	✓	✓	System is sleep mode compatible, but sleep mode is not enabled	
1ac0224b-7e1f-4d2f-afa2-34a5068e2906	Sarah Jessica Parker	Sarah Jessica Parker	✓	✓	iSense	

Showing 1 to 5 of 5 entries

1 / 10 / page

Sleep Mode active



Data

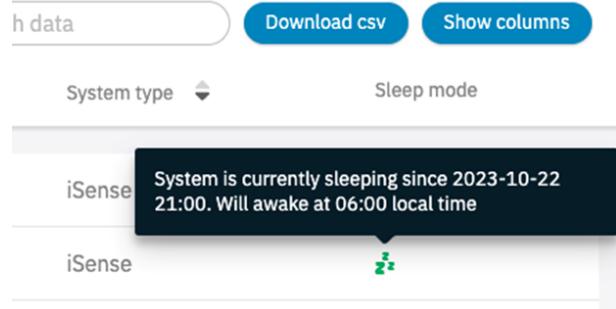
[Download csv](#) [Show columns](#)

System System is sleep mode compatible. Sleeping from 18:00 to 06:00

iSense 

iSense 

Sleeping



Data

[Download csv](#) [Show columns](#)

System type

Sleep mode

iSense System is currently sleeping since 2023-10-22 21:00. Will awake at 06:00 local time

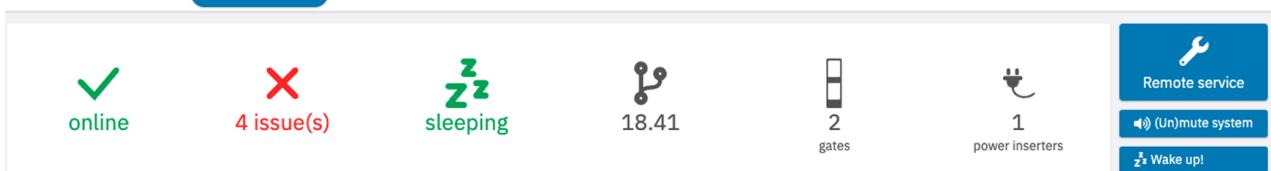
iSense 

System page

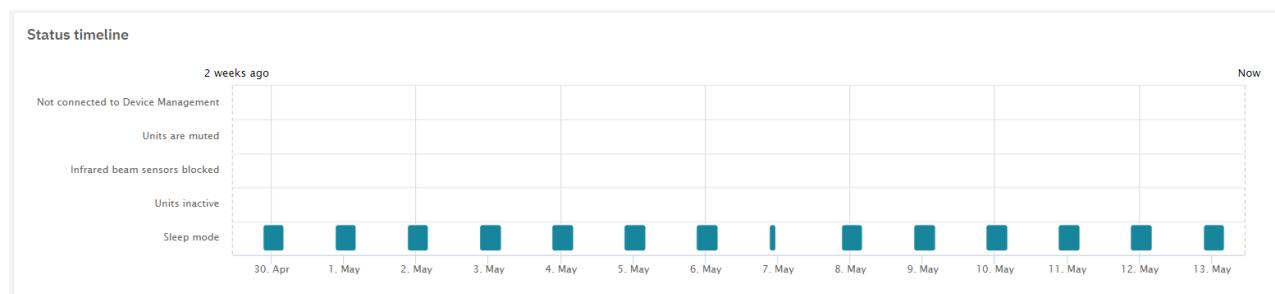
The 'System page' also shows the status of Sleep Mode.

Haupteingang renos

 Installed by John Doe on June 21st 2019 - 11:33
 1b4aadb3-7e85-471b-95eb-37a253ab54b4
 Last update was 2 years ago. Click [refresh](#) to request up-to-date settings.
 SSH access is not enabled. [Enable SSH access](#).



Also, the time that the system was 'sleeping' is visible in the 'Issues timeline':



Entering Sleep Mode



A system will only sleep when it is online and connected to Device Management



The command to go to sleep comes from Device Management,



The system itself initiates wake-up



If a technician is still connected to the system, it will not go to sleep



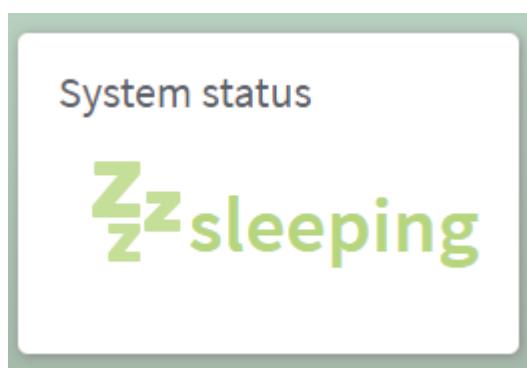
When a user is still logged in to the iSense technical dashboard, Sleep Mode will not be activated

The following is turned off during Sleep Mode:

- EAS RF
- EAS RFID
- Metal Detection
- Infrared customer counting
- External customer counting

Not turned off during Sleep Mode:

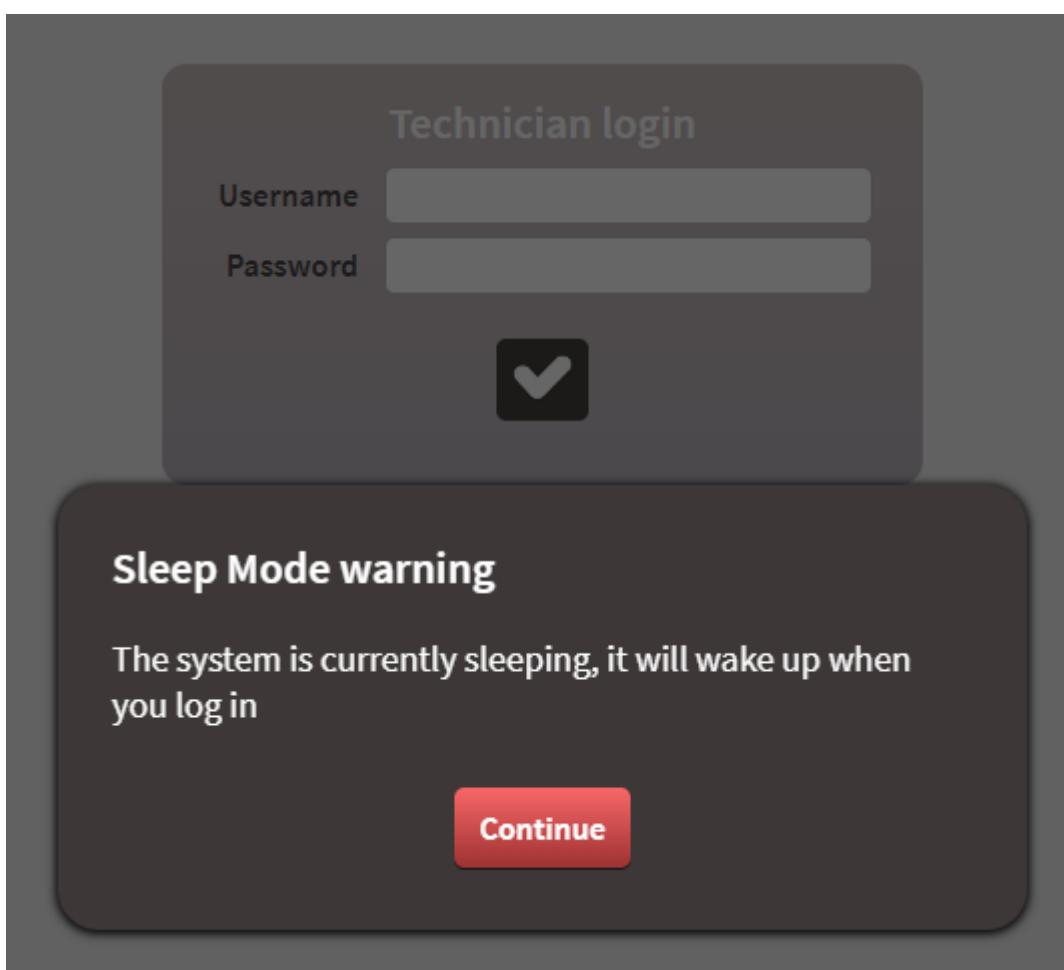
- Smart Deactivator
- External CC
- API
 - There will be no events from RF, RFID, MD, or CC
- Network
- iSense Dashboard
 - The system status will show that the system is sleeping.



Leaving Sleep Mode

When a system is in Sleep Mode, it will wake up when:

- The scheduled end time for that day has been reached. The system does not have to be online at that moment; the trigger to wake up is in the system itself.
- When one or more units are power-cycled or turned on, the system will wake up.
- Firmware updates via Device Management will continue to work and overrule the Sleep Mode that day.
- If a technician enters the Technical Dashboard, the system wakes up. A warning is shown.



- When the system leaves Sleep Mode, the RF, RFID, MD, and CC modules are turned on again. A startup filter is activated to prevent a large number of alarms.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap NV 2025

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 31

Document Last modification date 14 April 2025

Document PDF Exported 14 April 2025 by Nedap Retail | Operations



support-retail@nedap.com



**Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands**

nedap-retail.com

Connected Devices Guideline

iSense System Login

version 57, May 2024

Introduction	3
Obtain a Nedap Retail Account	3
How to access an iSense installation?.....	4
Options explained	5
How to log in to a system that is online	6
How to log in to an offline system	7
1. This laptop	8
2. Smartphone or tablet	9
3. Other devices	13
Ending the session or how to log out	16



Introduction

To improve the security of iSense systems, the login procedure will be managed with a Nedap Retail Account. This account is used to login to Device Management or Retail Analytics). With this account, it is possible to authenticate and monitor registered Nedap installation professionals.

Everyone who wants to access and configure an iSense system needs to have a Nedap Retail Account with the correct permissions.



Please consider this carefully when installing systems at night without having internet available.

Obtain a Nedap Retail Account

Nedap Retail Accounts are created and maintained within Device Management (DM). Within DM, a user is **invited** to an organization or a store. During this invitation process, the user will be given the appropriate permissions. Please ensure the permissions to install iSense systems are activated when inviting a user.

The manual for Device Management, which can be found on the Nedap Retail Partner Portal, explains how to create/enable new users within Device Management in detail.



How to access an iSense installation?

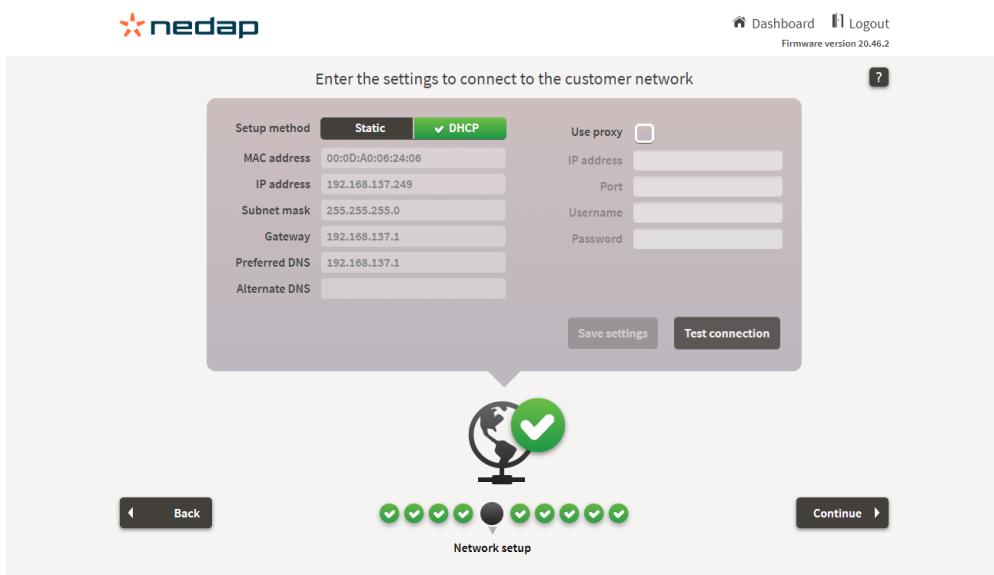
There are four options to validate your 'Nedap Retail account and log in:

1. Bring the system online (Customer network, 3G/4G modem), contact the Nedap server, and log in with your Nedap Retail Account credentials through the wizard.
2. The configuration PC is connected to the Internet; log in with your Nedap Retail Account credentials through the Internet on the PC.
3. Scan the QR code with a smartphone or tablet, then log in with your Nedap Retail Account credentials to create a one-time password (OTP).
4. Use another online device to validate your Nedap Retail Account credentials to create a one-time password (OTP).

Options explained

You can bring a new system online without logging in. This can be done in the first part of the wizard.

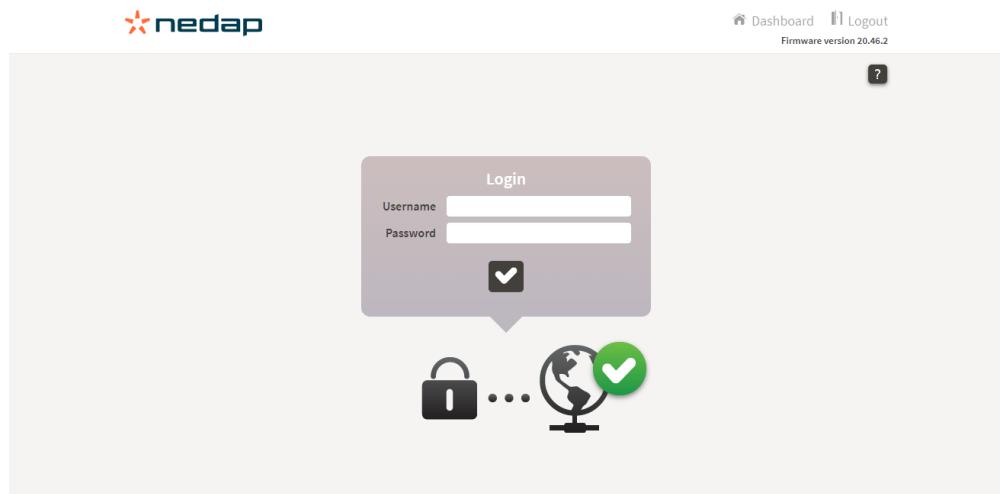
After the connection test is successful and you click Continue, you must log in.



How to log in to a system that is online

When the system is online, the screen below will appear. Please fill in your Nedap Retail Account credentials here.

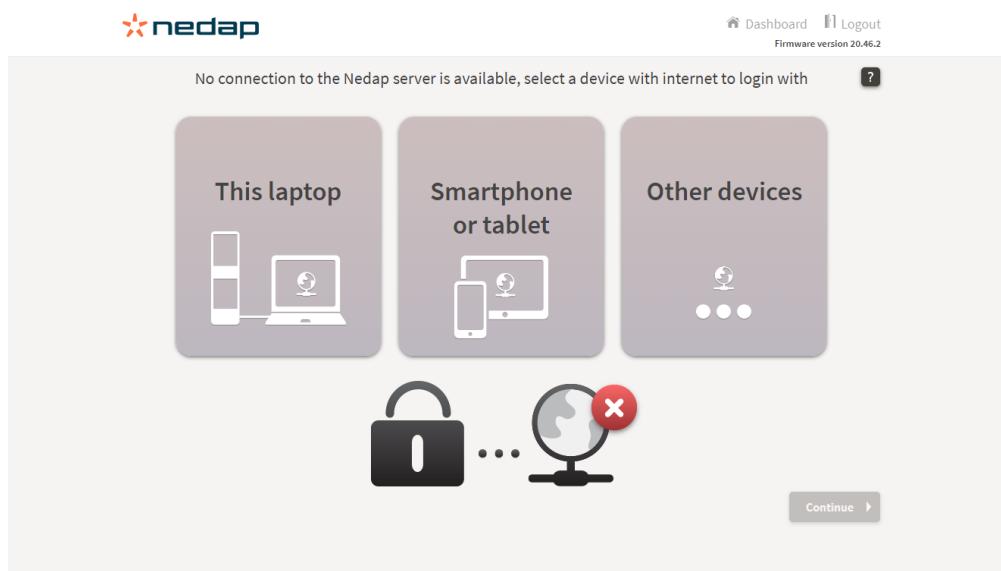
If you cannot log in, please contact your Technical manager and report the error message.



How to log in to an offline system

If the system is offline, there are three options to log in:

1. "This laptop" - Your laptop is connected to the internet
2. "Smartphone or tablet" - A device that can scan a QR code and is online (for example, a smartphone or tablet)
3. "Other devices" - Through another device or a call to someone with internet access.

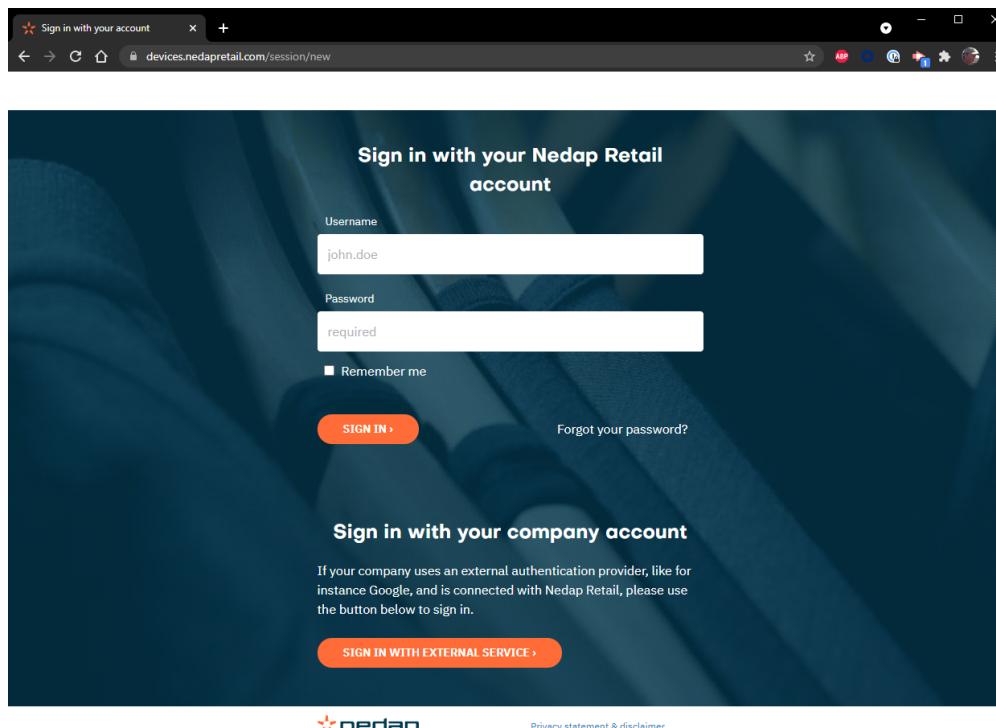


1. This laptop

When your laptop is online, select "This laptop" and click "Continue".



Log in with your Nedap Retail Account credentials:



2. Smartphone or tablet

When you have a separate device that is online (e.g., a smartphone), select "Smartphone or tablet" and click "Continue."



Scan the QR code with your device:



Go to the link:





Log in with your Nedap Retail Account credentials:

Sign in with your Nedap Retail account

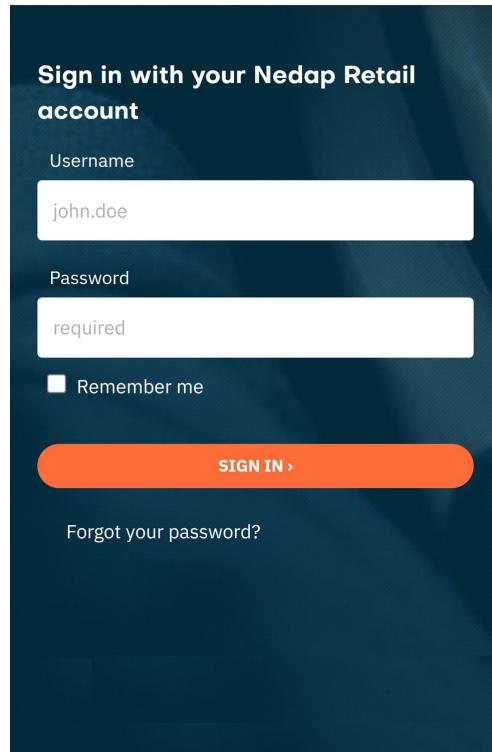
Username
john.doe

Password
required

Remember me

SIGN IN >

[Forgot your password?](#)



You will have to select the user:

One Time Password

User

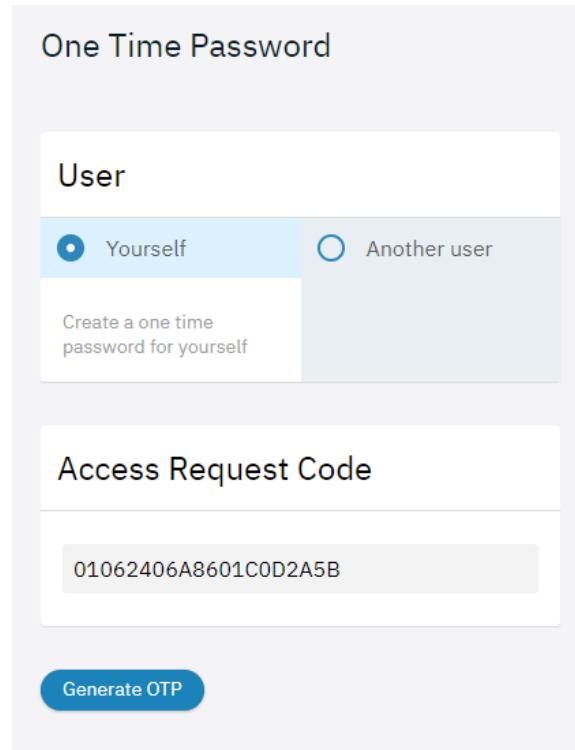
Yourself Another user

Create a one time password for yourself

Access Request Code

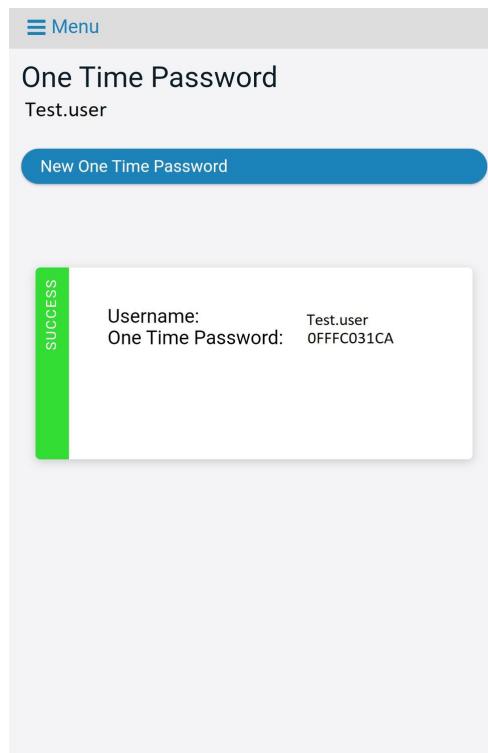
01062406A8601C0D2A5B

Generate OTP

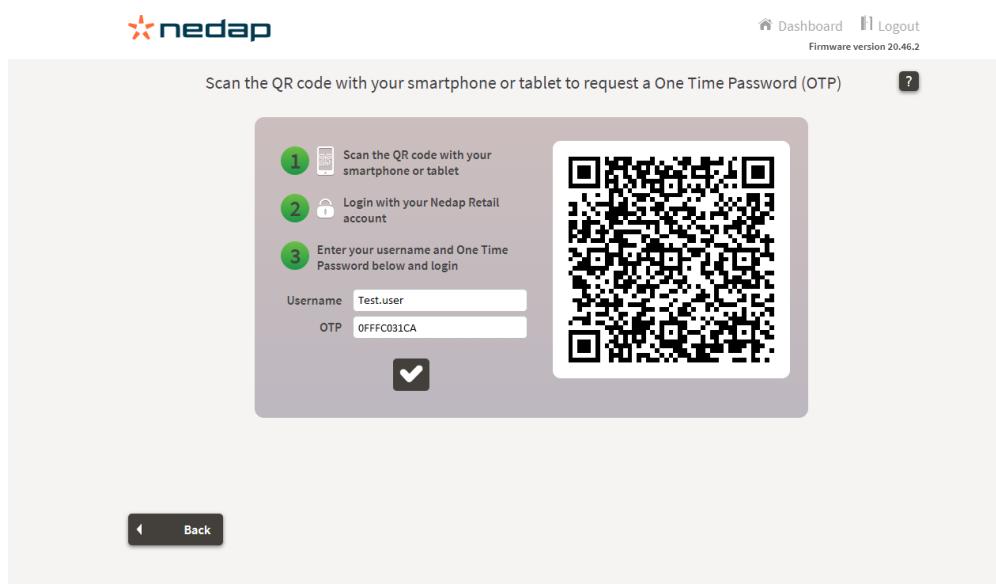




And then press the "Generate OTP" button:



Enter the "Username" and "OTP" into the Wizard:



3. Other devices

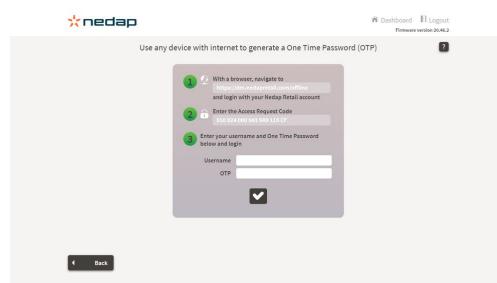
When no online devices are available to scan the QR code, select "Other devices" and press continue.



Call somebody at your office and let the other person go to the internet link:

.

Give this person the "Access Request Code."





The person on the phone needs to select the user.

A screenshot of a web-based application titled "Device Management" under the "nedap" brand. The left sidebar contains navigation links for Overview, Users & Access (with OAuth clients, Administrators, Issues, Registrations, and Firmware releases), Systems & Apps (Issues, Registrations, Firmware releases), and Finances (Debtors, Services, Email exports). The main content area is titled "One Time Password". It has two tabs: "User" (selected) and "Another user". Under "User", there are two radio buttons: "Yourself" (selected) and "Another user". A search bar below shows the query "Test user". Below the search bar is a text input field labeled "Access Request Code" containing the value "0106240552676FD4D0B0E". At the bottom right is a blue button labeled "Generate OTP".

Fill in the Access-Request Code and press "Generate OTP."

A screenshot of the same web-based application. The "Access Request Code" field now contains the generated OTP "0106240552676FD4D0B0E". The rest of the interface remains the same, showing the "User" tab selected and the "Generate OTP" button available.

The system will show the One Time Password.

A screenshot of the web-based application. The "Access Request Code" field now contains the generated OTP "0106240552676FD4D0B0E". The "New One Time Password" button is visible at the bottom of the "One Time Password" section. The right side of the screen displays a green vertical bar with the word "VISITER" and a table with columns "Username" and "One Time Password". The "Username" column shows "Test.user" and the "One Time Password" column shows "00000000000000000000000000000000".



Enter the "Username" and "OTP" into the wizard.

The screenshot shows a mobile application interface for Nedap. At the top, there is a navigation bar with icons for Dashboard, Logout, and Firmware version 20.46.2. Below this is a header bar with the text "Use any device with internet to generate a One Time Password (OTP)" and a question mark icon. The main content area contains three numbered steps:

- With a browser, navigate to <https://dm.nedapretail.com/offline> and login with your Nedap Retail account
- Enter the Access Request Code **010 624 060 043 9A9 115 CF**
- Enter your username and One Time Password below and login

Below the steps, there are two input fields: "Username" with value "Test.user" and "OTP" with value "000063EFD4". A large green checkmark button is at the bottom right. At the bottom left, there is a "Back" button with a left arrow icon.

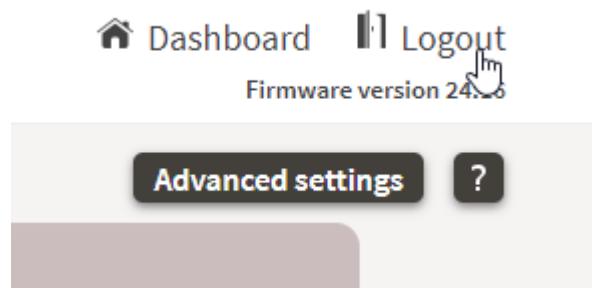
(i) OTP Validity

The OTP will be valid as long as you remain logged in to the iSense system, but you can also login to other units without needing a new OTP as long as you connect to the system again within 1 hour with the same laptop (Firmware 16.30 and higher)

Ending the session or how to log out

It is good practice to log out after your session, although the iSense system will close the session automatically after 8 hours from the login (since 24.16.1).

Press the `Logout` button, and the login screen will appear again.



It is now safe to end the connection.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Document Version 57

Document Last modification date 29 May 2024

Document PDF Exported 29 May 2024 by Nedap Retail | Operations

Copyright © Nedap Retail 2024

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.



support-retail@nedap.com

Nedap Sense Guideline

iSense Basic Installation Tools

version 16, February 2025

Introduction	3
Basic tools	4
Special tools	5
Network cable tester	5
RJ45 crimp tool EZ-RJPRO® HD Crimp Tool	6
Basic materials	7
Tools for the iSense configuration	7



Introduction

In this document, you will find the most essential tools for the mechanical iSense installation.

Basic tools

Tools you need for the mechanical iSense installation:

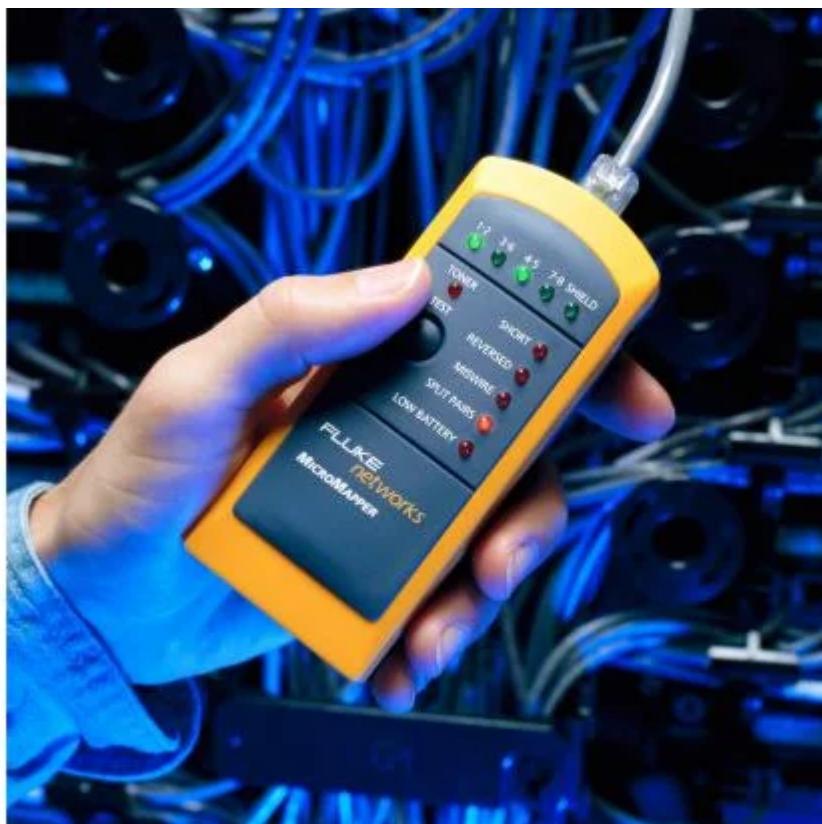
- Hammer drill
- Screwdriver (PZ1)
- Small flat screwdriver
- Stripping tool and Crimping tool
- Side cutter
- Ruler
- Pencil
- Industrial vacuum cleaner
- Multi-meter
- Angle grinder with diamond disc:
 - For example, Hilti DCG 230-DB Angle grinder 230 mm, including dust cover Hilti DC-EX 230/9 with connection for vacuum cleaner

Special tools

Network cable tester

This device can test the physical connection of the patch network cable and test if the twisting is correctly connected.

We advise you to use the **Fluke Networks MicroMapper™ - MT-8200-49A**. More information can be found on <http://www.flukenetworks.com/datacom-cabling/copper-testing/MicroMapper>



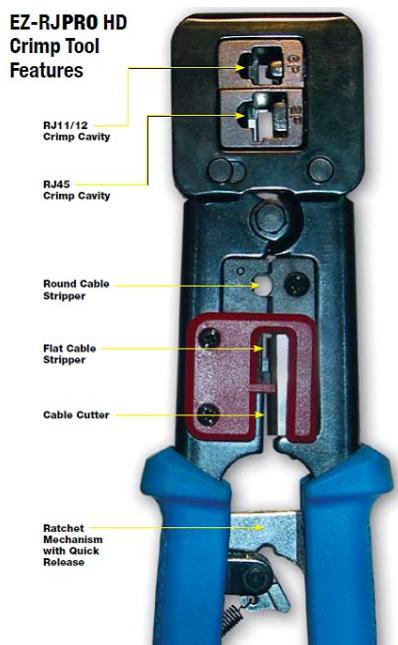
Another approved cable tester is the EZ Check Cable tester.

RJ45 crimp tool EZ-RJPRO® HD Crimp Tool

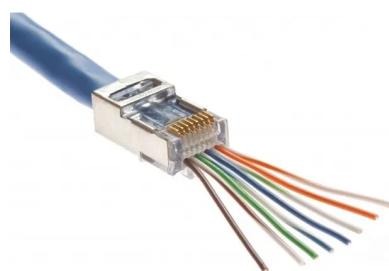
This tool can crimp and cut the RJ45 connector in one movement. When you move the RJ45 connector over the network cable, the wires come out on the end of the connector.

This way, you can check the color codes (White/Orange—Orange—White/Green—Blue—White/Blue—Green—White/Brown—Brown) and never have the problem of the wire not being connected to the RJ45 connector.

You can find more information at: <http://www.platinumtools.com/products/100054.php>



To use the EZ-RJPRO crimp tool, you need EZ-RJ45 connectors. These are included with the Gates and can be ordered as spare parts.



Basic materials

- Cement (in case of milled slots)
- Chemical fixing:
 - Drill 13 mm
 - Spanner 17
 - Hilti Hit HY 150 Fast curing injection
 - Hilti Dispenser (Hilti MD2000)
- M10 anchor rod
- 2 nuts M10 per antenna (not included)
- 2 metal washers M10 per antenna (not included)
- Ethernet cable CAT5E solid core with at least 24 AWG.

Tools for the iSense configuration

- Laptop with the following specifications:
 - Operating system: Microsoft Windows, Apple iOS or Linux
 - Up-to-date web browser
 - USB port
- If Microsoft Windows is used, you must install the RNDIS driver to communicate with Renos (this driver can be found on the Nedap Retail Portal). Install the RNDIS driver.
- The cable connecting the laptop to Renos is a USB 2.0 male to mini 5-pin male cable. A longer cable gives you more space to place your computer comfortably.
- Test label

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap Retail 2025

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 16

Document Last modification date 11 February 2025

Document PDF Exported 11 February 2025 by Nedap Retail | Operations



support-retail@nedap.com

Nedap Sense Manual

iSense iD Top (OVR)

version 94, October 2024

Introduction	4
Disclaimers	4
Safety precautions	5
RFID Regions	5
Product Overview	6
Box contents	6
Components	7
Dimensions	9
Connections	11
Preparing the installation.....	12
Defining the system	12
Detection distance, aisle width, and label-free zone	13
RFID installation requirements	14
Power Inserter	16
Orientation of products	17
Executing the installation.....	21
Removing the cover	21
Physical installation - on the ceiling	21
Physical installation - with VESA compatible mount	23
Installing cabling	24
Renos Status LEDs	25
Configuring the installation	28
Driver installation	28
Supported browsers	28
Connecting a laptop to the Renos unit	29
Entering the configuration wizard	29
Authentication	30
Getting help in the wizard	30
Factory reset and Firmware change	31
System ID	31
Integrating the installation with other systems	32
Software integration with local APIs	32
Servicing the installation.....	33



Device Management	33
SNMP	33
Troubleshooting.....	34
Physical installation	34
Configuration	35
Warranty and spare parts.....	36
Regulatory information	37
FCC and IC Compliance Statement	37
FCC and IC Radiation Exposure Statement	37
FCC Information to the user	37
Information for Taiwan	38
CE WEEE	38
CE - UKCA Declaration of Conformity	39
Disposal of this product	39
About Nedap.....	40
Together, we make merchandise simply available	40
Our vision for inventory visibility	40
Contact	40

Introduction

The Nedap OVR-line products (iD Tops) are ceiling-mounted integrated readers with ultra-high-frequency (UHF) RFID. They are designed explicitly for in-store retail applications, such as Electronic Article Surveillance (EAS), stock room to sales floor transition, and goods receiving.



This manual provides an overview of the products, installation, and configuration basics. Several guidelines are available on the Nedap Retail portal to obtain more details.

This manual covers the following products:

Article Number	Article Name	Commercial Name	Technologies	Model Name
9982191	ASSY OV37R RFID R1 WHITE	iD Top	UHF RFID	
9982205	ASSY OV37R RFID R2 WHITE	iD Top	UHF RFID	ASSY OVR RFID
9982213	ASSY OV37R RFID R3 WHITE	iD Top	UHF RFID	

Disclaimers



Nedap intends to make this manual accurate and complete. However, Nedap does not warrant that the information contained herein covers all details, conditions or variations, nor does it provide for every possible contingency in connection with the installation or use of this product. Nedap disclaims any liability for damage to property or personal injury resulting, in whole or in part, from improper installation, modification, use, or misuse of its products. The information contained in this document is subject to change without notice.



This equipment should only be installed, operated, serviced, and repaired by skilled personnel. The installation and interconnection of this equipment to facility wiring and other equipment must be done by a competent, skilled craftsman familiar with applicable standards and codes governing the installation. Installation methods, practices or procedures that are unauthorized or done improperly are dangerous and could result in serious personal injury or damage to property and equipment.

Safety precautions



Do not place cards equipped with a magnetic strip or chip (i.e., ID, travel, debit, and credit cards) close to the equipment to avoid possible card failures.



To avoid potential interference with medical devices (pacemakers, cochlear implants, etc.), keep a distance of at least 20cm (8 inches) between them and the equipment.

RFID Regions

Region 1: Europe, Eastern Europe, Middle East, Africa and India

Region 2: North America and South America

Region 3: Asia and Oceania

Product Overview



In this document, the following abbreviations and terms will be used:

- 'RFID technology' is an abbreviation for UHF RFID technology.
- 'Reader' and 'OVR' are synonyms of the iD Top

Box contents

Article Number	Article Name	Box Contents
9982191	ASSY OV37R RFID R1 WHITE	<ul style="list-style-type: none">• OV37 Integrated Reader with Renos, RFID reader, and RFID antenna
9982205	ASSY OV37R RFID R2 WHITE	<ul style="list-style-type: none">• OV37 Integrated Reader with Renos, RFID reader, and RFID antenna
9982213	ASSY OV37R RFID R3 WHITE	<ul style="list-style-type: none">• OV37 Integrated Reader with Renos, RFID reader, and RFID antenna

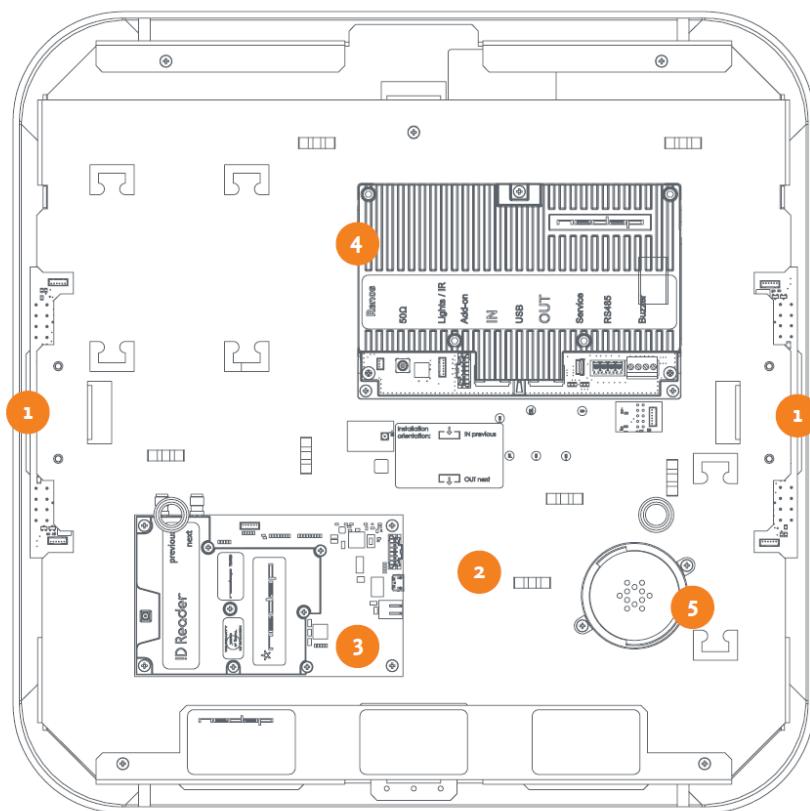


Please note that the mounting set, including steel cabling, is available as a separate article and is not included in the unit's box. For more information, please refer to the Nedap Retail Partner Portal.

Article Number	Article Name
9983007	MOUNTING SET OV37R STEEL CABLE

Components

The OVR line of products is based on the Renos platform. The Renos platform is developed by Nedap Retail specifically for retail applications. OVR products have several serviceable parts. These are explained in the table and highlighted in the schematic drawings.



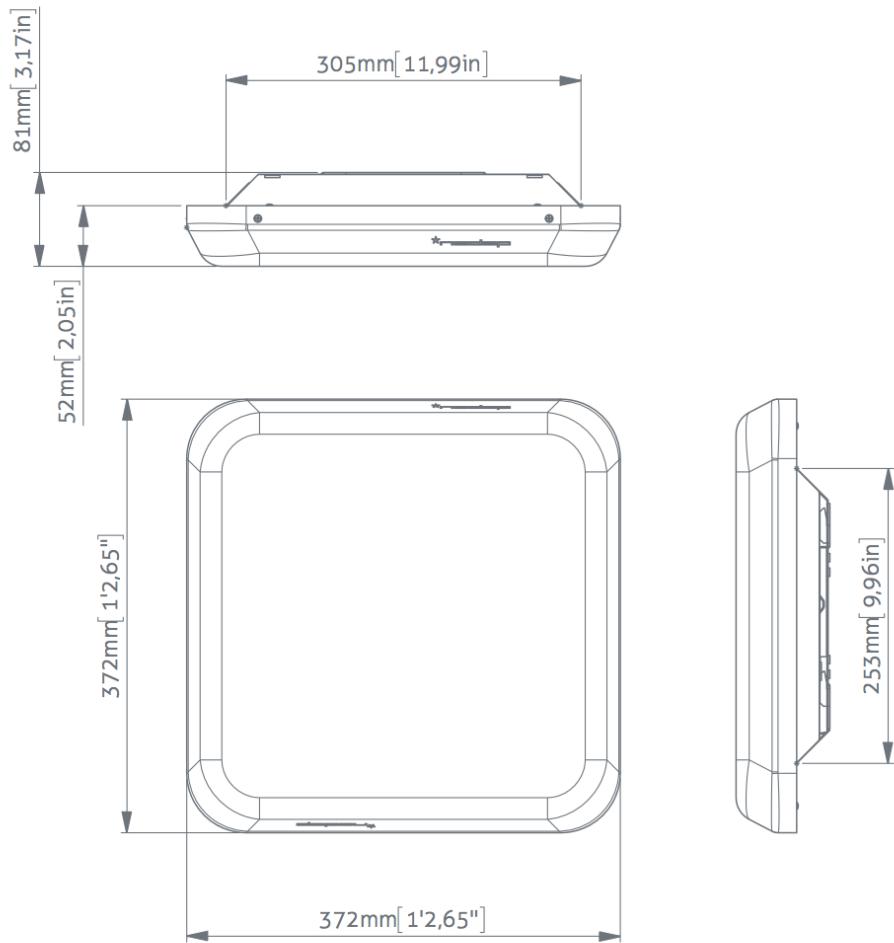
No.	Component	Description
1	Lights	The red LED lights can be used for user feedback or alarms.
2	RFID antenna	The RFID antenna.
3	RFID reader	The RFID reader reads RFID labels. It is connected to the Renos unit and to the RFID antennas.
4	Renos unit	The Renos unit is the central processing unit of an OVR. It powers the system and facilitates data communication between units and the outside world.

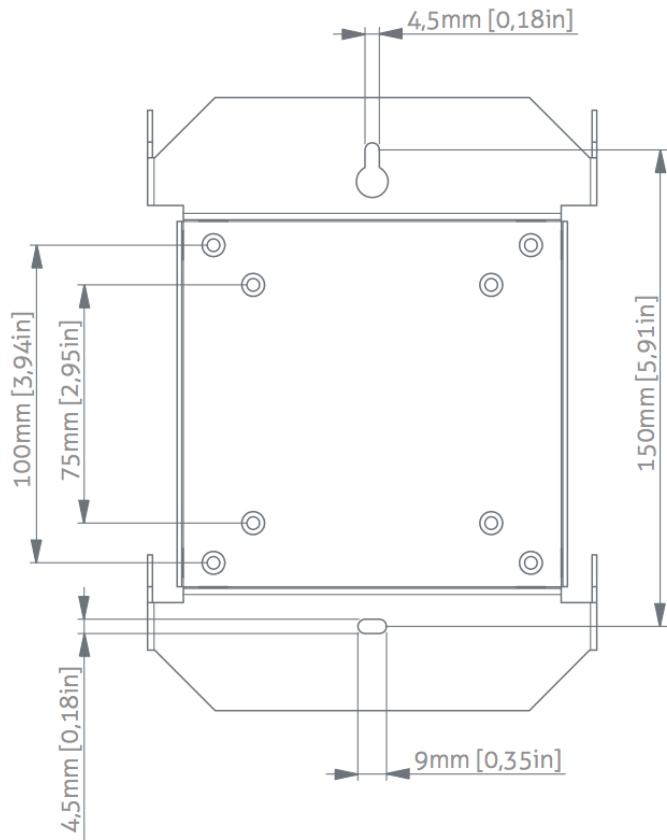
No.	Component	Description
5	Buzzer	The buzzer can be used for user feedback or alarms.

Dimensions

The dimensions of the gates can be found in the drawings below.

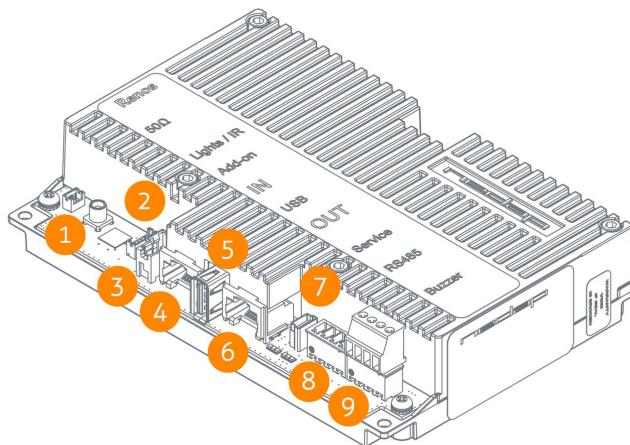
The next picture shows the mounting plate, which can be used as a wall or ceiling mount and is also connected to a VESA mount.





Connections

This is a Renos unit, describing all its connectors and their use.



No.	Connector	Usage
1	50 ohm	Not used in the OVR line.
2	Infrared beams	Connect to the lights.
3	Add-on	Provide power and synchronization to add-ons, like the RFID reader.
4	Network IN	Connected to the Network OUT of a previous Renos unit or a Power Inserter.
5	USB	Connect accessories to Renos, like the RFID Reader.
6	Network OUT	Connected to the Network IN of the next unit or a Power Inserter. It can also be left unconnected or connected to the customer network.
7	Mini USB service port	Connect your laptop to configure the Renos system.
8	RS485 connector	Not used in the OVR line.
9	Buzzer connector	Connect to the included buzzer.

The LED indicators on the Renos unit will be discussed later in this manual.

Preparing the installation

When preparing an installation with OVR-line products, there are a few things that should be taken into account:

- How many iD Tops (OVRs) do you need to cover an entrance or door?
- Placement concerning the environment (walls and other objects)
- The number of Power Inserters needed to power the system.
- The firewall settings that need to be in place to enable Device Management
- Orientation of the product

If the placement of the OVR products is decided, the next step is to evaluate the cabling and placement of Power Inserters.

Defining the system

When a store requires iD Tops to be placed at several locations, there needs to be a decision on how to combine these tops into one or multiple systems. The following rules need to be taken into account:

1. **A different role is a separate system.** Combining iD Tops for Electronic Article Surveillance (EAS) with tops for the stockroom to the sales floor in one system is impossible. Both roles need different systems with their own Power Inserter and customer network connection.
2. **Within the EAS role, combine all iD Tops into one system.** The Renos platform has a built-in synchronization mechanism for RFID technology to minimize interference between tops. The iD Tops must be connected to one system for this synchronization mechanism.
3. **However, the maximum cable length requirements must be considered.** If it is impossible to put all the tops within a role in one system due to the maximum cable length requirements, you can split the installation into two or more systems.



Build a separate system for the stockroom to the sales floor and goods receiving roles when there is a different door or entrance.

Role/Store Position	Max. System Size
EAS	30
Stockroom / Salesfloor	1
Goods receiving	1

Detection distance, aisle width, and label-free zone

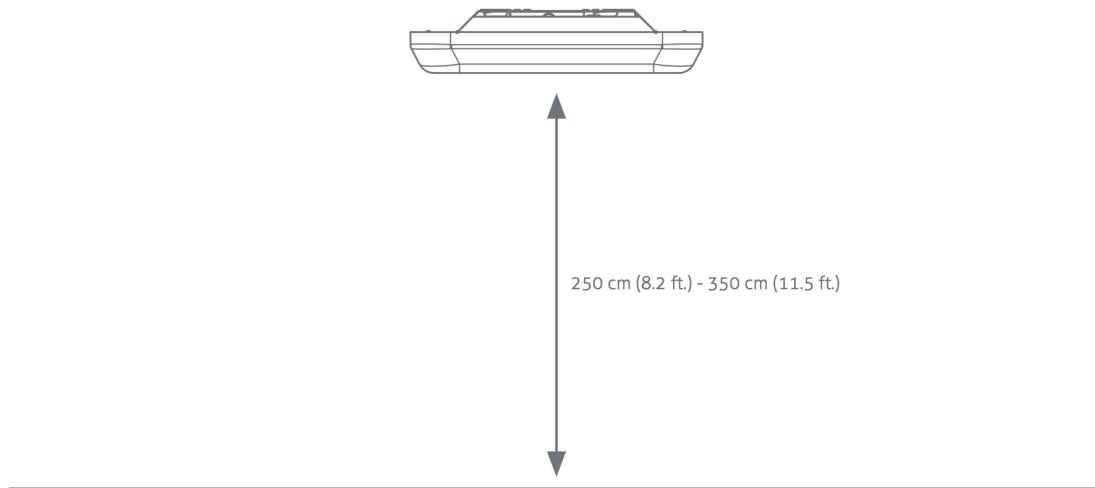
The first decision is how many readers you need and where to place them. This depends on the aisle width and detection height of the system. There is no fixed answer to this question; it depends on many factors, like customer expectations, the quality of the tags, the environment, etc.

The recommendations below are based on the Nedap RFID hard tag (for RFID).

It is possible to mount an OVR between 250 cm and 350 cm (8.2 ft. to 11.5 ft.) height.



The recommended height for the OVR is 2.5 m (8.2 ft.). When the OVR is lower, the RFID field is smaller and more controlled, which generally results in more stable performance!



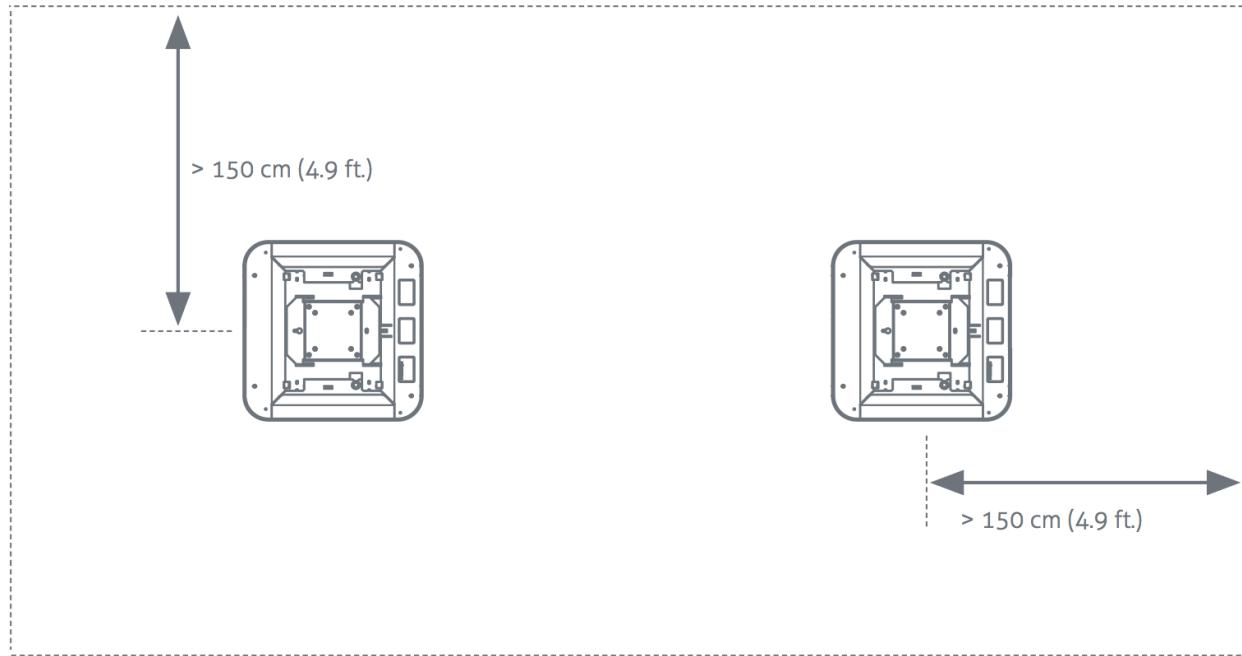
We recommend placing the OVRs at 220 cm (7.2 ft.) - 250 cm (8.2 ft.) aisle width, depending on the space at the entrance.





Only the recommended 'detection distance' or 'aisle width' is specified. Depending on the tag used and the environment the gates are placed in, sometimes larger values are obtainable. You are advised to test this before using it in a store.

We recommend having a label-free zone of more than 150 cm (4.9 ft.) from the center of the antenna.



RFID installation requirements

When RFID technology is used, there are different installation requirements compared to RF technology. Since the RFID field is much less strictly defined than with RF technology, there is a larger area where tags could be detected. Unlike RF, RFID is much less sensitive to coupling or interference issues.

Automatic tag muting

The RFID reader's maximum read throughput is around 200 tag reads per second, which is used to monitor the tags' status continuously.

When many tags are placed close to or in the label-free zone, the reader might need to be busier with those tags than with other tags. This will impact the system's performance. If this happens, the reader will mute some tags to have time for other tags.

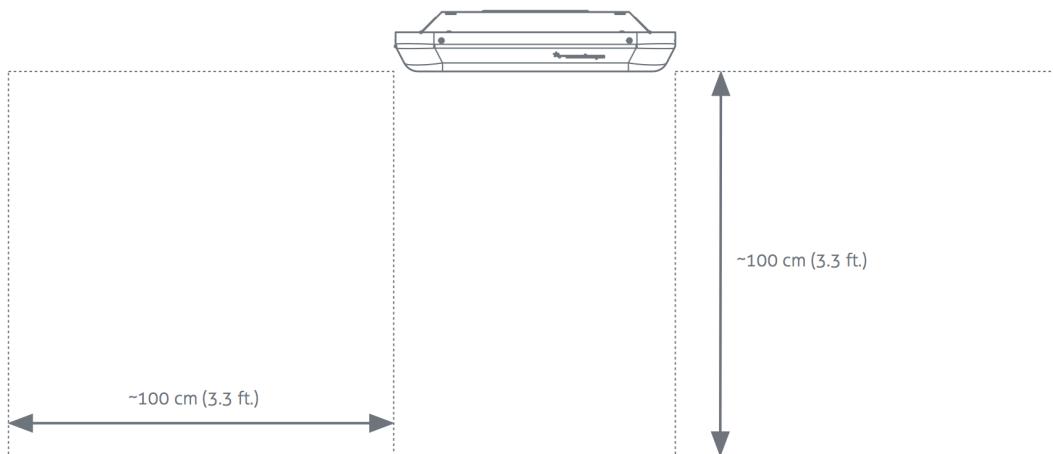
This feature is called 'Automatic Tag Muting.'

Some tags in the system's neighborhood are muted and will not cause an alarm when moved along the reader.

Metal surfaces

Metal surfaces reflect the RFID field, which might confuse the Dynamic Beam Steering algorithms and influence (change or enlarge) the detection field.

Avoid metallic surfaces near readers. The front and back areas of the unit should be completely metal-free, as defined in the following picture.



When it is impossible to make the above-indicated zone metal-free due to installation requirements by the customer or the mall, this will cause false alarms and less detection quality.

Power Inserter

When the installation location of the products is precise, the location of the Power Inserters needs to be defined. A maximum number of Renos units can be connected to one Power Inserter.

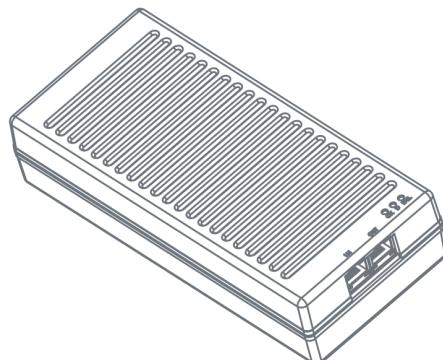
Technologies In Use	#Units / PI 230V	#Units / PI 115V
RFID	5	5

Index:

- RFID = RAIN Radio Frequency Identification (~900 MHz)



Please note that you can only use a Nedap Power Inserter (Power-over-Ethernet) to power Renos systems. Generic Power-over-Ethernet switches or stand-alone inserters are not possible.



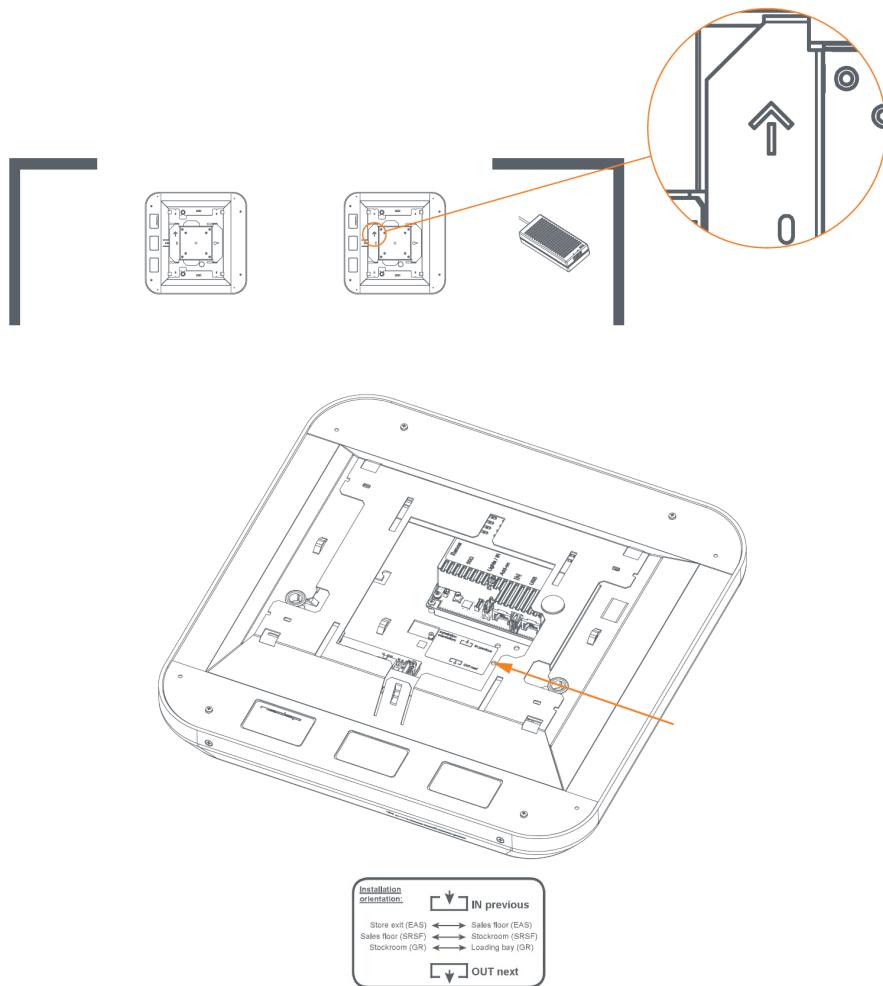
It is recommended that the Power Inserter be connected to an always-on power socket. This allows continuous system monitoring and remote firmware updates during the night.



Do not disconnect network cables in the system while it is still powered! First, disconnect the power cable from the Power Inserter(s).

Orientation of products

Due to the orientation-sensitivity of the RFID antennas, the readers all need to be oriented in the same way. There is an arrow in the product bracket to indicate the correct orientation and a label with an indication.



If this procedure is not executed correctly, the RFID technology will not work.

Cabling

When the basis placement and orientation are clear, the cabling must be implemented. The OVR line uses a daisy chain topology, which means that all devices are connected as a chain:

1. a cable from a Power Inserter OUT to a Renos unit IN,
2. from that Renos unit OUT to the next Renos unit IN,
3. etc.

The units are connected only to an Ethernet cable. When standing on the sales floor looking outside the store, the system should be wired from right to left, as shown in the drawing below!

The following cable specifications are recommended for the iSense system:

- Use UTP Cat5e with a stranded copper core, with 24 AWG (0,51mm) core diameter.

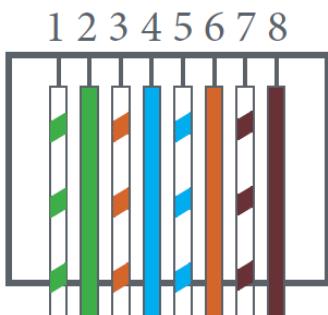


Always connect **all four pairs** using the **T568B** termination standard or T568A if specifically required!

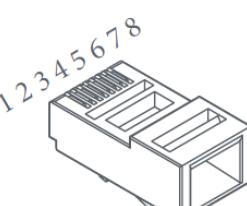
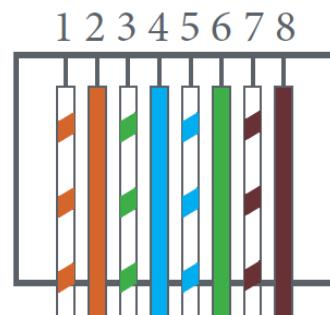


Never use CCA (copper cladding aluminum) or CCS/CCF (copper cladding steel) cable!

T568A



T568B



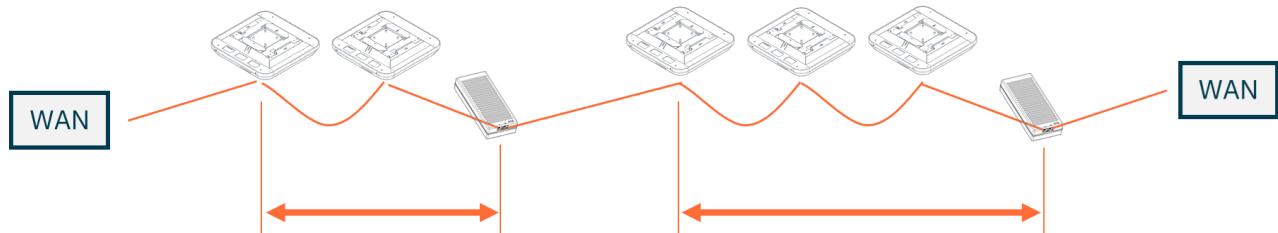
8P8C (RJ45)

Pin	T568A	T568B (Preferred)
1	Green + White	Orange + White
2	Green	Orange
3	Orange + White	Green + White
4	Blue	Blue
5	Blue + White	Blue + White
6	Orange	Green
7	Brown + White	Brown + White
8	Brown	Brown

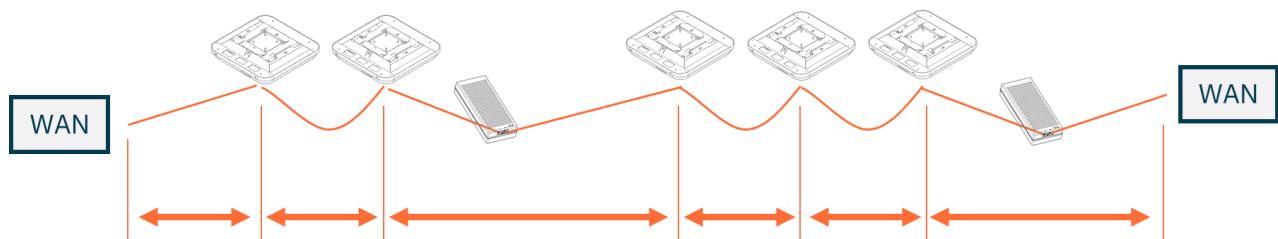
Cable length



Maximum cable length of **80 meters / 250 ft** between a Power Inserter and the last Renos unit that receives the power from this Power Inserter:



Maximum cable length of **80 meters / 250 ft** between Renos units (excluding Power Inserters) and between the first (or last) Renos unit and the WAN connection in the store:



Remarks

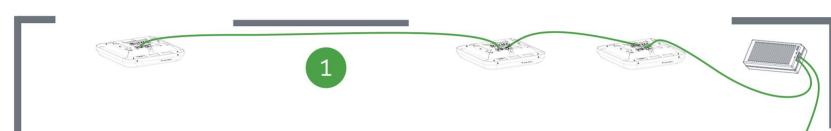
- It is possible to use your own preferred connectors.
- Make sure that the connectors are suitable for the cable and that the correct crimping tool is used for the connector.
- Follow the recommendations of the cable manufacturer.
- Local regulations may dictate using a specific cable type or rating.



We recommend placing the Power Inserter in the switch room (near a power socket) when the ethernet cable lengths allow. This way, the customer only has to arrange an ethernet outlet near the system.



If the cable lengths between two groups exceed approximately 50 meters / 164 ft, consider splitting a system into two.



Cable Number	Type Of Cable
1	Ethernet cable

Executing the installation

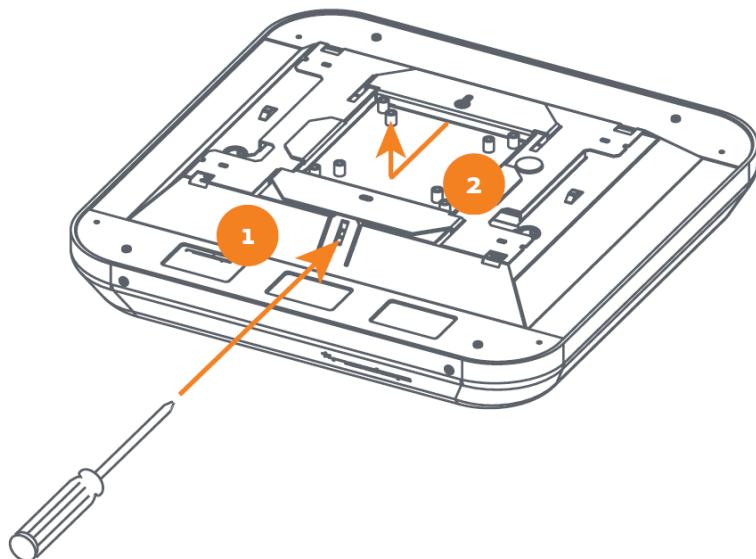
When all the preparations are considered, the installation can occur. This chapter will explain the physical installation, placing the cabling, and checking the system's status.

The reader can be mounted on the ceiling, on the wall, or with a VESA-compatible mount.

Removing the cover

The cover can be removed by:

1. Gently push a screwdriver at the indicated location.
2. Hold the screwdriver, and slide the cover towards the indicated direction. It will come from the unit.

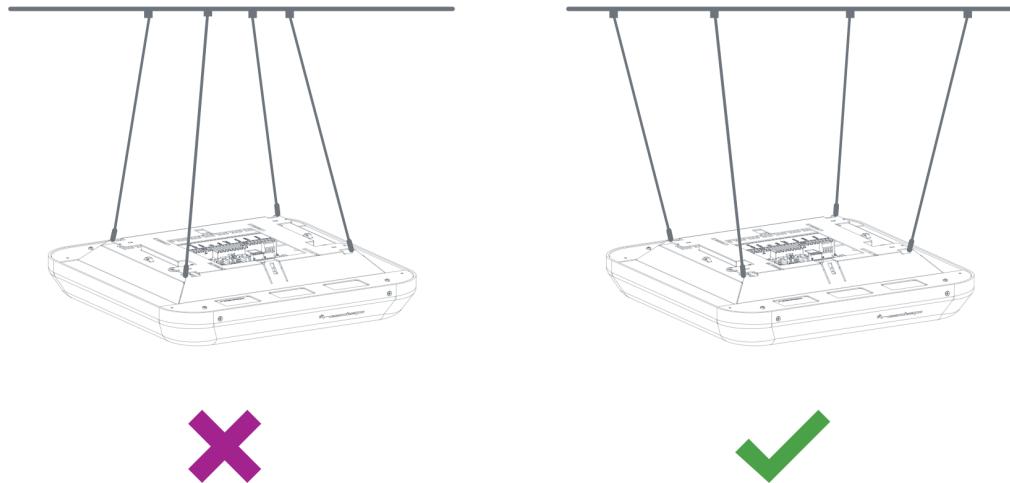


Physical installation - on the ceiling

The steel cabling set can mount the unit on the ceiling. It should be mounted in a 'V' shape (as indicated in the picture below) so that the unit will not easily swing due to wind or heaters. When mounted in an 'A' shape, this will easily happen.



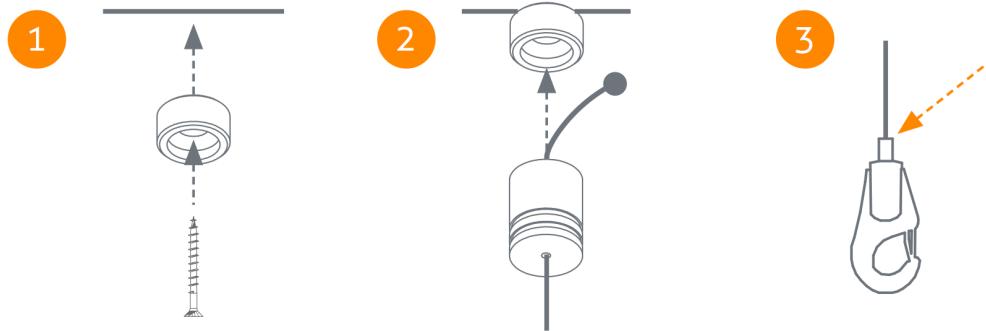
Please note that the installation set with steel cabling is available as a separate article and not included in the unit's box. For more information, please refer to the Nedap Retail Partner Portal.



Follow the next steps when mounting the unit:

- Mark the drilling holes in the ceiling.
 - Drill the holes and install the plugs.
1. Mount the base unit (with the threaded rod) with a 4x40 screw.
 2. Slide the steel cable through the bus unit (ensure the round sphere is on top).
Screw it on the base unit.
 3. Slide the adjustable hook over the steel cable.

If you want to release it, press the indicated button on the hook.



Place the mounting plate back in the unit when the installation is completed. The mounting plate doubles as dust protection for the inner components of the unit.

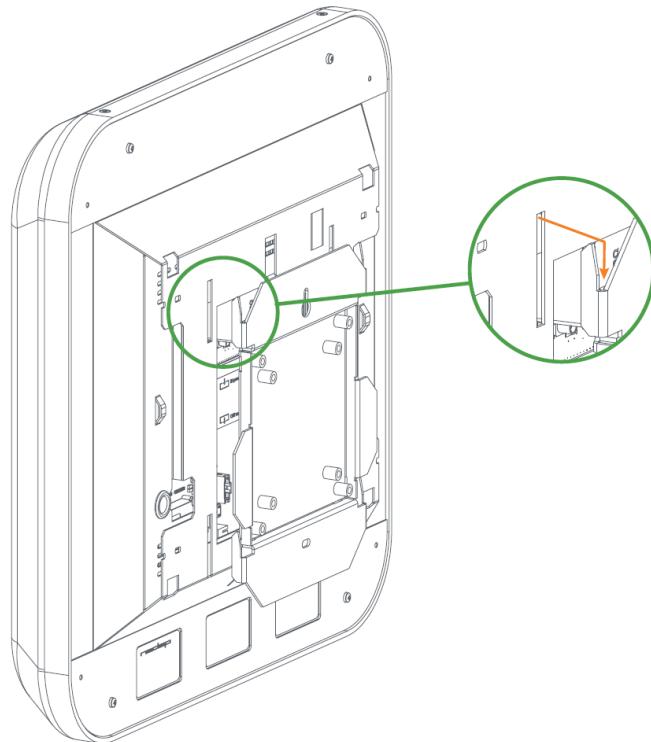
Physical installation - with VESA compatible mount

The mounting plate has the following VESA-compatible mounts:

Standard	Pattern Size	Screw Thread	Screw Length Excl. Bracket
MIS-D 75mm	75 x 75 mm (2.95 x 2.95 in.)	M4	7.4 mm (291 mil)
MIS-D	100 x 100 mm (3.93 x 3.93 in.)	M4	7.4 mm (291 mil)

The installation process is as follows:

- Mount the VESA mount to the mounting plate.
- Install all cabling to the reader.
- Slide the reader over the mounting plate as indicated in the picture.



Installing cabling

The exact cabling required was already determined during the preparation phase. Now, these cables can be placed.

Ethernet cables

Connect the Ethernet cable from the OUT port with the IN port of the next Renos unit.

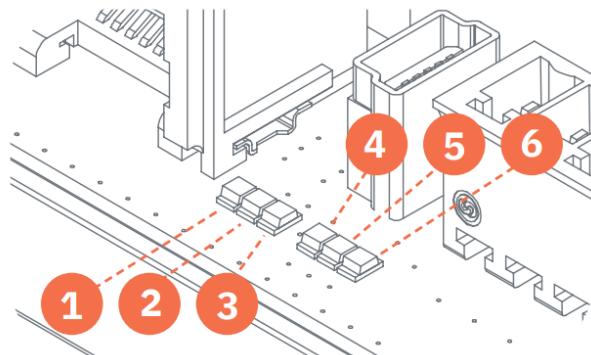
First, in all aisles, connect the Ethernet OUT port with the IN port of the next Renos unit, always following the directions of the arrows in the cabling indicated in the image below.



Please ensure that every newly created Ethernet cable is tested with an Ethernet cable tester for all four pairs (eight wires). This will prevent errors down the road.

Renos Status LEDs

The electronics inside the unit have several status LEDs that can be used to discover the status of each part of the electronics.



Status LEDs of the Renos unit

LED	Color	Status	Explanation
1	Green	On	There is a Renos unit connected to the OUT port of this unit
		Off	There is no Renos unit connected to the OUT port of this unit
2	Blue	Blinking	There is no device connected to the OUT port of this unit
		On	There is a Power Inserter connected to the OUT port of this unit
3	Red	On	There is an issue with the power supply at the OUT port of this unit (too little current drawn)
		Blinking	There is an issue with the power supply at the OUT port of this unit (too much current drawn)
		Off	There is no issue with the power supply at the OUT port of this unit
4	Yellow	Blinking	The operating system on the Renos unit is running
		Off	The operating system on the Renos unit is not running
5	Green	Blinking	The storage flash on the Renos unit is accessed
		Off	The storage flash on the Renos unit is not accessed
6	Green	On	The firmware on the Renos unit is running

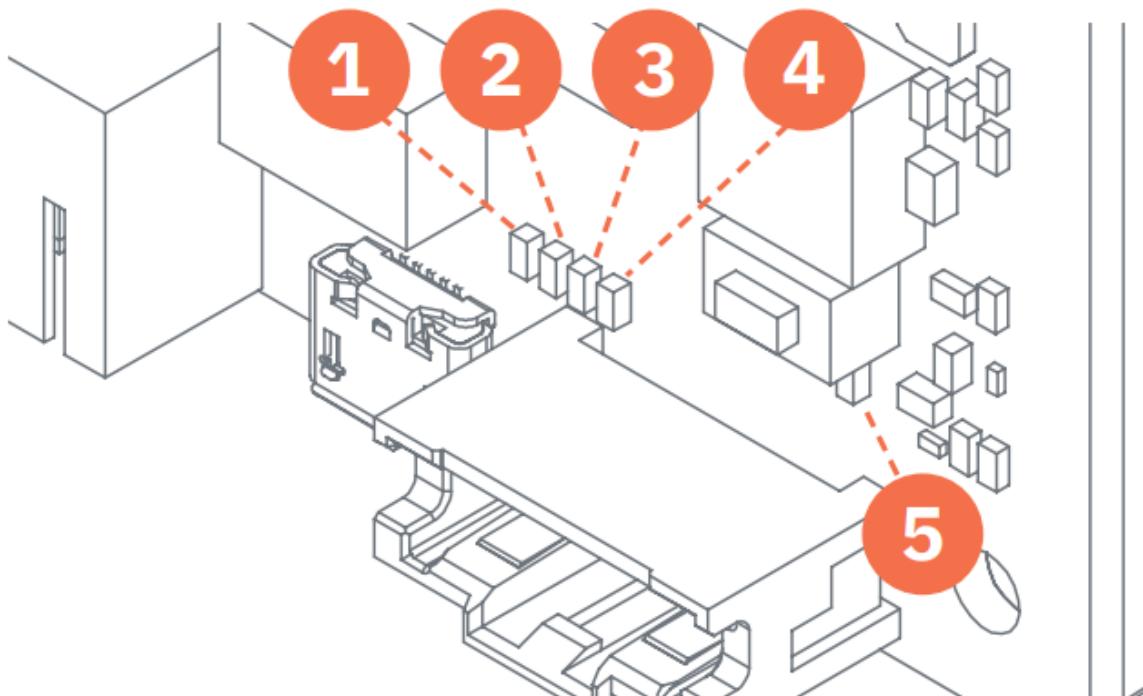
LED	Color	Status	Explanation
		Off	The firmware on the Renos unit is not (yet) running

Please look at the Troubleshooting chapter later in this manual to resolve erroneous conditions.



If the Renos unit has a firmware error, the rightmost three LEDs (4, 5, and 6) will remain off when powered. This can be solved using a 'Local - single unit' firmware update, as described in the "iSense firmware version manual."

RFID reader



LED	Color	Status	Explanation
1	Blue	On	The RFID Reader is connected to the Renos firmware
		Blinking	The RFID Reader has received a command from the Renos firmware
		Off	The RFID reader is not connected to the Renos firmware
2	Orange	Blinking slow	The firmware on the RFID Reader is running
		Off	The firmware on the RFID reader is not running
3	Red	On	There is an error with the RFID output

LED	Color	Status	Explanation
		Off	There is no error with the RFID output
4	Green	On	The RFID output is active
		Blinking	The reader is reading RFID labels
		Off	The RFID output is not active
5	Green	On	The Renos unit powers the RFID reader
		Off	The Renos unit does not power the RFID reader



The RFID reader will not be active when the system has not been configured yet. This means that only the 'firmware running' orange LED is blinking.

Configuring the installation

The following tools are required to complete the configuration.

- Mini-USB cable.
- Laptop with installed driver and recent browser.

Driver installation

A Windows driver needs to be installed to configure an iSense system. Please check the table below for what is required based on your operating system.

Operating System	Driver
Windows	Download the driver from the portal.
Mac OS X	You don't need to install a driver.
Linux	You don't need to install a driver.

Once you have installed the driver, please check if it works by plugging it into a Renos unit.

Supported browsers

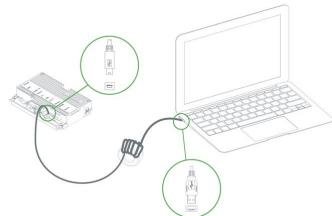
To configure the system, the latest versions of the following browsers are supported:

- Google Chrome
- Mozilla Firefox
- Apple Safari

If you don't have one of these browsers installed on your laptop, please install them before the installation.

Connecting a laptop to the Renos unit

You can connect your laptop via a Mini-USB cable to the service port on the Renos unit. In the iSense system, you can choose any Renos unit.



We advise using a good-quality USB cable about 5m / 16ft long. This provides more comfort during the configuration, as you can find an excellent place to put your laptop (instead of on the stairs or the floor next to the gate). Besides, some laptops interfere with RF technology, so it is better to place them further away.



We advise configuring Renos using a ferrite ring core filter around the mini USB cable. These can be ordered as spare parts with Nedap. Please take a look at the Nedap Retail Portal for more information.

Entering the configuration wizard

You can enter the configuration wizard by opening your browser and navigating to:

<http://192.168.133.1>



Ensure no other network connections are active in the same range.



Authentication

During the configuration, the user is required to authenticate himself. How this is done is dependent on the availability of Device Management.

- The system is connected to Device Management: you can enter your Nedap Retail username and password directly.
- The system is not connected to Device Management, and you don't have a Nedap Retail authentication software: choose one of the following steps:
 - If your laptop can connect to Device Management via a 4G/5G router or Wi-Fi, you can use this option to enter your username and password.
 - If that is not available, you can use your smartphone.
 - If your smartphone has no internet access, call your main technician for an authentication code.

Please reach out to support for more details on how to obtain a Nedap Retail username and password.

Getting help in the wizard

If something needs clarification, each page has a question mark button in the top right corner. You can click this to get more information on what is expected to do on a specific page.

Factory reset and Firmware change

It is essential to use the latest firmware version and start new installations with factory default units.

Details on how to perform a firmware update and factory default can be found in separate guidelines on the Partner Portal:

- iSense firmware version manual
- iSense factory reset procedure

Firmware change

There are four ways to change the firmware version on a Renos-based system:

1. Local—single unit overwrite. To execute the overwriting, insert a USB stick with the correct firmware into the USB port.
2. Local—complete system overwrite. You can execute the overwriting with files on your laptop during the configuration wizard.
3. Local - complete system update. The update can be executed during the configuration wizard with files on your laptop.
4. Device Management update. The update can be executed via the Device Management service.

Factory default

There are two ways to factory default a Renos-based system:

1. Local - single unit over-write. The factory default can be executed using a USB cable to connect the USB port to the service port.
2. Local - complete system factory default. The factory default can be executed during the configuration wizard.

System ID

You need the System ID to set up a Device Management system. The firmware version is displayed in the top right of the configuration wizard. If you click the firmware version, a pop-up shows the System ID during the configuration.



Integrating the installation with other systems

Integrating the iSense product into other solutions by the end customer is highly recommended.

Software integration with local APIs

The Renos platform offers local API endpoints for data analysis and status information. For more information, please refer to the Software Integration page on the Nedap Retail portal, which includes documentation and examples.

Servicing the installation

When the installation has been completed and delivered, it can be serviced via Nedap Device Management. We also provide monitoring options locally via SNMP.

Device Management

Nedap Retail systems can be connected to the online Device Management platform to ensure that systems can be managed remotely and work optimally globally.

The Nedap Device Management service provides four main functions on system level:

- **Monitoring:** Critical system parameters are monitored 24/7. If a system has issues, an alert is generated and sent to the supporting partner.
- **Remote Service:** using the Device Management website, an authorized Nedap-certified engineer can access the system's user interface to make changes to the configuration or access system logs.
- **Firmware Update:** an authorized Nedap-certified engineer can install new firmware releases remotely using the Device Management website.
- **Data Collection:** events per system are collected (e.g., to be displayed in the Analytics platform).
- **Sleep mode:** Enable sleep mode to conserve energy during nighttime hours, following the schedule configured in Device Management

For further details, please refer to the document on the portal about network information.

SNMP

Simple Network Management Protocol (SNMP) is available to allow for local monitoring of iSense systems. For example:

- One or more Renos units are not reachable
- The system is connected to Device Management

iSense systems use SNMP version 2c, community public. The MIB file is available on the iSense system itself via the URL [http://\(ip address of the system\)/snmp](http://(ip address of the system)/snmp) (for example, that is **http://192.168.133.1/snmp** when connected to the USB service port).

Troubleshooting

If the system is malfunctioning, please check the troubleshooting options below. If you still can't solve your issue, you can find support options in the next chapter.

Physical installation

Symptom	Cause	Solution
The red LED (3) on a Renos unit is on.	The current drawn-out of the OUT port of the Renos unit is too low. The cabling at the OUT port of the Renos unit does not satisfy the maximum length requirements.	Verify whether the cabling length in the system satisfies the requirements posed earlier in this document.
	The current drawn-out of the OUT port of the Renos unit is too low. The connectors of the Ethernet cable at the OUT port of the Renos unit are not mated properly.	Check the Ethernet cable at the OUT port of the Renos unit with an Ethernet cable tester.
The red LED (3) on a Renos unit is blinking.	The current drawn-out of the Renos unit's OUT port is too high. There are too many Renos units and add-ons connected to one Power Inserter.	Verify the number of Renos units and add-ons connected to the Power Inserters with the table earlier in this document.
	The current drawn-out of the Renos unit's OUT port is too high. A short circuit in the cabling leaves this Renos unit's OUT port.	Check the Ethernet cable at the OUT port of the Renos unit with an Ethernet cable tester.
The green LED (1) on a Renos unit is off, but there is a unit behind this unit.	There is an issue in the cabling between those units, so the following unit is not recognized.	Check Ethernet cabling with an Ethernet cable tester.
The red LED (3) on the RFID reader is on.	The RFID reader is having trouble starting to read. An erroneous antenna or a cabling error might cause this.	Log in to the Renos configuration interface to see the exact error.

Configuration

Symptom	Cause	Solution
It is not possible to access the configuration web interface.	Renos unit has not started yet.	Verify the green "firmware running" LED on the Renos unit (6). If this LED is not on, verify the system has power, or wait five minutes and try again.
	Mini USB cable not attached to Renos unit and laptop	Attach the cable to Renos unit and laptop.
	Driver not installed	On Windows 7 and older, you manually install a driver to support Renos.
I have put a system together, but during the hardware discovery, I see only part of all the units.	The WAN access port will be 'closed' for internal network traffic during configuration. If you combine two systems later on, this needs to be re-opened.	Do a factory reset on the previously used WAN entry point unit. If that doesn't work, do a factory reset on all units.
	There is a cabling error.	Please check all Ethernet cabling with an Ethernet cable tester.
	Not all Power Inserters are powered, or some Renos units are not fully started.	Verify the green "firmware running" LED on the Renos unit (6). If this LED is not on, verify the system has power, or wait five minutes and try again.
The Renos unit's all three LEDs, 4, 5, and 6, are off, indicating a firmware failure.	Something might have gone wrong with a firmware update.	The 'local - single' unit firmware update mechanism restores the unit.
I have configured RFID, but it detects labels outside the aisle, not inside.	Gates are positioned the wrong way.	Check the "Orientation of products" section in the manual and correct the orientation of the gates.



Warranty and spare parts

- Please consult the Nedap Retail Business Partner from whom you purchased this product regarding the applicable warranty conditions.
- This product cannot be used for any other purpose described in this document.
- If the product is not installed according to this document, the warranty provided is not applicable.
- At the sole discretion of Nedap N.V., Nedap N.V. may decide to change the conditions of Page 7 of 19 Compliance information for technical manuals warranty policy.
- You agree that Nedap N.V. can compensate you for the pro-rata value of the warranty involved rather than replacing or repairing the product based on its technical or economical value.
- Prior to applying the warranty, please verify that you comply with the warranty conditions of the warranty policy and that you can successfully apply for the replacement or repair of a defective part.
- Parts can only be replaced with original Nedap parts; otherwise, the warranty policy will not apply to the product.
- If the warranty is applicable, please contact the dealer or send the defective parts to the dealer.

Regulatory information

FCC and IC Compliance Statement

This device complies with part 15 of the FCC Rules and RSS210 of Industry Canada. 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.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Cet appareil se conforme aux normes CNR210 exemptés de license du Industry Canada. L'opération est soumis aux deux conditions suivantes:

- (1) cet appareil ne doit causer aucune interférence, et*
- (2) cet appareil doit accepter n'importe quelle interférence, y inclus interférence qui peut causer une opération non pas voulu de cet appareil.*

Les changements ou modifications n'ayant pas été expressément approuvés par la partie responsable de la conformité peuvent faire perdre à l'utilisateur l'autorisation de faire fonctionner le matériel.

FCC and IC Radiation Exposure Statement

This equipment complies with FCC and Canadian radiation exposure limits for an uncontrolled environment. It should be installed and operated with a minimum distance of 20 cm between the radiator and your body. This transmitter must not be co-located or operated with any other antenna or transmitter.

Cet équipement est conforme a CNR102 limites énoncées pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et votre corps.

This Class B digital apparatus complies with Canadian ICES-3. Cet appareil numérique de Classe B est conforme à la norme Canadienne NMB-3.

FCC Information to the user

Note: This equipment has been tested and found to comply with the limits for class B digital devices, according to part 15 of the FCC Rules. These limits are designed to protect reasonably against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency

energy and, if not installed and used following the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. Suppose this equipment does not cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on. In that case, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from the receiver's.



Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. To ensure compliance with FCC regulations, use only the shielded interface cables provided with the product or additional specified components or accessories that can be used to install the product.

Information for Taiwan

第十二條 經型式認證合格之低功率射頻電機，非經許可，
公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；
經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。
低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

CE WEEE

This European Standard specifies a marking:

- of electrical and electronic equipment following Article 11(2) of Directive 2002/96/EC (WEEE); This is in addition to the marking requirement in Article 10(3) of this Directive, which requires producers to mark electrical and electronic equipment put on the market after 13 August 2005 with a 'crossed-out wheeled bin' symbol.
- that applies to electrical and electronic equipment falling under Annex IA of Directive 2002/96/EC, provided the equipment concerned is not part of another type of equipment that does not fall within the scope of this Directive. Annex IB of Directive 2002/96/EC contains an indicative list of the products that fall under the categories set out in Annex IA of this Directive;



- that identifies the equipment producer clearly and that the equipment has been put on the market after 13 August 2005.

CE - UKCA Declaration of Conformity

With this, Nedap N.V. declares that the subject equipment is in compliance for CE with directives 2014/53/EU (Radio Equipment Directive) and 2011/65/EU (RoHS). And for UKCA with SI 2017/1206 (radio Equipment Regulations 2017) and with SI 2012/3032 UK Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 (RoHS). The full text of the declarations of conformity is available at the following internet address: <https://portal.nedapretail.com/>, where, if applicable, REACH information can also be found.

Disposal of this product

This product's owner or last user is responsible for properly disposing of (parts of) the product as required by local rules and regulations.





About Nedap

Together, we make merchandise simply available

At Nedap, we believe in ‘Technology for Life’. Nedap Retail enables retailers to serve their customers better. Using technology, we allow for perfect inventory visibility, total control, no waste, and no losses.

Our vision for inventory visibility

Today, established retailers need more information about where their items are. Without this knowledge, providing an omnichannel experience leads to heavy overstocking, waste, and eroding margins. Solving this requires a fundamental change in the retailers’ supply chain and information systems.

Our mission is to simplify the process of ensuring that retailers always have the right products available at the right place and time.

We do this by giving retailers perfect inventory visibility for a seamless shopping experience. This way, retailers can meet the changing consumer needs while remaining profitable.

Nedap works with the largest and most successful retailers in the world. We take complete ownership of our projects—failure is never an option. A unique combination of the best technology and industry teams at Nedap Retail achieves this.

Nedap solutions are built upon 45 years of global experience, market expertise, and close cooperation with leading retailers. A flexible network of certified partners worldwide supports our worldwide operations. Nedap systems are future-proof (RFID-ready), cost-efficient, and Eco-friendly. Our mission is to ensure retailers' customers maintain the best shopping experience while we help retailers protect their profits.

Contact

If you need further details or help preparing, executing, or servicing an installation, please contact our support team at support-retail@nedap.com.

Suggestions for improving our products and documentation are much appreciated.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Document Version 94

Document Last modification date 31 October 2024

Document PDF Exported 21 March 2025 **by** Nedap Retail | Operations

Copyright © Nedap NV 2025

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com



Nedap Sense Manual

iSense Integrated Antenna

version 131, October 2024

Introduction	4
Disclaimers	4
Product Overview	5
Box contents	5
Components	6
Dimensions	7
Connections	8
Add-ons	10
Preparing the installation.....	12
Defining the system	12
Field distribution	13
Detection distance or aisle width	14
RF installation requirements	14
Power Inserter	15
Cabling	17
Executing the installation.....	21
Physical installation	22
Installing cabling and filters	25
Renos Status LEDs	27
Configuring the installation	29
Driver installation	29
Supported browsers	29
Connecting a laptop to the Renos unit	30
Entering the configuration wizard	30
Authentication	31
Getting help in the wizard	31
Factory reset and Firmware change	32
System ID	32
Integrating the installation with other systems.....	33
Software integration with local APIs	33
Physical integration using an IO Box	33
URL trigger	33
Servicing the installation.....	34



Device Management	34
SNMP	34
Troubleshooting.....	35
Physical installation	35
Configuration	36
RF technology issues	37
Warranty and spare parts.....	39
Regulatory information	40
FCC and IC Compliance Statement	40
FCC and IC Radiation Exposure Statement	40
FCC Information to the user	40
Information for Taiwan	41
CE WEEE	41
CE - UKCA Declaration of Conformity	42
Disposal of this product	42
About Nedap.....	43
Together, we make merchandise simply available	43
Our vision for inventory visibility	43
Contact	43

Introduction

The Nedap Integrated Antenna is a standard gate equipped with audiovisual signaling by a built-in buzzer and a signal LED. The antenna is designed explicitly for building a POS application, such as Electronic Article Surveillance (EAS) at, for example, a supermarket.



This manual provides an overview of the products, as well as the installation and configuration basics. Several guidelines are available on the Nedap Retail Partner Portal to obtain more details.

This manual covers the following products:

Article Number	Article Name	Commercial Name	Technologies	Model Name
9566694	ASSY CO252R RF	Integrated Antenna	8.2 MHz RF	ASSY CO252R RF

Disclaimers



Nedap intends to make this manual accurate and complete. However, Nedap does not warrant that the information contained herein covers all details, conditions or variations, nor does it provide for every possible contingency in connection with the installation or use of this product. Nedap disclaims any liability for damage to property or personal injury resulting, in whole or in part, from improper installation, modification, use, or misuse of its products. The information contained in this document is subject to change without notice.



This equipment should only be installed, operated, serviced, and repaired by skilled personnel. The installation and interconnection of this equipment to facility wiring and other equipment must be done by a competent, skilled craftsman familiar with applicable standards and codes governing the installation. Installation methods, practices or procedures that are unauthorized or done improperly are dangerous and could result in serious personal injury or damage to property and equipment.

Product Overview

The Integrated antenna is only an 8.2 MHz RF installation and can only be used as a built-in antenna.

The antenna housing is created from uncoated aluminum, which functions as a shield and contains an HPL sheet on the front.



In this document, the following abbreviations will be used from here onward:

- 'RF technology' is an abbreviation for 8.2 MHz RF technology.

Box contents

Article Number	Article Name	Box Contents
9566694	ASSY CO252R RF	<ul style="list-style-type: none">• ASSY CO252R RF (Antenna assembly)• Wired signal LED (packaged in one of the sides of the folded carton)• Installation set• Quick Reference

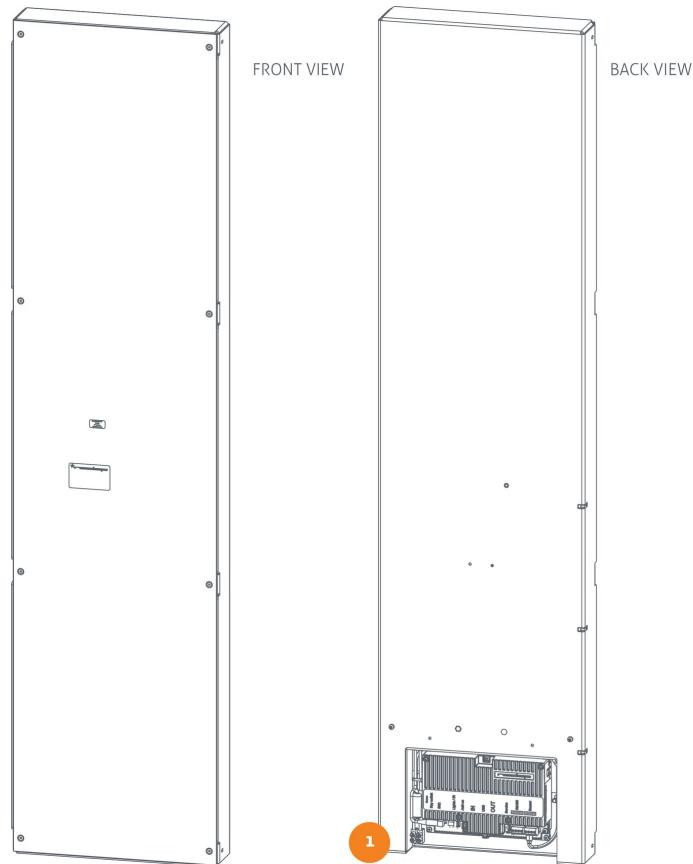


⚠ Use the Integrated Antenna only as a built-in antenna. The antenna is not designed to be visible in a store or shop. (Shield is uncoated Aluminum)

DO NOT break the warranty label or open the antenna to re-adjust the antenna. (RMA procedure is **NOT** possible with a broken warranty label)

Components

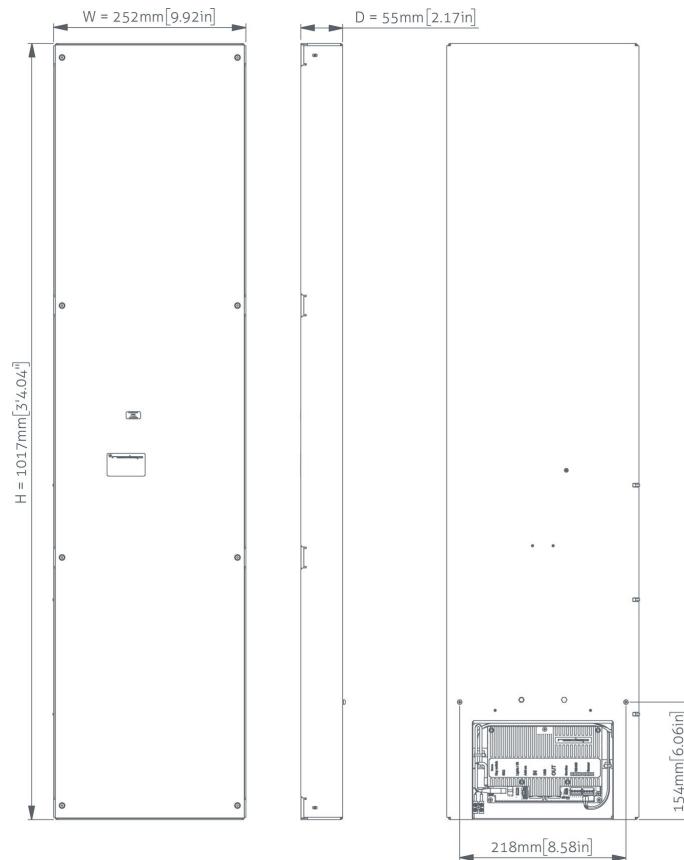
The Integrated Antenna is based on the Renos platform. The Renos platform is developed by Nedap Retail specifically for retail applications. The Renos is visible on the back view of the antenna, marked with '1'.



No.	Component	Description
1	Renos unit	The Renos unit is the central processing unit of an iSense product. It powers the system and data communication between units and the outside world.

Dimensions

The dimensions of the Integrated Antenna can be found in the views below.



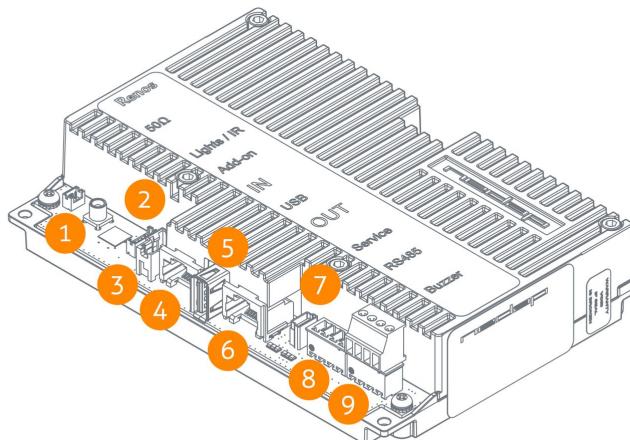
The indicated width of the CO252R antenna is **excluding 1 mm** due to the use of three cable ties mounted at the side of the antenna.



2x ground- and mounting point at the Renos side, M3x10-screws with toothed washer, 154mm above the bottom surface with a center distance of 218mm.

Connections

View of a Renos unit, with a description of all its connectors and what they are used for.



No.	Connector	Usage
1	50 ohm	Connect the Renos unit to the 50-ohm PCB. The 50-ohm PCB connects both the light and the RF antenna.
2	Lights/IR	Connects to the audiovisual signaling and the customer counter. (Lights are powered from the Key switch connector in this antenna)
3	Add-on	Provide power and synchronization to add-ons.
4	Network IN	Connected to the Network OUT of a previous Renos unit or a Power Inserter.
5	USB	Connect accessories to Renos.
6	Network OUT	Connected to the Network IN of the next unit or a Power Inserter. It can also be left unconnected or connected to the customer network.
7	Mini USB service port	Connect your laptop to configure the Renos system.
8	RS485 connector	Connect to the optional Nedap RF Smart Deactivator.
9	Buzzer connector	Connection to the buzzer is not possible for products in the iSense Lumen series. Alarm signaling is created in.

The LED indicators on the Renos unit will be discussed later in this manual.



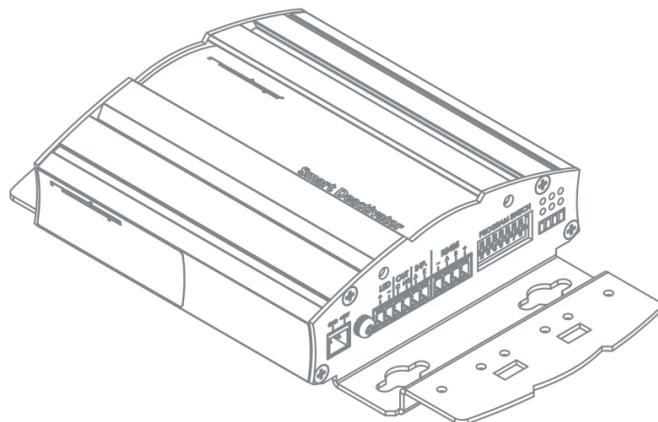
Using a keyswitch is **not** possible, the 3-way connector on the Renos PCB is used for the LED signaling light.

Add-ons

There are add-ons available for the iSense series products. The add-ons have their manual; however, we will briefly discuss the function of those add-ons here.

RF Smart Deactivator

The RF Smart Deactivator can be used to deactivate RF labels at the checkout. When connected to an iSense system, it can be powered by a Renos unit. The Renos unit can also gather information from the deactivator, like whether it is operational.



The RF Smart Deactivator integration cannot be used in iSense systems where RF is not enabled.



iSense Dashboard

The iSense system has a built-in security dashboard, the iSense Dashboard. It can be enabled by entering a purchased license key during the configuration wizard. The customer can then visit the dashboard via a web browser. To make this work, the iSense system should be in the same network, either connected to the customer network or a stand-alone set-up with a router should be made.

The iSense Dashboard allows the iSense system to be monitored inside the store. It creates an overview and provides real-time information for more effective reactions. The iSense Dashboard contains:

- Real-time overview of which gate or attention button is alarming: the ‘recent alarms’ provide controls to react quickly and accurately to alarms.
- The System Health widget shows the system’s performance to identify whether the system is functioning correctly quickly.
- The Alarm Data widget shows the number of RF/RFID/MD alarms per day as a percentage and compares this to the same time last day.
- The Visitor widget shows the number of customers today and the percentage change compared to the last hour.
- All information is saved for the last seven days to evaluate your store’s statistics and improve its operation.

Preparing the installation

When preparing an installation with products from the iSense series, there are a few things that should be taken into account:

- The number of Power Inserters that are needed to power the system
- Which cabling needs to be installed
- The firewall settings that need to be in place to enable Device Management

Defining the system

When a store requires gates to be placed at several locations, there needs to be a decision on how to combine these gates into one or multiple systems. The following rules need to be taken into account:

1. **Try to combine all gates into one system.** The Renos platform has a built-in synchronization mechanism for RF technology to minimize gate interference. For this synchronization mechanism, the gates must be connected to one system.
2. **However, the maximum cable length requirements need to be satisfied.** If it is impossible to put all the gates within a role in one system due to the maximum cable length requirements, you can split the gates into two or more systems. In this case, assign each system a different *multi-system channel* during the RF configuration.

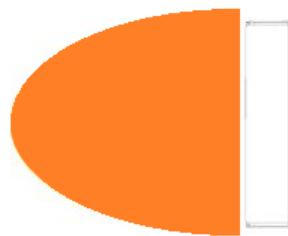
Role/Store Position	Max. System Size
EAS	100

Field distribution

RF technology has several modes of operation. The mode can be configured during the configuration wizard.

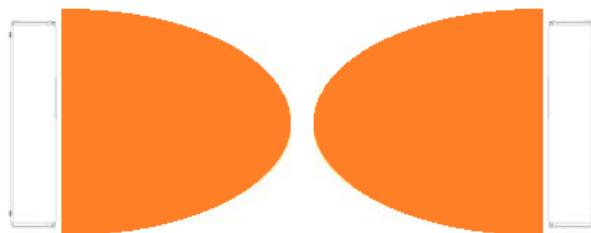
CO252R antenna "Standalone"

The CO252R antenna is stand-alone and built into a Check Out POS.



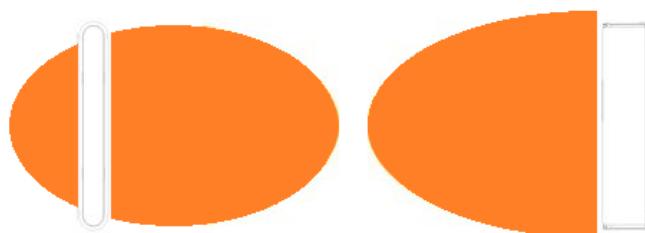
Combine the CO252R antenna with a second antenna.

It is possible to have two CO25R antennas facing each other, but the checkout furniture must allow for this. Two CO25R antennas should run in full field.



It is also possible to combine a CO252R antenna with, for instance, an FL30R gate built into a Check Out POS.

This setup should be considered in focused field mode to limit the detection range at the rear side of the non-shielded FL30R.



Detection distance or aisle width

After the field distribution, the next step is figuring out how many gates you need. This depends on the system's detection distance (half of the aisle width). There is no fixed answer to this question; it depends on many factors, like customer expectations, the quality of the tags, the environment, etc.

The recommendations below are based on the Nedap NT4040 (reference label) for RF.



Only the recommended 'detection distance' or 'aisle width' is specified. Depending on the tag used and the environment the gates are placed in, sometimes larger values can be achieved. You are advised to test this before using it in a store.

The CO252R antenna itself has a very low back detection. When RF is set to full field, the following recommendations are in place:

Position Of Nedap NT4040- Label	Detection Distance	Remark
Front detection	75 - 85 cm	
Back detection	maximum 10 cm	maximum possible back detection at the top of the antenna or where the antenna field connects with metal surfaces of the POS

RF installation requirements

The operation of RF technology is affected by both coupling issues (the antenna couples with other objects) and by active interference (other devices that transmit a signal around 8.2 MHz).

Objects that cause coupling effects could be windows, doors, metal framing around the checkout, etc. Another RF system, LED drivers, motors driving doors, or roller shutters can also create interference.



Before the installation, it is advised to gain information on the flooring that is below the antenna. If a dry-walk floor mat is used, it might have metal components that influence RF detection performance. In that case, a cut must be made in the floor mat to break conduction between the metal components in the mat and the antenna.

Power Inserter

When the installation location of the products is precise, the location of the Power Inserters needs to be defined. Depending on which technologies are used and the number of add-ons in use, a maximum number of Renos units can be connected to one power inserter.

The table below shows the Power Inserters needed for each hardware configuration.

Technologies In Use	#Units / PI 230V	#Units / PI 115V
RF	5	5
RF + 2 SD's	4	4

Index:

- RF = Radio Frequency 8.2 MHz
- 2 SDs = 2 connected smart deactivators

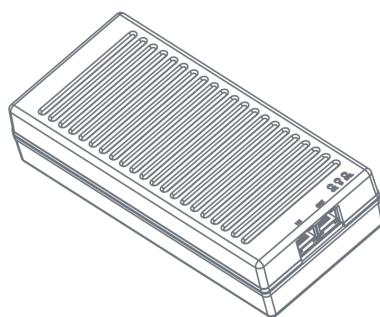
Of course, putting fewer gate units on a Power Inserter is also possible.



MD (Metal Detection) and RFID (RAIN Radio Frequency Identification) are NOT possible with the CO252R antenna.



Please note that you can only use a Nedap Power Inserter (Power-over-Ethernet) to power Renos systems. It is not possible to use generic Power-over-Ethernet switches or stand-alone inserters.



The Power Inserter is recommended to be connected to an always-on power socket. This allows continuous monitoring of the system and remote firmware updates during the night.



Ensure the Power Inserter is placed at least 1 m or 3.3 ft. from the gates. When placed closer to the gate, it might cause interference with the RF technology.



Do not disconnect network cables in the system while it is still powered! First, disconnect the power cable from the power inserter(s).

Cabling

When the number of gates and the number of Power Inserters is precise, the next step is to determine the cabling to be used for the system. Depending on the technologies that are used, different cables are required.

The iSense series uses a daisy chain topology, which means that all devices are connected as a chain:

1. a cable from a Power Inserter OUT to a Renos unit IN,
2. from that Renos unit OUT to the next Renos unit IN,
3. etc.

Technologies In Use	Cables That Need To Be Installed
Only RF	Ethernet cable between each unit and the Power Inserter

If the system should be connected to the customer network or Device Management, an ethernet cable from the system must be connected to the customer network or a 3G/4G router.

Cable specifications - Ethernet cable

The following cable specifications are recommended for the iSense system:

- Use UTP Cat5e with a stranded copper core, with 24 AWG (0,51mm) core diameter.

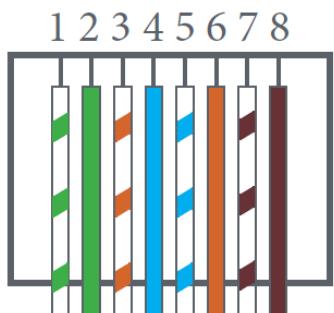


Always connect **all four pairs** using the **T568B** termination standard or T568A if specifically required!

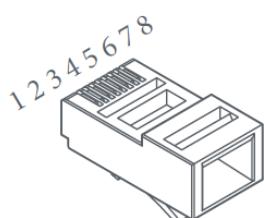
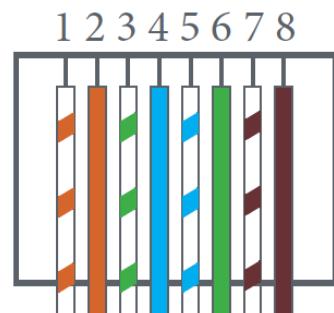


Never use CCA (copper cladding aluminum) or CCS/CCF (copper cladding steel) cable!

T568A



T568B



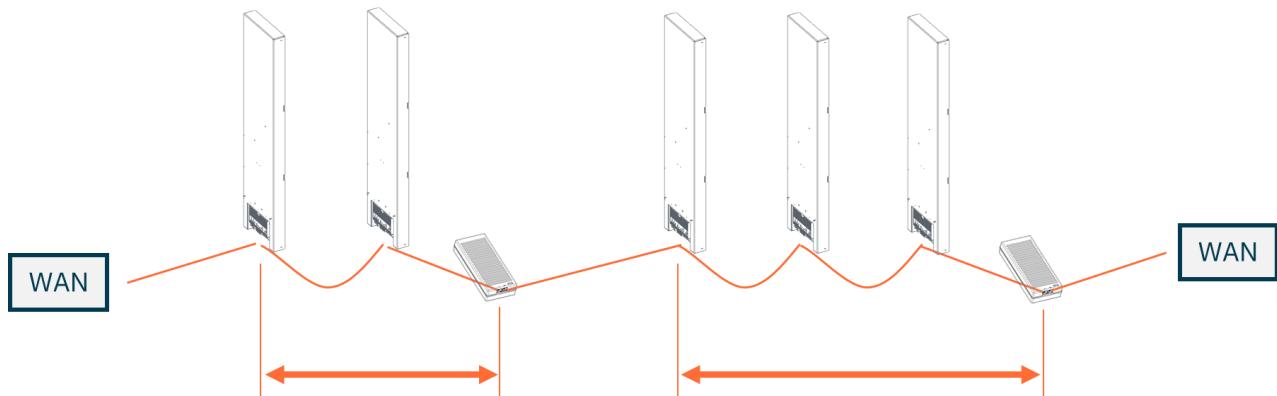
8P8C (RJ45)

Pin	T568A	T568B (Preferred)
1	Green + White	Orange + White
2	Green	Orange
3	Orange + White	Green + White
4	Blue	Blue
5	Blue + White	Blue + White
6	Orange	Green
7	Brown + White	Brown + White
8	Brown	Brown

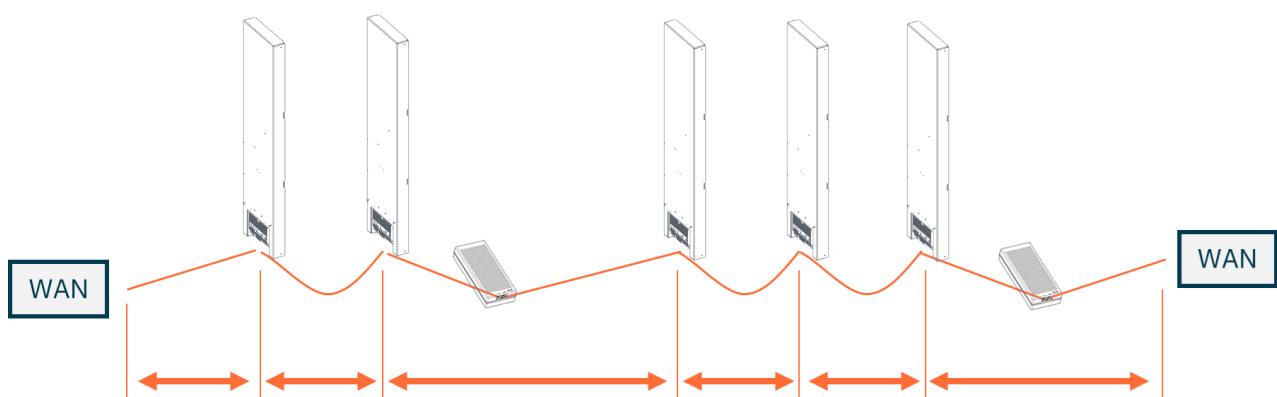
Cable length



Maximum cable length of **80 meters / 250 ft** between a Power Inserter and the last Renos unit that receives the power from this Power Inserter:



Maximum cable length of **80 meters / 250 ft** between Renos units (excluding Power Inserters) and between the first (or last) Renos unit and the WAN connection in the store:



Remarks

- It is possible to use your own preferred connectors.
- Make sure that the connectors are suitable for the cable and that the correct crimping tool is used for the connector.
- Follow the recommendations of the cable manufacturer.
- Local regulations may dictate using a specific cable type or rating.



We recommend placing the Power Inserter in the switch room (near a power socket) when the ethernet cable lengths allow. This way, the customer only has to arrange an ethernet outlet near the system.



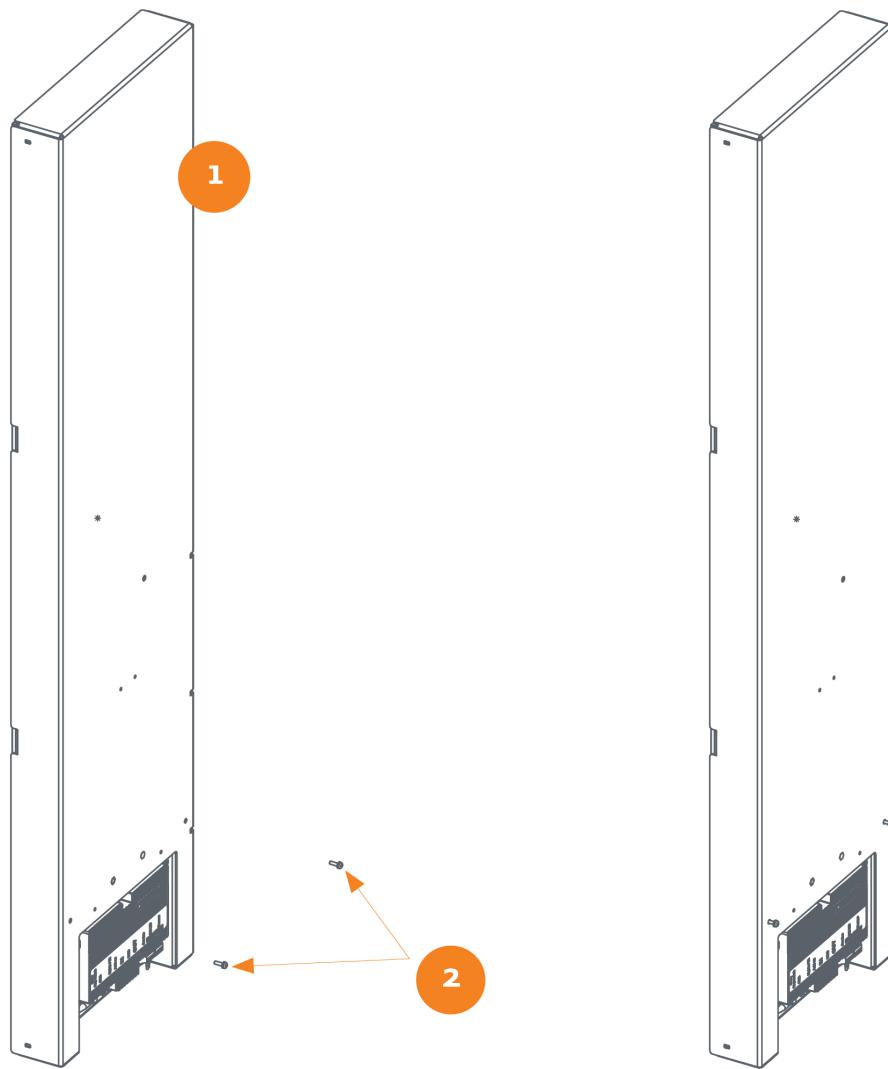
If the cable lengths between two groups exceed approximately 50 meters / 164 ft, consider splitting a system into two.

Executing the installation

When all the preparations are taken into account, the system can be installed. The installation consists of physically mounting the system in the correct orientation, installing the cabling, and applying power to the system.

Physical installation

Apply screws (fix antenna and 2x ground points of the antenna)

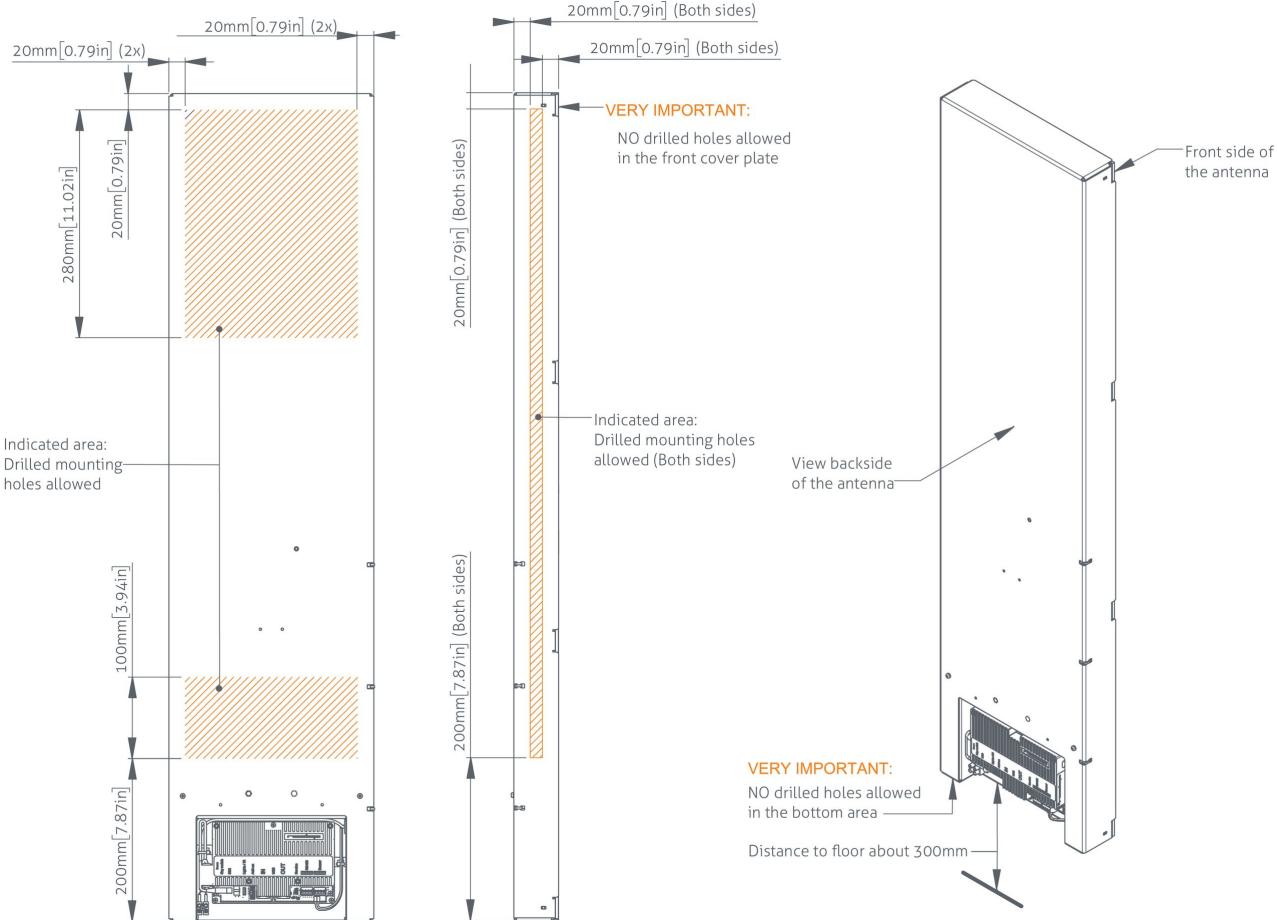


1. ASSY CO252R
2. Screw M3x10, with toothed washer



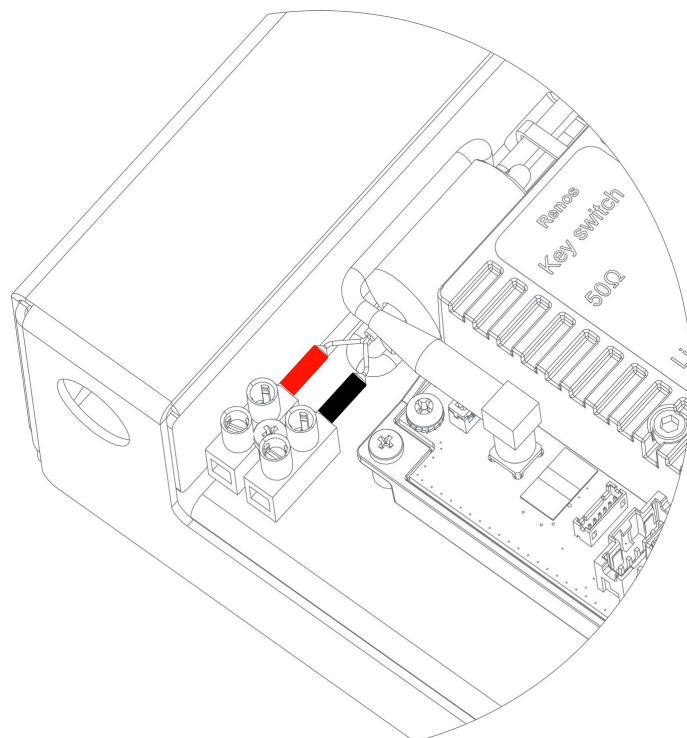
For the position of the screws, see 2.3: Product overview, Dimensions

Drill holes safely to mount the antenna



DO NOT drill any holes outside the indicated areas of the CO252R antenna. Doing so may damage or dis-adjust the antenna or create a major malfunction.

Mounting the wires of the signal LED



Detailed view of the LED connector. The signal LED, including 1500mm twin red and black wire, is delivered in the mounting set.



Connection of the LED wires:

1. The left side of the terminal block: Red wire (+ lamp)
2. Right side of the terminal block: Black wire (gnd)

Cabling and filters from the Power Inserter to the Renos



See chapter: Installing cabling and filters, Filters

Installing cabling and filters

During the preparation phase, the exact cabling required was already determined. Now, these cables can be placed.



All wiring should be done according to local regulations.

When cables are put in the slit or conduit, it is recommended to mark them with IN and OUT, as this will allow you to distinguish them from each other.

Filters

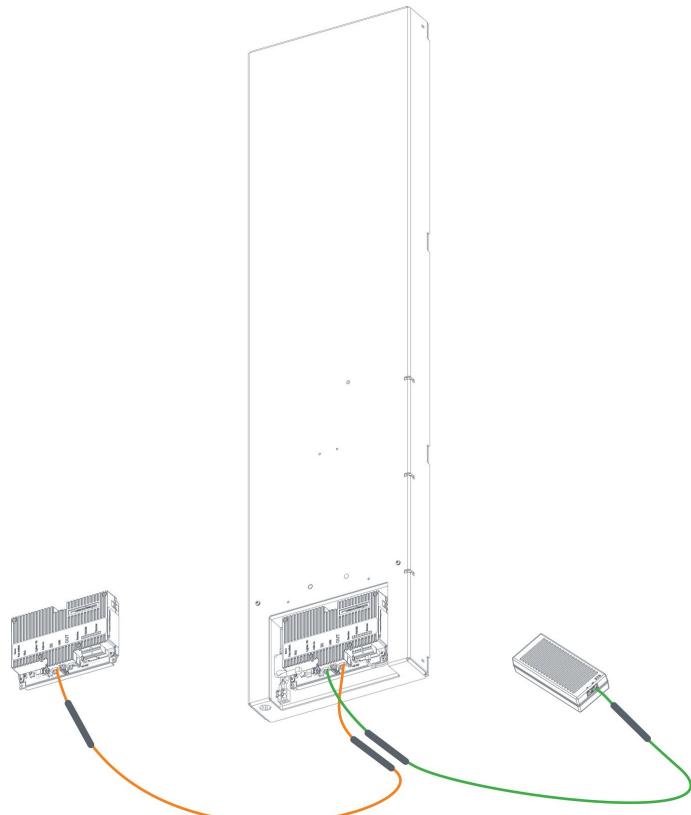
Please note that filters should be placed around the cables to reduce interference with other systems. These filters are delivered together with the system.

Filters should be placed at:

- Every Power Inserter: around the Ethernet cable, both at the OUT and IN port.
- Every Renos unit: around the Ethernet cable, both at the OUT and IN port.
- Every 9 m (30 ft.) for longer Ethernet cables.



To save yourself a lot of frustration, please place the filters *before* attaching the connectors. The other way around is not possible, and many have tried before.



View of the Power Inserter, CO252R antenna, and Renos. The Renos can be built into an I37R or FL30R Antenna.



Nedap offers the opportunity to order filters as spare parts. For more information, please refer to the Nedap Retail Portal.

The filters closest to a Renos unit should be placed inside the foot of the gate. If multiple filters are in the foot of the gate, they should be tied together.

Ethernet cables

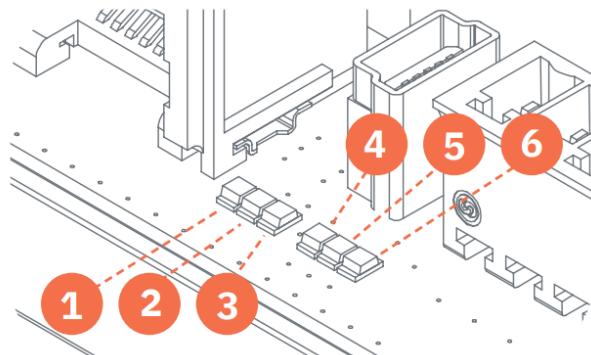
Connect the Ethernet cable from the OUT port with the IN port of the next Renos unit.



Please test every Ethernet cable for correct connections and pair all four pairs (8 wires) with an Ethernet cable tester. This will ensure that the system can function correctly.

Renos Status LEDs

The electronics inside the unit have several status LEDs that can be used to discover the status of each part of the electronics.



Status LEDs of the Renos unit

LED	Color	Status	Explanation
1	Green	On	There is a Renos unit connected to the OUT port of this unit
		Off	There is no Renos unit connected to the OUT port of this unit
2	Blue	Blinking	There is no device connected to the OUT port of this unit
		On	There is a Power Inserter connected to the OUT port of this unit
3	Red	On	There is an issue with the power supply at the OUT port of this unit (too little current drawn)
		Blinking	There is an issue with the power supply at the OUT port of this unit (too much current drawn)
		Off	There is no issue with the power supply at the OUT port of this unit
4	Yellow	Blinking	The operating system on the Renos unit is running
		Off	The operating system on the Renos unit is not running
5	Green	Blinking	The storage flash on the Renos unit is accessed
		Off	The storage flash on the Renos unit is not accessed
6	Green	On	The firmware on the Renos unit is running

LED	Color	Status	Explanation
		Off	The firmware on the Renos unit is not (yet) running

Please look at the Troubleshooting chapter later in this manual to resolve erroneous conditions.



If the Renos unit has a firmware error, the rightmost three LEDs (4, 5, and 6) will remain off when powered. This can be solved using a 'Local - single unit' firmware update, as described in the "iSense firmware version manual."

Configuring the installation

The following tools are required to complete the configuration.

- Mini-USB cable.
- Laptop with installed driver and recent browser.

Driver installation

A Windows driver needs to be installed to configure an iSense system. Please check the table below for what is required based on your operating system.

Operating System	Driver
Windows	Download the driver from the portal.
Mac OS X	You don't need to install a driver.
Linux	You don't need to install a driver.

Once you have installed the driver, please check if it works by plugging it into a Renos unit.

Supported browsers

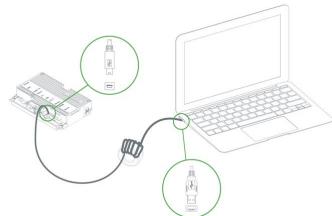
To configure the system, the latest versions of the following browsers are supported:

- Google Chrome
- Mozilla Firefox
- Apple Safari

If you don't have one of these browsers installed on your laptop, please install them before the installation.

Connecting a laptop to the Renos unit

You can connect your laptop via a Mini-USB cable to the service port on the Renos unit. In the iSense system, you can choose any Renos unit.



We advise using a good-quality USB cable about 5m / 16ft long. This provides more comfort during the configuration, as you can find an excellent place to put your laptop (instead of on the stairs or the floor next to the gate). Besides, some laptops interfere with RF technology, so it is better to place them further away.



We advise configuring Renos using a ferrite ring core filter around the mini USB cable. These can be ordered as spare parts with Nedap. Please take a look at the Nedap Retail Portal for more information.

Entering the configuration wizard

You can enter the configuration wizard by opening your browser and navigating to:

<http://192.168.133.1>



Ensure no other network connections are active in the same range.



Authentication

During the configuration, the user is required to authenticate himself. How this is done is dependent on the availability of Device Management.

- The system is connected to Device Management: you can enter your Nedap Retail username and password directly.
- The system is not connected to Device Management, and you don't have a Nedap Retail authentication software: choose one of the following steps:
 - If your laptop can connect to Device Management via a 4G/5G router or Wi-Fi, you can use this option to enter your username and password.
 - If that is not available, you can use your smartphone.
 - If your smartphone has no internet access, call your main technician for an authentication code.

Please reach out to support for more details on how to obtain a Nedap Retail username and password.

Getting help in the wizard

If something needs clarification, each page has a question mark button in the top right corner. You can click this to get more information on what is expected to do on a specific page.

Factory reset and Firmware change

It is essential to use the latest firmware version and start new installations with factory default units.

Details on how to perform a firmware update and factory default can be found in separate guidelines on the Partner Portal:

- iSense firmware version manual
- iSense factory reset procedure

Firmware change

There are four ways to change the firmware version on a Renos-based system:

1. Local—single unit overwrite. To execute the overwriting, insert a USB stick with the correct firmware into the USB port.
2. Local—complete system overwrite. You can execute the overwriting with files on your laptop during the configuration wizard.
3. Local - complete system update. The update can be executed during the configuration wizard with files on your laptop.
4. Device Management update. The update can be executed via the Device Management service.

Factory default

There are two ways to factory default a Renos-based system:

1. Local - single unit over-write. The factory default can be executed using a USB cable to connect the USB port to the service port.
2. Local - complete system factory default. The factory default can be executed during the configuration wizard.

System ID

You need the System ID to set up a Device Management system. The firmware version is displayed in the top right of the configuration wizard. If you click the firmware version, a pop-up shows the System ID during the configuration.

Integrating the installation with other systems

Integrating the iSense product into other solutions by the end customer is highly recommended.

Software integration with local APIs

The Renos platform offers local API endpoints for data analysis and status information. For more information, please refer to the Software Integration page on the Nedap Retail portal, which includes documentation and examples.

Physical integration using an IO Box

Integrating other systems via relay contact outputs and inputs is also possible. The Renos unit does not provide this directly; however, it can be accomplished via a 3rd party IO Box.



The following 3rd party IO Box is currently supported: **MOXA ioLogik E1214**.



The IO Box should be connected to a Renos unit via a USB to Ethernet adapter.

An output on an IO Box can be activated when specific events occur, depending on the capabilities of the chosen hardware.

URL trigger

The URL trigger mode can be triggered by network-based devices that have an HTTP-based API. At this moment, Axis cameras and Renos pagers are supported.

An event can trigger a control URL (a link containing information) for this device, which should be created on the device.

The communication can be further configured in the configuration wizard. Make sure that this device is reachable by the iSense system.

Servicing the installation

When the installation has been completed and delivered, it can be serviced via Nedap Device Management. We also provide monitoring options locally via SNMP.

Device Management

Nedap Retail systems can be connected to the online Device Management platform to ensure that systems can be managed remotely and work optimally globally.

The Nedap Device Management service provides four main functions on system level:

- **Monitoring:** Critical system parameters are monitored 24/7. If a system has issues, an alert is generated and sent to the supporting partner.
- **Remote Service:** using the Device Management website, an authorized Nedap-certified engineer can access the system's user interface to make changes to the configuration or access system logs.
- **Firmware Update:** an authorized Nedap-certified engineer can install new firmware releases remotely using the Device Management website.
- **Data Collection:** events per system are collected (e.g., to be displayed in the Analytics platform).
- **Sleep mode:** Enable sleep mode to conserve energy during nighttime hours, following the schedule configured in Device Management

For further details, please refer to the document on the portal about network information.

SNMP

Simple Network Management Protocol (SNMP) is available to allow for local monitoring of iSense systems. For example:

- One or more Renos units are not reachable
- The system is connected to Device Management

iSense systems use SNMP version 2c, community public. The MIB file is available on the iSense system itself via the URL [http://\(ip address of the system\)/snmp](http://(ip address of the system)/snmp) (for example, that is **http://192.168.133.1/snmp** when connected to the USB service port).

Troubleshooting

If the system is malfunctioning, please check the troubleshooting options below.

Physical installation

Symptom	Cause	Solution
The red LED (3) on a Renos unit is on.	The current drawn-out of the OUT port of the Renos unit is too low. The cabling at the OUT port of the Renos unit does not satisfy the maximum length requirements.	Verify whether the cabling length in the system satisfies the requirements posed earlier in this document.
	The current drawn-out of the OUT port of the Renos unit is too low. The connectors of the Ethernet cable at the OUT port of the Renos unit are not mated properly.	Check the Ethernet cabling at the OUT port of the Renos unit with a Ethernet cable tester.
The red LED (3) on a Renos unit is blinking.	The current drawn-out of the OUT port of the Renos unit is too high. Too many Renos units and add-ons connected to one Power Inserter.	Verify the number of Renos units and add-ons connected to the Power Inserters with the table earlier in this document.
	The current drawn-out of the OUT port of the Renos unit is too high. There is a short circuit in the cabling leaving the OUT port of this Renos unit.	Check the Ethernet cabling at the OUT port of the Renos unit with an Ethernet cable tester.
The green LED (1) on a Renos unit is off, but there is a unit behind this unit.	There is an issue in the cabling between those units, so the following unit is not recognized.	Check Ethernet cabling with an Ethernet cable tester.

Configuration

Symptom	Cause	Solution
It is not possible to access the configuration web interface.	Renos unit has not started yet.	Verify the green "firmware running" LED on the Renos unit (6). If this LED is not on, verify the system has power or wait five minutes and try again.
	Mini USB cable not attached to Renos unit and laptop	Attach the cable to Renos unit and laptop.
	Driver not installed	On Windows 7 and older you manually need to install a driver to support Renos.
I have put a system together, but I only see a part of all units during the hardware discovery.	During configuration, the WAN access port will be 'closed' for internal network traffic. If you combine two systems later, it needs to be reopened.	Do a factory reset on the unit that was previously used as WAN entry point. If that doesn't work, do a factory reset on all units.
	There is a cabling error.	Please check all Ethernet cabling with an Ethernet cable tester.
	Not all Power Inserters are powered, or some Renos units are not fully started.	Verify the green "firmware running" LED on the Renos unit (6). If this LED is not on, verify the system has power or wait five minutes and try again.
There is a firmware failure, indicated by the fact that all three LEDs 4, 5 and 6 are off on the Renos unit.	Something might have gone wrong with a firmware update.	The 'local - single' unit firmware update mechanism is used to restore the unit.

RF technology issues

When there are issues with RF technology during the configuration (the gates show as orange or red in the wizard), please follow the following steps:

1. Check the parameters in the RF Advanced Config of the configuration wizard and the RF gate performance section. One of those parameters is probably red or orange.
2. Disable all transmitters.
 - a. If all parameters in the RF gate performance section turn green again, a coupling problem exists (the transmitter couples with a label-like object in the environment). Please continue to the 'coupling problem' section.
 - b. If all parameters in the RF gate performance section remain orange or red, there is an active interferer (another device that transmits radio waves around the 8.2 MHz RF spectrum, like another EAS system, an engine, or a power supply). Please continue to the 'active interferer' section.

Coupling problem

Coupling problems are caused by objects that act as labels to the RF system. This includes metallic doorframes, checkouts, and cabling—everything that runs in a loop and is metallic.

To solve these problems, there are a few things you can try:

- Tighten screws in the metallic construction. This might work for checkouts or customer guidance rails.
- Try to interrupt the metallic loop. This can be done by using non-metallic parts inside those loops or by making a cut in them.
- Create a shortcut in the metallic loop to make it smaller. This will make it resonate at a different frequency.

If the above solutions don't solve the problem, you can decrease the system's sensitivity by ticking the 'reduced sensitivity' button in the RF Advanced Config.



If a decreased sensitivity doesn't work, and there is only one type of label or tag in the store, you also have the option to increase the 'receiver delay.' When higher than 6dB, the label detection will be limited.



The problem could also be solved with additional hardware (not available for all gates):

- **A 3-loop only 50 ohm PCB.** This will work when the coupling loop is located in the middle height of the gate.

- **Shielding.** This will work in many cases. However, the detection distance will be reduced by about 20 cm (0.7 ft.). The field will also slightly creep around the shield. This is called 'back detection'.



The 3-loop only 50 ohm PCB is only available in Europe with CE-certified products. Using it in other regions invalidates the local certifications.

If these things don't solve the problem, please contact support.

Active interferer

The first step is to locate the active interferer's source. You can do this by unplugging electronic devices around the gate (or moving them away) and seeing if the parameters in the 'RF gate performance' section improve or when the average height of the spectrum is reduced. If this is the case, you have identified the active interferer.

When the active interferer is known, the following solutions are possible:

1. Try to move the active interferer away from the gate as far as possible.
2. Try to apply filters around the cabling of the active interferer.
3. Shield the active interferer with aluminum foil.

If the above solutions don't solve the problem, you can decrease the system's sensitivity by ticking the 'reduced sensitivity' button in the RF Advanced Config.



The problem could also be solved with additional hardware:

- **A shielding.** This will work in a lot of cases. However, the detection distance will be reduced by about 20 cm (0.7ft.). The field will also slightly creep around the shield. This is called 'back detection'.



There are also round ferrites available that can reduce active interference sources and find ferrites with optimal impedance at around 8.2MHz.

If these things don't solve the problem, please contact support.



Warranty and spare parts

- Please consult the Nedap Retail Business Partner from whom you purchased this product regarding the applicable warranty conditions.
- This product cannot be used for any other purpose described in this document.
- If the product is not installed according to this document, the warranty provided is not applicable.
- At the sole discretion of Nedap N.V., Nedap N.V. may decide to change the conditions of Page 7 of 19 Compliance information for technical manuals warranty policy.
- You agree that Nedap N.V. can compensate you for the pro-rata value of the warranty involved rather than replacing or repairing the product based on its technical or economical value.
- Prior to applying the warranty, please verify that you comply with the warranty conditions of the warranty policy and that you can successfully apply for the replacement or repair of a defective part.
- Parts can only be replaced with original Nedap parts; otherwise, the warranty policy will not apply to the product.
- If the warranty is applicable, please contact the dealer or send the defective parts to the dealer.

Regulatory information

FCC and IC Compliance Statement

This device complies with part 15 of the FCC Rules and RSS210 of Industry Canada. 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.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Cet appareil se conforme aux normes CNR210 exemptés de license du Industry Canada. L'opération est soumis aux deux conditions suivantes:

- (1) cet appareil ne doit causer aucune interférence, et*
- (2) cet appareil doit accepter n'importe quelle interférence, y inclus interférence qui peut causer une opération non pas voulu de cet appareil.*

Les changements ou modifications n'ayant pas été expressément approuvés par la partie responsable de la conformité peuvent faire perdre à l'utilisateur l'autorisation de faire fonctionner le matériel.

FCC and IC Radiation Exposure Statement

This equipment complies with FCC and Canadian radiation exposure limits for an uncontrolled environment. It should be installed and operated with a minimum distance of 20 cm between the radiator and your body. This transmitter must not be co-located or operated with any other antenna or transmitter.

Cet équipement est conforme a CNR102 limites énoncées pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et votre corps.

This Class B digital apparatus complies with Canadian ICES-3. Cet appareil numérique de Classe B est conforme à la norme Canadienne NMB-3.

FCC Information to the user

Note: This equipment has been tested and found to comply with the limits for class B digital devices, according to part 15 of the FCC Rules. These limits are designed to protect reasonably against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency

energy and, if not installed and used following the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. Suppose this equipment does not cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on. In that case, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from the receiver's.



Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. To ensure compliance with FCC regulations, use only the shielded interface cables provided with the product or additional specified components or accessories that can be used to install the product.

Information for Taiwan

第十二條 經型式認證合格之低功率射頻電機，非經許可，
公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；
經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。
低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

CE WEEE

This European Standard specifies a marking:

- of electrical and electronic equipment following Article 11(2) of Directive 2002/96/EC (WEEE); This is in addition to the marking requirement in Article 10(3) of this Directive, which requires producers to mark electrical and electronic equipment put on the market after 13 August 2005 with a 'crossed-out wheeled bin' symbol.
- that applies to electrical and electronic equipment falling under Annex IA of Directive 2002/96/EC, provided the equipment concerned is not part of another type of equipment that does not fall within the scope of this Directive. Annex IB of Directive 2002/96/EC contains an indicative list of the products that fall under the categories set out in Annex IA of this Directive;



- that identifies the equipment producer clearly and that the equipment has been put on the market after 13 August 2005.

CE - UKCA Declaration of Conformity

With this, Nedap N.V. declares that the subject equipment is in compliance for CE with directives 2014/53/EU (Radio Equipment Directive) and 2011/65/EU (RoHS). And for UKCA with SI 2017/1206 (radio Equipment Regulations 2017) and with SI 2012/3032 UK Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 (RoHS). The full text of the declarations of conformity is available at the following internet address: <https://portal.nedapretail.com/>, where, if applicable, REACH information can also be found.

Disposal of this product

This product's owner or last user is responsible for properly disposing of (parts of) the product as required by local rules and regulations.





About Nedap

Together, we make merchandise simply available

At Nedap, we believe in ‘Technology for Life’. Nedap Retail enables retailers to serve their customers better. Using technology, we allow for perfect inventory visibility, total control, no waste, and no losses.

Our vision for inventory visibility

Today, established retailers need more information about where their items are. Without this knowledge, providing an omnichannel experience leads to heavy overstocking, waste, and eroding margins. Solving this requires a fundamental change in the retailers’ supply chain and information systems.

Our mission is to simplify the process of ensuring that retailers always have the right products available at the right place and time.

We do this by giving retailers perfect inventory visibility for a seamless shopping experience. This way, retailers can meet the changing consumer needs while remaining profitable.

Nedap works with the largest and most successful retailers in the world. We take complete ownership of our projects—failure is never an option. A unique combination of the best technology and industry teams at Nedap Retail achieves this.

Nedap solutions are built upon 45 years of global experience, market expertise, and close cooperation with leading retailers. A flexible network of certified partners worldwide supports our worldwide operations. Nedap systems are future-proof (RFID-ready), cost-efficient, and Eco-friendly. Our mission is to ensure retailers' customers maintain the best shopping experience while we help retailers protect their profits.

Contact

If you need further details or help preparing, executing, or servicing an installation, please contact our support team at support-retail@nedap.com.

Suggestions for improving our products and documentation are much appreciated.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Document Version 131

Document Last modification date 31 October 2024

Document PDF Exported 21 March 2025 by Nedap Retail | Operations

Copyright © Nedap NV 2025

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com



Nedap Sense Manual

iSense PA15R

i15 Go

version 25, November 2024

Introduction:	4
Color	4
Disclaimers	5
Safety precautions	5
Product Overview	6
Box contents	6
Renos platform	6
Components	7
Dimensions	8
Connections	9
Add-ons	10
Preparing the installation	13
Defining the system	13
Aisle width or detection distance	14
Label-free zone	14
RF installation requirements	14
Power Inserter	17
Executing the installation	21
Conduit or slit	21
Physical installation	21
Orientation of products and the first gate	23
Installing cabling and filters	24
Renos Status LEDs	26
RF-on light	27
Configuring the installation	28
Driver installation	28
Supported browsers	28
Connecting a laptop to the Renos unit	29
Entering the configuration wizard	29
Authentication	30
Getting help in the wizard	30
Factory reset and Firmware change	31
System ID	31



Integrating the installation with other systems	32
Software integration with local APIs	32
Physical integration using an IO Box	32
URL trigger	32
Servicing the installation.....	33
Device Management	33
SNMP	33
Troubleshooting.....	34
Physical installation	34
Configuration	35
Warranty and spare parts.....	36
RF technology issues	36
CE WEEE	37
CE - UKCA Declaration of Conformity	38
Disposal of this product	38
Regulatory information	39
FCC and IC Compliance Statement	39
FCC and IC Radiation Exposure Statement	39
FCC Information to the user	39
Information for Taiwan	40
CE WEEE	37
CE - UKCA Declaration of Conformity	38
Disposal of this product	38
About Nedap.....	42
Together, we make merchandise simply available	42
Our vision for inventory visibility	42
Contact	42

Introduction:

The i15 Go is a state-of-the-art 8.2 MHz RF gate designed to optimize sales space for narrow entrances.



This manual overviews the product, installation, and configuration basics. For more details, several guidelines are available on the Nedap Retail portal.

This manual covers the following product:

Article Number	Article Name	Commercial Name	Technologies	Model Name
9567674	ASSY PA15R RF GREY	i15 Go	8.2 MHz RF	ASSY FC180R RF

Color



The Article name describes a GREY product. It is a light grey color, RAL code 7047.

Disclaimers



Nedap intends to make this manual accurate and complete. However, Nedap does not warrant that the information contained herein covers all details, conditions or variations, nor does it provide for every possible contingency in connection with the installation or use of this product. Nedap disclaims any liability for damage to property or personal injury resulting, in whole or in part, from improper installation, modification, use, or misuse of its products. The information contained in this document is subject to change without notice.



This equipment should only be installed, operated, serviced, and repaired by skilled personnel. The installation and interconnection of this equipment to facility wiring and other equipment must be done by a competent, skilled craftsman familiar with applicable standards and codes governing the installation. Installation methods, practices or procedures that are unauthorized or done improperly are dangerous and could result in serious personal injury or damage to property and equipment.

Safety precautions



Do not place cards equipped with a magnetic strip or chip (i.e., ID, travel, debit, and credit cards) close to the equipment to avoid possible card failures.



To avoid potential interference with medical devices (pacemakers, cochlear implants, etc.), keep a distance of at least 20cm (8 inches) between them and the equipment.

Product Overview



In this document, the following abbreviations will be used from here onwards:

- 'RF technology' is an abbreviation for 8.2 MHz RF technology.

Box contents

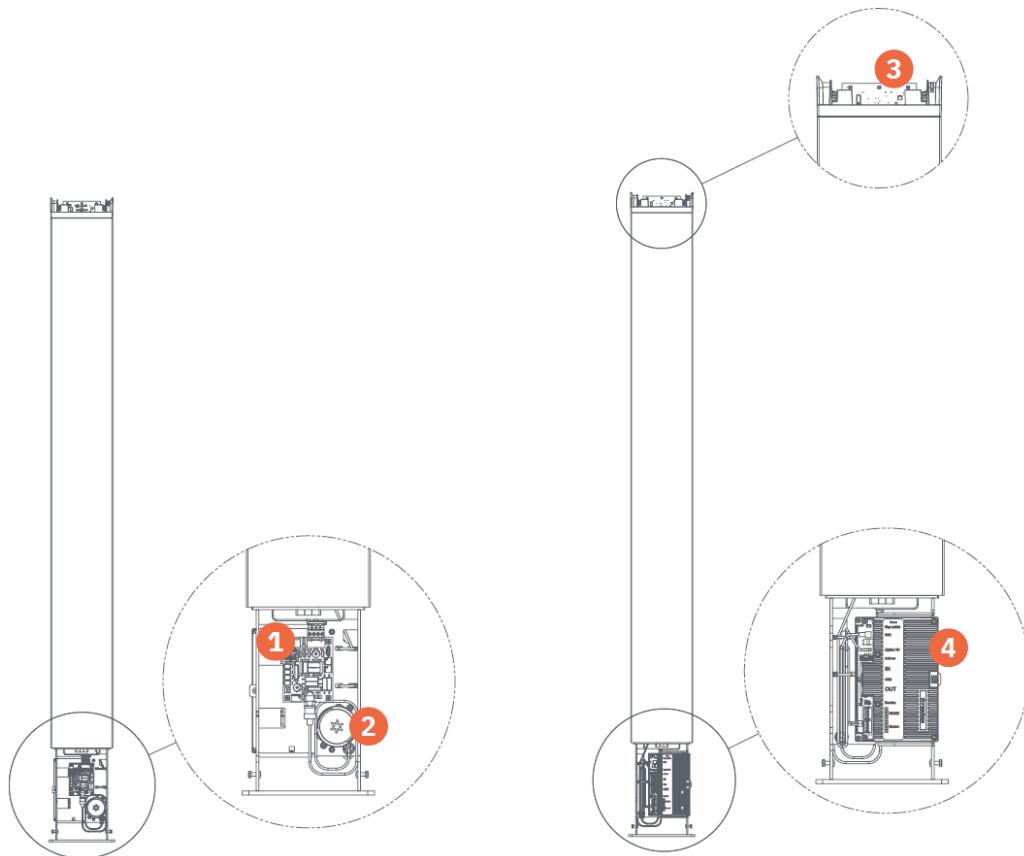
Article Number	Article Name	Box Contents
9567674	ASSY PA15R RF GREY	<ul style="list-style-type: none">• PA15R RF gate with Renos RF technology• Installation set• Quick Reference

Renos platform

The i15 Go is based on the Renos platform. The Renos platform is developed by Nedap Retail specifically for retail applications.

Components

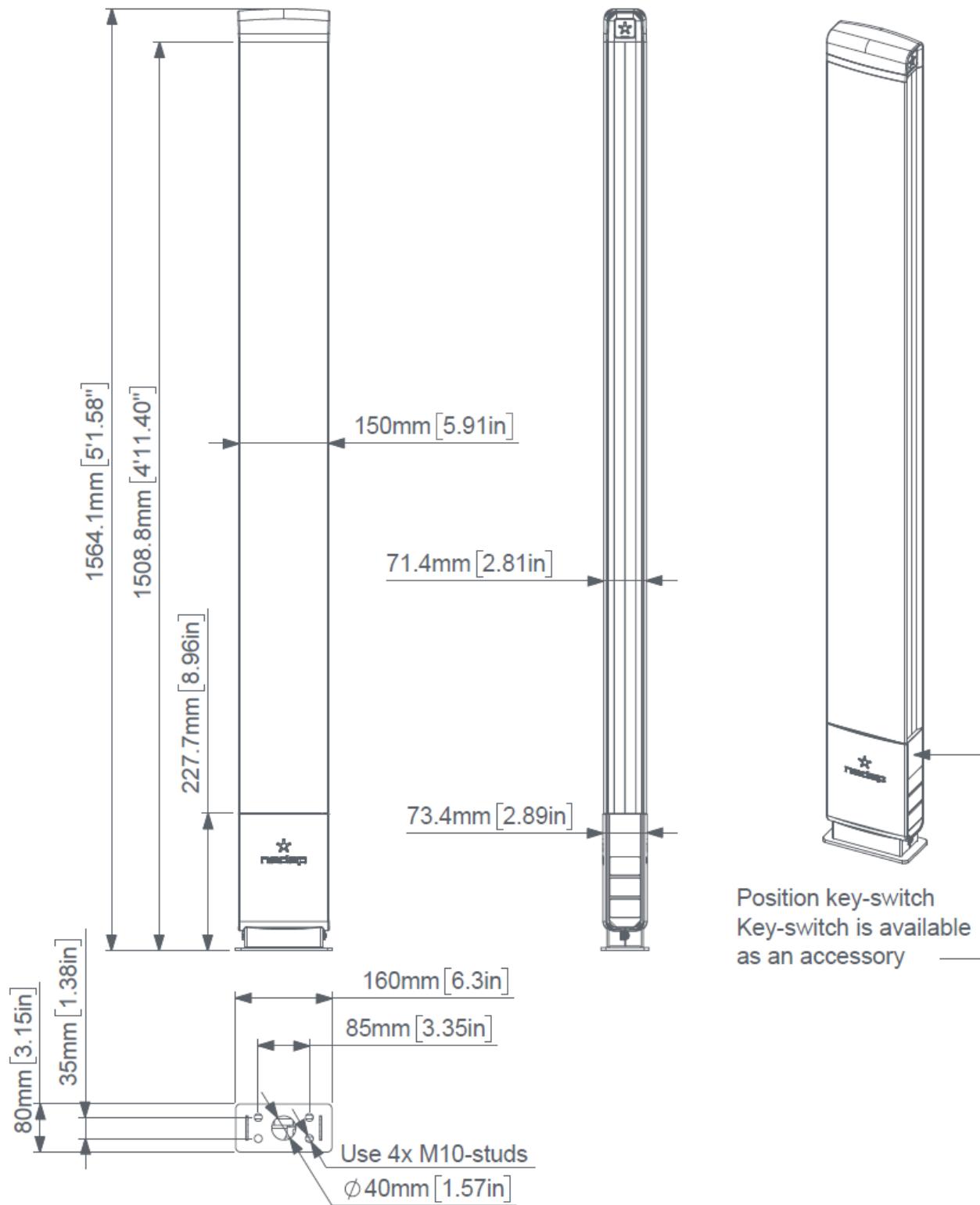
The i15 Go is fitted with several serviceable parts:



Number	Component	Description
1	50 ohm PCB	The 50-ohm PCB connects the Renos unit, the RF antenna, and the lights.
2	Buzzer	The buzzer can be used for user feedback or alarms.
3	Lights	Red LED lights on both long sides can be used for user feedback or alarms White LED lights on both narrow sides indicate that RF detection is available.
4	Renos unit	The Renos unit is the gate's main processing unit. It powers the system, communicates data between units, and communicates with the outside world. It is equipped with an RF detection engine.

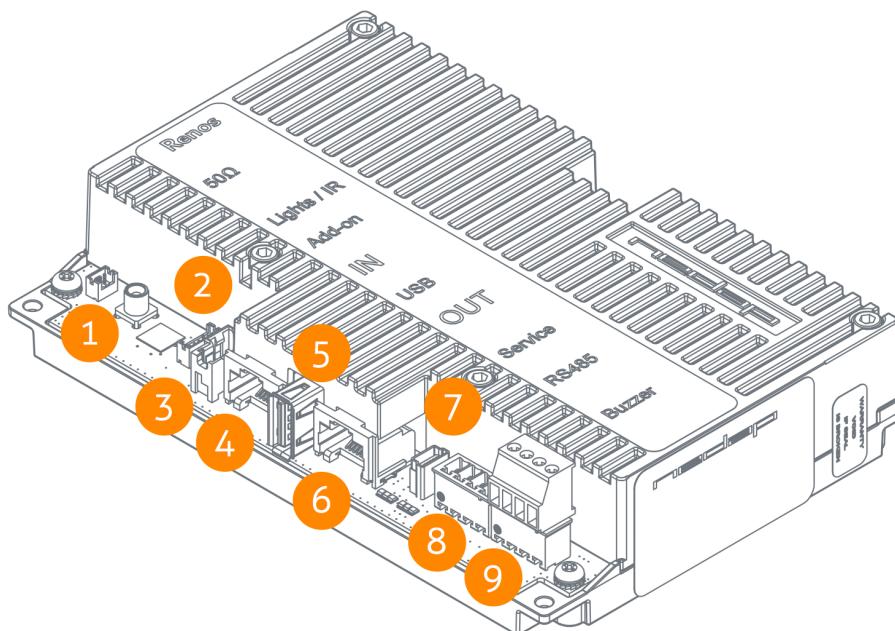
Dimensions

This section presents dimensional drawings of the gate. The holes in the mounting plate can be used as a template to draw the locations for drilling holes in the floor.



Connections

This is a Renos unit; this chapter describes all its connectors and their use.



Number	Connector	Usage
1	50 ohm	Connect the Renos unit to the 50-ohm PCB. The 50-ohm PCB connects both the light and the RF antenna.
2	Infrared beams	Connect to the optional infrared beam sensors (not applicable for the i15 Go).
3	Add-on	Provide power and synchronization to add-ons.
4	Network IN	Connected to the Network OUT of a previous Renos unit or a Power Inserter.
5	USB	Connect accessories to Renos.
6	Network OUT	It can be connected to the Network IN of the next unit or a Power Inserter, left unconnected, or connected to the customer network.
7	Mini USB service port	Connect your laptop to configure the Renos system.

Number	Connector	Usage
8	RS485 connector	Connect to the optional Nedap RF Smart Deactivator.
9	Buzzer connector	Connect to the included buzzer.

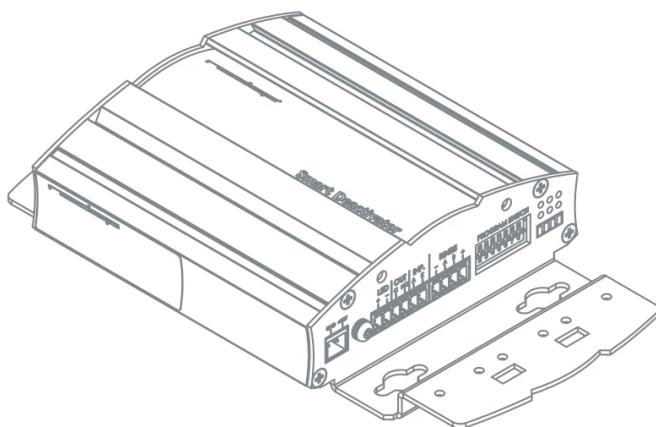
The LED indicators on the Renos unit will be discussed later in this manual.

Add-ons

Several add-ons are available for the i15 Go. Each add-on has its own manual/guideline. However, we will discuss the function of those add-ons here.

RF Smart Deactivator

The RF Smart Deactivator can be used to deactivate RF labels at the checkout. When connected to an iSense system, it can be powered by a Renos unit. The Renos unit can also gather information from the deactivator, like whether it is operational.

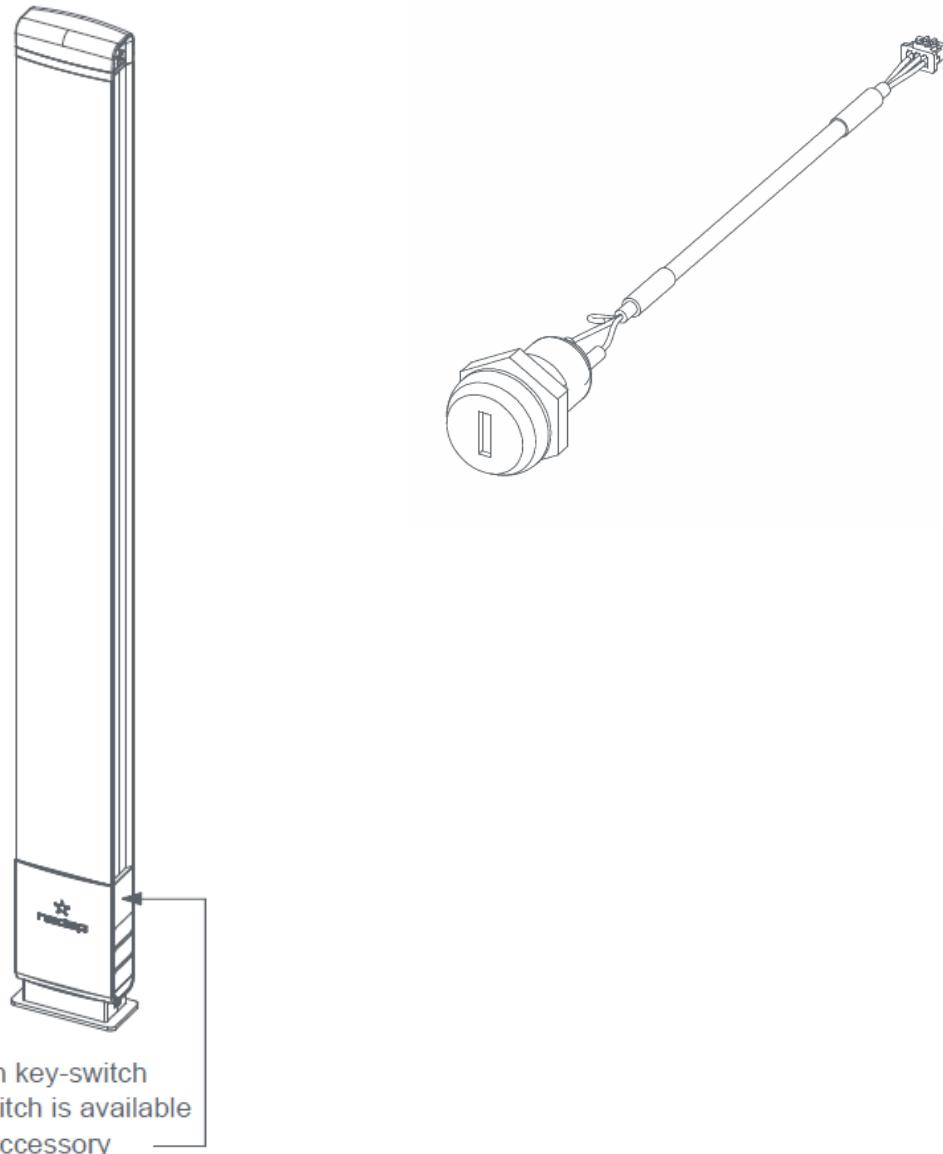


The RF Smart Deactivator integration cannot be used in iSense systems where RF is not enabled.

Key switch

Installing a Key Switch on the iSense gate can be helpful if you want to temporarily turn off the system.

The Key Switch must be connected directly to the Renos unit inside the iSense gate. For the installation, please carefully follow the quick reference enclosed for the Key Switch!



Each gate needs a key switch.



iSense Dashboard

The iSense system has a built-in security dashboard, the iSense Dashboard. It can be enabled by entering a purchased license key during the configuration wizard. The customer can then visit the dashboard via a web browser. To make this work, the iSense system should be in the same network, either connected to the customer network or a stand-alone set-up with a router should be made.

The iSense Dashboard allows the iSense system to be monitored inside the store. It creates an overview and provides real-time information for more effective reactions. The iSense Dashboard contains:

- Real-time overview of which gate or attention button is alarming: the ‘recent alarms’ provide controls to react quickly and accurately to alarms.
- The System Health widget shows the system’s performance to identify whether the system is functioning correctly quickly.
- The Alarm Data widget shows the number of RF/RFID/MD alarms per day as a percentage and compares this to the same time last day.
- The Visitor widget shows the number of customers today and the percentage change compared to the last hour.
- All information is saved for the last seven days to evaluate your store’s statistics and improve its operation.

Preparing the installation

A few things should be considered when preparing an installation with the i15 Go.

Defining the system

When a store requires gates to be placed at several locations, there needs to be a decision on how to combine these gates into one or multiple systems. The following rules need to be taken into account:

1. **Try to combine all units into one system.** The Renos platform has a built-in synchronization mechanism for RF technology to minimize interference. The units must be connected to one system for this synchronization mechanism.
2. **However, the maximum cable length requirements need to be taken into account.** If it is impossible to put all the gates in one system due to the maximum cable length requirements, you can split the installation into two or more systems. In this case, each system will be assigned a different *multi-system channel* during the RF configuration.

Aisle width or detection distance

The next step is figuring out how many gates you need. This depends on the system's detection distance (half of the aisle width). There is no fixed answer to this question; it depends on many factors, like customer expectations, the quality of the tags, the environment, etc.



An aisle width of 160 cm (5.2 ft.) is recommended (based on the Nedap NT4040 RF label).

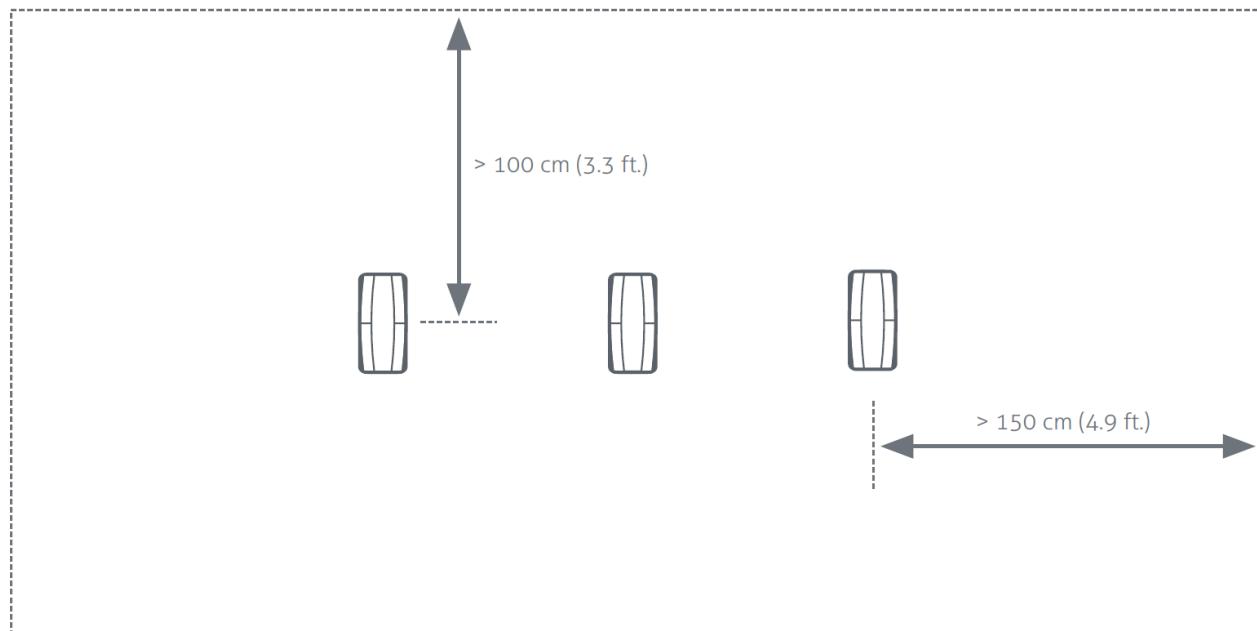


The aisle width depends on the tags used and the environment in which the gates are placed. It is advised to test this before using it in a store.

Label-free zone

Again, the recommendations are based on the Nedap NT4040 (reference label) for RF.

For RF, it is recommended that a label-free zone be at least 150 cm (4.9 ft.) from the center of the gate behind the gate and 100 cm (3.3 ft.) into the store.

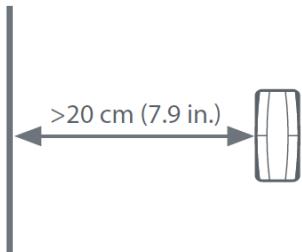


RF installation requirements

The operation of RF technology is affected by coupling issues (the antenna couples with other objects) and active interference (other devices that transmit a signal around 8.2 MHz). Objects that cause coupling effects could be windows, doors, metal framing around the checkout, etc. Interference can be created by another RF system, LED drivers, or motors driving doors or roller shutters.

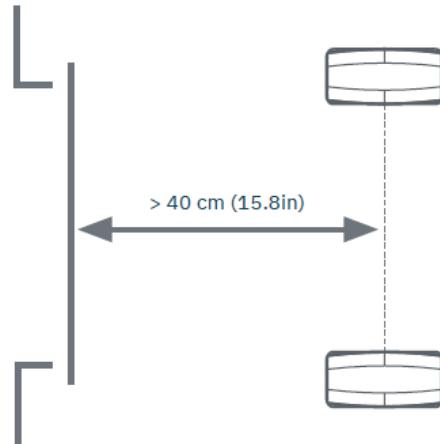
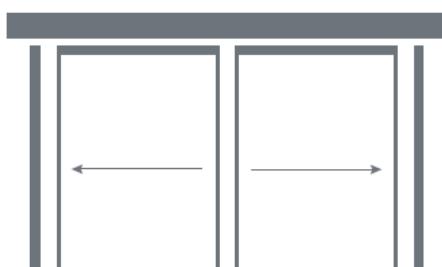
Take the following placement requirements into account when projecting the location of gates:

- There should be a minimum distance of 20 cm (7.9 in.) between the center of the gate and the wall.



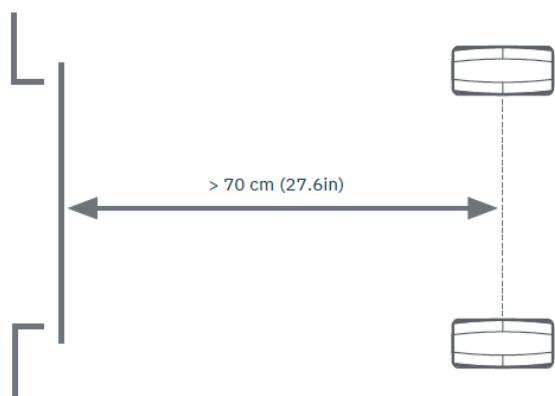
In addition, when **regular** or **sliding doors** are present:

- There should be a minimum distance of 40 cm (15.8 in.) between the center of the gate and the door.

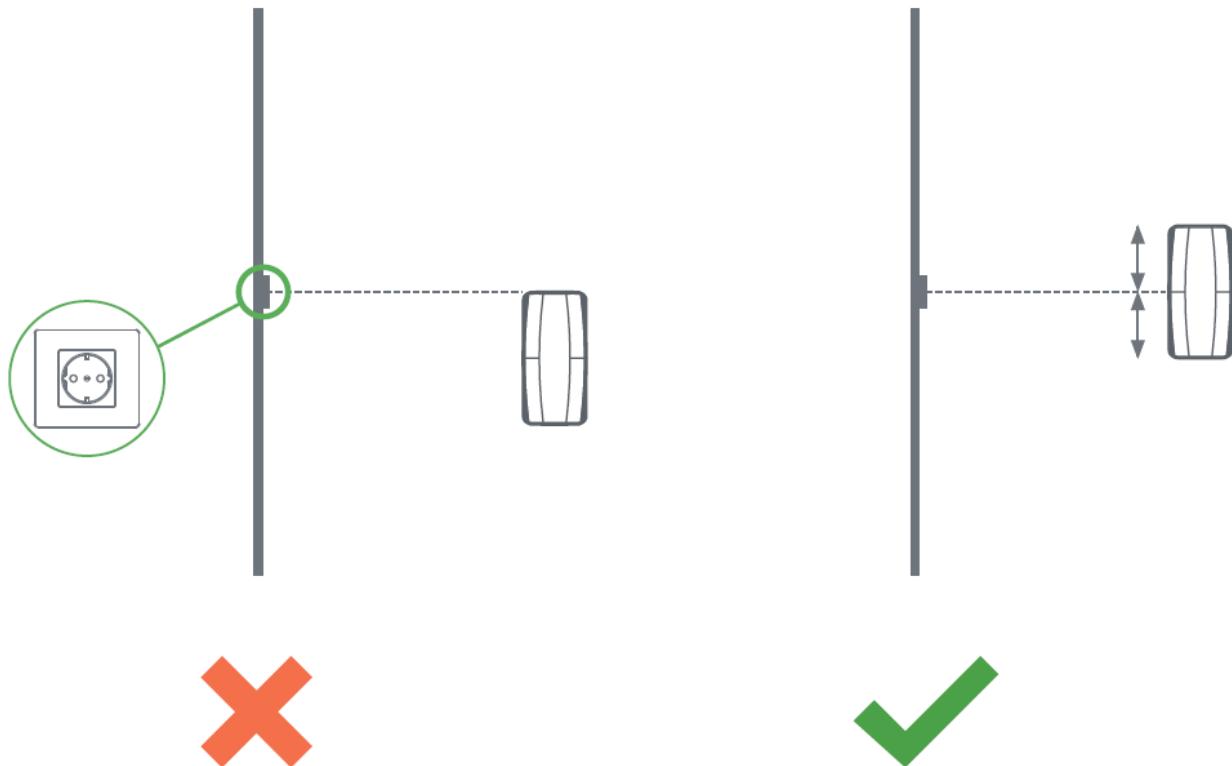


In addition, when a **roller shutter** is present:

- There should be a minimum distance of 70 cm (27.6 in.) between the center of the gate and the roller shutter.



If a power socket is less than 50 cm (19.7 in.) from the gate, the center of the gate should be aligned with the power socket.



Before installation, it is advised to gain information on the flooring below the antenna. If a dry-walk floor mat is used, it might have metal components that influence RF detection performance. In that case, make a cut in the floor mat to break conduction between the metal components and the antenna.



Please ensure there is no conducting connection between the gate and the checkout to prevent interference and coupling issues.

Power Inserter

Once the position of the gates is established, the location of the Power Inserters can be determined. A maximum number of Renos units can be connected to one Power Inserter, depending on which technologies are used and the number of add-ons in use. The table shows the number of Power Inserters needed for each hardware configuration.

Cable conditions: a CAT5E cable with a recommended maximum length of 80 meters / 250ft.

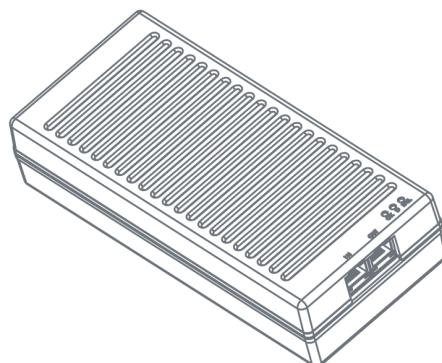
Technologies In Use	#Units / PI 230V	#Units / PI 115V
RF	6	5
RF + 2 SD's	5	4

Index:

- RF = Radio Frequency 8.2 MHz
- 2 SD's = 2 connected smart deactivators



Please note: Always use a Nedap Power Inserter (Power-over-Ethernet) to power Renos systems. It is not possible to use generic Power-over-Ethernet switches or stand-alone inserters.



⚠ Make sure that the Power Inserter is connected to an always-on power socket! This is better for the firmware/hardware, continuous system monitoring, and remote firmware updates during the night.



⚠ Ensure the Power Inserter is placed at least 1m (3.3 ft.) from the gates. When placed closer to the gate, it might cause interference with the RF technology.



⚠ Do not disconnect network cables in the system when still powered! First, disconnect the power cable from the power inserter(s).

Cable specifications - Ethernet cables

The following cable specifications are recommended for the iSense system:

- Use UTP Cat5e with a stranded copper core, with 24 AWG (0,51mm) core diameter.

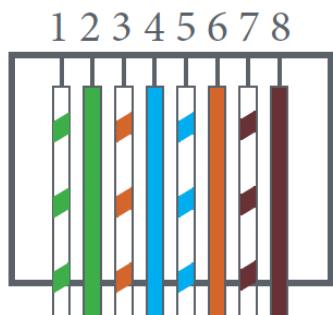


Always connect **all four pairs** using the **T568B** termination standard or T568A if specifically required!

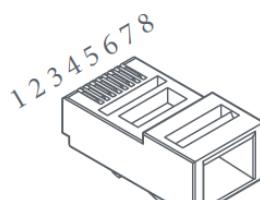
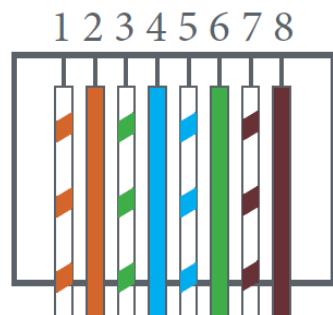


Never use CCA (copper cladding aluminum) or CCS/CCF (copper cladding steel) cable!

T568A



T568B



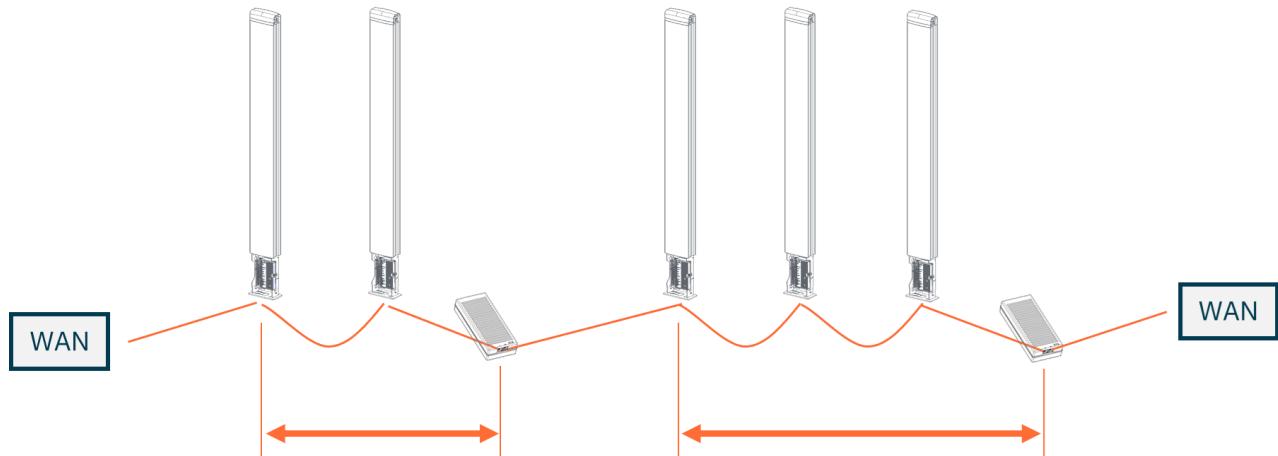
8P8C (RJ45)

Pin	T568A	T568B (Preferred)
1	Green + White	Orange + White
2	Green	Orange
3	Orange + White	Green + White
4	Blue	Blue
5	Blue + White	Blue + White
6	Orange	Green
7	Brown + White	Brown + White
8	Brown	Brown

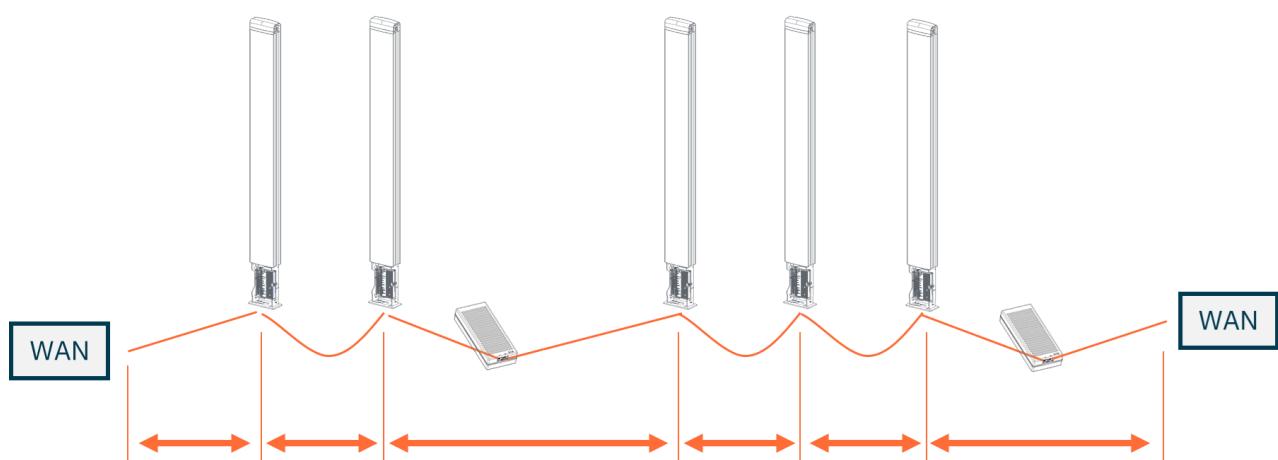
Cable length



Maximum cable length of **80 meters / 250 ft** between a Power Inserter and the last Renos unit that receives the power from this Power Inserter:



Maximum cable length of **80 meters / 250 ft** between Renos units (excluding Power Inserters) and between the first (or last) Renos unit and the WAN connection in the store:



Remarks

- It is possible to use your own preferred connectors.
- Make sure that the connectors are suitable for the cable and that the correct crimping tool is used for the connector.
- Follow the recommendations of the cable manufacturer.
- Local regulations may dictate using a specific cable type or rating.



We recommend placing the Power Inserter in the switch room (near a power socket) when the ethernet cable lengths allow. This way, the customer only has to arrange an ethernet outlet near the system.



If the cable lengths between two groups exceed approximately 50 meters / 164 ft, consider splitting a system into two.

Executing the installation

When all the preparations are considered, the system can be installed. The installation consists of physically mounting the system in the correct orientation, installing the cabling, and applying power to the system.



When cables are installed, it is recommended that they be marked with “IN” and “OUT,” allowing easy identification of the cables during installation.

Conduit or slit

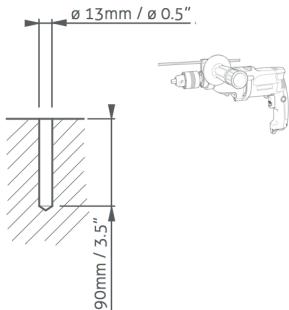
We always suggest that you place a conduit, as this allows easy replacement of cables when necessary. If not possible, a slit can be made as well.

The conduit or slit in which the cables are placed should be precisely in the middle of the gate, perpendicular to the gate. This is explained in the following pictures.



Physical installation

- Make sure the hole positions are marked on the floor in the correct locations according to the dimensions sketched earlier in this document.
- Drill the holes.

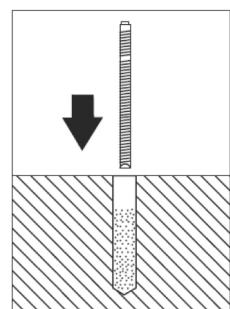
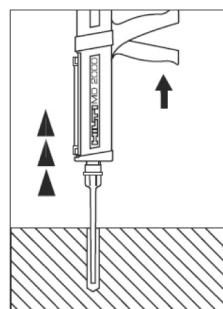
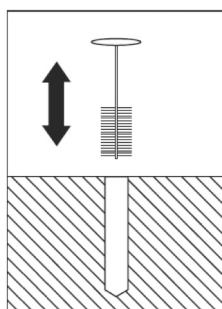


Then, follow these steps to place the studs.

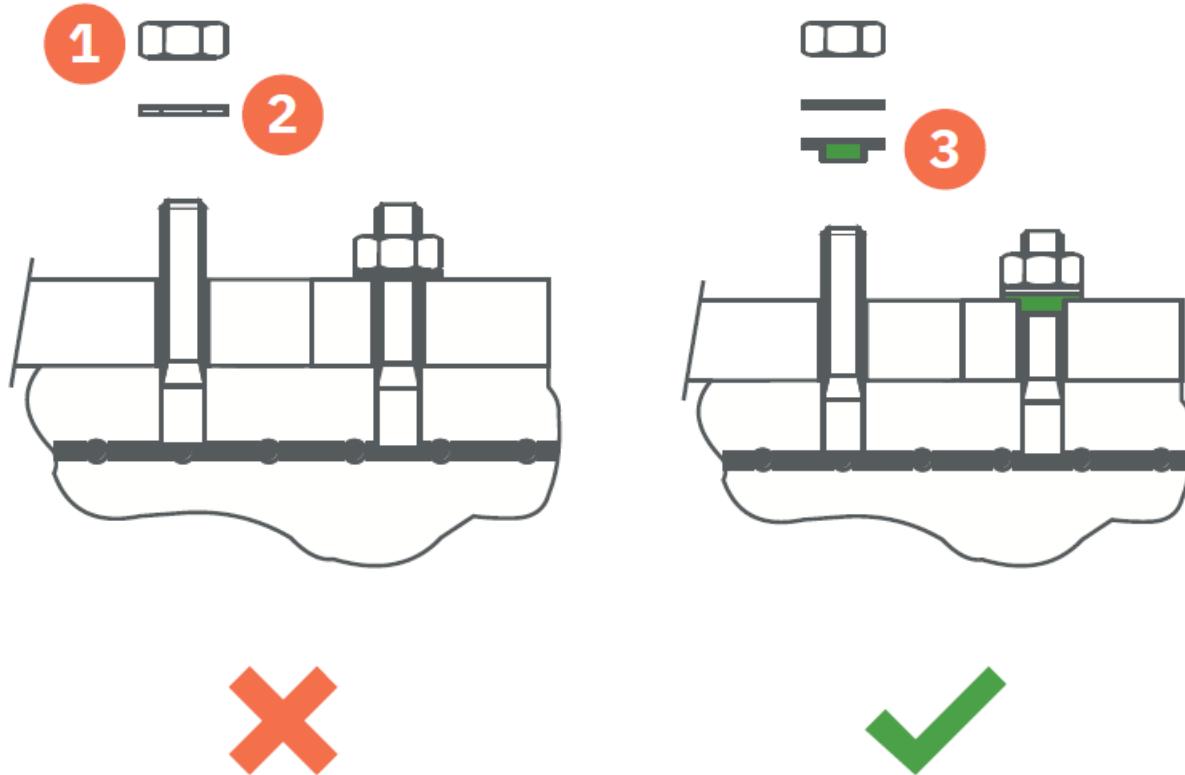
1. Clean the hole.
2. Insert Hilti-hit.
3. Place the stud.



Hilti-hit and studs are not included in the installation set.



Always use a nylon insulation ring to insulate the gate from the floor.



Number	Description
1	Nut M10 (not included in installation set)
2	Retainer ring M10 (not included in installation set)
3	Nylon insulation ring M10 (included in installation set)



If the gate is not adequately isolated from the floor, this might cause RF interference issues.

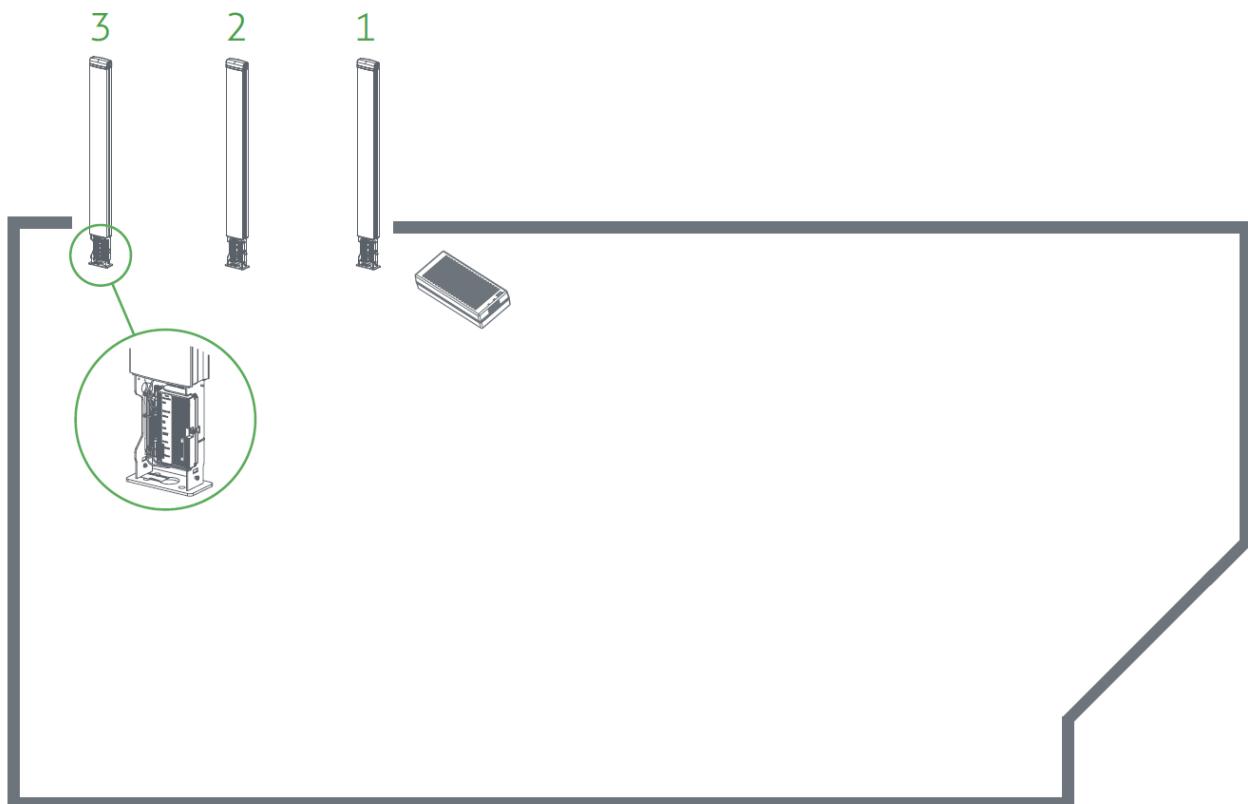
Orientation of products and the first gate



The i15 Go does **not** have specific orientation requirements, allowing them to be placed in the most convenient position based on the store's layout.



However, it is recommended to use the same installation method as with other Nedap gates to have one way of working, meaning: Determine gate 1 by standing inside the store and looking out towards the exit (Power inserter on the right side of the first gate, and Renos be on the left side of all gates)



Installing cabling and filters

The required cabling was determined during the preparation phase. Now, these cables can be placed.



All wiring should be installed according to local regulations.

When cables are put in the slit or conduit, it is recommended to mark them with IN and OUT, as this will allow you to distinguish them from each other.

Filters

Please note that filters should be placed around the cables to reduce interference with other systems. These filters are delivered together with the system.

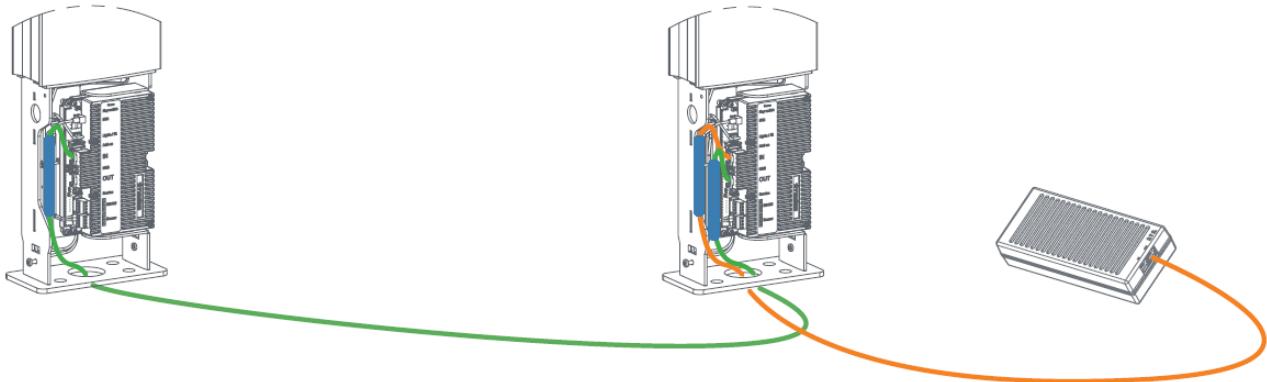
Filter should be placed at:

- Every Power Inserter is around the ethernet cable at the OUT and IN ports.

- Every Renos unit: around the ethernet cable at the OUT and IN ports.
- Every 9 m (30 ft.) for longer ethernet cables.



Place the filters **before** attaching the connectors. The other way around is not possible.



Nedap offers the opportunity to order filters as spare parts. For more information, please visit the Nedap Retail Portal.

The filters close to a Renos unit should be placed inside the foot of the gate. If multiple filters are at the foot of the gate, they should be tied together.

Ethernet cables

Connect the ethernet cable from the OUT port of the Power Inserter(s) or the Renos unit with the IN port of the next Renos unit.

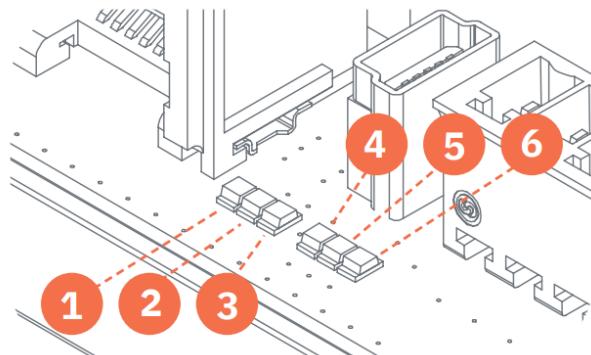


Please test every Ethernet cable for correct connections and pair all four pairs (8 wires) with an ethernet cable tester to ensure that the system can function correctly.

After the ethernet cables are connected, power up the Power Inserters.

Renos Status LEDs

The electronics inside the unit have several status LEDs that can be used to discover the status of each part of the electronics.



Status LEDs of the Renos unit

LED	Color	Status	Explanation
1	Green	On	There is a Renos unit connected to the OUT port of this unit
		Off	There is no Renos unit connected to the OUT port of this unit
2	Blue	Blinking	There is no device connected to the OUT port of this unit
		On	There is a Power Inserter connected to the OUT port of this unit
3	Red	On	There is an issue with the power supply at the OUT port of this unit (too little current drawn)
		Blinking	There is an issue with the power supply at the OUT port of this unit (too much current drawn)
		Off	There is no issue with the power supply at the OUT port of this unit
4	Yellow	Blinking	The operating system on the Renos unit is running
		Off	The operating system on the Renos unit is not running
5	Green	Blinking	The storage flash on the Renos unit is accessed
		Off	The storage flash on the Renos unit is not accessed
6	Green	On	The firmware on the Renos unit is running

LED	Color	Status	Explanation
		Off	The firmware on the Renos unit is not (yet) running

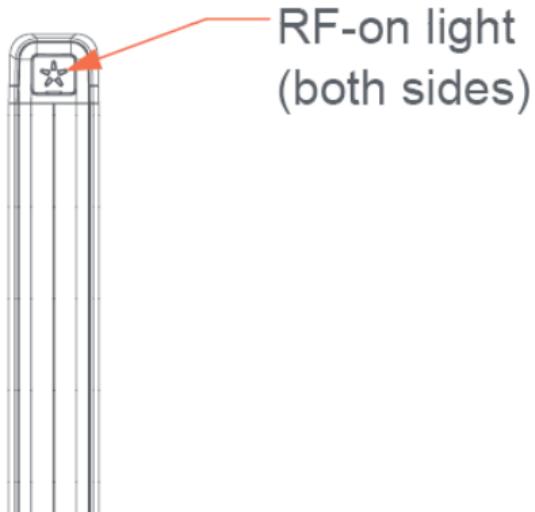
Please look at the Troubleshooting chapter later in this manual to resolve erroneous conditions.



If the Renos unit has a firmware error, the rightmost three LEDs (4, 5, and 6) will remain off when powered. This can be solved using a 'Local - single unit' firmware update, as described in the "iSense firmware version manual."

RF-on light

The PA15R has a white LED light on both sides, indicating the RF system is active.



State	Status LEDs RF-On Light
Default	On
Sleeping	Off
Key switch active	Off

Configuring the installation

The following tools are required to complete the configuration.

- Mini-USB cable.
- Laptop with installed driver and recent browser.

Driver installation

A Windows driver needs to be installed to configure an iSense system. Please check the table below for what is required based on your operating system.

Operating System	Driver
Windows	Download the driver from the portal.
Mac OS X	You don't need to install a driver.
Linux	You don't need to install a driver.

Once you have installed the driver, please check if it works by plugging it into a Renos unit.

Supported browsers

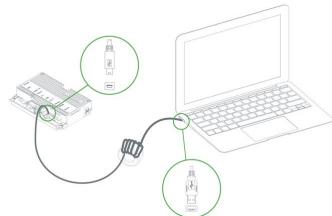
To configure the system, the latest versions of the following browsers are supported:

- Google Chrome
- Mozilla Firefox
- Apple Safari

If you don't have one of these browsers installed on your laptop, please install them before the installation.

Connecting a laptop to the Renos unit

You can connect your laptop via a Mini-USB cable to the service port on the Renos unit. In the iSense system, you can choose any Renos unit.



We advise using a good-quality USB cable about 5m / 16ft long. This provides more comfort during the configuration, as you can find an excellent place to put your laptop (instead of on the stairs or the floor next to the gate). Besides, some laptops interfere with RF technology, so it is better to place them further away.



We advise configuring Renos using a ferrite ring core filter around the mini USB cable. These can be ordered as spare parts with Nedap. Please take a look at the Nedap Retail Portal for more information.

Entering the configuration wizard

You can enter the configuration wizard by opening your browser and navigating to:

<http://192.168.133.1>



Ensure no other network connections are active in the same range.



Authentication

During the configuration, the user is required to authenticate himself. How this is done is dependent on the availability of Device Management.

- The system is connected to Device Management: you can enter your Nedap Retail username and password directly.
- The system is not connected to Device Management, and you don't have a Nedap Retail authentication software: choose one of the following steps:
 - If your laptop can connect to Device Management via a 4G/5G router or Wi-Fi, you can use this option to enter your username and password.
 - If that is not available, you can use your smartphone.
 - If your smartphone has no internet access, call your main technician for an authentication code.

Please reach out to support for more details on how to obtain a Nedap Retail username and password.

Getting help in the wizard

If something needs clarification, each page has a question mark button in the top right corner. You can click this to get more information on what is expected to do on a specific page.

Factory reset and Firmware change

It is essential to use the latest firmware version and start new installations with factory default units.

Details on how to perform a firmware update and factory default can be found in separate guidelines on the Partner Portal:

- iSense firmware version manual
- iSense factory reset procedure

Firmware change

There are four ways to change the firmware version on a Renos-based system:

1. Local—single unit overwrite. To execute the overwriting, insert a USB stick with the correct firmware into the USB port.
2. Local—complete system overwrite. You can execute the overwriting with files on your laptop during the configuration wizard.
3. Local - complete system update. The update can be executed during the configuration wizard with files on your laptop.
4. Device Management update. The update can be executed via the Device Management service.

Factory default

There are two ways to factory default a Renos-based system:

1. Local - single unit over-write. The factory default can be executed using a USB cable to connect the USB port to the service port.
2. Local - complete system factory default. The factory default can be executed during the configuration wizard.

System ID

You need the System ID to set up a Device Management system. The firmware version is displayed in the top right of the configuration wizard. If you click the firmware version, a pop-up shows the System ID during the configuration.

Integrating the installation with other systems

Integrating the iSense product into other solutions by the end customer is highly recommended.

Software integration with local APIs

The Renos platform offers local API endpoints for data analysis and status information. For more information, please refer to the Software Integration page on the Nedap Retail portal, which includes documentation and examples.

Physical integration using an IO Box

Integrating other systems via relay contact outputs and inputs is also possible. The Renos unit does not provide this directly; however, it can be accomplished via a 3rd party IO Box.



The following 3rd party IO Box is currently supported: **MOXA ioLogik E1214**.



The IO Box should be connected to a Renos unit via a USB to Ethernet adapter.

An output on an IO Box can be activated when specific events occur, depending on the capabilities of the chosen hardware.

URL trigger

The URL trigger mode can be used to trigger network-based devices with an HTTP-based API. Make sure that the iSense system can reach this device.

Servicing the installation

When the installation has been completed and delivered, it can be serviced via Nedap Device Management. We also provide monitoring options locally via SNMP.

Device Management

Nedap Retail systems can be connected to the online Device Management platform to ensure that systems can be managed remotely and work optimally globally.

The Nedap Device Management service provides four main functions on system level:

- **Monitoring:** Critical system parameters are monitored 24/7. If a system has issues, an alert is generated and sent to the supporting partner.
- **Remote Service:** using the Device Management website, an authorized Nedap-certified engineer can access the system's user interface to make changes to the configuration or access system logs.
- **Firmware Update:** an authorized Nedap-certified engineer can install new firmware releases remotely using the Device Management website.
- **Data Collection:** events per system are collected (e.g., to be displayed in the Analytics platform).
- **Sleep mode:** Enable sleep mode to conserve energy during nighttime hours, following the schedule configured in Device Management

For further details, please refer to the document on the portal about network information.

SNMP

Simple Network Management Protocol (SNMP) is available to allow for local monitoring of iSense systems. For example:

- One or more Renos units are not reachable
- The system is connected to Device Management

iSense systems use SNMP version 2c, community public. The MIB file is available on the iSense system itself via the URL [http://\(ip address of the system\)/snmp](http://(ip address of the system)/snmp) (for example, that is **http://192.168.133.1/snmp** when connected to the USB service port).

Troubleshooting

If the system is malfunctioning, please check the troubleshooting options below. Consult the support options in the next chapter when the issue cannot be solved.

Physical installation

Symptom	Cause	Solution
The red LED (3) on a Renos unit is on.	The current drawn-out of the OUT port of the Renos unit is too low. The cabling at the OUT port of the Renos unit does not satisfy the maximum length requirements.	Verify whether the cabling length in the system satisfies the requirements posed earlier in this document.
	The current drawn-out of the OUT port of the Renos unit is too low. The connectors of the Ethernet cable at the OUT port of the Renos unit are not mated properly.	Check the ethernet cable at the OUT port of the Renos unit with an ethernet cable tester.
The red LED (3) on a Renos unit is blinking.	The current drawn-out of the Renos unit's OUT port is too high. There are too many Renos units and add-ons connected to one Power Inserter.	Verify the number of Renos units and add-ons connected to the Power Inserters with the table earlier in this document.
	The current drawn-out of the Renos unit's OUT port is too high. There is a short circuit in the cabling leaving this Renos unit's OUT port.	Check the Ethernet cable at the OUT port of the Renos unit with an Ethernet cable tester.
The green LED (1) on a Renos unit is off, but there is a unit behind this unit.	There is an issue in the cabling between those units, so the following unit is not recognized.	Check Ethernet cabling with an Ethernet cable tester.

Configuration

Symptom	Cause	Solution
It is not possible to access the configuration web interface.	Renos unit has not started yet.	Verify the green "firmware running" LED on the Renos unit (6). If this LED is not on, verify the system has power, or wait five minutes and try again.
	Mini USB cable not attached to Renos unit and laptop	Attach the cable and laptop to the Renos unit.
	Driver not installed	On Windows 7 and older operating systems, manually install a driver to support Renos.
I have put a system together, but during the hardware discovery, I only see part of all the units.	During configuration, the WAN access port will be 'closed' for internal network traffic. If you combine two systems later, it needs to be reopened.	Do a factory reset on the unit previously used as a WAN entry point. If that doesn't work, do a factory reset on all units.
	There is a cabling error.	Please check all Ethernet cabling with an Ethernet cable tester.
	Not all Power Inserters are powered, or some Renos units are not fully started.	Verify the green "firmware running" LED on the Renos unit (6). If this LED is not on, verify the system has power, or wait five minutes and try again.
There is a firmware failure, indicated by the fact that all three LEDs 4, 5, and 6 are off on the Renos unit.	Something might have gone wrong with a firmware update.	Use the 'local - single' unit firmware update mechanism to restore the unit.

Warranty and spare parts

- Please consult the Nedap Retail Business Partner from whom you purchased this product regarding the applicable warranty conditions.
- This product cannot be used for any other purpose described in this document.
- If the product is not installed according to this document, the warranty provided is not applicable.
- At the sole discretion of Nedap N.V., Nedap N.V. may decide to change the conditions of Page 7 of 19 Compliance information for technical manuals warranty policy.
- You agree that Nedap N.V. can compensate you for the pro-rata value of the warranty involved rather than replacing or repairing the product based on its technical or economical value.
- Prior to applying the warranty, please verify that you comply with the warranty conditions of the warranty policy and that you can successfully apply for the replacement or repair of a defective part.
- Parts can only be replaced with original Nedap parts; otherwise, the warranty policy will not apply to the product.
- If the warranty is applicable, please contact the dealer or send the defective parts to the dealer.

RF technology issues

When there are issues with RF technology during the configuration (the gates show as orange or red in the wizard), please follow the following steps:

1. Check the parameters in the RF Advanced Config of the configuration wizard and the RF gate performance section. One of those parameters is probably red or orange.
2. Disable all transmitters.
 - a. If all parameters in the RF gate performance section turn green again, a coupling problem exists (the transmitter couples with a label-like object in the environment). Please continue to the 'coupling problem' section.
 - b. If all parameters in the RF gate performance section remain orange or red, there is an active interferer (another device that transmits radio waves around the 8.2 MHz RF spectrum, like another EAS system, an engine, or a power supply). Please continue to the 'active interferer' section.

Coupling problem

Coupling problems are caused by objects that act as labels to the RF system. This includes metallic doorframes, checkouts, and cabling—everything that runs in a loop and is metallic.

To solve these problems, there are a few things you can try:

- Tighten screws in the metallic construction. This might work for checkouts or customer guidance rails.

- Try to interrupt the metallic loop. This can be done by using non-metallic parts inside those loops or by making a cut in them.
- Create a shortcut in the metallic loop to make it smaller. This will make it resonate at a different frequency.

If the above solutions don't solve the problem, you can decrease the system's sensitivity by ticking the 'reduced sensitivity' button in the RF Advanced Config.



If a decreased sensitivity doesn't work, and there is only one type of label or tag in the store, you also have the option to increase the 'receiver delay', in steps of 3 dB.

If these things don't solve the problem, please contact support.

Active interferer

The first step is to locate the active interferer's source. You can do this by unplugging electronic devices around the gate (or moving them away) and seeing if the parameters in the 'RF gate performance' section improve or when the average height of the spectrum is reduced. If this is the case, you have identified the active interferer.

When the active interferer is known, the following solutions are possible:

- Try to move the active interferer away from the gate as far as possible.
- Try to apply filters around the cabling of the active interferer.
- Shield the active interferer with aluminum foil of at least 0.05 mm (2 mil.).

If the above solutions don't solve the problem, you can decrease the system's sensitivity by ticking the 'reduced sensitivity' button in the RF Advanced Config.



There are also round ferrites available that can be used to reduce active interference sources, find ferrites with optimal impedance at around 8.2MHz

If these things don't solve the problem, please contact support.

CE WEEE

This European Standard specifies a marking:

- of electrical and electronic equipment following Article 11(2) of Directive 2002/96/EC (WEEE); This is in addition to the marking requirement in Article 10(3) of this Directive, which requires producers to mark electrical and electronic equipment put on the market after 13 August 2005 with a 'crossed-out wheeled bin' symbol.

- that applies to electrical and electronic equipment falling under Annex IA of Directive 2002/96/EC, provided the equipment concerned is not part of another type of equipment that does not fall within the scope of this Directive. Annex IB of Directive 2002/96/EC contains an indicative list of the products that fall under the categories set out in Annex IA of this Directive;
- that identifies the equipment producer clearly and that the equipment has been put on the market after 13 August 2005.

CE - UKCA Declaration of Conformity

With this, Nedap N.V. declares that the subject equipment is in compliance for CE with directives 2014/53/EU (Radio Equipment Directive) and 2011/65/EU (RoHS). And for UKCA with SI 2017/1206 (radio Equipment Regulations 2017) and with SI 2012/3032 UK Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 (RoHS). The full text of the declarations of conformity is available at the following internet address: <https://portal.nedapretail.com/>, where, if applicable, REACH information can also be found.

Disposal of this product

This product's owner or last user is responsible for properly disposing of (parts of) the product as required by local rules and regulations.



Regulatory information

FCC and IC Compliance Statement

This device complies with part 15 of the FCC Rules and RSS210 of Industry Canada. 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.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Cet appareil se conforme aux normes CNR210 exemptés de license du Industry Canada. L'opération est soumis aux deux conditions suivantes:

- (1) cet appareil ne doit causer aucune interférence, et*
- (2) cet appareil doit accepter n'importe quelle interférence, y inclus interférence qui peut causer une opération non pas voulu de cet appareil.*

Les changements ou modifications n'ayant pas été expressément approuvés par la partie responsable de la conformité peuvent faire perdre à l'utilisateur l'autorisation de faire fonctionner le matériel.

FCC and IC Radiation Exposure Statement

This equipment complies with FCC and Canadian radiation exposure limits for an uncontrolled environment. It should be installed and operated with a minimum distance of 20 cm between the radiator and your body. This transmitter must not be co-located or operated with any other antenna or transmitter.

Cet équipement est conforme a CNR102 limites énoncées pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et votre corps.

This Class B digital apparatus complies with Canadian ICES-3. Cet appareil numérique de Classe B est conforme à la norme Canadienne NMB-3.

FCC Information to the user

Note: This equipment has been tested and found to comply with the limits for class B digital devices, according to part 15 of the FCC Rules. These limits are designed to protect reasonably against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency

energy and, if not installed and used following the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. Suppose this equipment does not cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on. In that case, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from the receiver's.



Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. To ensure compliance with FCC regulations, use only the shielded interface cables provided with the product or additional specified components or accessories that can be used to install the product.

Information for Taiwan

第十二條 經型式認證合格之低功率射頻電機，非經許可，
公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；
經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。
低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

CE WEEE

This European Standard specifies a marking:

- of electrical and electronic equipment following Article 11(2) of Directive 2002/96/EC (WEEE); This is in addition to the marking requirement in Article 10(3) of this Directive, which requires producers to mark electrical and electronic equipment put on the market after 13 August 2005 with a 'crossed-out wheeled bin' symbol.
- that applies to electrical and electronic equipment falling under Annex IA of Directive 2002/96/EC, provided the equipment concerned is not part of another type of equipment that does not fall within

the scope of this Directive. Annex IB of Directive 2002/96/EC contains an indicative list of the products that fall under the categories set out in Annex IA of this Directive;

- that identifies the equipment producer clearly and that the equipment has been put on the market after 13 August 2005.

CE - UKCA Declaration of Conformity

With this, Nedap N.V. declares that the subject equipment is in compliance for CE with directives 2014/53/EU (Radio Equipment Directive) and 2011/65/EU (RoHS). And for UKCA with SI 2017/1206 (radio Equipment Regulations 2017) and with SI 2012/3032 UK Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 (RoHS). The full text of the declarations of conformity is available at the following internet address: <https://portal.nedapretail.com/>, where, if applicable, REACH information can also be found.

Disposal of this product

This product's owner or last user is responsible for properly disposing of (parts of) the product as required by local rules and regulations.





About Nedap

Together, we make merchandise simply available

At Nedap, we believe in ‘Technology for Life’. Nedap Retail enables retailers to serve their customers better. Using technology, we allow for perfect inventory visibility, total control, no waste, and no losses.

Our vision for inventory visibility

Today, established retailers need more information about where their items are. Without this knowledge, providing an omnichannel experience leads to heavy overstocking, waste, and eroding margins. Solving this requires a fundamental change in the retailers’ supply chain and information systems.

Our mission is to simplify the process of ensuring that retailers always have the right products available at the right place and time.

We do this by giving retailers perfect inventory visibility for a seamless shopping experience. This way, retailers can meet the changing consumer needs while remaining profitable.

Nedap works with the largest and most successful retailers in the world. We take complete ownership of our projects—failure is never an option. A unique combination of the best technology and industry teams at Nedap Retail achieves this.

Nedap solutions are built upon 45 years of global experience, market expertise, and close cooperation with leading retailers. A flexible network of certified partners worldwide supports our worldwide operations. Nedap systems are future-proof (RFID-ready), cost-efficient, and Eco-friendly. Our mission is to ensure retailers' customers maintain the best shopping experience while we help retailers protect their profits.

Contact

If you need further details or help preparing, executing, or servicing an installation, please contact our support team at support-retail@nedap.com.

Suggestions for improving our products and documentation are much appreciated.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap NV 2025

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 25

Document Last modification date 28 November 2024

Document PDF Exported 21 March 2025 by Nedap Retail | Operations



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com



Nedap Sense Manual

iSense Lumen Series

iL45 / iL45 Hybrid / Upgrade iL45 RFID / iL33

version 119, March 2025

Introduction	4
Disclaimers	4
Safety precautions	5
RFID Regions	5
Product Overview	6
Box contents	6
Components	7
Dimensions	10
Connections	13
Add-ons	14
Preparing the installation.....	17
Defining the system	17
Aisle width or detection distance	19
Label-free zone	19
RF installation requirements	20
RFID installation requirements	23
Power Inserter	24
Cabling	26
Executing the installation.....	31
Conduit or slit	31
Physical installation	32
Orientation of products and the first gate	34
Installing cabling and filters	37
Renos Status LEDs	39
Configuring the installation	43
Driver installation	43
Supported browsers	43
Connecting a laptop to the Renos unit	44
Entering the configuration wizard	44
Authentication	45
Getting help in the wizard	45
Factory reset and Firmware change	46
System ID	46



Integrating the installation with other systems	47
Software integration with local APIs	47
Physical integration using an IO Box	47
URL trigger	47
System behavior	48
Light and sound signaling	48
Servicing the installation.....	51
Device Management	51
SNMP	51
Troubleshooting.....	52
Physical installation	52
Configuration	53
RF technology issues	54
Warranty and spare parts.....	56
Regulatory information	57
FCC and IC Compliance Statement	57
FCC and IC Radiation Exposure Statement	57
FCC Information to the user	57
Information for Taiwan	58
CE WEEE	58
CE - UKCA Declaration of Conformity	59
Disposal of this product	59
About Nedap.....	60
Together, we make merchandise simply available	60
Our vision for inventory visibility	60
Contact	60

Introduction

The Nedap iSense Lumen products are standard gates with advanced audiovisual signaling. They are designed explicitly for in-store retail applications, such as Electronic Article Surveillance (EAS), stockroom-to-sales floor transition, and goods receiving.



This manual overviews the products, installation, and configuration basics. For more details, several guidelines are available on the Nedap Retail portal.

This manual covers the following products:

Article Number	Article Name	Commercial Name	Technology	Model Name
9565736	ASSY AD46R RF IR GREY	Lumen iL45	8.2 MHz RF	ASSY AD46R RF
9565744	ASSY AD46R RF+RFID IR R1 GREY	iD Hybrid Lumen iL45	8.2 MHz RF, UHF RFID	ASSY AD46R RF+RFID
9565752	ASSY AD46R RF+RFID IR R2 GREY	iD Hybrid Lumen iL45	8.2 MHz RF, UHF RFID	ASSY AD46R RF+RFID
9565779	ASSY AD46R RF+RFID IR R3 GREY	iD Hybrid Lumen iL45	8.2 MHz RF, UHF RFID	ASSY AD46R RF+RFID
9985751	ADD-ON AD46R RFID R1 UPGRADE	Upgrade iL45 Grey RFID Region 1	UHF RFID	
9985778	ADD-ON AD46R RFID R2 UPGRADE	Upgrade iL45 Grey RFID Region 2	UHF RFID	
9565795	ASSY T325R RF IR	Lumen iL33	8.2 MHz RF	ASSY T325R RF

Disclaimers



Nedap intends to make this manual accurate and complete. However, Nedap does not warrant that the information contained herein covers all details, conditions or variations, nor does it provide for every possible contingency in connection with the installation or use of this product.

Nedap disclaims any liability for damage to property or personal injury resulting, in whole or in part, from improper installation, modification, use, or misuse of its products. The information contained in this document is subject to change without notice.



This equipment should only be installed, operated, serviced, and repaired by skilled personnel. The installation and interconnection of this equipment to facility wiring and other equipment must be done by a competent, skilled craftsman familiar with applicable standards and codes governing the installation. Installation methods, practices or procedures that are unauthorized or done improperly are dangerous and could result in serious personal injury or damage to property and equipment.

Safety precautions



Do not place cards equipped with a magnetic strip or chip (i.e., ID, travel, debit, and credit cards) close to the equipment to avoid possible card failures.



To avoid potential interference with medical devices (pacemakers, cochlear implants, etc.), keep a distance of at least 20cm (8 inches) between them and the equipment.

RFID Regions

Region 1: Europe, Eastern Europe, Middle East, Africa and India

Region 2: North America and South America

Region 3: Asia and Oceania

Product Overview

Multiple variations within the iSense Lumen series support different technologies and upgrade kits that can later upgrade an 8.2 MHz RF installation to UHF RFID (only for the iL45).



In this document, the following abbreviations will be used from here onward:

- 'RF technology' is an abbreviation for 8.2 MHz RF technology.
- 'RFID technology' is an abbreviation for UHF RFID technology.

Box contents

Article Number	Article Name	Box Contents
9565736	ASSY AD46R RF IR GREY	<ul style="list-style-type: none">• Lumen iL45 gate with Renos RF• Installation set• Quick Reference
9565744	ASSY AD46R RF+RFID IR R1 GREY	<ul style="list-style-type: none">• iD Hybrid Lumen iL45 gate with Renos, RF, RFID reader, and RFID antennas• 3.5 m (11.5 ft.) RFID coaxial cable• Installation set• Quick Reference
9985751 9985778	ADD-ON AD46R RFID R1 UPGRADE ADD-ON AD46R RFID R2 UPGRADE	<ul style="list-style-type: none">• RFID reader and RFID antennas (only compatible with AD46R gate)• 3.5 m (11.5 ft.) RFID coaxial cable• Installation set• Quick Reference
9565795	ASSY T325R RF IR	<ul style="list-style-type: none">• Lumen iL33 gate with Renos RF• Installation set• Quick Reference

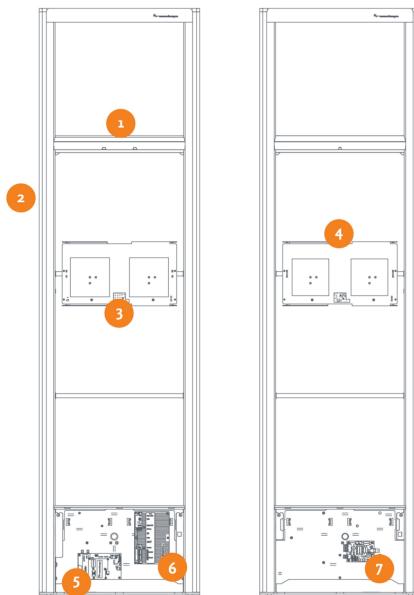


Partly using RF or RFID technology in one system is impossible.

Components

iSense Lumen products are based on the Renos platform. The Renos platform is developed by Nedap Retail, especially for retail applications. The iSense Lumen series has several serviceable parts. These are explained in the table and highlighted in the schematic drawings.

iSense iD Hybrid Lumen iL45



No.	Component	Description
1	Light and sound + customer counter	The light and sound unit signals and differentiates between different types of alarms. This unit also includes the customer counter.
2	RF antenna	The antenna is integrated into the aluminum frame.
3	RFID antenna NEXT	The RFID antenna points to the NEXT gate.
4	RFID antenna PREVIOUS	The RFID antenna points to the PREVIOUS gate.
5	RFID reader	The RFID reader reads RFID labels. It is connected to the Renos unit and to the RFID antennas.
6	Renos unit	The Renos unit is the main processing unit of an iSense Lumen product. It powers the system and communicates data between units and the outside world.
7	50 ohm PCB	The 50-ohm PCB connects the Renos unit and the RF antenna.

iSense Lumen iL33

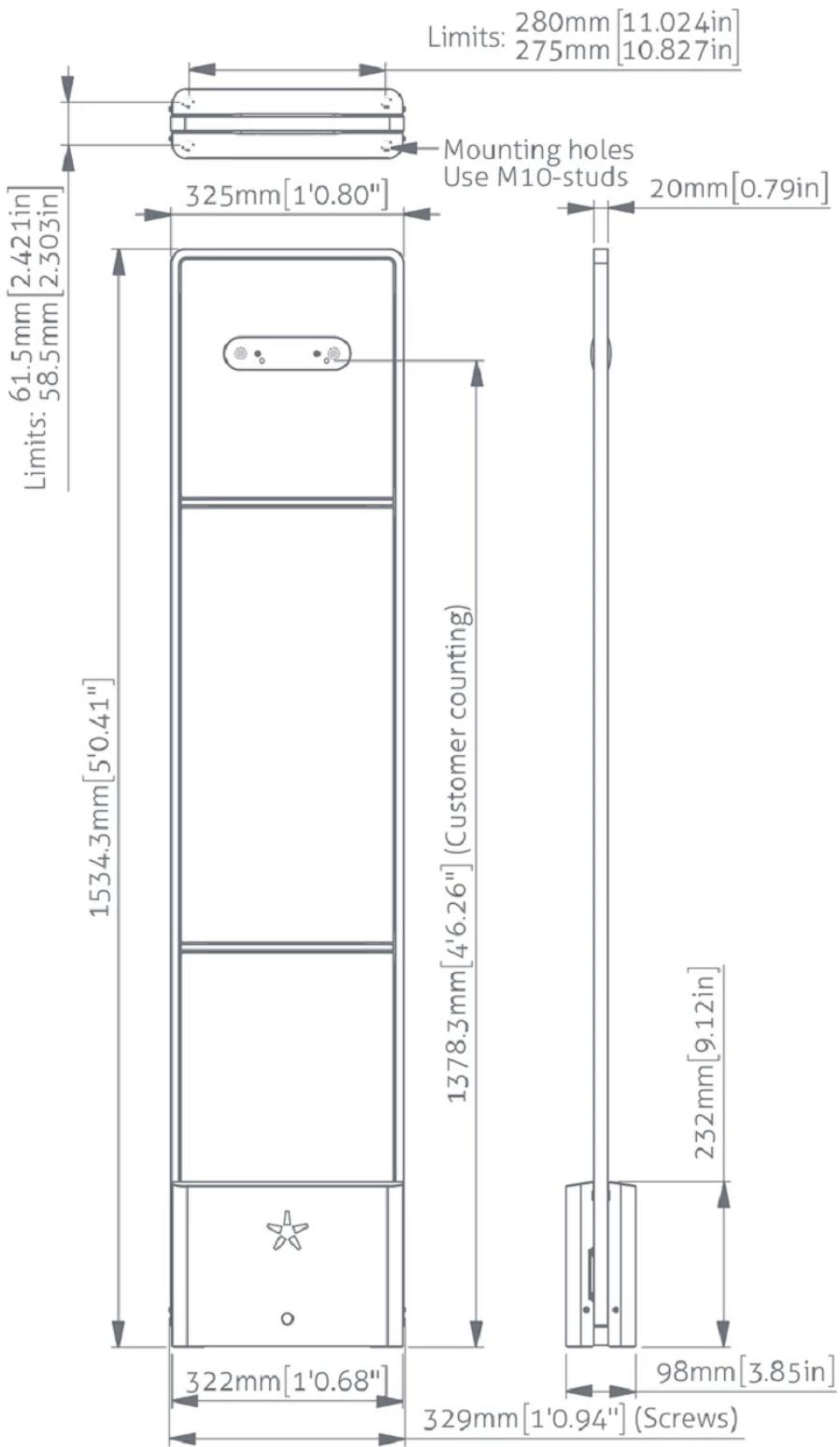


No.	Component	Description
1	Light and sound + customer counter	The light and sound unit signals and differentiates between different types of alarms. This unit also includes the customer counter.
2	RF antenna	The antenna is integrated into the perspex plate.
3	Renos unit	The Renos unit is the central processing unit of an iSense Lumen product. It powers the system and communicates data between units and the outside world.
4	50 ohm PCB	The 50-ohm PCB connects the Renos unit and the RF antenna.

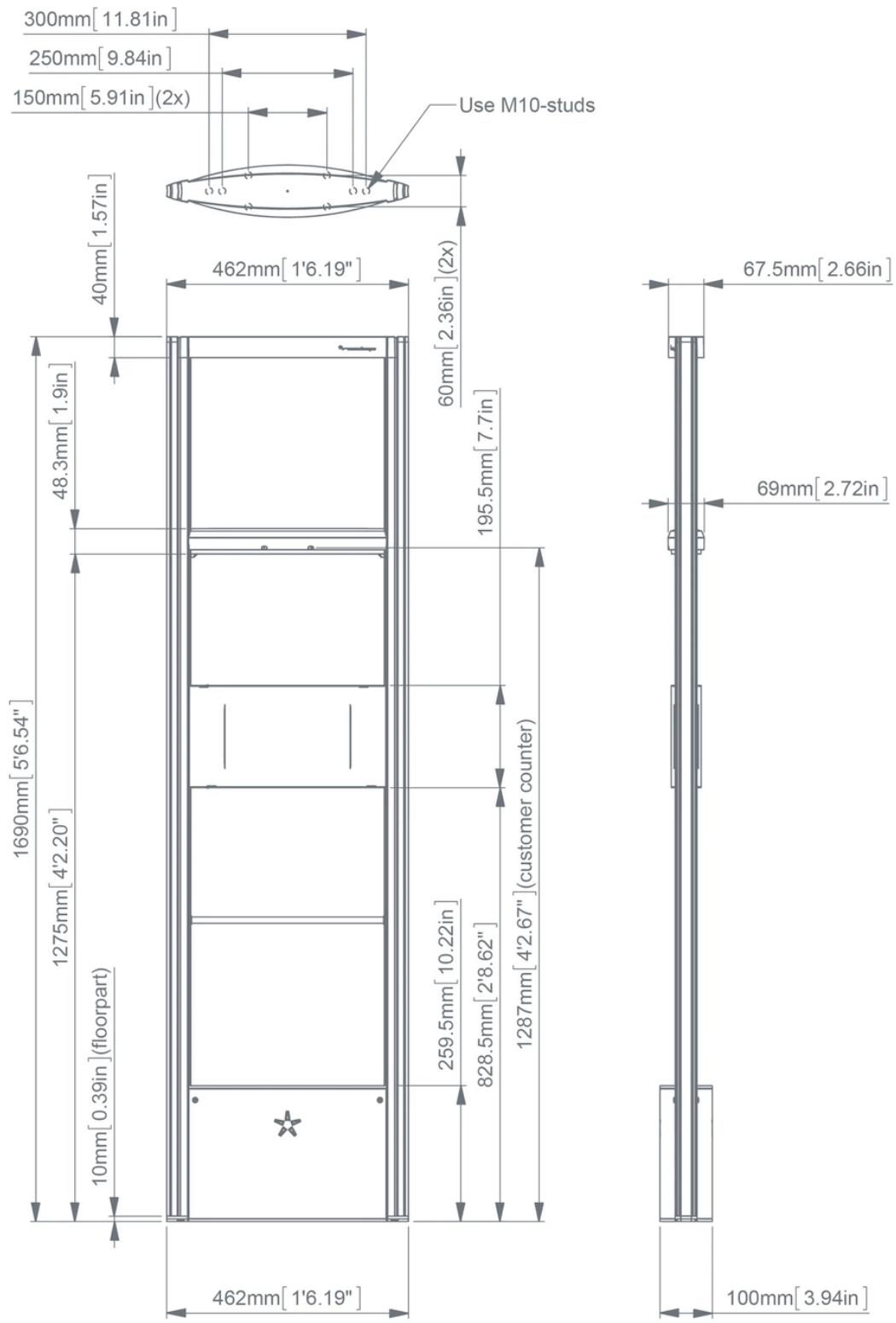
Dimensions

This section presents dimensional drawings of the gates. The holes in the mounting plate can be used as a template to draw the locations for drilling holes in the floor.

iSense Lumen iL33

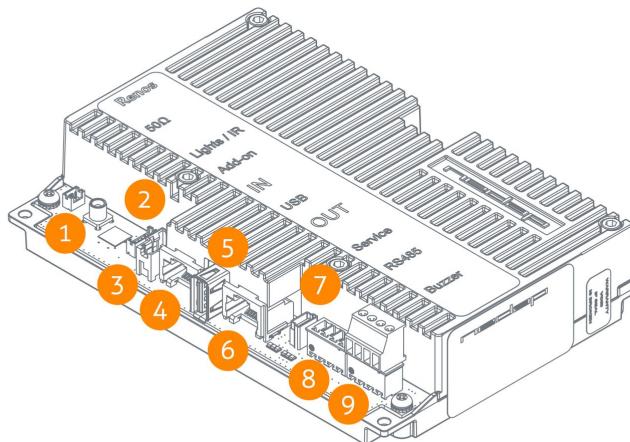


iSense iD Hybrid Lumen iL45



Connections

This is a Renos unit, describing all its connectors and their use.



No.	Connector	Usage
1	50 ohm	Connect the Renos unit to the 50-ohm PCB. The 50-ohm PCB connects both the light and the RF antenna.
2	Lights/IR	Connects to the audiovisual signaling and the customer counter.
3	Add-on	Provide power and synchronization to add-ons, like the RFID reader.
4	Network IN	Connected to the Network OUT of a previous Renos unit or a Power Inserter.
5	USB	Connect accessories to Renos, like the RFID Reader.
6	Network OUT	It can be connected to the Network IN of the next unit or a Power Inserter, left unconnected, or connected to the customer network.
7	Mini USB service port	Connect your laptop to configure the Renos system.
8	RS485 connector	Connect to the optional Nedap RF Smart Deactivator.
9	Buzzer connector	Products in the iSense Lumen series are not connected to a buzzer, but alarm signaling is already built in.

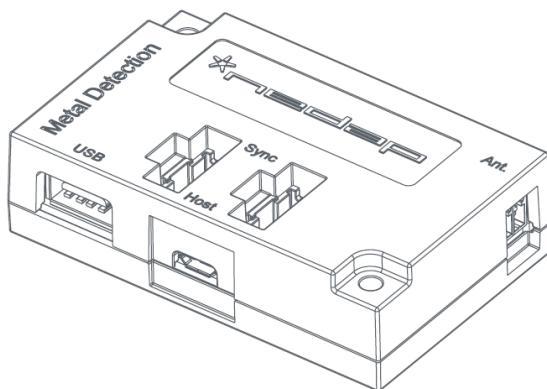
The LED indicators on the Renos unit will be discussed later in this manual.

Add-ons

Several add-ons are available for the iSense Lumen series products. Each add-on has its manual; however, we will briefly discuss its function here.

Metal Detection

The iSense Metal Detection unit can detect foil-lined bags, which thieves sometimes use to prevent the RF and RFID tags from being read by the detection system or reader. With Metal Detection, we can detect metal objects and provide a discrete alarm to the store employees.



For metal detection to work, you need a minimum of 2 gates and 1 Metal Detection unit in each gate within a group.



The distance between large (Metal) doors and the gates with Metal Detection must be at least 1.5 meters. Doors swinging open to the outside must be at least 1 meter away.



The maximum distance between the two gates is the same as specified for RF, with one exception.

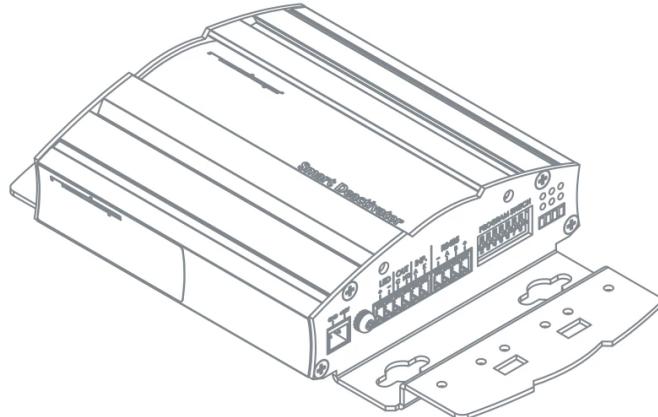
For the Lumen iL33, the maximum distance changes when shielding is used:

- With shielding at one side, the maximum distance between all the gates in this group becomes 1.5m (instead of 1.65m)
- If the group contains two gates and both are shielded, the distance becomes 1.25m

Remember that the shielding also influences the RF performance!

RF Smart Deactivator

The RF Smart Deactivator can be used to deactivate RF labels at the checkout. When connected to an iSense system, it can be powered by a Renos unit. The Renos unit can also gather information from the deactivator, like whether it is operational.

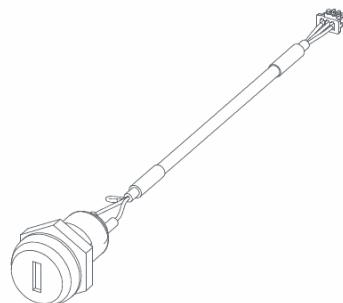


The RF Smart Deactivator integration cannot be used in iSense systems where RF is not enabled.

Key switch

Installing a Key Switch on the iSense gate can be helpful if you want to temporarily disable the system (both RF and RFID, depending on the available hardware).

The Key Switch must be connected directly to the Renos unit inside the iSense gate. For the installation, please carefully follow the quick reference enclosed for the Key Switch!



You need one key switch per gate.



iSense Dashboard

The iSense system has a built-in security dashboard, the iSense Dashboard. It can be enabled by entering a purchased license key during the configuration wizard. The customer can then visit the dashboard via a web browser. To make this work, the iSense system should be in the same network, either connected to the customer network or a stand-alone set-up with a router should be made.

The iSense Dashboard allows the iSense system to be monitored inside the store. It creates an overview and provides real-time information for more effective reactions. The iSense Dashboard contains:

- Real-time overview of which gate or attention button is alarming: the ‘recent alarms’ provide controls to react quickly and accurately to alarms.
- The System Health widget shows the system’s performance to identify whether the system is functioning correctly quickly.
- The Alarm Data widget shows the number of RF/RFID/MD alarms per day as a percentage and compares this to the same time last day.
- The Visitor widget shows the number of customers today and the percentage change compared to the last hour.
- All information is saved for the last seven days to evaluate your store’s statistics and improve its operation.

Preparing the installation

When preparing an installation with products from the iSense Lumen series, there are a few things that should be taken into account:

- How many gates do you need to cover an entrance or door?
- Where are the gates relative to the environment to minimize interference (RF) and reflections (RFID)?
- The number of Power Inserters needed to power the system.
- Which cabling should be installed?
- Are you ready for an RFID upgrade? When required, consider the number of Power Inserters, and you may want to lay the coaxial cables on the floor for future RFID activation.
- Customer counting, Metal Detection, and RFID will only work within an aisle (between two gates).
- The firewall settings that need to be in place to enable Device Management.

Those requirements differ depending on which technology is used (RF, RFID, or both), so both technologies are described in a separate section.



Take proper crash protection precautions if the gate is freestanding in a supermarket or hypermarket environment. When customer guidance rails are available, you can place the antenna behind or after them to protect it against crashes.
When unavailable, use the Nedap crash protection against damage by shopping carts.

Defining the system

When a store requires gates to be placed at several locations, there needs to be a decision on how to combine these gates into one or multiple systems. The following rules need to be taken into account:

1. **A different role is a separate system.** Combining gates for Electronic Article Surveillance (EAS) with gates from the stockroom to the sales floor is impossible in one system. Both roles need different systems with their own Power Inserter and customer network connection.
2. **Within the EAS role, all gates are combined into one system.** To minimize interference between gates, the Renos platform has a built-in synchronization mechanism for both RF and RFID technology. The gates must be connected to one system for this synchronization mechanism.
3. **However, the maximum cable length requirements must be considered.** If it is impossible to put all the gates within a role in one system due to the maximum cable length requirements, you can split the installation into two or more systems. In this case, assign each system a different *multi-system channel* during the RF configuration.



Build a separate system for the stockroom to the sales floor and goods receiving roles when there is a different door or entrance.

Role/Store Position	Product	Max. System Size (Gates)
EAS	RF Gates	100
	Hybrid RF/RFID	30
	RFID gates	30
Stockroom / Salesfloor	RFID gates	2
Goods receiving	RFID gates	2



It is not possible to combine gates with RFID and without RFID in one system. Either all gates should have RFID or no gates should have RFID.

Aisle width or detection distance

The next step is to determine how many gates you need. This depends on the system's detection distance (half of the aisle width). There is no fixed answer to this question; it depends on many factors, such as customer expectations, the quality of the tags, the environment, etc.

The recommendations are based on the Nedap NT4040 (reference label) for RF and the Nedap RFID hard tag (for RFID).



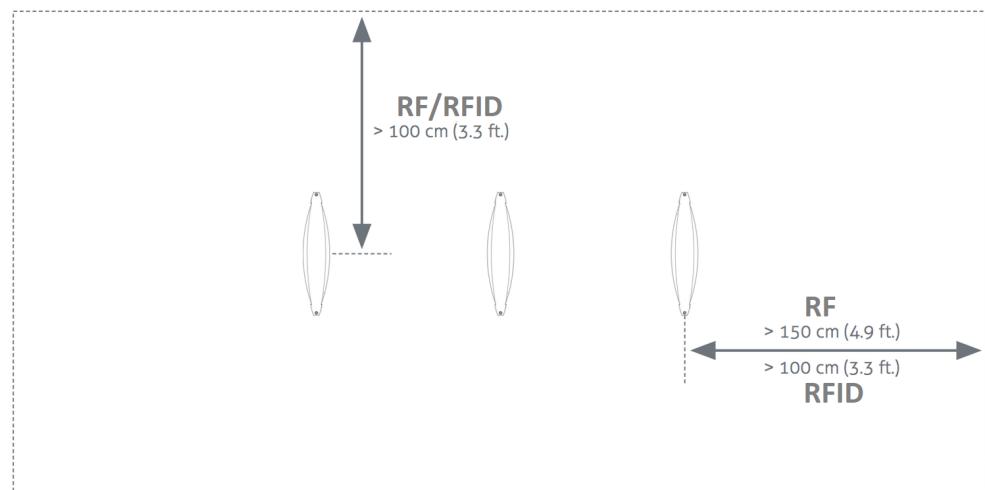
Please note that only the recommended aisle width is specified. Depending on the tag used and the environment the gates are placed in, sometimes larger values can be achieved. It is advised to test this, before using it in a store.

- For the Lumen iL33 gate, an aisle width of 170 cm (5.6 ft.) is recommended.
- For the Lumen iL45 gate, an aisle width of 200 cm (6.6 ft.) is recommended.

Label-free zone

Again, the recommendations are based on the Nedap NT4040 (reference label) for RF and the Nedap RFID hard tag (for RFID).

It is recommended that a label-free zone of at least 150 cm (4.9 ft.) for RF and 100cm (4.9 ft.) for RFID be created from the center of the gate behind the gate and 100 cm (3.3 ft.) into the store.

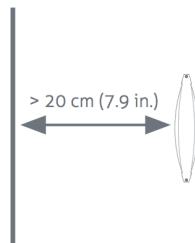


RF installation requirements

The operation of RF technology is affected by both coupling issues (the antenna couples with other objects) and active interference (other devices that transmit a signal around 8.2 MHz). Objects that cause coupling effects could be windows, doors, metal framing around the checkout, etc. Interference can be created by another RF system, LED drivers, or motors driving doors or roller shutters.

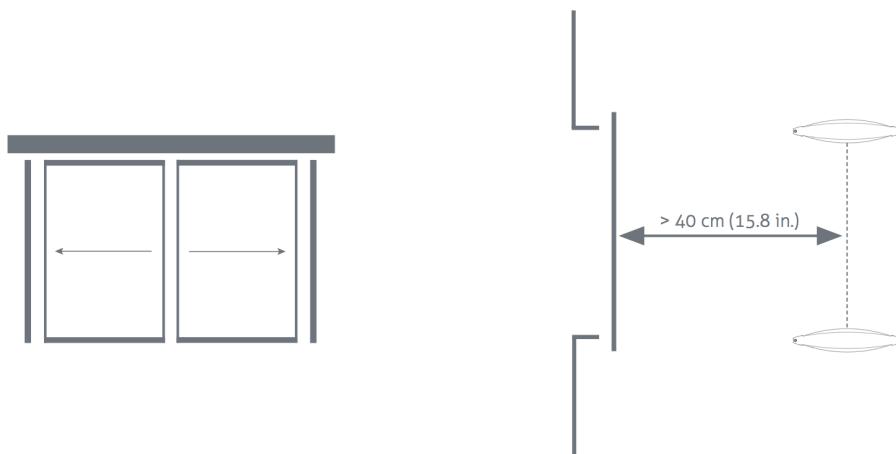
Take the following placement requirements into account when projecting the location of gates:

- There should be a minimum distance of 20 cm (7.9 in.) between the center of the gate and the wall.
- There should be a minimum distance of 200 cm (6.6 ft.) between 8.2 MHz tags and labels and the nearest antenna. If this is not possible, the labels and tags can be stored in a metal box at the checkout.



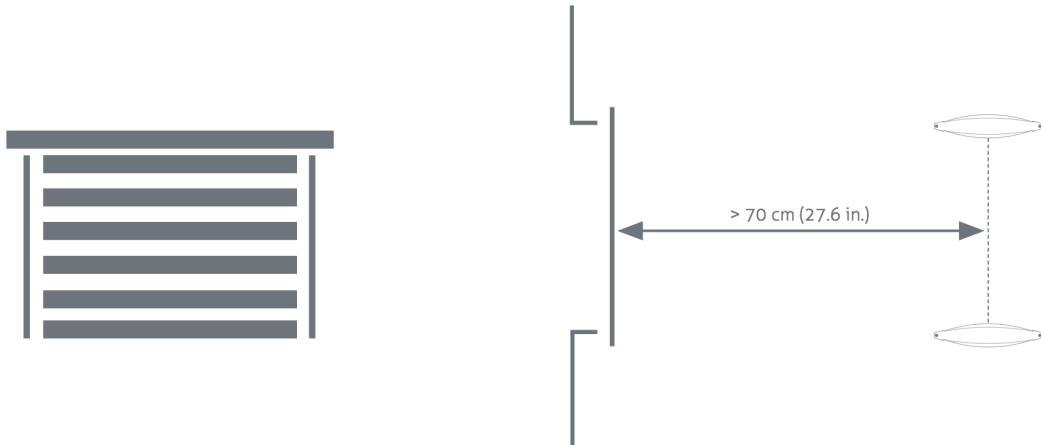
In addition, when **standard** or **sliding doors** are present:

- There should be a minimum distance of 40 cm (15.8 in.) between the center of the gate and the door.

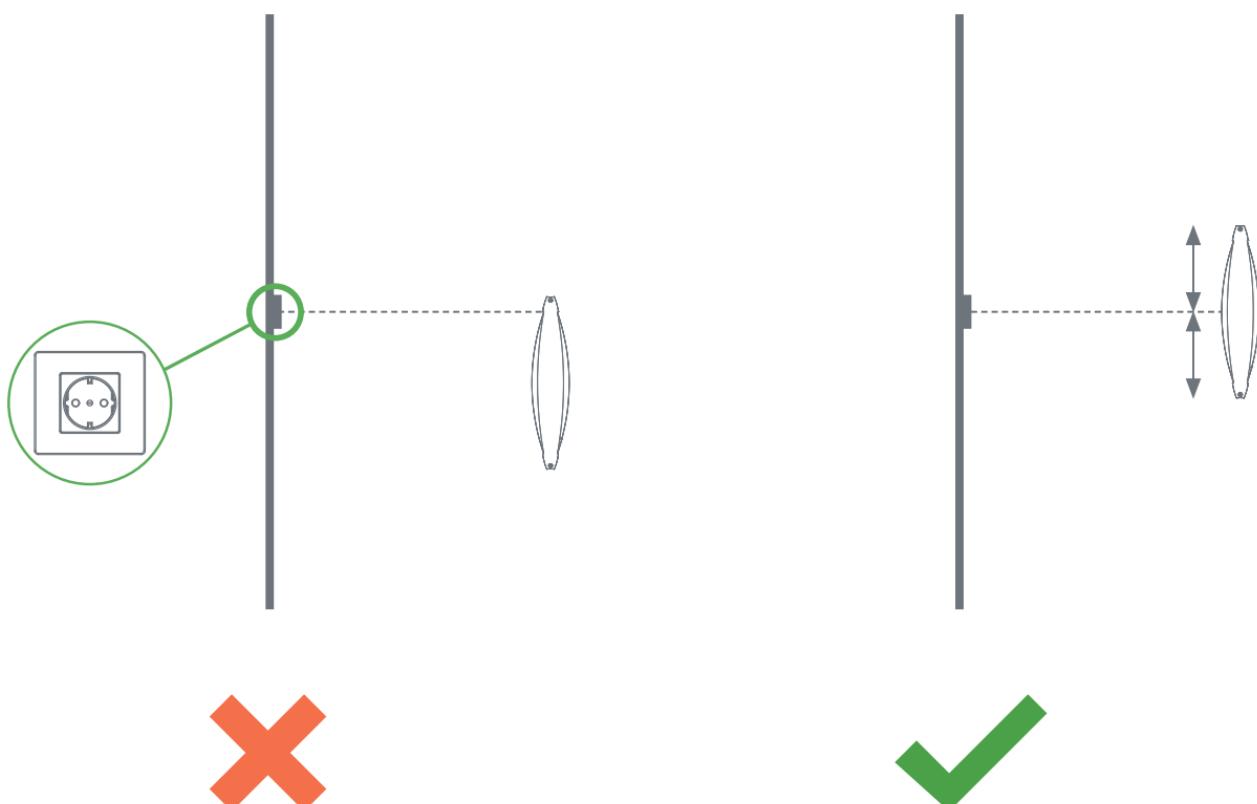


In addition, when a **roller shutter** is present:

- There should be a minimum distance of 70 cm (27.6 in.) between the center of the gate and the roller shutter.



If a power socket is less than 50 cm (19.7 in.) from the gate, the center of the gate should be aligned with the power socket.



Before installation, it is advised to gain information on the flooring below the antenna. If a dry-walk floor mat is used, it might have metal components that influence RF detection performance. In that case, a cut needs to be made in the floor mat to break conduction between the metal components and the antenna.

When the antennas are placed right next to a checkout that contains significant metallic parts, we advise always using a shield.



Please ensure there is no conducting connection between the gate and the checkout to prevent interference and coupling issues.

RFID installation requirements

When RFID technology is used, there are different installation requirements compared to RF technology. Since the RFID field is much less strictly defined than with RF technology, there is a larger area where tags could be detected. In comparison with RF, RFID is much less sensitive to coupling or interference issues.

Automatic tag muting

The RFID reader has a maximum performance. If this happens, the reader will mute some tags to have time for other tags. This feature is called *automatic tag muting*. Therefore, some tags in the system's surroundings might be muted and will not cause an alarm when moved through the gates.

Metallic surfaces

Metallic surfaces reflect the RFID field, which might confuse the Dynamic Beam Steering algorithms and influence (change or enlarge) the detection field. That is why it is advised to avoid metallic surfaces around RFID-enabled gates.

Power Inserter

Once the position of the gates is established, the location of the Power Inserters can be determined. A maximum number of Renos units can be connected to one Power Inserter, depending on which technologies are used and the number of add-ons in use. The table shows the number of power inserters needed for each hardware configuration.

Cable conditions: a CAT5E cable with a recommended maximum length of 80 meters / 250ft.

Technologies In Use	#Units / PI 230V	#Units / PI 115V
RF	5	5
RFID	5	5*
RF + RFID	3	3
RF + MD	5	4
RF + 2 SD's	4	4
RF + MD + 2 SD's	4	3
RF + RFID + MD	3	3
RF + RFID + MD + 2 SD's	Three**	Three**

Index:

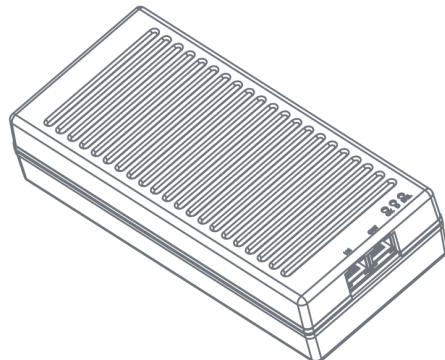
- RF = Radio Frequency 8.2 MHz
- RFID = RAIN Radio Frequency Identification (~900 MHz)
- MD = Metal Detection
- 2 SD's = 2 connected smart deactivators

* if the RFID units are operated monostatically, only four gates can be connected to a single power inserter.

** If the RFID units are operated monostatically, only two gates can be connected to a single power inserter.



Please note: Always use a Nedap Power Inserter (Power-over-Ethernet) to power Renos systems. It is not possible to use generic Power-over-Ethernet switches or stand-alone inserters.



If the retailer wants to upgrade an 8.2 MHz RF system to RFID later on, please consider the power requirements for RFID.



Make sure that the Power Inserter is connected to an always-on power socket! This is better for the firmware/hardware, continuous system monitoring, and remote firmware updates during the night.



Ensure the Power Inserter is placed at least 1 m (3.3 ft.) from the gates. When placed closer to the gate, it might cause interference with the RF technology.



Do not disconnect network cables in the system when still powered! First, disconnect the power cable from the power inserter(s).

Cabling

Now that the number of gates and Power Inserters is defined, the next step is determining the system's cabling. Different cables are required depending on the technologies used.

The iSense Lumen series uses a daisy chain set-up, which means that all devices are connected as a chain:

1. a cable from a Power Inserter OUT to a Renos unit IN,
2. from that Renos unit OUT to the next Renos unit IN,
3. etc.

Technologies In Use	Cables That Need To Be Installed
Only RF	Ethernet cable between each unit and the Power Inserter
Only RFID	Ethernet cable between each unit and the Power Inserter RFID Coaxial cable (included with the product) between each unit in the same group
Both RF and RFID	Ethernet cable between each unit and the Power Inserter RFID Coaxial cable (included with the product) between each unit in the same group

If the system is connected to the customer network or Device Management, an Ethernet cable must be installed between the system and the customer network, or a 3G/4G router must be set up.

Cable specifications - Ethernet cable

The following cable specifications are recommended for the iSense system:

- Use UTP Cat5e with a stranded copper core, with 24 AWG (0,51mm) core diameter.

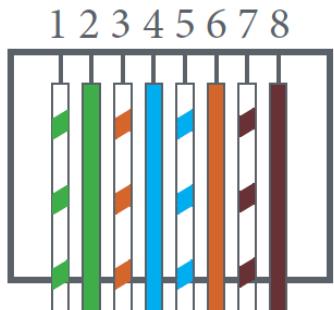


Always connect **all four pairs** using the **T568B** termination standard or T568A if specifically required!

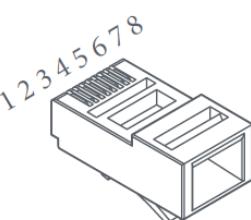
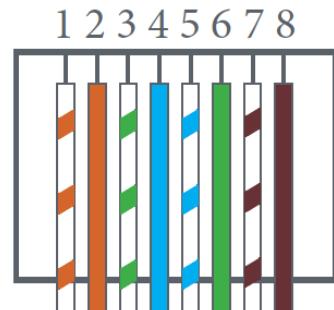


Never use CCA (copper cladding aluminum) or CCS/CCF (copper cladding steel) cable!

T568A



T568B



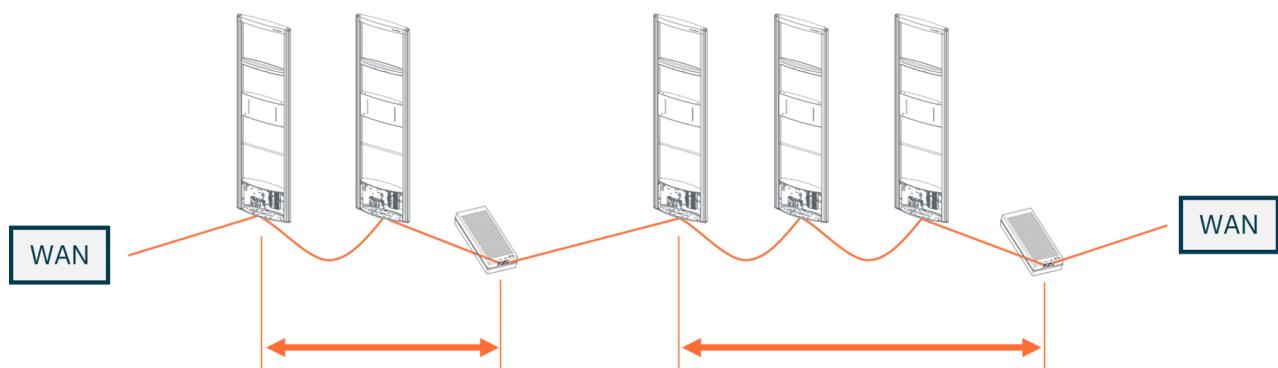
8P8C (RJ45)

Pin	T568A	T568B (Preferred)
1	Green + White	Orange + White
2	Green	Orange
3	Orange + White	Green + White
4	Blue	Blue
5	Blue + White	Blue + White
6	Orange	Green
7	Brown + White	Brown + White
8	Brown	Brown

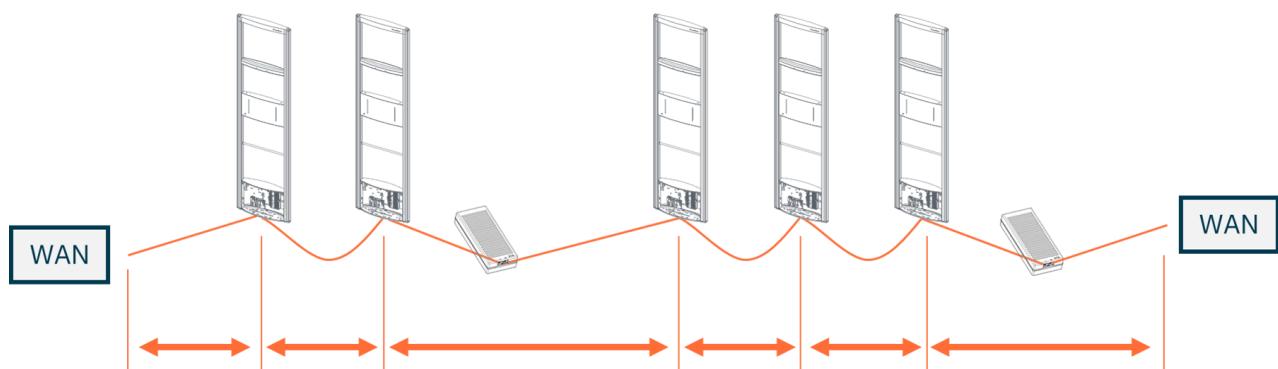
Cable length



Maximum cable length of **80 meters / 250 ft** between a Power Inserter and the last Renos unit that receives the power from this Power Inserter:



Maximum cable length of **80 meters / 250 ft** between Renos units (excluding Power Inserters) and between the first (or last) Renos unit and the WAN connection in the store:



Remarks

- It is possible to use your own preferred connectors.
- Make sure that the connectors are suitable for the cable and that the correct crimping tool is used for the connector.
- Follow the recommendations of the cable manufacturer.
- Local regulations may dictate using a specific cable type or rating.



We recommend placing the Power Inserter in the switch room (near a power socket) when the ethernet cable lengths allow. This way, the customer only has to arrange an ethernet outlet near the system.



If the cable lengths between two groups exceed approximately 50 meters / 164 ft, consider splitting a system into two.

RFID coaxial cable

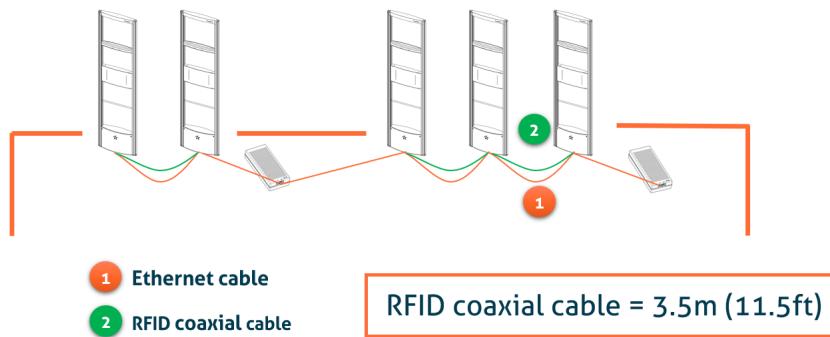
The RFID coaxial cable supplied with the product is 3.5 m (11.5 ft.) long. As the quality of this cable strongly influences the system's performance, it is supplied with every RFID gate. It is not possible to use third-party cables.



Only the RFID coaxial cable between units in the same group is necessary. An RFID coaxial cable is not required to connect groups.



The RFID coax cable has a fixed length of 3.5 m (11.5 ft.) to minimize signal loss. If the cable is not run through a slit but through a basement or other conduit, please check whether the path is not longer than approximately 2.5 m (8.2 ft.).



Cable Number	Type Of Cable	Required For RF	Required For RFID
1	Ethernet cable	Yes	Yes
2	RFID coaxial cable	No	Yes

Executing the installation

When all the preparations are considered, the system can be installed. The installation consists of physically mounting the system in the correct orientation, installing the cabling, and applying power to the system.

Conduit or slit

We always suggest that you place a conduit, as this allows easy replacement of cables when necessary. If not possible, a slit can be made as well.



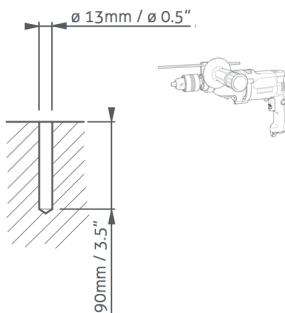
- When a system upgrades to RFID in the future, please install a conduit to add the RFID coax cable. You can also choose to install the RFID coax cable already. This is especially important when relying on a floor cut.

The conduit or slit in which the cables are placed should be precisely in the middle of the gate, perpendicular to the gate. This is explained in the following pictures.



Physical installation

Make sure the holes are marked on the floor in the correct locations according to the dimensions sketched earlier in this document. Drill the holes.



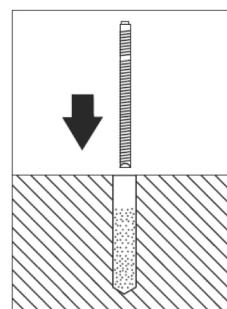
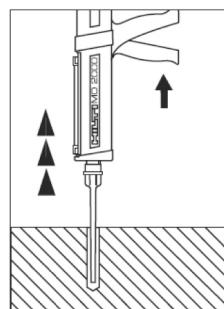
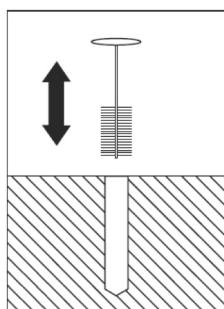
If RF technology is to be used, always keep enough space to place a shielding afterward. You will only know whether you need shielding when configuring the system (for example, when you find too much interference during the configuration).

Then, follow these steps to place the studs.

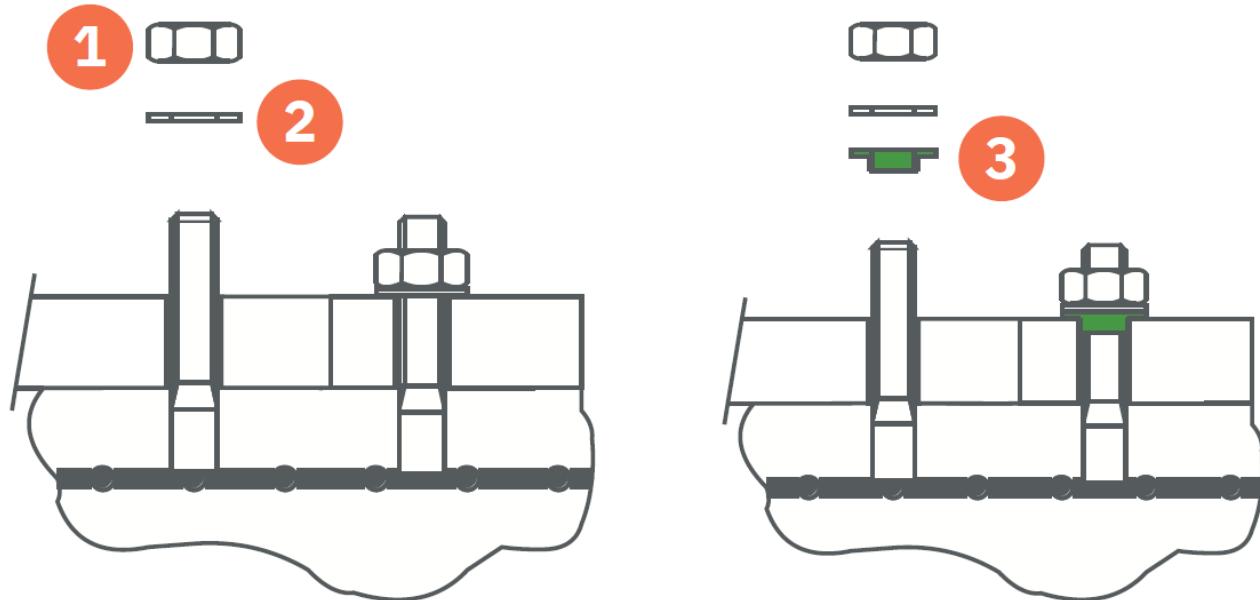
1. Clean the hole.
2. Insert Hilti-hit.
3. Place the stud.



Hilti-hit and studs are not included in the installation set.



Always use a nylon insulation ring to insulate the gate from the floor.



Number	Description
1	Nut M10 (not included in installation set)
2	Retainer ring M10 (not included in installation set)
3	Nylon insulation ring M10 (included in installation set)



If the gate is not adequately isolated from the floor, this might cause RF interference issues.

Orientation of products and the first gate

The gates must be orientated similarly for the system to function correctly, and the 1st power inserter should be connected to the correct gate. The orientation and gate 1 (the first gate to receive power from the first power inserter) can be determined depending on the role of the system as follows:

- EAS Role – Determine gate 1 by standing **inside the store and looking out towards the exit** (Power inserter on the right side of the first gate, and Renos should be on the left side of all gates)
- Goods movement role – Determine gate 1 by standing **inside the stock room and looking towards the store** (Power inserter on the right side of the first gate, and Renos should be on the left side of all gates)
- Goods receiving role – Determine gate 1 by standing **on the receiving dock and looking in towards the stockroom** (Power inserter on the right side of the first gate, and Renos should be on the left side of all gates)

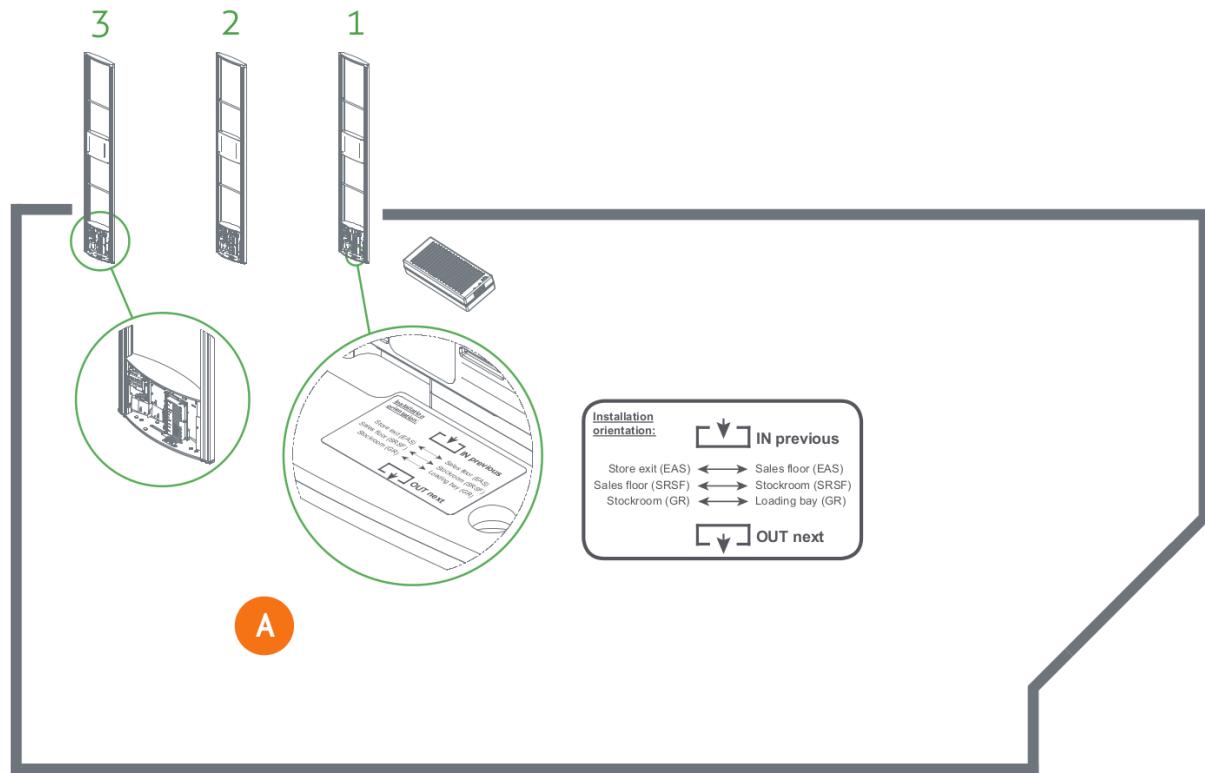


If this procedure is not executed correctly, the RFID technology will not work.

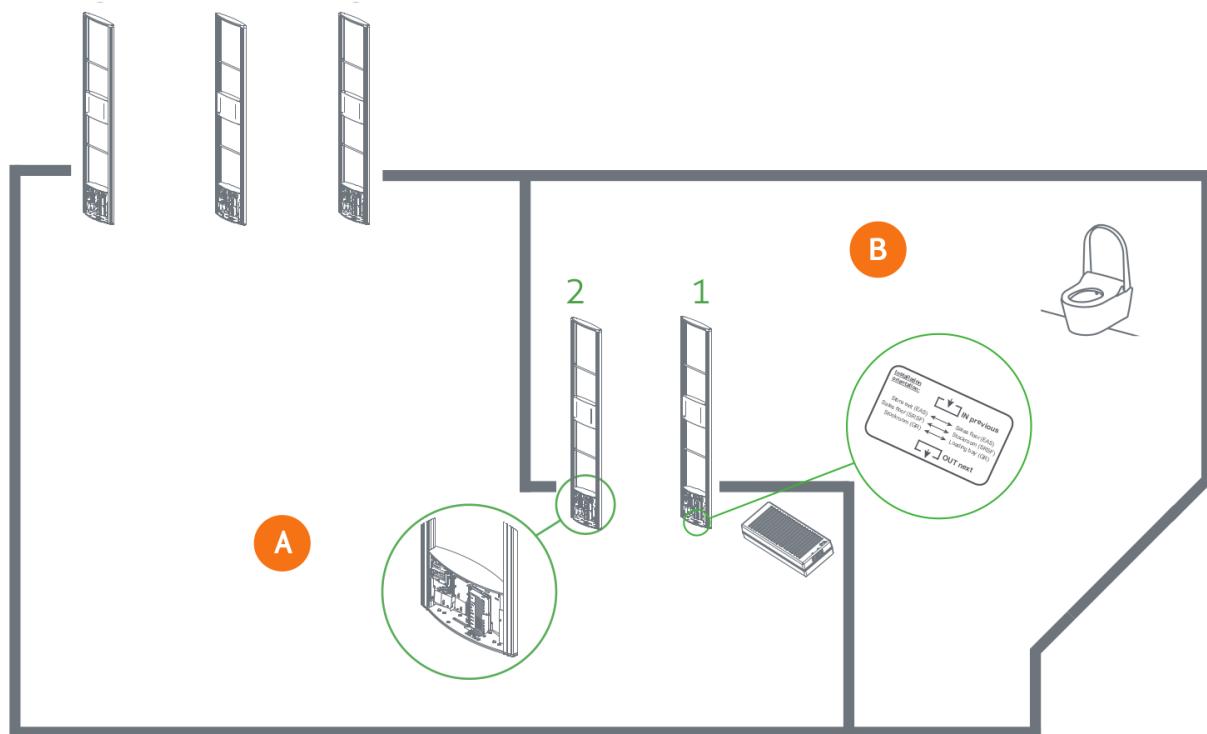
In the following examples, the location types in the table below occur.

Letter	Location Type
A	Salesfloor
B	Toilet
C	Stock room

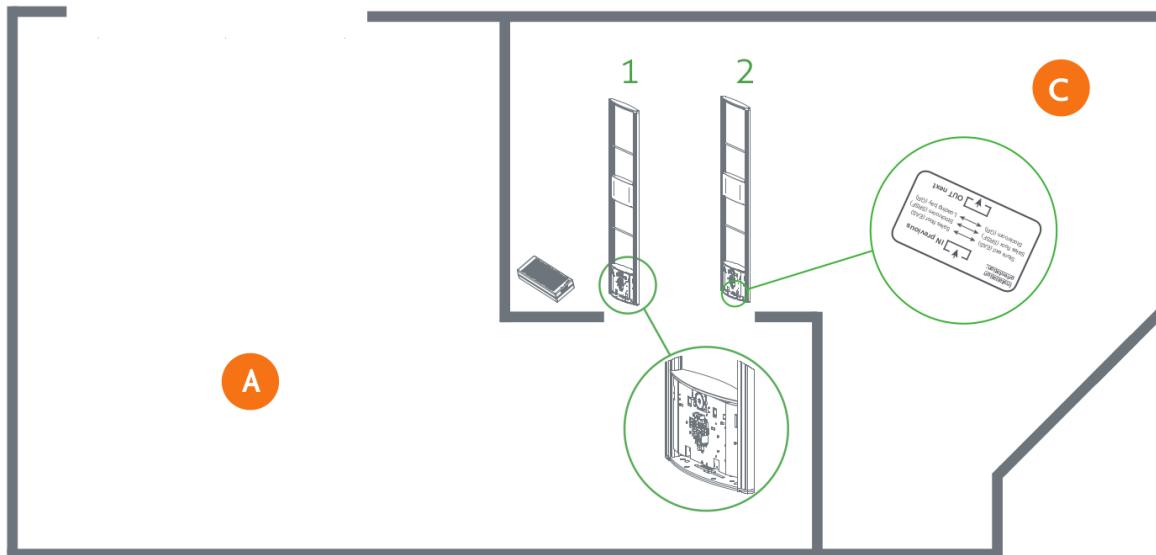
Example of EAS role



Example of EAS role, with toilet

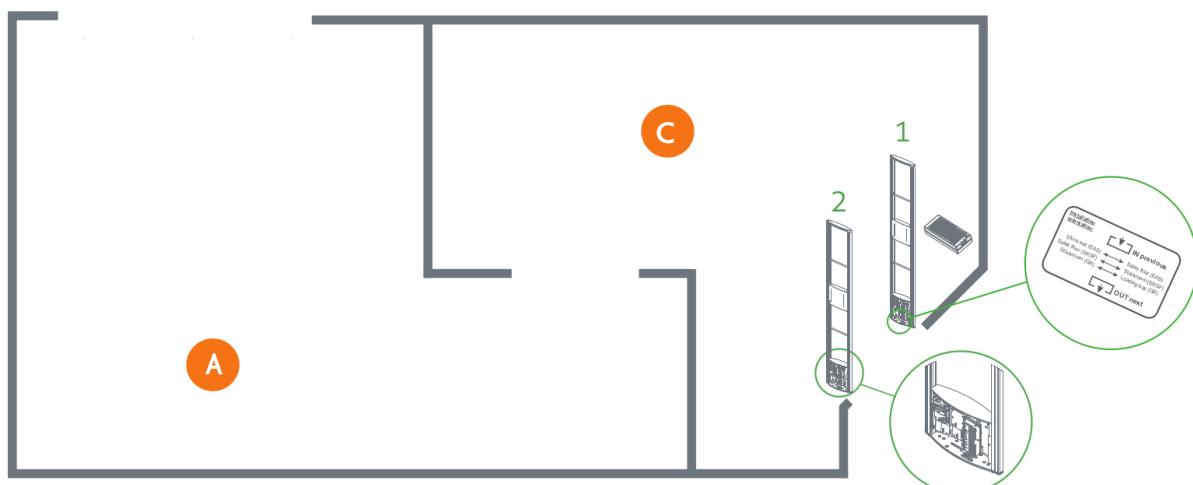


Example of stock room to sales floor role



Please note that when you compare the stockroom to sales floor role to EAS with the toilet, the orientation of the gates is precisely the opposite! This is because all gates should face the store's customer entrance/exit, except the toilet.

Example of goods receiving role



Installing cabling and filters

The exact cabling required was already determined during the preparation phase. Now, these cables can be placed.



All wiring should be done according to local regulations.

When cables are put in the slit or conduit, it is recommended to mark them with IN and OUT or PREVIOUS and NEXT, as this will allow you to distinguish them from each other.

Filters

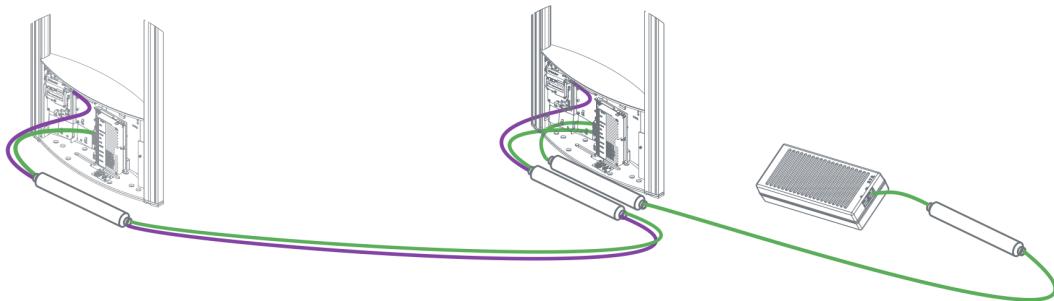
Please note that filters should be placed around the cables to reduce interference with other systems. These filters are delivered together with the system.

Filter should be placed at:

- Every Power Inserter: around the Ethernet cable at the OUT and IN ports.
- Every Renos unit is around the Ethernet and RFID coaxial cables (when used) at the OUT and IN ports.
- Every 9 m (30 ft.) for longer Ethernet cables.



Place the filters **before** attaching the connectors. The other way around is not possible.



Nedap offers the opportunity to order filters as spare parts. For more information, please visit the Nedap Retail Portal.

The filters close to a Renos unit should be placed inside the foot of the gate. If multiple filters are at the foot of the gate, they should be tied together.

Ethernet cables

Connect the Ethernet cable from the OUT port of the Power Inserter(s) or the Renos unit with the IN port of the next Renos unit.



Please test every Ethernet cable for correct connections and pair all four pairs (8 wires) with an Ethernet cable tester to ensure that the system can function correctly.

After the ethernet cables are connected, power up the Power Inserters.

RFID coaxial cable

If the Ethernet cable is connected, connect the RFID coaxial cable similarly. Connect from Gate 1 (next) to Gate 2 (previous), from Gate 2 (next) to Gate 3 (previous), etc.

The RFID coaxial cables should be connected from the NEXT port of one reader to the PREVIOUS port of the second reader. PREVIOUS and NEXT are related to the order of units about the first Power Inserter.



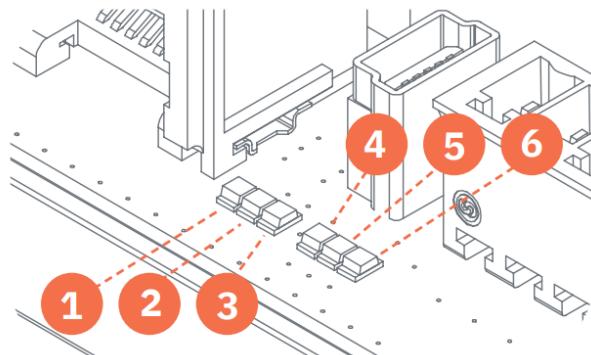
Please avoid making sharp bends in the RFID coaxial cable. This will affect the system's performance.



Don't use a tool to tighten the RFID coaxial cable connectors. This is not necessary and might break the connectors. If the connector is drawn by hand, that is good enough.

Renos Status LEDs

The electronics inside the unit have several status LEDs that can be used to discover the status of each part of the electronics.



Status LEDs of the Renos unit

LED	Color	Status	Explanation
1	Green	On	There is a Renos unit connected to the OUT port of this unit
		Off	There is no Renos unit connected to the OUT port of this unit
2	Blue	Blinking	There is no device connected to the OUT port of this unit
		On	There is a Power Inserter connected to the OUT port of this unit
3	Red	On	There is an issue with the power supply at the OUT port of this unit (too little current drawn)
		Blinking	There is an issue with the power supply at the OUT port of this unit (too much current drawn)
		Off	There is no issue with the power supply at the OUT port of this unit
4	Yellow	Blinking	The operating system on the Renos unit is running
		Off	The operating system on the Renos unit is not running
5	Green	Blinking	The storage flash on the Renos unit is accessed
		Off	The storage flash on the Renos unit is not accessed
6	Green	On	The firmware on the Renos unit is running

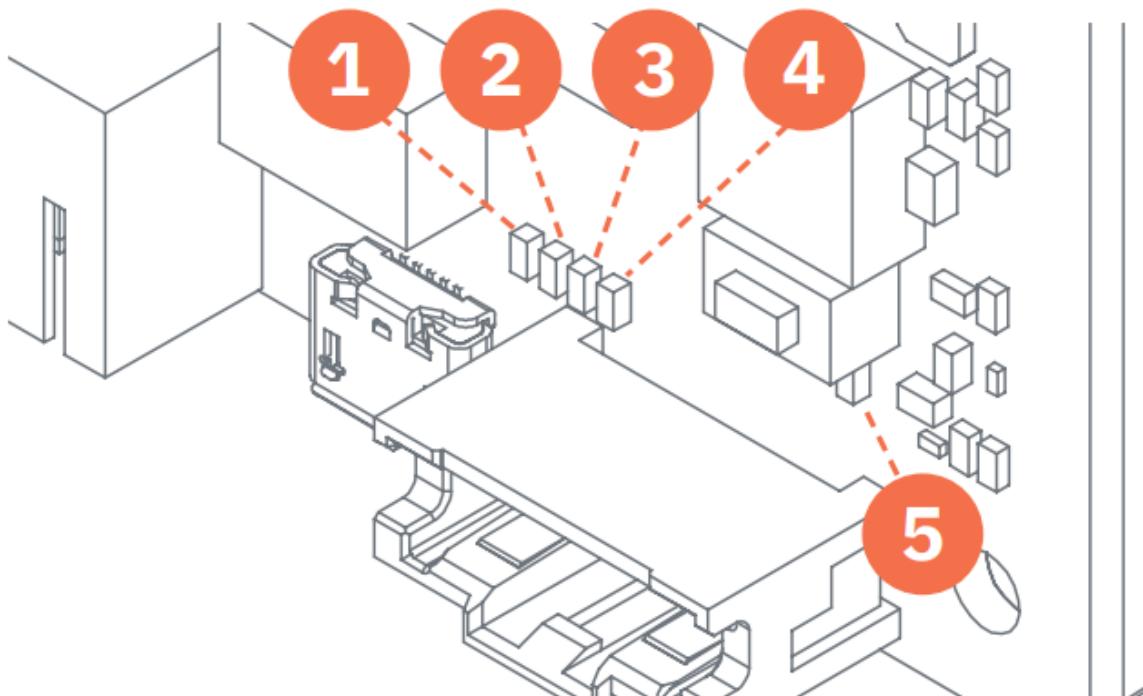
LED	Color	Status	Explanation
		Off	The firmware on the Renos unit is not (yet) running

Please look at the Troubleshooting chapter later in this manual to resolve erroneous conditions.



If the Renos unit has a firmware error, the rightmost three LEDs (4, 5, and 6) will remain off when powered. This can be solved using a 'Local - single unit' firmware update, as described in the "iSense firmware version manual."

RFID reader



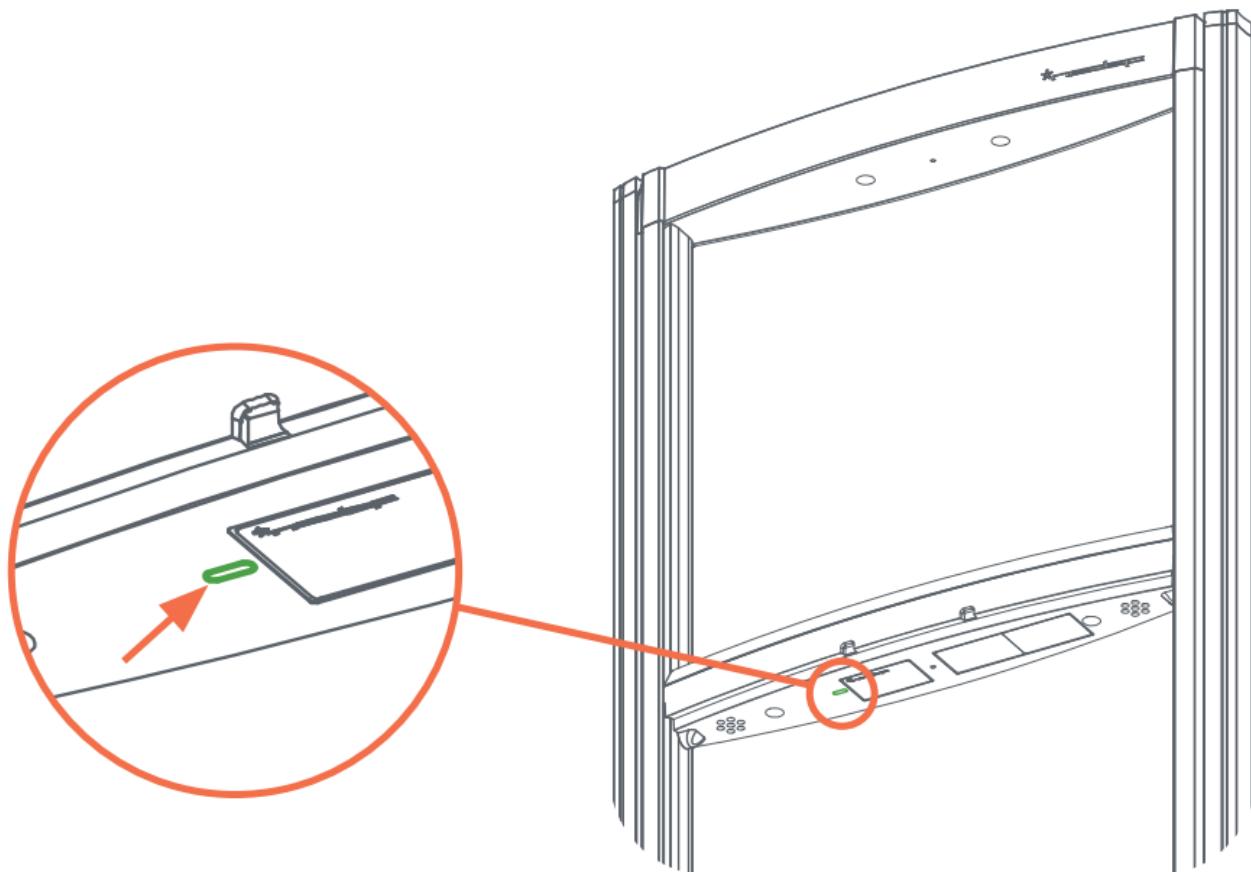
LED	Color	Status	Explanation
1	Blue	On	The RFID Reader is connected to the Renos firmware
		Blinking	The RFID Reader has received a command from the Renos firmware
		Off	The RFID reader is not connected to the Renos firmware
2	Orange	Blinking slow	The firmware on the RFID Reader is running
		Off	The firmware on the RFID reader is not running
3	Red	On	There is an error with the RFID output

LED	Color	Status	Explanation
		Off	There is no error with the RFID output
4	Green	On	The RFID output is active
		Blinking	The reader is reading RFID labels
		Off	The RFID output is not active
5	Green	On	The Renos unit powers the RFID reader
		Off	The Renos unit does not power the RFID reader



The RFID reader will not be active when the system has not been configured yet. This means that only the 'firmware running' orange LED is blinking.

AVCC (Audio Visual Customer Counting) unit of the iSense Lumen iL45



Color	Status	Explanation
Blue	on	Renos is running
	blinking	Renos is starting up
	off	The gate is not powered
Green	on	The system is connected to Nedap Device Management & Analytics
	off	There is no connection to Nedap Device Management & Analytics

Configuring the installation

The following tools are required to complete the configuration.

- Mini-USB cable.
- Laptop with installed driver and recent browser.

Driver installation

A Windows driver needs to be installed to configure an iSense system. Please check the table below for what is required based on your operating system.

Operating System	Driver
Windows	Download the driver from the portal.
Mac OS X	You don't need to install a driver.
Linux	You don't need to install a driver.

Once you have installed the driver, please check if it works by plugging it into a Renos unit.

Supported browsers

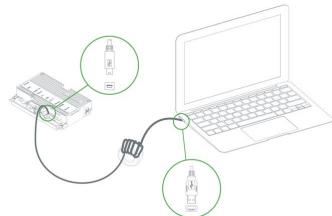
To configure the system, the latest versions of the following browsers are supported:

- Google Chrome
- Mozilla Firefox
- Apple Safari

If you don't have one of these browsers installed on your laptop, please install them before the installation.

Connecting a laptop to the Renos unit

You can connect your laptop via a Mini-USB cable to the service port on the Renos unit. In the iSense system, you can choose any Renos unit.



We advise using a good-quality USB cable about 5m / 16ft long. This provides more comfort during the configuration, as you can find an excellent place to put your laptop (instead of on the stairs or the floor next to the gate). Besides, some laptops interfere with RF technology, so it is better to place them further away.



We advise configuring Renos using a ferrite ring core filter around the mini USB cable. These can be ordered as spare parts with Nedap. Please take a look at the Nedap Retail Portal for more information.

Entering the configuration wizard

You can enter the configuration wizard by opening your browser and navigating to:

<http://192.168.133.1>



Ensure no other network connections are active in the same range.



Authentication

During the configuration, the user is required to authenticate himself. How this is done is dependent on the availability of Device Management.

- The system is connected to Device Management: you can enter your Nedap Retail username and password directly.
- The system is not connected to Device Management, and you don't have a Nedap Retail authentication software: choose one of the following steps:
 - If your laptop can connect to Device Management via a 4G/5G router or Wi-Fi, you can use this option to enter your username and password.
 - If that is not available, you can use your smartphone.
 - If your smartphone has no internet access, call your main technician for an authentication code.

Please reach out to support for more details on how to obtain a Nedap Retail username and password.

Getting help in the wizard

If something needs clarification, each page has a question mark button in the top right corner. You can click this to get more information on what is expected to do on a specific page.

Factory reset and Firmware change

It is essential to use the latest firmware version and start new installations with factory default units.

Details on how to perform a firmware update and factory default can be found in separate guidelines on the Partner Portal:

- iSense firmware version manual
- iSense factory reset procedure

Firmware change

There are four ways to change the firmware version on a Renos-based system:

1. Local—single unit overwrite. To execute the overwriting, insert a USB stick with the correct firmware into the USB port.
2. Local—complete system overwrite. You can execute the overwriting with files on your laptop during the configuration wizard.
3. Local - complete system update. The update can be executed during the configuration wizard with files on your laptop.
4. Device Management update. The update can be executed via the Device Management service.

Factory default

There are two ways to factory default a Renos-based system:

1. Local - single unit over-write. The factory default can be executed using a USB cable to connect the USB port to the service port.
2. Local - complete system factory default. The factory default can be executed during the configuration wizard.

System ID

You need the System ID to set up a Device Management system. The firmware version is displayed in the top right of the configuration wizard. If you click the firmware version, a pop-up shows the System ID during the configuration.

Integrating the installation with other systems

Integrating the iSense product into other solutions by the end customer is highly recommended.

Software integration with local APIs

The Renos platform offers local API endpoints for data analysis and status information. For more information, please refer to the Software Integration page on the Nedap Retail portal, which includes documentation and examples.

Physical integration using an IO Box

Integrating other systems via relay contact outputs and inputs is also possible. The Renos unit does not provide this directly; however, it can be accomplished via a 3rd party IO Box.



The following 3rd party IO Box is currently supported: **MOXA ioLogik E1214**.



The IO Box should be connected to a Renos unit via a USB to Ethernet adapter.

An output on an IO Box can be activated when specific events occur, depending on the capabilities of the chosen hardware.

URL trigger

The URL trigger mode can be used to trigger network-based devices with an HTTP-based API. Make sure that the iSense system can reach this device.

System behavior

Light and sound signaling

In comparison to iSense FLR gates, iSense Lumen products use different light and sound signals for different event types:

EAS role

Color	Meaning	Description
	orange	RFID alarm When beam steering is used, an alarm will only be raised for outgoing RFID events.
	red	RF alarm
	pink	RF alarm - outgoing Only when RF direction signaling is enabled will the alarm be red first and then pink when the direction is detected.
	white	RF alarm - incoming Only when RF direction signaling is enabled will the alarm be red first and then turn white when the direction is detected.
	dark blue	Metal detected Only when metal detection signaling is enabled. Only shown on one gate in the aisle (receiver)
	light blue	Wrong way event Only when wrong-way signaling is enabled does it signal when a person walks in the outgoing direction.

Stock room - sales floor & goods receiving roles

When the IR direction sensors are configured:

Color		Meaning	Description
	green	Direction event	The lights will turn green when a direction event is detected. As long as the lights are active, all detected RFID labels will be added to this transition event. Do not walk in the opposite direction when the lights are still active. If RFID labels have been detected, a sound will be played at the end of the detection period.
	red	Conflicting directions detected.	Opposite directions were detected while the green lights were still active, so the system could not decide on a direction. To properly set the location of the items in the database, walk back with the items, wait for all lights to dim, and walk through the aisle again in the direction you intended.
	light blue	IR sensors are blocked.	Some objects block the infrared beams between the gates, preventing the system from detecting directionality. Please remove the object to fix this.

When no IR direction sensors are configured:

Color		Meaning	Description
	green	One or more RFID labels have been detected.	Only when RFID observation signaling is enabled.

Servicing the installation

When the installation has been completed and delivered, it can be serviced via Nedap Device Management. We also provide monitoring options locally via SNMP.

Device Management

Nedap Retail systems can be connected to the online Device Management platform to ensure that systems can be managed remotely and work optimally globally.

The Nedap Device Management service provides four main functions on system level:

- **Monitoring:** Critical system parameters are monitored 24/7. If a system has issues, an alert is generated and sent to the supporting partner.
- **Remote Service:** using the Device Management website, an authorized Nedap-certified engineer can access the system's user interface to make changes to the configuration or access system logs.
- **Firmware Update:** an authorized Nedap-certified engineer can install new firmware releases remotely using the Device Management website.
- **Data Collection:** events per system are collected (e.g., to be displayed in the Analytics platform).
- **Sleep mode:** Enable sleep mode to conserve energy during nighttime hours, following the schedule configured in Device Management

For further details, please refer to the document on the portal about network information.

SNMP

Simple Network Management Protocol (SNMP) is available to allow for local monitoring of iSense systems. For example:

- One or more Renos units are not reachable
- The system is connected to Device Management

iSense systems use SNMP version 2c, community public. The MIB file is available on the iSense system itself via the URL [http://\(ip address of the system\)/snmp](http://(ip address of the system)/snmp) (for example, that is <http://192.168.133.1/snmp> when connected to the USB service port).

Troubleshooting

If the system is malfunctioning, please check the troubleshooting options below. If you still can't solve your issue, you can find support options in the next chapter.

Physical installation

Symptom	Cause	Solution
The red LED (3) on a Renos unit is on.	The current drawn-out of the OUT port of the Renos unit is too low. The cabling at the OUT port of the Renos unit does not satisfy the maximum length requirements.	Verify whether the cabling length in the system satisfies the requirements posed earlier in this document.
	The current drawn-out of the OUT port of the Renos unit is too low. The connectors of the Ethernet cable at the OUT port of the Renos unit are not mated properly.	Check the Ethernet cable at the OUT port of the Renos unit with an Ethernet cable tester.
The red LED (3) on a Renos unit is blinking.	The current drawn-out of the Renos unit's OUT port is too high. There are too many Renos units and add-ons connected to one Power Inserter.	Verify the number of Renos units and add-ons connected to the Power Inserters with the table earlier in this document.
	The current drawn-out of the Renos unit's OUT port is too high. A short circuit in the cabling leaves this Renos unit's OUT port.	Check the Ethernet cable at the OUT port of the Renos unit with an Ethernet cable tester.
The green LED (1) on a Renos unit is off, but there is a unit behind this unit.	There is an issue in the cabling between those units, so the following unit is not recognized.	Check Ethernet cabling with an Ethernet cable tester.
The red LED (3) on the RFID reader is on.	The RFID reader is having trouble starting to read. An erroneous antenna or a cabling error might cause this.	Log in to the Renos configuration interface to see the exact error.

Configuration

Symptom	Cause	Solution
It is not possible to access the configuration web interface.	Renos unit has not started yet.	Verify the green "firmware running" LED on the Renos unit (6). If this LED is not on, verify the system has power, or wait five minutes and try again.
	Mini USB cable not attached to Renos unit and laptop	Attach the cable to Renos unit and laptop.
	Driver not installed	On Windows 7 and older, you manually install a driver to support Renos.
I have put a system together, but during the hardware discovery, I see only part of all the units.	The WAN access port will be 'closed' for internal network traffic during configuration. If you combine two systems later on, this needs to be re-opened.	Do a factory reset on the previously used WAN entry point unit. If that doesn't work, do a factory reset on all units.
	There is a cabling error.	Please check all Ethernet cabling with an Ethernet cable tester.
	Not all Power Inserters are powered, or some Renos units are not fully started.	Verify the green "firmware running" LED on the Renos unit (6). If this LED is not on, verify the system has power, or wait five minutes and try again.
The Renos unit's all three LEDs, 4, 5, and 6, are off, indicating a firmware failure.	Something might have gone wrong with a firmware update.	The 'local - single' unit firmware update mechanism restores the unit.
I have configured RFID, but it detects labels outside the aisle, not inside.	Gates are positioned the wrong way.	Check the "Orientation of products" section in the manual and correct the orientation of the gates.

RF technology issues

When there are issues with RF technology during the configuration (the gates show as orange or red in the wizard), please follow the following steps:

1. Check the parameters in the RF Advanced Config of the configuration wizard and the RF gate performance section. One of those parameters is probably red or orange.
2. Disable all transmitters.
 - a. If all parameters in the RF gate performance section turn green again, a coupling problem exists (the transmitter couples with a label-like object in the environment). Please continue to the 'coupling problem' section.
 - b. If all parameters in the RF gate performance section remain orange or red, there is an active interferer (another device that transmits radio waves around the 8.2 MHz RF spectrum, like another EAS system, an engine, or a power supply). Please continue to the 'active interferer' section.

Coupling problem

Coupling problems are caused by objects that act as labels to the RF system. This includes metallic doorframes, checkouts, and cabling—everything that runs in a loop and is metallic.

To solve these problems, there are a few things you can try:

- Tighten screws in the metallic construction. This might work for checkouts or customer guidance rails.
- Try to interrupt the metallic loop. This can be done by using non-metallic parts inside those loops or by making a cut in them.
- Create a shortcut in the metallic loop to make it smaller. This will make it resonate at a different frequency.

If the above solutions don't solve the problem, you can decrease the system's sensitivity by ticking the 'reduced sensitivity' button in the RF Advanced Config.



If a decreased sensitivity doesn't work, and there is only one type of label or tag in the store, you also have the option to increase the 'receiver delay.' When higher than 6dB, the label detection will be limited.



The problem could also be solved with additional hardware (not available for all gates):

- **A 3-loop only 50 ohm PCB.** This will work when the coupling loop is located in the middle height of the gate.

- **Shielding.** This will work in many cases. However, the detection distance will be reduced by about 20 cm (0.7 ft.). The field will also slightly creep around the shield. This is called 'back detection'.



The 3-loop only 50 ohm PCB is only available in Europe with CE-certified products. Using it in other regions invalidates the local certifications.

If these things don't solve the problem, please contact support.

Active interferer

The first step is to locate the active interferer's source. You can do this by unplugging electronic devices around the gate (or moving them away) and seeing if the parameters in the 'RF gate performance' section improve or when the average height of the spectrum is reduced. If this is the case, you have identified the active interferer.

When the active interferer is known, the following solutions are possible:

1. Try to move the active interferer away from the gate as far as possible.
2. Try to apply filters around the cabling of the active interferer.
3. Shield the active interferer with aluminum foil.

If the above solutions don't solve the problem, you can decrease the system's sensitivity by ticking the 'reduced sensitivity' button in the RF Advanced Config.



The problem could also be solved with additional hardware:

- **A shielding.** This will work in a lot of cases. However, the detection distance will be reduced by about 20 cm (0.7ft.). The field will also slightly creep around the shield. This is called 'back detection'.



There are also round ferrites available that can reduce active interference sources and find ferrites with optimal impedance at around 8.2MHz.

If these things don't solve the problem, please contact support.



Warranty and spare parts

- Please consult the Nedap Retail Business Partner from whom you purchased this product regarding the applicable warranty conditions.
- This product cannot be used for any other purpose described in this document.
- If the product is not installed according to this document, the warranty provided is not applicable.
- At the sole discretion of Nedap N.V., Nedap N.V. may decide to change the conditions of Page 7 of 19 Compliance information for technical manuals warranty policy.
- You agree that Nedap N.V. can compensate you for the pro-rata value of the warranty involved rather than replacing or repairing the product based on its technical or economical value.
- Prior to applying the warranty, please verify that you comply with the warranty conditions of the warranty policy and that you can successfully apply for the replacement or repair of a defective part.
- Parts can only be replaced with original Nedap parts; otherwise, the warranty policy will not apply to the product.
- If the warranty is applicable, please contact the dealer or send the defective parts to the dealer.

Regulatory information

FCC and IC Compliance Statement

This device complies with part 15 of the FCC Rules and RSS210 of Industry Canada. 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.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Cet appareil se conforme aux normes CNR210 exemptés de license du Industry Canada. L'opération est soumis aux deux conditions suivantes:

- (1) cet appareil ne doit causer aucune interférence, et*
- (2) cet appareil doit accepter n'importe quelle interférence, y inclus interférence qui peut causer une opération non pas voulu de cet appareil.*

Les changements ou modifications n'ayant pas été expressément approuvés par la partie responsable de la conformité peuvent faire perdre à l'utilisateur l'autorisation de faire fonctionner le matériel.

FCC and IC Radiation Exposure Statement

This equipment complies with FCC and Canadian radiation exposure limits for an uncontrolled environment. It should be installed and operated with a minimum distance of 20 cm between the radiator and your body. This transmitter must not be co-located or operated with any other antenna or transmitter.

Cet équipement est conforme a CNR102 limites énoncées pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et votre corps.

This Class B digital apparatus complies with Canadian ICES-3. Cet appareil numérique de Classe B est conforme à la norme Canadienne NMB-3.

FCC Information to the user

Note: This equipment has been tested and found to comply with the limits for class B digital devices, according to part 15 of the FCC Rules. These limits are designed to protect reasonably against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency

energy and, if not installed and used following the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. Suppose this equipment does not cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on. In that case, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from the receiver's.



Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. To ensure compliance with FCC regulations, use only the shielded interface cables provided with the product or additional specified components or accessories that can be used to install the product.

Information for Taiwan

第十二條 經型式認證合格之低功率射頻電機，非經許可，
公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；
經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。
低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

CE WEEE

This European Standard specifies a marking:

- of electrical and electronic equipment following Article 11(2) of Directive 2002/96/EC (WEEE); This is in addition to the marking requirement in Article 10(3) of this Directive, which requires producers to mark electrical and electronic equipment put on the market after 13 August 2005 with a 'crossed-out wheeled bin' symbol.
- that applies to electrical and electronic equipment falling under Annex IA of Directive 2002/96/EC, provided the equipment concerned is not part of another type of equipment that does not fall within the scope of this Directive. Annex IB of Directive 2002/96/EC contains an indicative list of the products that fall under the categories set out in Annex IA of this Directive;



- that identifies the equipment producer clearly and that the equipment has been put on the market after 13 August 2005.

CE - UKCA Declaration of Conformity

With this, Nedap N.V. declares that the subject equipment is in compliance for CE with directives 2014/53/EU (Radio Equipment Directive) and 2011/65/EU (RoHS). And for UKCA with SI 2017/1206 (radio Equipment Regulations 2017) and with SI 2012/3032 UK Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 (RoHS). The full text of the declarations of conformity is available at the following internet address: <https://portal.nedapretail.com/>, where, if applicable, REACH information can also be found.

Disposal of this product

This product's owner or last user is responsible for properly disposing of (parts of) the product as required by local rules and regulations.





About Nedap

Together, we make merchandise simply available

At Nedap, we believe in ‘Technology for Life’. Nedap Retail enables retailers to serve their customers better. Using technology, we allow for perfect inventory visibility, total control, no waste, and no losses.

Our vision for inventory visibility

Today, established retailers need more information about where their items are. Without this knowledge, providing an omnichannel experience leads to heavy overstocking, waste, and eroding margins. Solving this requires a fundamental change in the retailers’ supply chain and information systems.

Our mission is to simplify the process of ensuring that retailers always have the right products available at the right place and time.

We do this by giving retailers perfect inventory visibility for a seamless shopping experience. This way, retailers can meet the changing consumer needs while remaining profitable.

Nedap works with the largest and most successful retailers in the world. We take complete ownership of our projects—failure is never an option. A unique combination of the best technology and industry teams at Nedap Retail achieves this.

Nedap solutions are built upon 45 years of global experience, market expertise, and close cooperation with leading retailers. A flexible network of certified partners worldwide supports our worldwide operations. Nedap systems are future-proof (RFID-ready), cost-efficient, and Eco-friendly. Our mission is to ensure retailers' customers maintain the best shopping experience while we help retailers protect their profits.

Contact

If you need further details or help preparing, executing, or servicing an installation, please contact our support team at support-retail@nedap.com.

Suggestions for improving our products and documentation are much appreciated.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap NV 2025

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 119

Document Last modification date 19 March 2025

Document PDF Exported 21 March 2025 by Nedap Retail | Operations



support-retail@nedap.com



**Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands**

nedap-retail.com

Nedap Sense Manual

iSense FLR Series

Gates i30 / i45 / i45 Hybrid and Upgrade i45 RFID

version 292, March 2025

Introduction	4
Disclaimers	5
Safety precautions	5
RFID Regions	5
Product Overview	6
Box contents	6
Components	7
Dimensions	9
Connections	11
Add-ons	12
Preparing the installation.....	16
Defining the system	16
Aisle width or detection distance	18
Label-free zone	18
RF installation requirements	19
RFID installation requirements	22
Power Inserter	23
Cabling	25
Device Management	30
Executing the installation.....	31
Conduit or slit	31
Physical installation	32
Orientation of products and the first gate	34
Installing cabling and filters	37
Renos Status LEDs	39
Configuring the installation	43
Driver installation	43
Supported browsers	43
Connecting a laptop to the Renos unit	44
Entering the configuration wizard	44
Authentication	45
Getting help in the wizard	45
Factory reset and Firmware change	46

System ID	46
Integrating the installation with other systems	47
Software integration with local APIs	47
Physical integration using an IO Box	47
URL trigger	47
Servicing the installation.....	48
Device Management	30
SNMP	48
Troubleshooting.....	49
Physical installation	49
Configuration	50
RF technology issues	51
Warranty and spare parts.....	53
Regulatory information	54
FCC and IC Compliance Statement	54
FCC and IC Radiation Exposure Statement	54
FCC Information to the user	54
Information for Taiwan	55
CE WEEE	55
CE - UKCA Declaration of Conformity	56
Disposal of this product	56
About Nedap.....	57
Together, we make merchandise simply available	57
Our vision for inventory visibility	57
Contact	57

Introduction

The Nedap FLR-line gates are equipped with Ultra-High-Frequency (UHF) RFID and/or 8.2 MHz RF detection technology to detect active RF/RFID labels and hard tags.

In addition, it is possible to add infrared beam sensors for direction detection or customer counting.

The gates are designed explicitly for in-store retail applications, such as Electronic Article Surveillance (EAS), stock room to sales floor transition, and goods receiving.



This manual overviews the products, installation, and configuration basics. For more details, several guidelines are available on the Nedap Retail portal.

This manual covers the following products:

Article Number	Article Name	Commercial Name	Technologies	Model Name
9563873	ASSY FL30R RF GREY	Gate i30 Grey	8.2 MHz RF	ASSY FLR RF
9563881	ASSY FL45R RF GREY	Gate i45 Grey	8.2 MHz RF	ASSY FLR RF
9982221	ASSY FL45R RF+RFID R1 GREY	Gate i45 Hybrid Grey Region 1	8.2 MHz RF, UHF RFID	
9982132	ASSY FL45R RF+RFID R2 GREY	Gate i45 Hybrid Grey Region 2	8.2 MHz RF, UHF RFID	ASSY FLR RF+RFID
9982159	ASSY FL45R RF+RFID R3 GREY	Gate i45 Hybrid Grey Region 3	8.2 MHz RF, UHF RFID	
9982248	ADD-ON FL45R RFID R1 UPGRADE-RENOS	Upgrade i45 Grey RFID Region 1	UHF RFID	
9982302	ADD-ON FL45R RFID R2 UPGRADE-RENOS	Upgrade i45 Grey RFID Region 2	UHF RFID	ASSY FLR RF+RFID
9982175	ADD-ON FL45R RFID R3 UPGRADE-RENOS	Upgrade i45 Grey RFID Region 3	UHF RFID	



For the physical installation of the upgrade kit for the following products, an additional manual is available that contains instructions on how to install the upgrade kit:

- 9982248 - ADD-ON FL45R RFID R1 UPGRADE-RENOS
- 9982302 - ADD-ON FL45R RFID R2 UPGRADE-RENOS
- 9982175 - ADD-ON FL45R RFID R3 UPGRADE-RENOS

Disclaimers



Nedap intends to make this manual accurate and complete. However, Nedap does not warrant that the information contained herein covers all details, conditions or variations, nor does it provide for every possible contingency in connection with the installation or use of this product. Nedap disclaims any liability for damage to property or personal injury resulting, in whole or in part, from improper installation, modification, use, or misuse of its products. The information contained in this document is subject to change without notice.



This equipment should only be installed, operated, serviced, and repaired by skilled personnel. The installation and interconnection of this equipment to facility wiring and other equipment must be done by a competent, skilled craftsperson familiar with applicable standards and codes governing the installation. Installation methods, practices or procedures that are unauthorized or done improperly are dangerous and could result in serious personal injury or damage to property and equipment.

Safety precautions



Do not place cards equipped with a magnetic strip or chip (i.e., ID, travel, debit, and credit cards) close to the equipment to avoid possible card failures.



To avoid potential interference with medical devices (pacemakers, cochlear implants, etc.), keep a distance of at least 20cm (8 inches) between them and the equipment.

RFID Regions

Region 1: Europe, Eastern Europe, Middle East, Africa and India

Region 2: North America and South America

Region 3: Asia and Oceania

Product Overview

Multiple variations within the FLR line support different technologies and upgrade kits, which can later be used to upgrade an 8.2 MHz RF installation to UHF RFID.



In this document, the following abbreviations will be used:

- 'RF technology' is an abbreviation for 8.2 MHz RF technology.
- 'RFID technology' is an abbreviation for UHF RFID technology.

Box contents

Article Number	Article Name	Box Contents
9563873	ASSY FL30R RF GREY	<ul style="list-style-type: none">• Gate i30 gate with Renos RF• Installation set• Quick Reference
9563881	ASSY FL45R RF GREY	<ul style="list-style-type: none">• Gate i45 gate with Renos RF• Installation set• Quick Reference
9982124	ASSY FL45R RFID R1 GREY	<ul style="list-style-type: none">• Gate i45 gate with Renos, RFID reader, and RFID antennas• 3.5 m (11.5 ft.) RFID coaxial cable• Installation set• Quick Reference
9982221 9982132 9982159	ASSY FL45R RF+RFID R1 GREY ASSY FL45R RF+RFID R2 GREY ASSY FL45R RF+RFID R3 GREY	<ul style="list-style-type: none">• Gate i45 gate with Renos RF, RFID reader, and RFID antennas• 3.5 m (11.5 ft.) RFID coaxial cable• Installation set• Quick Reference

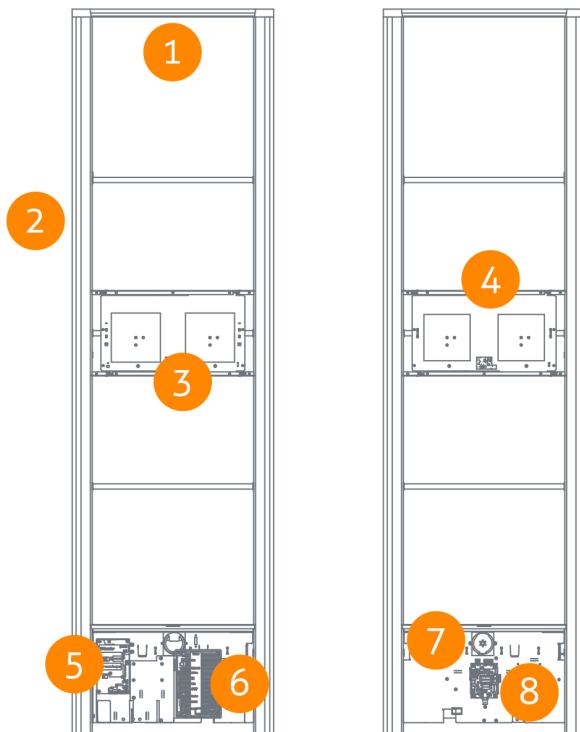
Article Number	Article Name	Box Contents
9982248	ADD-ON FL45R RFID R1 UPGRADE-RENOS	<ul style="list-style-type: none"> RFID reader and RFID antennas (only compatible with i45 gate)
9982302	ADD-ON FL45R RFID R2 UPGRADE-RENOS	<ul style="list-style-type: none"> 3.5 m (11.5 ft.) RFID coaxial cable
9982175	ADD-ON FL45R RFID R3 UPGRADE-RENOS	<ul style="list-style-type: none"> Installation set Quick Reference



It is not possible to combine different articles in one system.

Components

The FLR line iSense products are based on the Renos platform. The Renos platform is developed by Nedap Retail specifically for retail applications. The FLR line of products has several serviceable parts. These are explained in the table and highlighted in the schematic drawings.



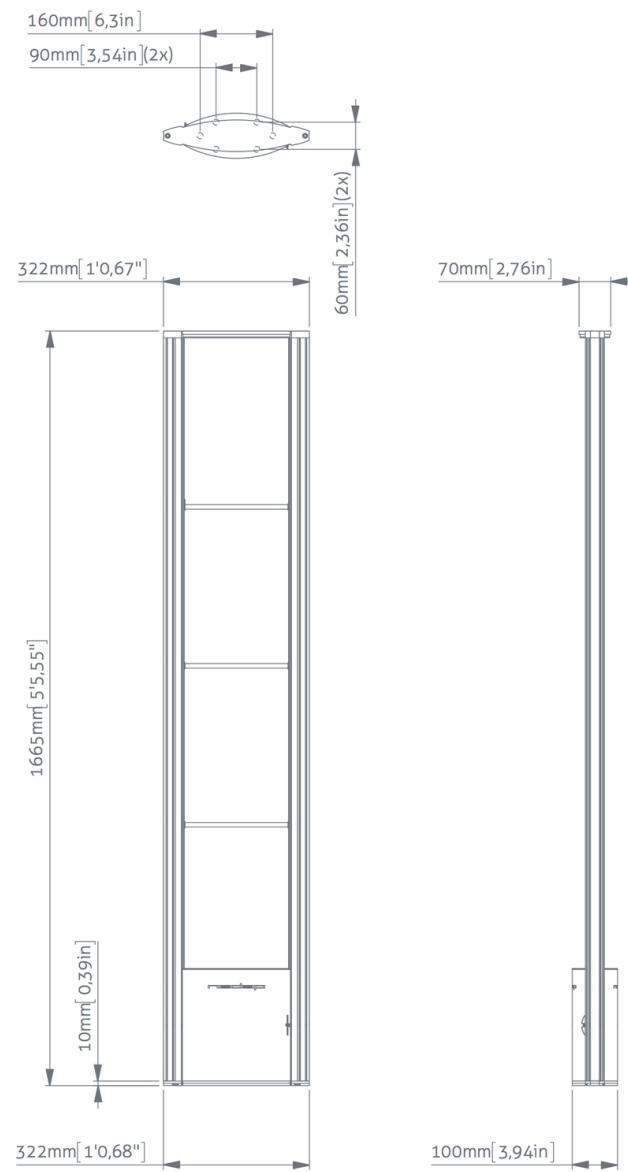
No.	Component	Description
1	Lights	The red LED lights can be used for user feedback or alarms.
2	RF antenna	The antenna is integrated into the aluminum frame.

No.	Component	Description
3	RFID antenna NEXT	The RFID antenna, pointing to the NEXT gate (not included in all variations).
4	RFID antenna PREVIOUS	The RFID antenna, pointing to the PREVIOUS gate (not included in all variations).
5	RFID reader	The RFID reader processes the reading of RFID labels. It is connected to the Renos unit and the RFID antennas (not included in all variations).
6	Renos unit	The Renos unit is the central processing unit of an iSense FLR product. It powers the system and data communication between units and the outside world. Most products are equipped with an RF detection engine - except the RFID-only systems used in Region 1 to be compatible with the OST platform.
7	Buzzer	The buzzer can be used for user feedback or alarms.
8	50 ohm PCB	The 50-ohm PCB connects the Renos unit, the RF antenna, and the lights.

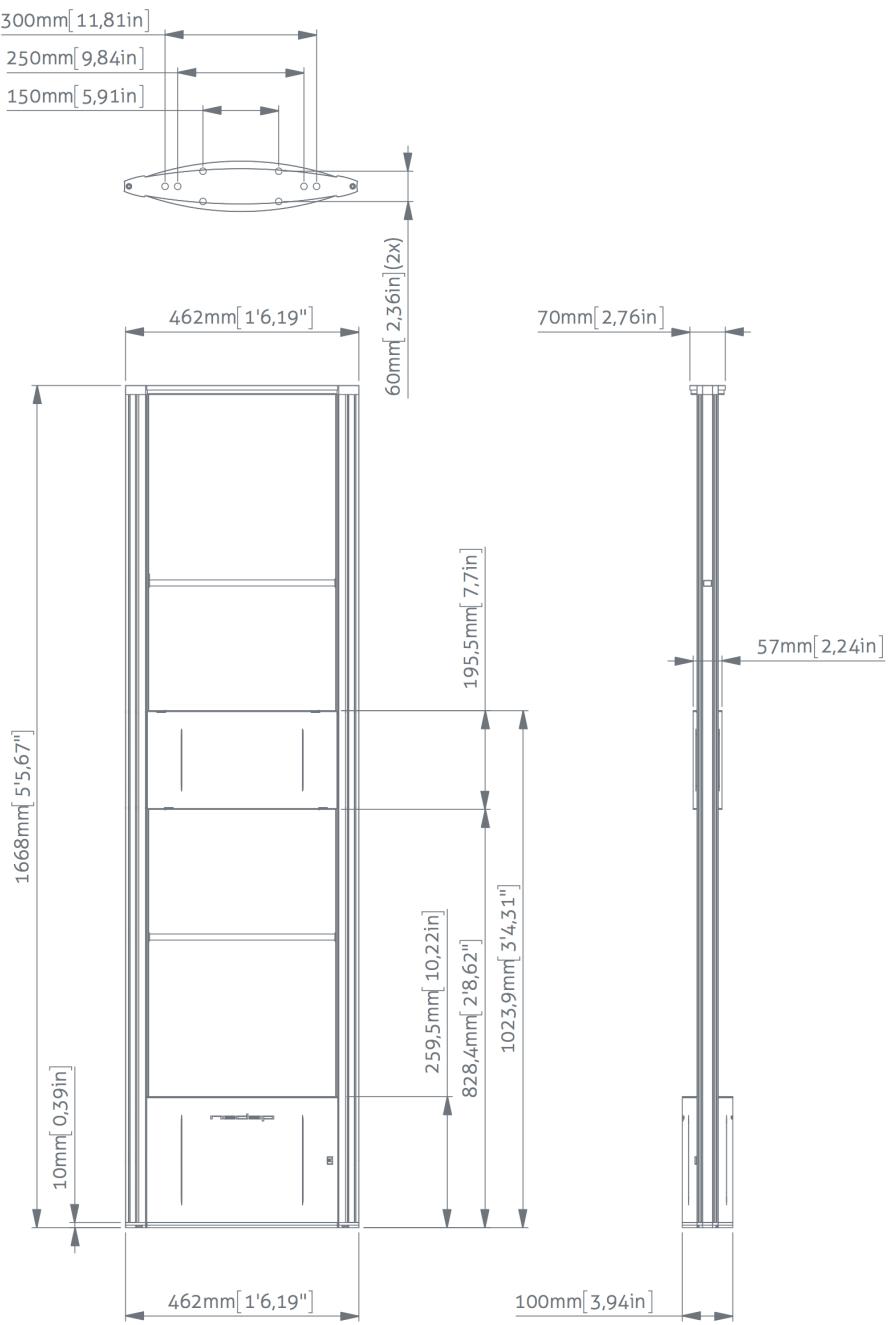
Dimensions

This section presents dimensional drawings of the gates. The holes in the mounting plate can be used as a template to draw the locations for drilling holes in the floor.

iSense FL30R (i30)

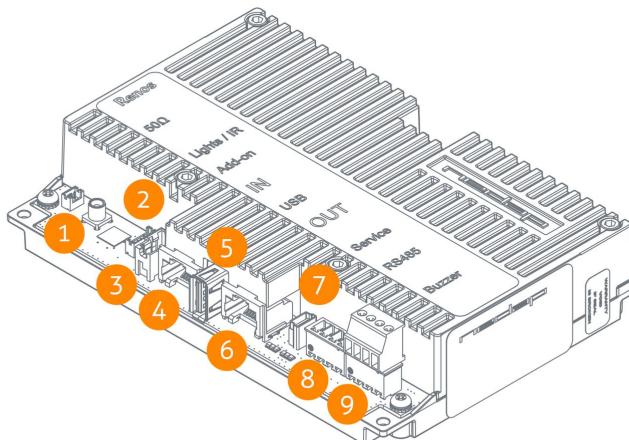


iSense FL45R (i45)



Connections

This is a Renos unit, describing all its connectors and what they are used for.



No.	Connector	Usage
1	50 ohm	Connect the Renos unit to the 50-ohm PCB. The 50-ohm PCB connects both the light and the RF antenna.
2	Infrared beams	Connect to the optional infrared beam sensors.
3	Add-on	Provide power and synchronization to add-ons, like the RFID reader.
4	Network IN	Connected to the Network OUT of a previous Renos unit or a Power Inserter.
5	USB	Connect accessories to Renos, like the RFID Reader.
6	Network OUT	Connected to the Network IN of the next unit or a Power Inserter. It can also be left unconnected or connected to the customer network.
7	Mini USB service port	Connect your laptop to configure the Renos system.
8	RS485 connector	Connect to the optional Nedap RF Smart Deactivator.
9	Buzzer connector	Connect to the included buzzer.

The LED indicators on the Renos unit will be discussed later in this manual.

Add-ons

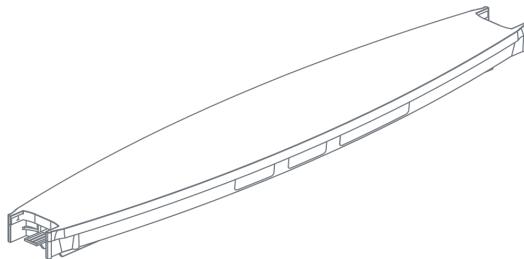
Several add-ons are available for the FLR-line products. Each add-on has its own manual/guideline. However, we will discuss the function of those add-ons here.

Infrared beam sensors

Infrared beam sensors can be used for two purposes:

- Customer counting in EAS role (both RF and RFID)
- Direction detection when the system is used between the stock room and sales floor (RFID only)

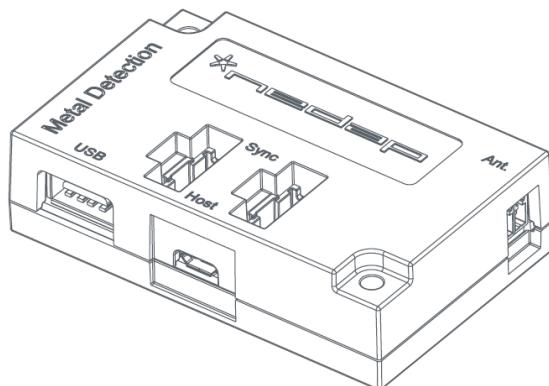
The infrared beam sensors are plug-and-play and can be easily 'clicked' in a FLR-line gate.



Please note that if you want to use infrared beam sensors with an FLR-line product, ensure that every gate in a group has sensors installed. It is impossible to have sensors only in a group's first and last gate.

Metal Detection

The iSense Metal Detection unit can detect foil-lined bags, which thieves sometimes use to prevent the RF and RFID tags from being read by the detection system or reader. With Metal Detection, we can detect metal objects and provide a discrete alarm to the store employees.



For metal detection to work, you need a minimum of 2 gates and 1 Metal Detection unit in each gate within a group.



The distance between large (Metal) doors and the gates with Metal Detection must be at least 1.5 meters. Doors swinging open to the outside must be at least 1 meter away.



The maximum distance between the two gates is the same as specified for RF, with one exception.

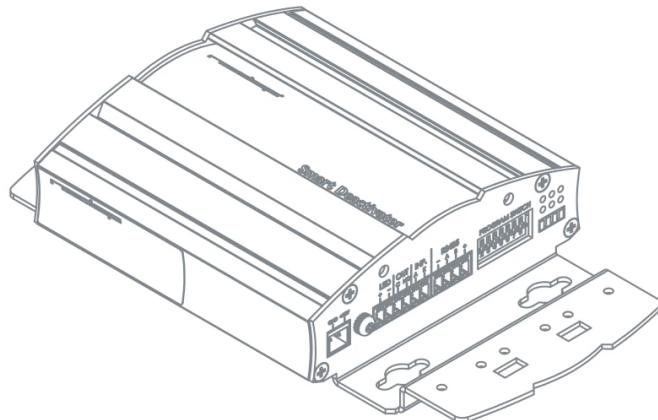
For the Lumen iL33, the maximum distance changes when shielding is used:

- With shielding at one side, the maximum distance between all the gates in this group becomes 1.5m (instead of 1.65m)
- If the group contains two gates and both are shielded, the distance becomes 1.25m

Remember that the shielding also influences the RF performance!

RF Smart Deactivator

The RF Smart Deactivator can be used to deactivate RF labels at the checkout. When connected to an iSense system, it can be powered by a Renos unit. The Renos unit can also gather information from the deactivator, like whether it is operational.

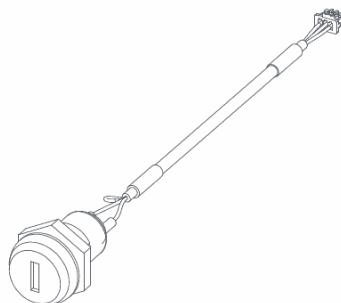


The RF Smart Deactivator integration cannot be used in iSense systems where RF is not enabled.

Key switch

Installing a Key Switch on the iSense gate can be helpful if you want to temporarily disable the system (both RF and RFID, depending on the available hardware).

The Key Switch must be connected directly to the Renos unit inside the iSense gate. For the installation, please carefully follow the quick reference enclosed for the Key Switch!



You need one key switch per gate.

iSense Dashboard

The iSense system has a built-in security dashboard, the iSense Dashboard. It can be enabled by entering a purchased license key during the configuration wizard. The customer can then visit the dashboard via a web browser. To make this work, the iSense system should be in the same network, either connected to the customer network or a stand-alone set-up with a router should be made.

The iSense Dashboard allows the iSense system to be monitored inside the store. It creates an overview and provides real-time information for more effective reactions. The iSense Dashboard contains:

- Real-time overview of which gate or attention button is alarming: the ‘recent alarms’ provide controls to react quickly and accurately to alarms.
- The System Health widget shows the system’s performance to identify whether the system is functioning correctly quickly.
- The Alarm Data widget shows the number of RF/RFID/MD alarms per day as a percentage and compares this to the same time last day.
- The Visitor widget shows the number of customers today and the percentage change compared to the last hour.
- All information is saved for the last seven days to evaluate your store’s statistics and improve its operation.

Preparing the installation

When preparing an installation with FLR-line products, there are a few things that should be taken into account:

- How many gates do you need to cover an entrance or door?
- Where are the gates relative to the environment to minimize interference (RF) and reflections (RFID)?
- The number of Power Inserters needed to power the system. Which cabling should be installed?
- Ready for an upgrade to RFID? Consider the number of Power Inserters when required, and you may want to lay the coaxial cables already in the floor for future RFID activation.
- Customer counting, Metal Detection, and RFID will only work within an aisle (between 2 gates).
- The firewall settings that need to be in place to enable Device Management.

Those requirements differ depending on which technology is used (RF, RFID, or both), so both technologies are described in a separate section.



If the gate is freestanding in a supermarket or hypermarket environment, take proper crash protection precautions. When customer guidance rails are available, you can place the antenna behind or after them to protect it against crashes.
When not available, use Nedap crash protection against damage from shopping carts.

Defining the system

When a store requires gates to be placed at several locations, there needs to be a decision on how to combine these gates into one or multiple systems. The following rules need to be taken into account:

1. **A different role is a separate system.** Combining gates for Electronic Article Surveillance (EAS) with gates from the stockroom to the sales floor is impossible in one system. Both roles need different systems with their own Power Inserter and customer network connection.
2. **Within the EAS role, all gates are combined into one system.** To minimize interference between gates, the Renos platform has a built-in synchronization mechanism for both RF and RFID technology. The gates must be connected to one system for this synchronization mechanism.
3. **However, the maximum cable length requirements must be considered.** If it is impossible to put all the gates within a role in one system due to the maximum cable length requirements, you can split the installation into two or more systems. In this case, assign each system a different *multi-system channel* during the RF configuration.



Build a separate system for the stockroom to the sales floor and goods receiving roles when there is a different door or entrance.

Role/Store Position	Product	Max. System Size (Gates)
EAS	RF Gates	100
	Hybrid RF/RFID	30
	RFID gates	30
Stockroom / Salesfloor	RFID gates	2
Goods receiving	RFID gates	2



It is not possible to combine gates with RFID and without RFID in one system. Either all gates should have RFID or no gates should have RFID.

Aisle width or detection distance

The next step is to determine how many gates you need. This depends on the system's detection distance (half the aisle width). There is no fixed answer to this question; it depends on many factors, such as customer expectations, the quality of the tags, the environment, etc.

The recommendations are based on the Nedap NT4040 (reference label) for RF and the Nedap RFID hard tag (for RFID).



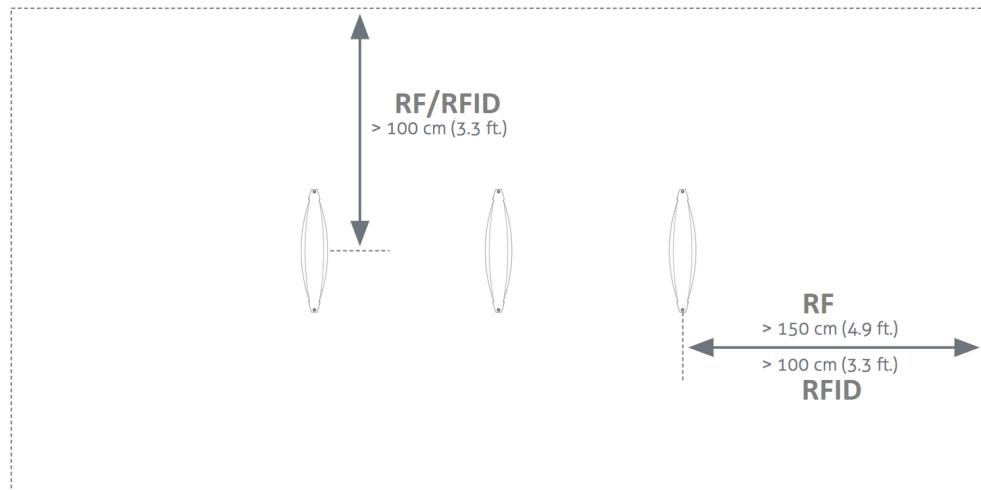
Please note that only the recommended aisle width is specified. Depending on the tag used and the environment in which the gates are placed, larger values can sometimes be achieved. You are advised to test this before using it in a store.

- For the FL30R gate, an aisle width of 170 cm (5.6 ft.) is recommended.
- For the FL45R gate, an aisle width of 200 cm (6.6 ft.) is recommended.

Label-free zone

Again, the recommendations are based on the Nedap NT4040 (reference label) for RF and the Nedap RFID hard tag (for RFID).

It is recommended that a label-free zone of at least 150 cm (4.9 ft.) for RF and 100cm (4.9 ft.) for RFID be created from the center of the gate behind the gate and 100 cm (3.3 ft.) into the store.

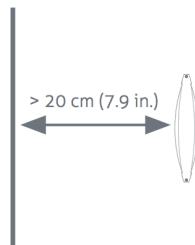


RF installation requirements

The operation of RF technology is affected by both coupling issues (the antenna couples with other objects) and active interference (other devices that transmit a signal around 8.2 MHz). Objects that cause coupling effects could be windows, doors, metal framing around the checkout, etc. Interference can be created by another RF system, LED drivers, or motors driving doors or roller shutters.

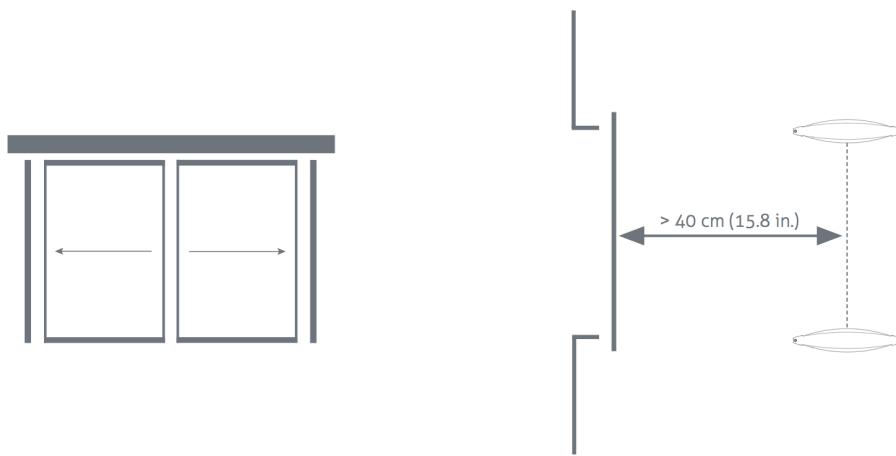
Take the following placement requirements into account when projecting the location of gates:

- There should be a minimum distance of 20 cm (7.9 in.) between the center of the gate and the wall.
- There should be a minimum distance of 200 cm (6.6 ft.) between 8.2 MHz tags and labels and the nearest antenna. If this is not possible, the labels and tags can be stored in a metal box at the checkout.



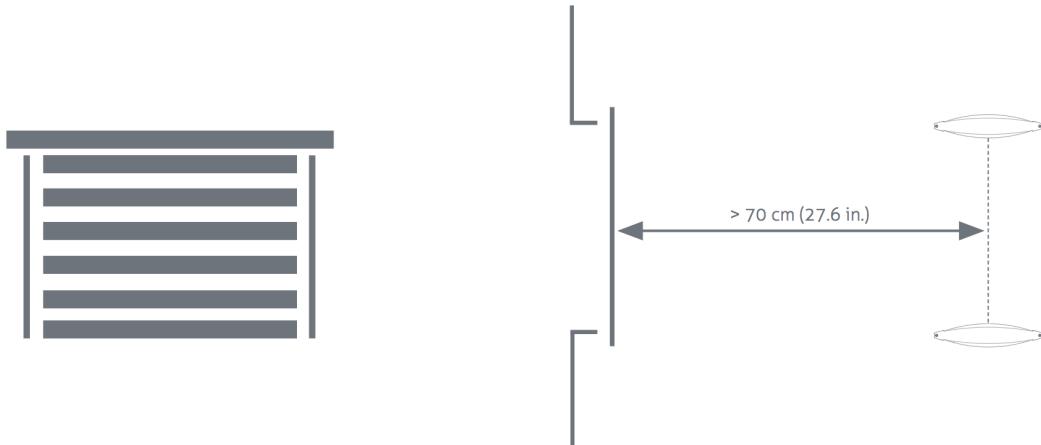
In addition, when **standard** or **sliding doors** are present:

- There should be a minimum distance of 40 cm (15.8 in.) between the center of the gate and the door.

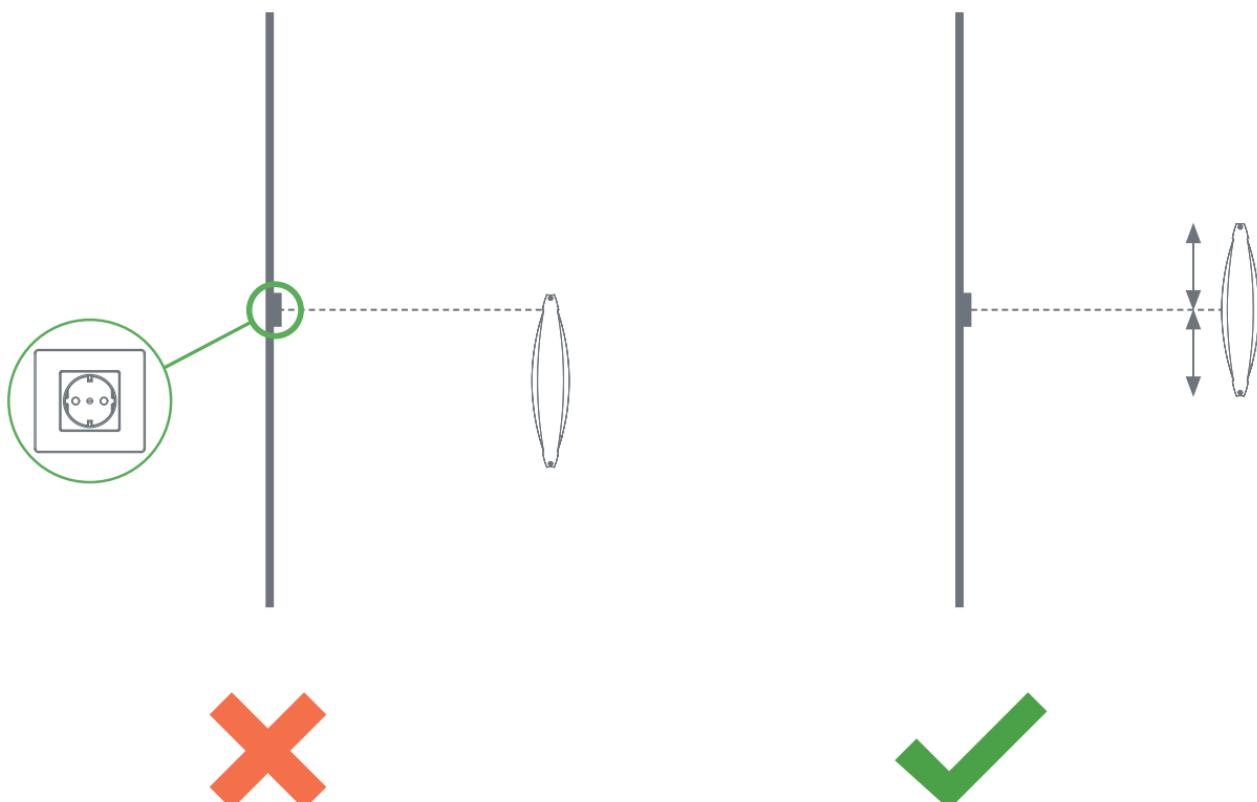


In addition, when a **roller shutter** is present:

- There should be a minimum distance of 70 cm (27.6 in.) between the center of the gate and the roller shutter.



If a power socket is less than 50 cm (19.7 in.) from the gate, the center of the gate should be aligned with the power socket.



Before installation, it is advised to gain information on the flooring below the antenna. If a dry-walk floor mat is used, it might have metal components that influence RF detection performance. In that case, a cut needs to be made in the floor mat to break conduction between the metal components and the antenna.

When the antennas are placed right next to a checkout that contains significant metallic parts, we advise always using a shield.



Please ensure there is no conducting connection between the gate and the checkout to prevent interference and coupling issues.

RFID installation requirements

When RFID technology is used, there are different installation requirements compared to RF technology. Since the RFID field is much less strictly defined than with RF technology, there is a larger area where tags could be detected. In comparison with RF, RFID is much less sensitive to coupling or interference issues.

Automatic tag muting

The RFID reader has a maximum performance. If this happens, the reader will mute some tags to have time for other tags. This feature is called *automatic tag muting*. Therefore, some tags in the system's surroundings might be muted and will not cause an alarm when moved through the gates.

Metallic surfaces

Metallic surfaces reflect the RFID field, which might confuse the Dynamic Beam Steering algorithms and influence (change or enlarge) the detection field. That is why it is advised to avoid metallic surfaces around RFID-enabled gates.

Power Inserter

Once the position of the gates is established, the location of the Power Inserters can be determined. A maximum number of Reno units can be connected to one Power Inserter, depending on which technologies are used and the number of add-ons in use. The table shows the number of Power Inserters needed for each hardware configuration.

Cable conditions: a CAT5E cable with a recommended maximum length of 80 meters / 250ft.

Technologies In Use	#Units / PI 230V	#Units / PI 115V
RF	6	5
RFID	5	5
RF + RFID	3	3
RF + MD	5	5
RF + 2 SD's	5	4
RF + MD + 2 SD's	4	4
RF + RFID + MD	3	3
RFID + MD	5	5
RF + RFID + MD + 2 SD's	3	3

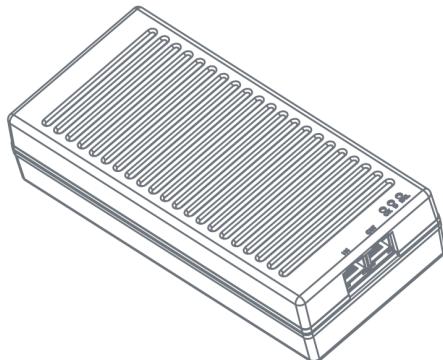
Index:

- RF = Radio Frequency 8.2 MHz
- RFID = RAIN Radio Frequency Identification (~900 MHz)
- MD = Metal Detection
- 2 SD's = 2 connected smart deactivators

- In all situations, it is possible to place Infrared beam sensors for, i.e., customer counting



Please note: Always use a Nedap Power Inserter (Power-over-Ethernet) to power Reno systems. It is not possible to use generic Power-over-Ethernet switches or stand-alone inserters.



If the retailer wants to upgrade an 8.2 MHz RF system to RFID later on, please consider the power requirements for RFID.



Make sure that the Power Inserter is connected to an always-on power socket! This is better for the firmware/hardware, continuous system monitoring, and remote firmware updates during the night.



Ensure the Power Inserter is placed at least 1 m (3.3 ft.) from the gates. When placed closer to the gate, it might cause interference with the RF technology.



Do not disconnect network cables in the system when still powered! First, disconnect the power cable from the power inserter(s).

Cabling

Now that the number of gates and Power Inserters is defined, the next step is to determine the system's cabling. Different cables are required depending on the technologies used.

The iSense FLR series uses a daisy chain setup, which means that all devices are connected as a chain:

1. a cable from a Power Inserter OUT to a Renos unit IN,
2. from that Renos unit OUT to the next Renos unit IN,
3. etc.

Technologies In Use	Cables That Need To Be Installed
Only RF	Ethernet cable between each unit and the Power Inserter
Only RFID	Ethernet cable between each unit and the Power Inserter RFID Coaxial cable (included with the product) between each unit in the same group
Both RF and RFID	Ethernet cable between each unit and the Power Inserter RFID Coaxial cable (included with the product) between each unit in the same group

If the system is connected to the customer network or Device Management, an Ethernet cable must be installed between the system and the customer network, or a 3G/4G router must be set up.

Cable specifications - Ethernet cable

The following cable specifications are recommended for the iSense system:

- Use UTP Cat5e with a stranded copper core, with 24 AWG (0,51mm) core diameter.

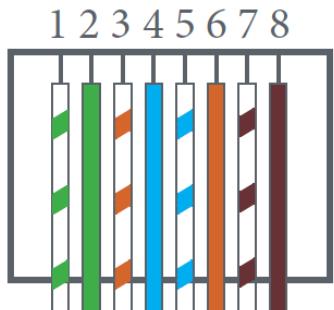


Always connect **all four pairs** using the **T568B** termination standard or T568A if specifically required!

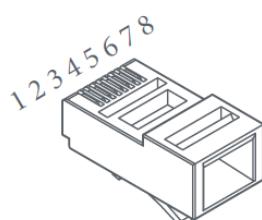
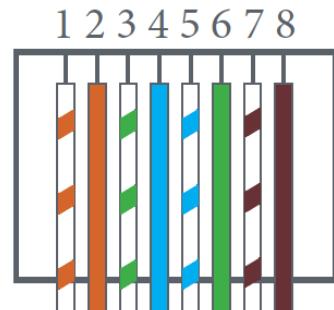


Never use CCA (copper cladding aluminum) or CCS/CCF (copper cladding steel) cable!

T568A



T568B



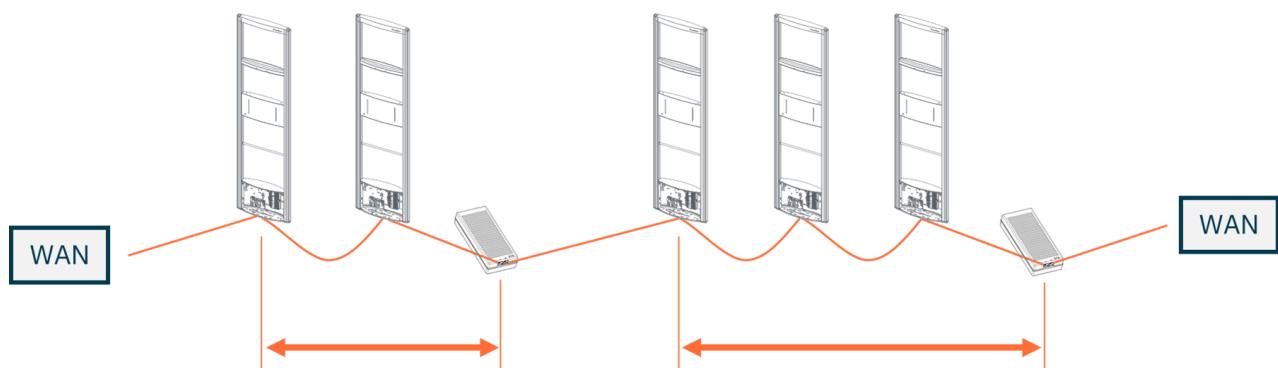
8P8C (RJ45)

Pin	T568A	T568B (Preferred)
1	Green + White	Orange + White
2	Green	Orange
3	Orange + White	Green + White
4	Blue	Blue
5	Blue + White	Blue + White
6	Orange	Green
7	Brown + White	Brown + White
8	Brown	Brown

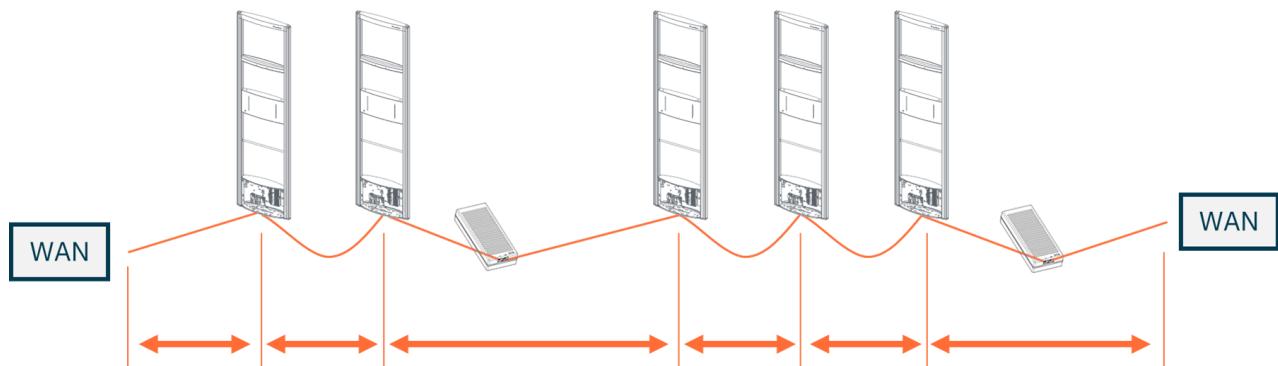
Cable length



Maximum cable length of **80 meters / 250 ft** between a Power Inserter and the last Renos unit that receives the power from this Power Inserter:



Maximum cable length of **80 meters / 250 ft** between Renos units (excluding Power Inserters) and between the first (or last) Renos unit and the WAN connection in the store:



Remarks

- It is possible to use your own preferred connectors.
- Make sure that the connectors are suitable for the cable and that the correct crimping tool is used for the connector.
- Follow the recommendations of the cable manufacturer.
- Local regulations may dictate using a specific cable type or rating.



We recommend placing the Power Inserter in the switch room (near a power socket) when the ethernet cable lengths allow. This way, the customer only has to arrange an ethernet outlet near the system.



If the cable lengths between two groups exceed approximately 50 meters / 164 ft, consider splitting a system into two.

RFID coaxial cable

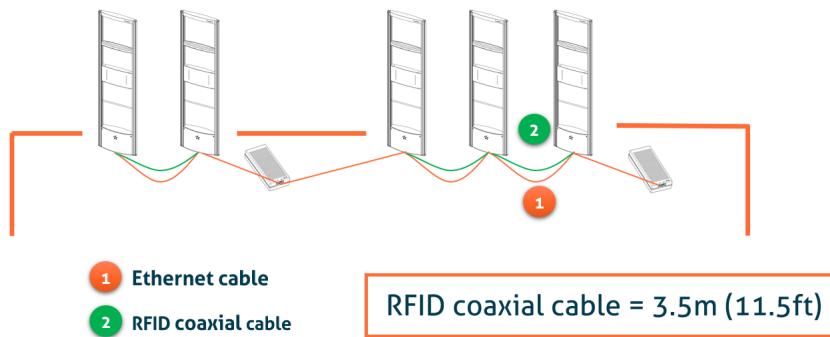
The RFID coaxial cable supplied with the product is 3.5 m (11.5 ft.) long. As the quality of this cable strongly influences the system's performance, it is supplied with every RFID gate. It is not possible to use third-party cables.



Only the RFID coaxial cable between units in the same group is necessary. An RFID coaxial cable is not required to connect groups.



The RFID coax cable has a fixed length of 3.5 m (11.5 ft.) to minimize signal loss. If the cable is not run through a slit but through a basement or other conduit, please check whether the path is not longer than approximately 2.5 m (8.2 ft.).



Cable Number	Type Of Cable	Required For RF	Required For RFID
1	Ethernet cable	Yes	Yes
2	RFID coaxial cable	No	Yes



Device Management

Nedap Retail systems can be connected to the online Device Management platform to ensure that systems can be managed remotely and work optimally globally.

The Nedap Device Management service provides four main functions on system level:

- **Monitoring:** Critical system parameters are monitored 24/7. If a system has issues, an alert is generated and sent to the supporting partner.
- **Remote Service:** using the Device Management website, an authorized Nedap-certified engineer can access the system's user interface to make changes to the configuration or access system logs.
- **Firmware Update:** an authorized Nedap-certified engineer can install new firmware releases remotely using the Device Management website.
- **Data Collection:** events per system are collected (e.g., to be displayed in the Analytics platform).
- **Sleep mode:** Enable sleep mode to conserve energy during nighttime hours, following the schedule configured in Device Management

For further details, please refer to the document on the portal about network information.

Executing the installation

When all the preparations are considered, the system can be installed. The installation consists of physically mounting the system in the correct orientation, installing the cabling, and applying power to the system.

Conduit or slit

We always suggest that you place a conduit, as this allows easy replacement of cables when necessary. If not possible, a slit can be made as well.



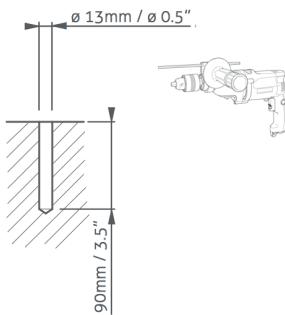
- When a system upgrades to RFID in the future, please install a conduit to add the RFID coax cable. You can also choose to install the RFID coax cable already. This is especially important when relying on a floor cut.

The conduit or slit in which the cables are placed should be precisely in the middle of the gate, perpendicular to the gate. This is explained in the following pictures.



Physical installation

Make sure the holes are marked on the floor in the correct locations according to the dimensions sketched earlier in this document. Drill the holes.



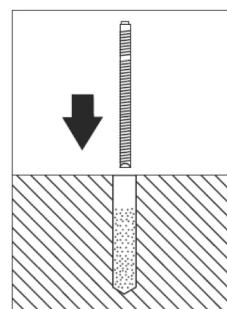
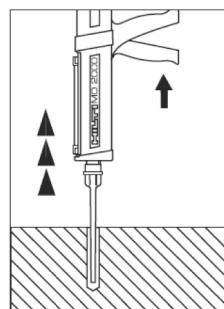
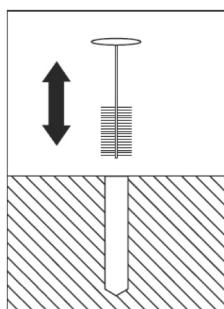
If RF technology is to be used, always keep enough space to place a shielding afterward. You will only know whether you need shielding when configuring the system (for example, when you find too much interference during the configuration).

Then, follow these steps to place the studs.

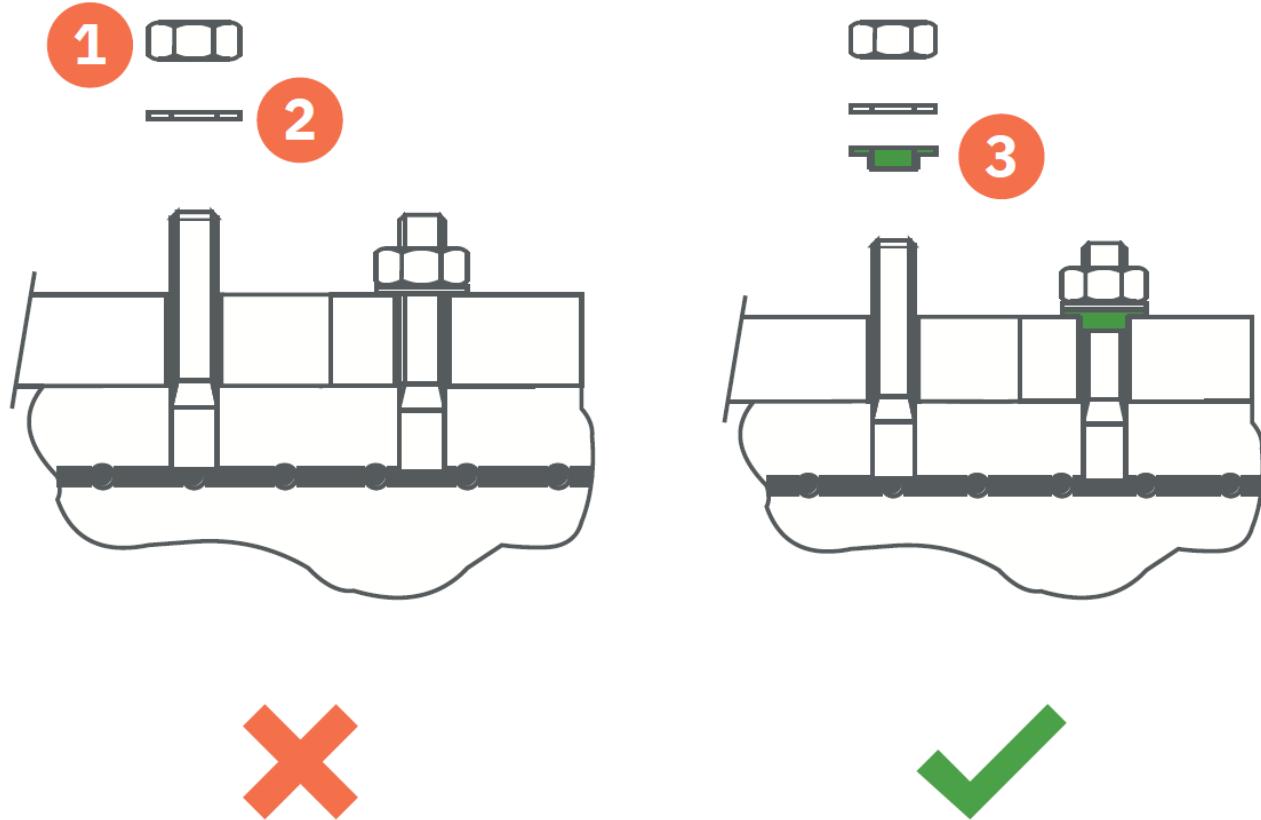
1. Clean the hole.
2. Insert Hilti-hit.
3. Place the stud.



Hilti-hit and studs are not included in the installation set.



Always use a nylon insulation ring to insulate the gate from the floor.



Number	Description
1	Nut M10 (not included in installation set)
2	Retainer ring M10 (not included in installation set)
3	Nylon insulation ring M10 (included in installation set)



If the gate is not adequately isolated from the floor, this might cause RF interference issues.

Orientation of products and the first gate

The gates must be orientated similarly for the system to function correctly, and the 1st power inserter should be connected to the correct gate. The orientation and gate 1 (the first gate to receive power from the first power inserter) can be determined depending on the role of the system as follows:

- EAS Role – Determine gate 1 by standing **inside the store and looking out towards the exit** (Power inserter on the right side of the first gate, and Renos should be on the left side of all gates)
- Goods movement role – Determine gate 1 by standing **inside the stock room and looking towards the store** (Power inserter on the right side of the first gate, and Renos should be on the left side of all gates)
- Goods receiving role – Determine gate 1 by standing **on the receiving dock and looking in towards the stockroom** (Power inserter on the right side of the first gate, and Renos should be on the left side of all gates)

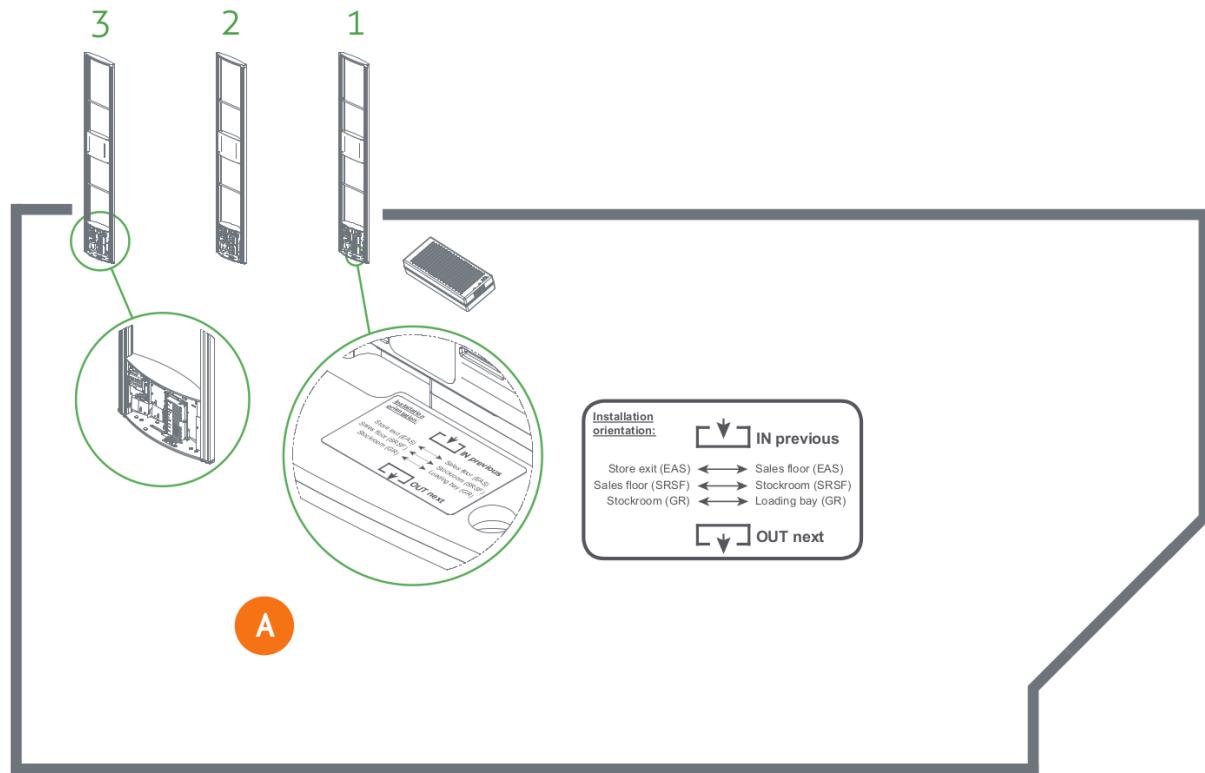


If this procedure is not executed correctly, the RFID technology will not work.

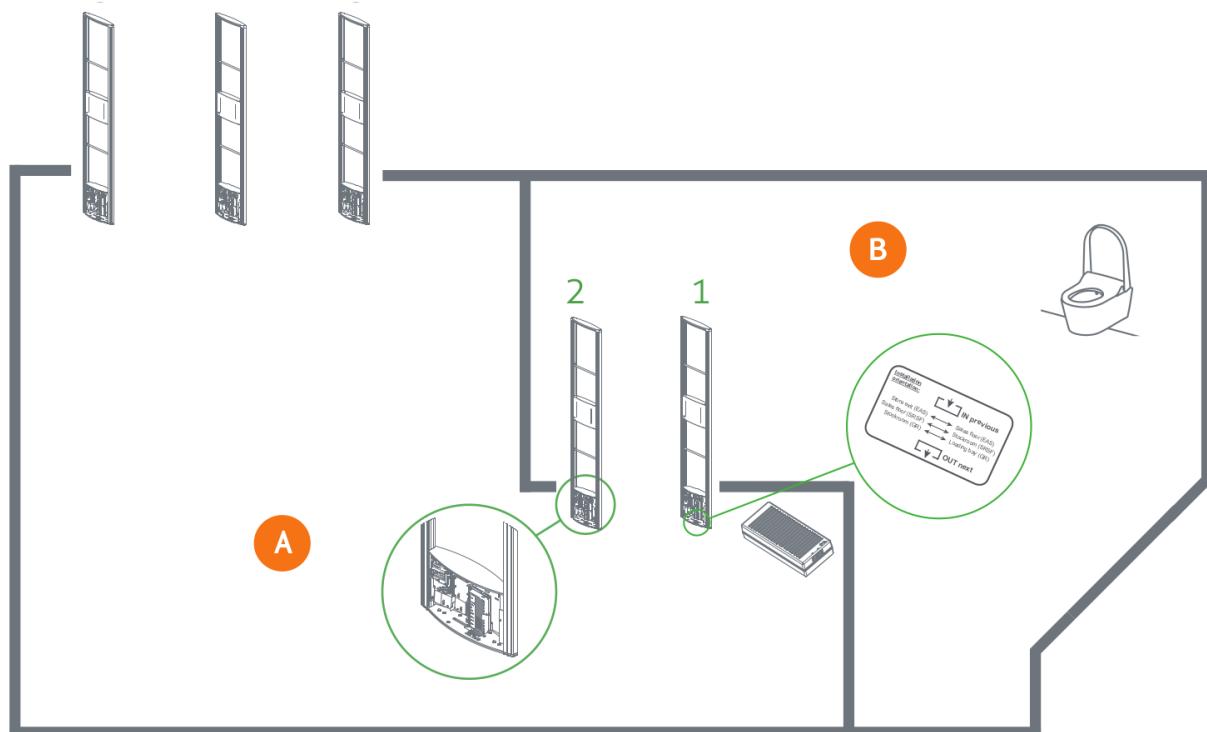
In the following examples, the location types in the table below occur.

Letter	Location Type
A	Salesfloor
B	Toilet
C	Stock room

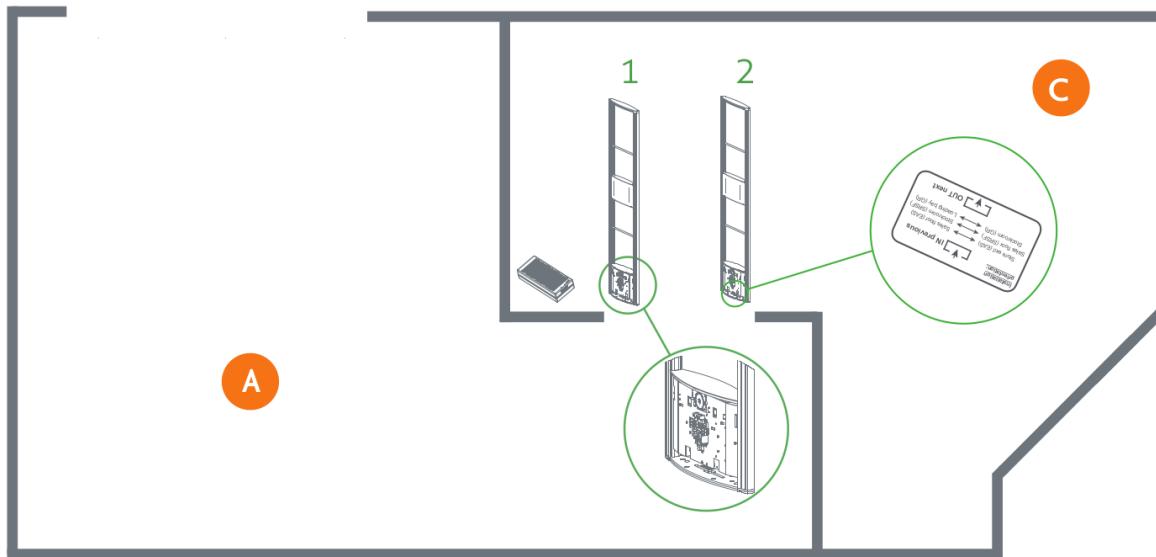
Example of EAS role



Example of EAS role, with toilet

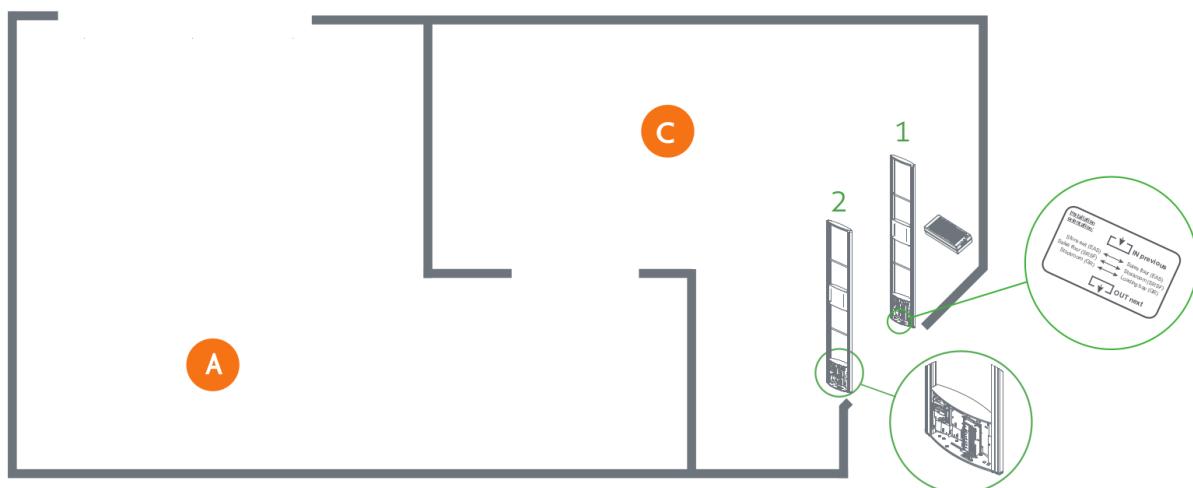


Example of stock room to sales floor role



Please note that when you compare the stockroom to sales floor role to EAS with the toilet, the orientation of the gates is precisely the opposite! This is because all gates should face the store's customer entrance/exit, except the toilet.

Example of goods receiving role



Installing cabling and filters

The exact cabling required was already determined during the preparation phase. Now, these cables can be placed.



All wiring should be done according to local regulations.

When cables are put in the slit or conduit, it is recommended to mark them with IN and OUT or PREVIOUS and NEXT, as this will allow you to distinguish them from each other.

Filters

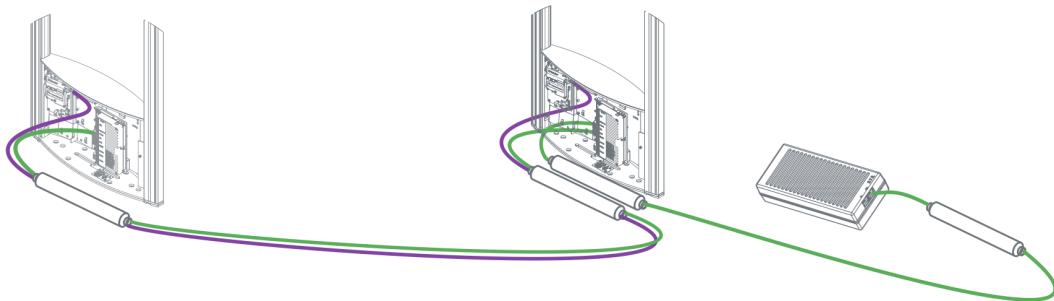
Please note that filters should be placed around the cables to reduce interference with other systems. These filters are delivered together with the system.

Filter should be placed at:

- Every Power Inserter: around the Ethernet cable at the OUT and IN ports.
- Every Renos unit is around the Ethernet and RFID coaxial cables (when used) at the OUT and IN ports.
- Every 9 m (30 ft.) for longer Ethernet cables.



Place the filters **before** attaching the connectors. The other way around is not possible.



Nedap offers the opportunity to order filters as spare parts. For more information, please visit the Nedap Retail Portal.

The filters close to a Renos unit should be placed inside the foot of the gate. If multiple filters are at the foot of the gate, they should be tied together.

Ethernet cables

Connect the Ethernet cable from the OUT port of the Power Inserter(s) or the Renos unit with the IN port of the next Renos unit.



Please test every Ethernet cable for correct connections and pair all four pairs (8 wires) with an Ethernet cable tester to ensure that the system can function correctly.

After the ethernet cables are connected, power up the Power Inserters.

RFID coaxial cable

If the Ethernet cable is connected, connect the RFID coaxial cable similarly. Connect from Gate 1 (next) to Gate 2 (previous), from Gate 2 (next) to Gate 3 (previous), etc.

The RFID coaxial cables should be connected from the NEXT port of one reader to the PREVIOUS port of the second reader. PREVIOUS and NEXT are related to the order of units about the first Power Inserter.



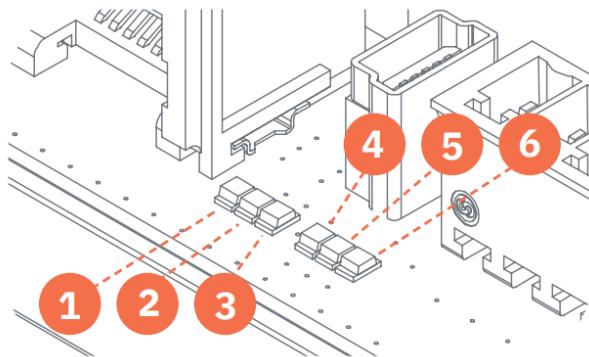
Please avoid making sharp bends in the RFID coaxial cable. This will affect the system's performance.



Don't use a tool to tighten the RFID coaxial cable connectors. This is not necessary and might break the connectors. If the connector is drawn by hand, that is good enough.

Renos Status LEDs

The electronics inside the unit have several status LEDs that can be used to discover the status of each part of the electronics.



Status LEDs of the Renos unit

LED	Color	Status	Explanation
1	Green	On	There is a Renos unit connected to the OUT port of this unit
		Off	There is no Renos unit connected to the OUT port of this unit
2	Blue	Blinking	There is no device connected to the OUT port of this unit
		On	There is a Power Inserter connected to the OUT port of this unit
3	Red	On	There is an issue with the power supply at the OUT port of this unit (too little current drawn)
		Blinking	There is an issue with the power supply at the OUT port of this unit (too much current drawn)
		Off	There is no issue with the power supply at the OUT port of this unit
4	Yellow	Blinking	The operating system on the Renos unit is running
		Off	The operating system on the Renos unit is not running
5	Green	Blinking	The storage flash on the Renos unit is accessed
		Off	The storage flash on the Renos unit is not accessed
6	Green	On	The firmware on the Renos unit is running

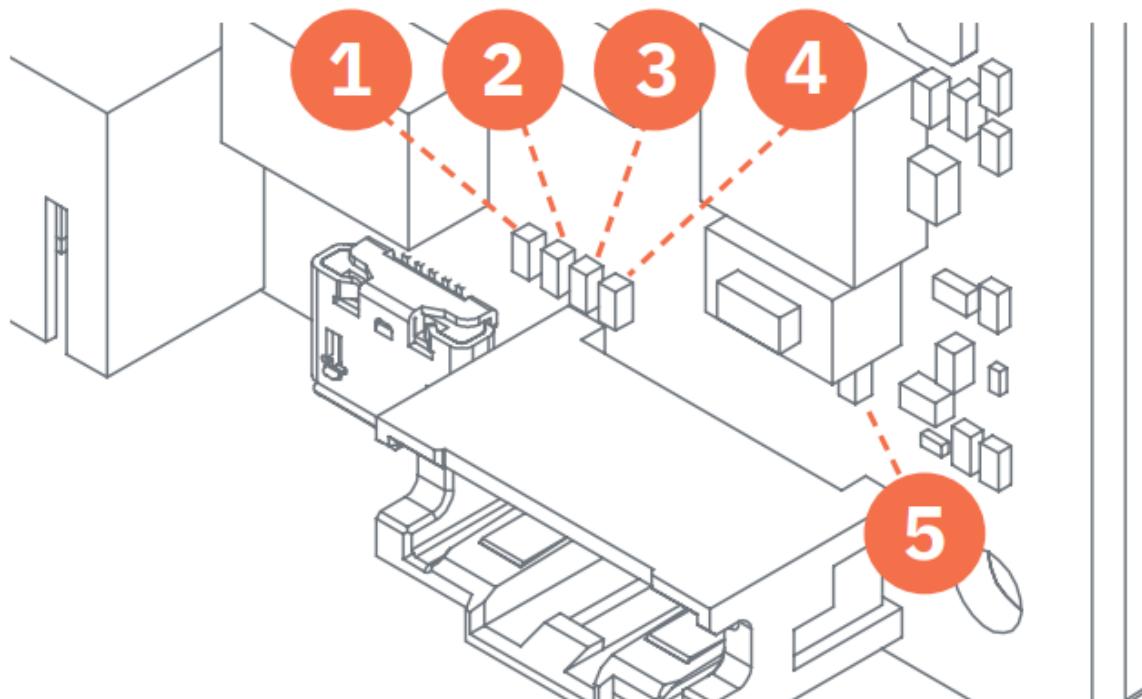
LED	Color	Status	Explanation
		Off	The firmware on the Renos unit is not (yet) running

Please look at the Troubleshooting chapter later in this manual to resolve erroneous conditions.



- If the Renos unit has a firmware error, the rightmost three LEDs (4, 5, and 6) will remain off when powered. This can be solved using a 'Local - single unit' firmware update, as described in the "iSense firmware version manual."

RFID reader



LED	Color	Status	Explanation
1	Blue	On	The RFID Reader is connected to the Renos firmware
		Blinking	The RFID Reader has received a command from the Renos firmware
		Off	The RFID reader is not connected to the Renos firmware
2	Orange	Blinking slow	The firmware on the RFID Reader is running
		Off	The firmware on the RFID reader is not running
3	Red	On	There is an error with the RFID output
		Off	There is no error with the RFID output
4	Green	On	The RFID output is active
		Blinking	The reader is reading RFID labels
		Off	The RFID output is not active
5	Green	On	The Renos unit powers the RFID reader
		Off	The Renos unit does not power the RFID reader



The RFID reader will not be active when the system has not been configured yet. This means that only the 'firmware running' orange LED is blinking.

Configuring the installation

The following tools are required to complete the configuration.

- Mini-USB cable.
- Laptop with installed driver and recent browser.

Driver installation

A Windows driver needs to be installed to configure an iSense system. Please check the table below for what is required based on your operating system.

Operating System	Driver
Windows	Download the driver from the portal.
Mac OS X	You don't need to install a driver.
Linux	You don't need to install a driver.

Once you have installed the driver, please check if it works by plugging it into a Renos unit.

Supported browsers

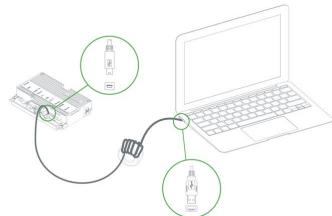
To configure the system, the latest versions of the following browsers are supported:

- Google Chrome
- Mozilla Firefox
- Apple Safari

If you don't have one of these browsers installed on your laptop, please install them before the installation.

Connecting a laptop to the Renos unit

You can connect your laptop via a Mini-USB cable to the service port on the Renos unit. In the iSense system, you can choose any Renos unit.



We advise using a good-quality USB cable about 5m / 16ft long. This provides more comfort during the configuration, as you can find an excellent place to put your laptop (instead of on the stairs or the floor next to the gate). Besides, some laptops interfere with RF technology, so it is better to place them further away.



We advise configuring Renos using a ferrite ring core filter around the mini USB cable. These can be ordered as spare parts with Nedap. Please take a look at the Nedap Retail Portal for more information.

Entering the configuration wizard

You can enter the configuration wizard by opening your browser and navigating to:

<http://192.168.133.1>



Ensure no other network connections are active in the same range.



Authentication

During the configuration, the user is required to authenticate himself. How this is done is dependent on the availability of Device Management.

- The system is connected to Device Management: you can enter your Nedap Retail username and password directly.
- The system is not connected to Device Management, and you don't have a Nedap Retail authentication software: choose one of the following steps:
 - If your laptop can connect to Device Management via a 4G/5G router or Wi-Fi, you can use this option to enter your username and password.
 - If that is not available, you can use your smartphone.
 - If your smartphone has no internet access, call your main technician for an authentication code.

Please reach out to support for more details on how to obtain a Nedap Retail username and password.

Getting help in the wizard

If something needs clarification, each page has a question mark button in the top right corner. You can click this to get more information on what is expected to do on a specific page.

Factory reset and Firmware change

It is essential to use the latest firmware version and start new installations with factory default units.

Details on how to perform a firmware update and factory default can be found in separate guidelines on the Partner Portal:

- iSense firmware version manual
- iSense factory reset procedure

Firmware change

There are four ways to change the firmware version on a Renos-based system:

1. Local—single unit overwrite. To execute the overwriting, insert a USB stick with the correct firmware into the USB port.
2. Local—complete system overwrite. You can execute the overwriting with files on your laptop during the configuration wizard.
3. Local - complete system update. The update can be executed during the configuration wizard with files on your laptop.
4. Device Management update. The update can be executed via the Device Management service.

Factory default

There are two ways to factory default a Renos-based system:

1. Local - single unit over-write. The factory default can be executed using a USB cable to connect the USB port to the service port.
2. Local - complete system factory default. The factory default can be executed during the configuration wizard.

System ID

You need the System ID to set up a Device Management system. The firmware version is displayed in the top right of the configuration wizard. If you click the firmware version, a pop-up shows the System ID during the configuration.

Integrating the installation with other systems

Integrating the iSense product into other solutions by the end customer is highly recommended.

Software integration with local APIs

The Renos platform offers local API endpoints for data analysis and status information. For more information, please refer to the Software Integration page on the Nedap Retail portal, which includes documentation and examples.

Physical integration using an IO Box

Integrating other systems via relay contact outputs and inputs is also possible. The Renos unit does not provide this directly; however, it can be accomplished via a 3rd party IO Box.



The following 3rd party IO Box is currently supported: **MOXA ioLogik E1214**.



The IO Box should be connected to a Renos unit via a USB to Ethernet adapter.

An output on an IO Box can be activated when specific events occur, depending on the capabilities of the chosen hardware.

URL trigger

The URL trigger mode can be used to trigger network-based devices with an HTTP-based API. Make sure that the iSense system can reach this device.

Servicing the installation

When the installation has been completed and delivered, it can be serviced via Nedap Device Management. We also provide monitoring options locally via SNMP.

Device Management

Nedap Retail systems can be connected to the online Device Management platform to ensure that systems can be managed remotely and work optimally globally.

The Nedap Device Management service provides four main functions on system level:

- **Monitoring:** Critical system parameters are monitored 24/7. If a system has issues, an alert is generated and sent to the supporting partner.
- **Remote Service:** using the Device Management website, an authorized Nedap-certified engineer can access the system's user interface to make changes to the configuration or access system logs.
- **Firmware Update:** an authorized Nedap-certified engineer can install new firmware releases remotely using the Device Management website.
- **Data Collection:** events per system are collected (e.g., to be displayed in the Analytics platform).
- **Sleep mode:** Enable sleep mode to conserve energy during nighttime hours, following the schedule configured in Device Management

For further details, please refer to the document on the portal about network information.

SNMP

Simple Network Management Protocol (SNMP) is available to allow for local monitoring of iSense systems. For example:

- One or more Renos units are not reachable
- The system is connected to Device Management

iSense systems use SNMP version 2c, community public. The MIB file is available on the iSense system itself via the URL [http://\(ip address of the system\)/snmp](http://(ip address of the system)/snmp) (for example, that is **http://192.168.133.1/snmp** when connected to the USB service port).

Troubleshooting

If the system is malfunctioning, please check the troubleshooting options below. If you still can't solve your issue, you can find support options in the next chapter.

Physical installation

Symptom	Cause	Solution
The red LED (3) on a Renos unit is on.	The current drawn-out of the OUT port of the Renos unit is too low. The cabling at the OUT port of the Renos unit does not satisfy the maximum length requirements.	Verify whether the cabling length in the system satisfies the requirements posed earlier in this document.
	The current drawn-out of the OUT port of the Renos unit is too low. The connectors of the Ethernet cable at the OUT port of the Renos unit are not mated properly.	Check the Ethernet cable at the OUT port of the Renos unit with an Ethernet cable tester.
The red LED (3) on a Renos unit is blinking.	The current drawn-out of the Renos unit's OUT port is too high. There are too many Renos units and add-ons connected to one Power Inserter.	Verify the number of Renos units and add-ons connected to the Power Inserters with the table earlier in this document.
	The current drawn-out of the Renos unit's OUT port is too high. A short circuit in the cabling leaves this Renos unit's OUT port.	Check the Ethernet cable at the OUT port of the Renos unit with an Ethernet cable tester.
The green LED (1) on a Renos unit is off, but there is a unit behind this unit.	There is an issue in the cabling between those units, so the following unit is not recognized.	Check Ethernet cabling with an Ethernet cable tester.
The red LED (3) on the RFID reader is on.	The RFID reader is having trouble starting to read. An erroneous antenna or a cabling error might cause this.	Log in to the Renos configuration interface to see the exact error.

Configuration

Symptom	Cause	Solution
It is not possible to access the configuration web interface.	Renos unit has not started yet.	Verify the green "firmware running" LED on the Renos unit (6). If this LED is not on, verify the system has power, or wait five minutes and try again.
	Mini USB cable not attached to Renos unit and laptop	Attach the cable to Renos unit and laptop.
	Driver not installed	On Windows 7 and older, you manually install a driver to support Renos.
I have put a system together, but during the hardware discovery, I see only part of all the units.	The WAN access port will be 'closed' for internal network traffic during configuration. If you combine two systems later on, this needs to be re-opened.	Do a factory reset on the previously used WAN entry point unit. If that doesn't work, do a factory reset on all units.
	There is a cabling error.	Please check all Ethernet cabling with an Ethernet cable tester.
	Not all Power Inserters are powered, or some Renos units are not fully started.	Verify the green "firmware running" LED on the Renos unit (6). If this LED is not on, verify the system has power, or wait five minutes and try again.
The Renos unit's all three LEDs, 4, 5, and 6, are off, indicating a firmware failure.	Something might have gone wrong with a firmware update.	The 'local - single' unit firmware update mechanism restores the unit.
I have configured RFID, but it detects labels outside the aisle, not inside.	Gates are positioned the wrong way.	Check the "Orientation of products" section in the manual and correct the orientation of the gates.

RF technology issues

When there are issues with RF technology during the configuration (the gates show as orange or red in the wizard), please follow the following steps:

1. Check the parameters in the RF Advanced Config of the configuration wizard and the RF gate performance section. One of those parameters is probably red or orange.
2. Disable all transmitters.
 - a. If all parameters in the RF gate performance section turn green again, a coupling problem exists (the transmitter couples with a label-like object in the environment). Please continue to the 'coupling problem' section.
 - b. If all parameters in the RF gate performance section remain orange or red, there is an active interferer (another device that transmits radio waves around the 8.2 MHz RF spectrum, like another EAS system, an engine, or a power supply). Please continue to the 'active interferer' section.

Coupling problem

Coupling problems are caused by objects that act as labels to the RF system. This includes metallic doorframes, checkouts, and cabling—everything that runs in a loop and is metallic.

To solve these problems, there are a few things you can try:

- Tighten screws in the metallic construction. This might work for checkouts or customer guidance rails.
- Try to interrupt the metallic loop. This can be done by using non-metallic parts inside those loops or by making a cut in them.
- Create a shortcut in the metallic loop to make it smaller. This will make it resonate at a different frequency.

If the above solutions don't solve the problem, you can decrease the system's sensitivity by ticking the 'reduced sensitivity' button in the RF Advanced Config.



If a decreased sensitivity doesn't work, and there is only one type of label or tag in the store, you also have the option to increase the 'receiver delay.' When higher than 6dB, the label detection will be limited.



The problem could also be solved with additional hardware (not available for all gates):

- **A 3-loop only 50 ohm PCB.** This will work when the coupling loop is located in the middle height of the gate.

- **Shielding.** This will work in many cases. However, the detection distance will be reduced by about 20 cm (0.7 ft.). The field will also slightly creep around the shield. This is called 'back detection'.



The 3-loop only 50 ohm PCB is only available in Europe with CE-certified products. Using it in other regions invalidates the local certifications.

If these things don't solve the problem, please contact support.

Active interferer

The first step is to locate the active interferer's source. You can do this by unplugging electronic devices around the gate (or moving them away) and seeing if the parameters in the 'RF gate performance' section improve or when the average height of the spectrum is reduced. If this is the case, you have identified the active interferer.

When the active interferer is known, the following solutions are possible:

1. Try to move the active interferer away from the gate as far as possible.
2. Try to apply filters around the cabling of the active interferer.
3. Shield the active interferer with aluminum foil.

If the above solutions don't solve the problem, you can decrease the system's sensitivity by ticking the 'reduced sensitivity' button in the RF Advanced Config.



The problem could also be solved with additional hardware:

- **A shielding.** This will work in a lot of cases. However, the detection distance will be reduced by about 20 cm (0.7ft.). The field will also slightly creep around the shield. This is called 'back detection'.



There are also round ferrites available that can reduce active interference sources and find ferrites with optimal impedance at around 8.2MHz.

If these things don't solve the problem, please contact support.



Warranty and spare parts

- Please consult the Nedap Retail Business Partner from whom you purchased this product regarding the applicable warranty conditions.
- This product cannot be used for any other purpose described in this document.
- If the product is not installed according to this document, the warranty provided is not applicable.
- At the sole discretion of Nedap N.V., Nedap N.V. may decide to change the conditions of Page 7 of 19 Compliance information for technical manuals warranty policy.
- You agree that Nedap N.V. can compensate you for the pro-rata value of the warranty involved rather than replacing or repairing the product based on its technical or economical value.
- Prior to applying the warranty, please verify that you comply with the warranty conditions of the warranty policy and that you can successfully apply for the replacement or repair of a defective part.
- Parts can only be replaced with original Nedap parts; otherwise, the warranty policy will not apply to the product.
- If the warranty is applicable, please contact the dealer or send the defective parts to the dealer.

Regulatory information

FCC and IC Compliance Statement

This device complies with part 15 of the FCC Rules and RSS210 of Industry Canada. 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.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Cet appareil se conforme aux normes CNR210 exemptés de license du Industry Canada. L'opération est soumis aux deux conditions suivantes:

- (1) cet appareil ne doit causer aucune interférence, et*
- (2) cet appareil doit accepter n'importe quelle interférence, y inclus interférence qui peut causer une opération non pas voulu de cet appareil.*

Les changements ou modifications n'ayant pas été expressément approuvés par la partie responsable de la conformité peuvent faire perdre à l'utilisateur l'autorisation de faire fonctionner le matériel.

FCC and IC Radiation Exposure Statement

This equipment complies with FCC and Canadian radiation exposure limits for an uncontrolled environment. It should be installed and operated with a minimum distance of 20 cm between the radiator and your body. This transmitter must not be co-located or operated with any other antenna or transmitter.

Cet équipement est conforme a CNR102 limites énoncées pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et votre corps.

This Class B digital apparatus complies with Canadian ICES-3. Cet appareil numérique de Classe B est conforme à la norme Canadienne NMB-3.

FCC Information to the user

Note: This equipment has been tested and found to comply with the limits for class B digital devices, according to part 15 of the FCC Rules. These limits are designed to protect reasonably against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency

energy and, if not installed and used following the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. Suppose this equipment does not cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on. In that case, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from the receiver's.



Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. To ensure compliance with FCC regulations, use only the shielded interface cables provided with the product or additional specified components or accessories that can be used to install the product.

Information for Taiwan

第十二條 經型式認證合格之低功率射頻電機，非經許可，
公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；
經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信法規定作業之無線電通信。
低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

CE WEEE

This European Standard specifies a marking:

- of electrical and electronic equipment following Article 11(2) of Directive 2002/96/EC (WEEE); This is in addition to the marking requirement in Article 10(3) of this Directive, which requires producers to mark electrical and electronic equipment put on the market after 13 August 2005 with a 'crossed-out wheeled bin' symbol.
- that applies to electrical and electronic equipment falling under Annex IA of Directive 2002/96/EC, provided the equipment concerned is not part of another type of equipment that does not fall within the scope of this Directive. Annex IB of Directive 2002/96/EC contains an indicative list of the products that fall under the categories set out in Annex IA of this Directive;



- that identifies the equipment producer clearly and that the equipment has been put on the market after 13 August 2005.

CE - UKCA Declaration of Conformity

With this, Nedap N.V. declares that the subject equipment is in compliance for CE with directives 2014/53/EU (Radio Equipment Directive) and 2011/65/EU (RoHS). And for UKCA with SI 2017/1206 (radio Equipment Regulations 2017) and with SI 2012/3032 UK Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 (RoHS). The full text of the declarations of conformity is available at the following internet address: <https://portal.nedapretail.com/>, where, if applicable, REACH information can also be found.

Disposal of this product

This product's owner or last user is responsible for properly disposing of (parts of) the product as required by local rules and regulations.





About Nedap

Together, we make merchandise simply available

At Nedap, we believe in ‘Technology for Life’. Nedap Retail enables retailers to serve their customers better. Using technology, we allow for perfect inventory visibility, total control, no waste, and no losses.

Our vision for inventory visibility

Today, established retailers need more information about where their items are. Without this knowledge, providing an omnichannel experience leads to heavy overstocking, waste, and eroding margins. Solving this requires a fundamental change in the retailers’ supply chain and information systems.

Our mission is to simplify the process of ensuring that retailers always have the right products available at the right place and time.

We do this by giving retailers perfect inventory visibility for a seamless shopping experience. This way, retailers can meet the changing consumer needs while remaining profitable.

Nedap works with the largest and most successful retailers in the world. We take complete ownership of our projects—failure is never an option. A unique combination of the best technology and industry teams at Nedap Retail achieves this.

Nedap solutions are built upon 45 years of global experience, market expertise, and close cooperation with leading retailers. A flexible network of certified partners worldwide supports our worldwide operations. Nedap systems are future-proof (RFID-ready), cost-efficient, and Eco-friendly. Our mission is to ensure retailers' customers maintain the best shopping experience while we help retailers protect their profits.

Contact

If you need further details or help preparing, executing, or servicing an installation, please contact our support team at support-retail@nedap.com.

Suggestions for improving our products and documentation are much appreciated.

Disclaimer

Nedap disclaims all responsibility for any loss, injury, claim, liability, or damage resulting from, arising out of, or in any way related to any errors in or omissions from this document and its content, including but not limited to technical inaccuracies and typographical errors. We only vouch for the goods being fit for the use intended by the purchaser, even if that use should have been mentioned to us if we have committed ourselves in writing.

Copyright © Nedap NV 2025

All rights reserved. No part of this document may be reproduced or distributed in any form or by any means or stored in a database retrieval system without the prior express permission of the copyright holder. No part of this document may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the publisher.

Document Version 292

Document Last modification date 19 March 2025

Document PDF Exported 21 March 2025 by Nedap Retail | Operations



support-retail@nedap.com

Nedap Retail
Parallelweg 2
NL7141 DC Groenlo
The Netherlands

nedap-retail.com

