VTAP100

Installation Guide - VTAP100 Wiegand Reader

VTAP100-PAC-W

Revised February 2025 v3.31

DOT ORIGIN

If you need help to set up or use your VTAP100, beyond what is contained in this Installation Guide, then please contact our support team.

Email: **vtap-support@dotorigin.com**

Download the latest documentation and firmware from **https://vtapnfc.com**

Telephone UK and Europe: +44 (0) 1428 685861

Telephone North America and Latin America: +1 (562) 262-9642

If you have any feedback on setting up or using your VTAP100 or this documentation, then please contact our support team. The product is constantly being reviewed and improved and we value feedback about your experience.

Dot Origin Ltd
Unit 7, Coopers Place Business Park, Combe Lane, Wormley
Godalming GU8 5SZ United Kingdom
+44 (0) 1428 685861

Contents

Safety instructions

WARNING: INTENDED USE

The VTAP100-PAC-W are boxed products for end-users. Although the enclosure may be opened when the device is not connected, components mounted on the VTAP PCB are not user-serviceable.

WARNING: ESD PRECAUTIONS

If the enclosure is opened to access the PCB, we recommend careful handling of Electrostatic Sensitive Devices (ESDs) .

WARNING: POWER SUPPLY

Use a standard micro-USB cable to connect the VTAP100-PAC-W model to a PC or **alternatively** power the unit by connecting it to an access controller, using the Wiegand connector cable. If the VTAP100 is being powered through its Wiegand connector, you can still make an additional USB data connection to a PC, provided that the PC is already powered before the connection is made.

EMC emissions and immunity certifications are only valid when using the VTAP100-PAC-W with the supplied cable.

1 Using this guide

This guide is for first-time users of the VTAP100-PAC-W.

Figure 1-1 VTAP100 in compact (-CC) or square (-SQ) case

It contains the information you need to install your VTAP100.

Consult the VTAP Configuration Guide for more about custom configuration and maintenance features for any VTAP100, including how to update the firmware on your VTAP100-PAC-W, when a new release is available.

If you need help beyond what is contained in this guide please contact **vtap-support@dotorigin.com**.

2 How the VTAP100 works

With the VTAP100-PAC-W connected to a PC, simply tap your smartphone against the VTAP. Your mobile NFC pass will be read and data sent to the connected PC. The extra facility with the VTAP100-PAC-W model only, is that it can alternatively be connected to an access controller, using the Wiegand connector supplied.

Of course, the data can only be read if your phone contains a mobile NFC pass, which has been issued in connection with the Merchant ID(s)/Collector ID(s) and ECC key(s) that are known to the VTAP. The unit comes with default values, so that you can test **Default operation on factory settings** before you begin customising any settings.

When the VTAP100-PAC-W is connected to a computer via USB cable, it appears as a generic mass storage device (like a memory stick). To configure your VTAP, you simply edit or create text files. These will be read automatically, and control the operation of the VTAP. There is information in **Provide pass reading parameters and keys** to take the first steps to configure your VTAP for use. The VTAP100-PAC-W must be configured over USB from a PC, before it will send pass data over the Wiegand interface. After being configured it does not need to be connected to a PC. Consult the VTAP Configuration Guide for more detail.

By default the VTAP is fully upgradable in the field. However, the VTAP can be locked in software or hardware, before deploying the unit, so that operation is no longer easily changed.

2.1 Default operation

Before anyone changes the configuration from its default, you can confirm that the unit is working.

These steps demonstrate that the hardware can detect and interact with an OriginPass demo mobile NFC pass, which is ready to work with the default configuration of your VTAP100.

1. Obtain an OriginPass from Dot Origin by visiting **https://originpass.com/VTAP/** and add it to Google or Apple Wallet. (You will require a username and password - contact **vtap-support@dotorigin.com** to get these.)
2. Connect the VTAP100 to your PC, using a USB cable.
3. Open a text editor, such as Windows Notepad.
4. When you tap the OriginPass on the VTAP100:
   - Pass contents will be displayed in the open text editor, through keyboard/barcode emulation.
   - The feedback LEDs on the VTAP100 PCB will flash green.
   - Your smartphone may signal with a buzz or beep.

> **Note:** Some Android phones will only interact if their screen is on, although it does not need to be unlocked. You may need to enable NFC in the settings for the smartphone.

> **Note:** If the pass detected does not match the key and ID on the VTAP, or is moved away too quickly to be read, the pass contents displayed may be an 8 digit random hex string, such as '08E22AC1', different on each presentation. OriginPass contents will be a consistent string, such as '3~ffymeK9f_mziYtA6~53999301628695~Valued'. Any separator, such as '~' or '|', will depend on your keyboard language settings. (See VTAP Commands Reference Guide for option to ignore random UIDs if needed.)

> **Note:** If local security settings prevent or limit the use of removable storage devices, or the connection of additional keyboards, an administrator may need to alter those permissions.

2.2 Start reading your own passes

If you navigate to the VTAP in the computer's file system, it will appear as an attached mass storage device and list the files contained, including the main `config.txt` file.

To read any mobile NFC pass, you will need to provide your pass reading parameters in the `config.txt` file. This means a collector ID or merchant ID and ECC keys. These allow you to read and decrypt pass data that is held by your users, on their smartphones. (There is a VTAP Application Note which explains more about ECC key pairs and how to generate your own keys.)

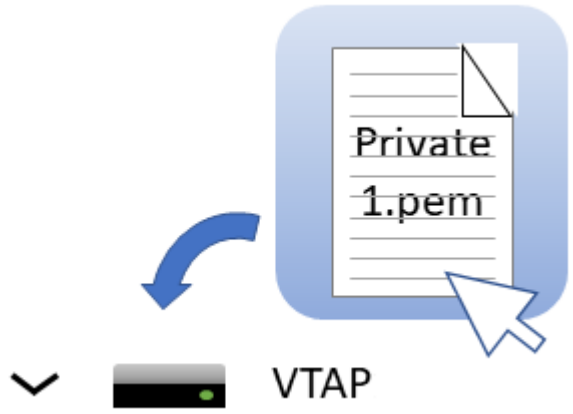
This first time, you will need to connect the VTAP100 to your PC, using a USB cable. (If needed, you can make changes remotely in future over a virtual COM port or serial port, see VTAP Serial Integration Guide.)

Step 1: Upload private key file(s) to your VTAP100

1. Ensure these are ECC private key(s). Each is stored in a file with the name `private#.pem`, following the `.pem` format, where `#` is replaced with a number from `1` to `6`, matching the key slot you will save it in. (The demo passes are accessed using the key in KeySlot 6, so don't overwrite this one unless you are finished with Dot Origin demo passes.)

   Note: A VTAP reader cannot use more than 6 private key files.

2. Load your keys by copying these files onto your VTAP100, which shows up in the file system of your PC as a mass storage device.



Note: When you reboot the VTAP100 your key will have been stored in hardware, and will no longer be listed as a file on the device. You can confirm key file(s) have been loaded when you **Check status in Boot.txt**. If the key file does not disappear and there is an error in `Boot.txt`, check your `.pem` file as it is likely it did not adhere to the standard - perhaps it was not an ECC key?

Step 2: Declare Merchant ID(s)/Collector ID(s) in the `config.txt` file

1. Open the file `config.txt` in a text editor (such as Windows Notepad). It already contains parameters for accessing the demo passes, prefixed `VAS1` and `ST1`, both relying on KeySlot 6. You can overwrite these, or keep them in addition to your own pass reading parameters.
2. Add your pass reading parameters in the `config.txt` file to access up to 6 Apple VAS and up to 6 Google Smart Tap IDs, and identify the keys to be used in each case.

   Note: Although the VTAP100 supports multiple IDs, Apple expect most users will only use one. Multiple collector IDs are not supported by Android, which means you cannot request more than one Collector ID from Google. Only one should be live at any one time. Multiple IDs is an advanced feature that should be used with care. The VAS# and ST# numbers define the order in which IDs will be requested from Apple or Android phones respectively. The lowest numbered ID will be requested first, then continuing in ascending numeric order. (There is a VTAP Application Note on Multiple Passes which explains more.)

   Put each parameter on a new line. Order of parameters does not matter to the VTAP100, but could help other people who need to edit the file. Start any comment lines in the `config.txt` file, that the VTAP100 should ignore, with a semicolon. Each parameter should only appear once - if it accidentally appears more than once then only the last instance will take effect.

   Example: Settings in `config.txt` to interact with both Apple VAS and Google Smart Tap mobile passes

```
!VTAPconfig

VAS1MerchantID=<your merchant ID>
VAS1KeySlot=1
; This says use the key added as file 'private1.pem' to read and
; decrypt any pass connected to your merchant ID on an Apple iPhone

ST1CollectorID=<your collector ID>
ST1KeySlot=2
ST1KeyVersion=1
; This says use the key added as file 'private2.pem' at key version 1
; to read and decrypt any pass connected to your collector ID
; on an Android phone
```

3. Save the amended config.txt file and these changes will take effect immediately. (A small number of changes to the `config.txt` file require a reboot to take effect, for instance to the status of the virtual COM port, but these are highlighted in later sections).

Note: If a `VAS#KeySlot` parameter is omitted, or set to 0, then all available keys will be automatically tried to choose the right key. If the data received by the VTAP100 cannot be decrypted, the Apple iphone will register a pass read, but the data will not be output.

Note: If an `ST#KeySlot` parameter is omitted, or set to 0, then authentication will be omitted and decryption will not be performed. In this case, Google Smart Tap data will be received and sent on by the VTAP100, only if the pass does not require authentication by the terminal.

2.3 Check status in BOOT.TXT

If you navigate to the VTAP100 in the computer's file system. It will appear as an attached mass storage device and list the files contained, including the BOOT.TXT file.

Inspecting BOOT.TXT will give you essential information about your VTAP100 set up, at time of last reboot, which might be helpful when troubleshooting.

```
VTAP100
Boot time: 2001/01/01 00:00:00
Firmware: V2.2.5.0
Storage: Dataflash
Status: 0
Hardware: 5.01
Expansion: VTAP100C-V1-a2
VCP enabled
NCI: 0471125005-8C00
Serial number: 563230-798AEC17D053C05ADE6F6C36C79A6B12
VTAP label: CC123456
API level: 4
AppKeys used: 123------
```

Figure 2-1 Example VTAP100 v5 BOOT.TXT file

You are most likely to need:

- 'Serial number' ('ATCA' on VTAP100 v4a or earlier) - the hardware serial number for your VTAP100.
- 'VTAP label' (if set) - the assigned serial number for your VTAP100, which matches that on its label. This will not show if not set.
- 'Firmware' - the VTAP100 core firmware version in use. You will find the latest firmware versions at **https://www.vtapnfc.com/download/**
- 'Hardware' - the VTAP100 hardware version in use.
- 'API level' - indicates which serial or OSDP API commands are supported.
- 'KeySlots used:' - Indicates the ECC private keys loaded on the VTAP to access VAS or Smart Tap passes. Helps you check whether you have uploaded the necessary ECC private keys, which can be unclear as the files are deleted when they are uploaded. These two examples show how to read this information:
  - 'KeySlots used:------' shows that no keys have been uploaded.
  - 'KeySlots used: 12--56' shows that key files 1 and 2 have been successfully uploaded, in addition to the defaults 5 and 6.
- 'AppKeys used:' Indicates the application keys (if any) uploaded to the VTAP for any other applications, such as keys loaded to use with DESFire applications.
- 'VCP enabled', if included - indicates that the virtual COM port has been enabled.

- 'Status' - should be 0 if operating normally, anything else indicates an error state.
- 'Expansion:' shows the name of the expansion board (if any) connected to the VTAP, for example: 'VTAP100W' for a Wiegand expansion board.
- 'Boot time' - The time at boot, which defaults to 1970/00/00 00:00:00 if power is removed to reboot.

If the configuration has been locked the `BOOT.TXT` file will end with the words LOCKED S/W or LOCKED H/W.

2.4 Send pass payload over a Wiegand interface

The Wiegand interface allows a mobile NFC pass payload to be passed straight to an access controller from your VTAP reader, like data from any other card reader.

To enable the Wiegand interface you will need to make changes to the `config.txt` file.

Example: Changes to `config.txt` to enable the Wiegand interface

```
!VTAPconfig

WiegandMode=1       ; Enable Wiegand interface
PassWiegandBits=56  ; See note below, this must match bit length expected
                    ;   by controller and data must contain this number
                    ;   of bits, =56 is default if omitted
```

Here `WiegandMode=1` enables data transmission over the Wiegand interface.

`WiegandSource` controls which types of data (pass reads, card/tag reads, serial commands) will be sent to the Wiegand interface. The default value is `A1`, which allows sending of all NFC pass and card/tag data. Refer to the VTAP Commands Reference Guide for other options, if data sources need to be restricted for your application.

Additional settings are needed if you want to **Send only part of pass payload**, which are discussed in the following section. And there are a number of settings which will allow you to adjust the **Format of pass data** before it is sent over the Wiegand interface, discussed later in this section.

Note: `PassWiegandBits` should be set to match the bit length expected by the controller and the pass payload must contain sufficient data to provide this number of bits. `PassWiegandBits` defaults to 56, so the expected form of the pass payload is 14 hex digits, unless `PassWiegandBits` is set to another value in your configuration.

2.4.1 Send only part of pass payload over Wiegand

`WiegandPassMode` allows you to extract only a part of each mobile NFC pass payload to send over the Wiegand interface. Setting `WiegandPassMode=1` enables all of the other `WiegandPass...` settings, to extract a short character sequence from the pass payload. This can then be interpreted as a decimal or hexadecimal number and sent over the Wiegand interface as a bit sequence. These settings let you fetch the specific section of the pass payload needed by your access control system, as in this example:

Example: Changes to `config.txt` to extract part of the full pass payload for Wiegand interface [VTAP100-PAC-W only]

```
!VTAPconfig

WiegandMode=1           ; Enable Wiegand interface
WiegandPassMode=1       ; Choose to extract only
                        ;  a part of the pass payload
WiegandPassSeparator=|  ; Set the separator character the VTAP should
                        ;  use to separate the payload into sections
WiegandPassSection=2    ; Section number to read based on that
                        ;  WiegandPassSeparator
PassWiegandBits=32
```

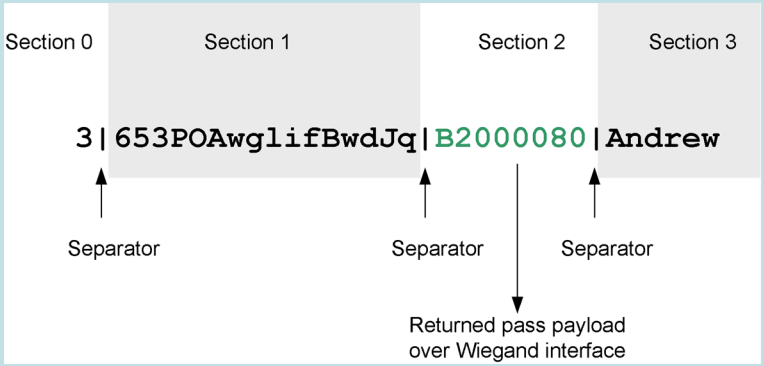


Figure 2-2 Separator |, Section 2 for Wiegand data (on VTAP100-PAC-W only)

Full pass payload:
3|653POAwglifBwdJq|B2000080|Andrew

Pass payload sent over the Wiegand interface:
B2000080

Refer to the VTAP Commands Reference Guide for all the possible `WiegandPass...` settings and options to extract even smaller parts of the pass payload.

2.4.2 Format of pass data sent over Wiegand

Wiegand data is usually a short bit pattern, rather than a sequence of characters. So there are several optional settings, to use in `config.txt`, which allow you to change the output

format for any data read, in terms of bit length, parity bits and identification of pass type, for data transferred over a Wiegand connection:

- `PassWiegandBits=56` lets you specify the number of bits (1 to 255) to output over the Wiegand interface, from the start of the filtered pass payload. If omitted it defaults to 56.

  (`TagWiegandBits` does the same for card/tag data.)

- `PassFormat=d` is a setting to interpret ASCII pass payload characters as either hex (h) or decimal (d), when converting the pass payload to a Wiegand bit sequence.

  (For cards and tags containing a sequence of ASCII characters, you may want `TagWiegandASCIIFormat` set to hex (`h`), decimal (`d`) or the default ASCII (`a`), along with `TagReadFormat=a`.)

- `PassWiegandParity=1` adds a single 'parity bit' equivalent to pass payload. This makes it possible to use mobile pass data formats that include parity bits. Parity bit equivalents can be used if the parity bit(s) are not being tested for validity. `PassWiegandParity=2` adds calculated odd and even parity bits to the data. Either can be used if `PassFormat=d` or `PassFormat=h`. Again, the default `=0` turns this feature off.

  (Use `TagWiegandParity` to do the same operation for card and tag data, used with `TagReadFormat=a` and `TagWiegandASCIIFormat=d` or `=h` to interpret the tag byte data as an ASCII string representing a decimal or hex number, and to convert this to the corresponding Wiegand bit sequence by adding extra parity bits, which might be expected by the controller.)

- `WiegandPassTypeIdent=1` inserts an additional leading byte of pass type identifier (01 for Apple VAS, or 02 for Google ST) in the Wiegand output. This makes it possible to distinguish between cards/tags and mobile wallet passes. This setting overrides `PassWiegandBits` and results in a Wiegand bit length of 64 bits. The default `=0` turns this feature off.

For more information about the Wiegand interface refer to the VTAP Application Notes on Access Control.

2.5 Wiegand wiring (for model VTAP100-PAC-W only)

Use the Wiegand connector supplied to make a Wiegand wiring connection to a configured VTAP100 Wiegand reader from your access controller, like any other reader.

Use 24-26AWG shielded multi-core, overall screened, cable for the connection between VTAP100 Wiegand reader and controller (for example Belden CR9538).

Note: Screened cable should always be used to connect VTAP100 readers to door controllers, to avoid interference from other equipment. The cable screen must be connected electrically to GND at both the VTAP100 reader and controller ends of the cable, using the bare wire 'drain' conductor.

If you have a square (SQ) case you will need to open the case to access the Wiegand connector. Press with a screwdriver in the slot at the base of the back to release the catch and open the case.

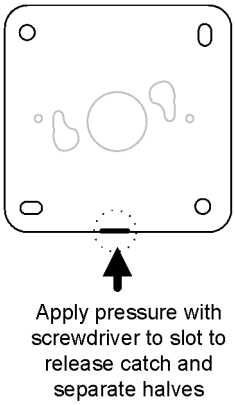


Figure 2-3 Where to press, to open the square case

If you have a compact (CC) case you need to remove the screw from the case (which may be either a security screw or Phillips head screw).

The cable can be routed out through the hole in the back of the VTAP case, and pressed into a guide channel when the product is reassembled. To do this you may need to break or remove a sticker on the rear of the case.

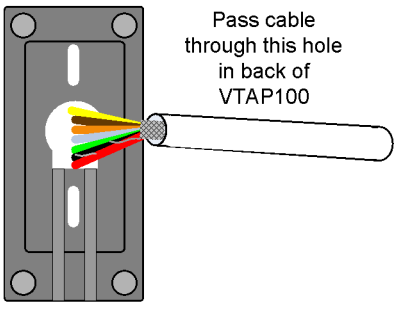


Figure 2-4 Where to pass cable into the compact case

Screw the back of the VTAP100 case to the wall before connecting the cable to the Wiegand connector.

> **CAUTION:** If the VTAP100 is being powered through its Wiegand connection, you can still make an additional USB data connection to a PC, provided that the PC is already powered before the connection is made. (This avoids the risk of damage to the USB interface on the PC, if the PC is not powered.)

Follow an appropriate figure and table to make the right connections in your access controller:

HID EH400

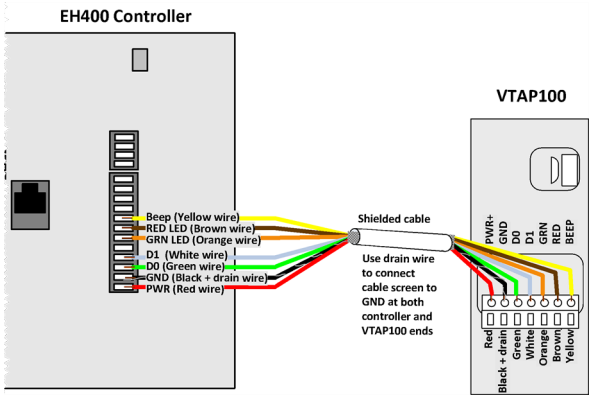


Figure 2-5 Connection between VTAP100-PAC-W v4a or v5 and HID EH400 access controller

HID EH400 Controller Signal Name	Wire colour (typical)	VTAP100 Signal Name (v4a or v5 hardware)
Beep	Yellow	BEEP
RED LED	Brown	RED
GRN LED	Orange	GRN
D1	White	D1
D0	Green	D0
GND	Black	GND
PWR	Red	PWR+

HID V2000

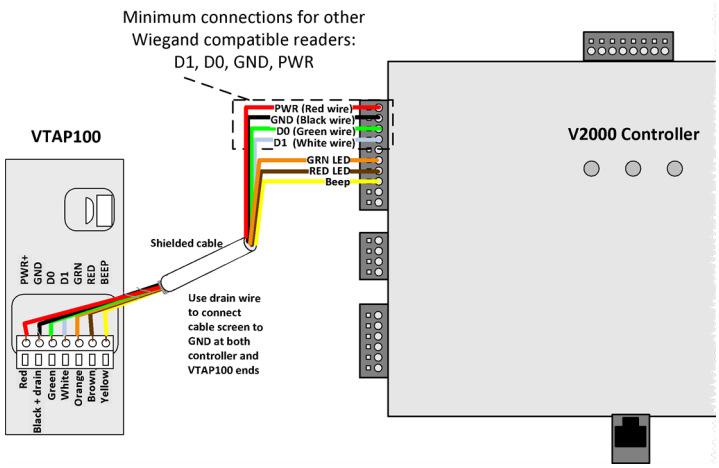


Figure 2-6 Connection between VTAP100-PAC-W v4a or v5 and HID V2000 access controller

HID V2000 Controller Signal Name	Wire colour (typical)	VTAP100 Signal Name (v4a or v5 hardware)
Beep	Yellow	BEEP
RED LED	Brown	RED
GRN LED	Orange	GRN
D1	White	D1
D0	Green	D0
GND	Black	GND
PWR	Red	PWR+

Axis A1001

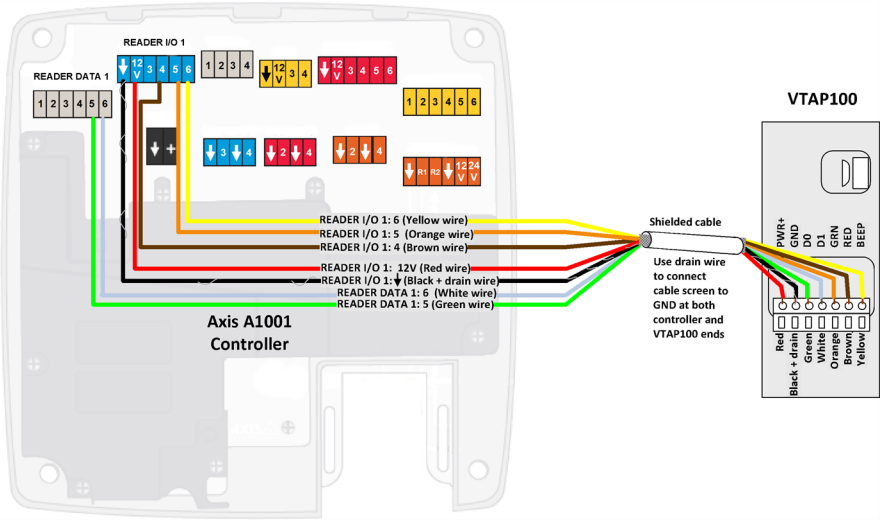


Figure 2-7 Connection between VTAP100-PAC-W v4a or v5 and Axis A1001 access controller

Axis A1001 Controller Signal Name	Wire colour (typical)	VTAP100 Signal Name (v4a or v5 hardware)
READER I/O 1: 6	Yellow	BEEP
READER I/O 1: 4	Brown	RED
READER I/O 1: 5	Orange	GRN
READER DATA 1: 6	White	D1
READER DATA 1: 5	Green	D0
READER I/O 1: ↓	Black	GND
READER I/O 1: 12V	Red	PWR+

Axis A1601

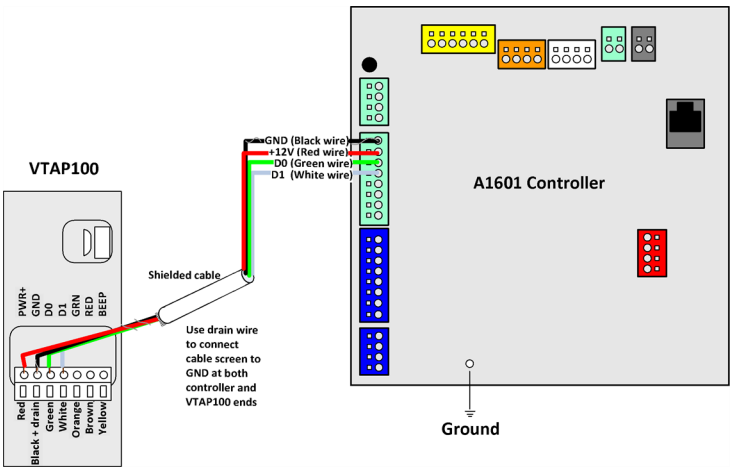


Figure 2-8 Connection between VTAP100-PAC-W v4a or v5 and Axis A1601 access controller

Axis A1601 Controller Signal Name	Wire colour (typical)	VTAP100 Signal Name (v4a or v5 hardware)
D1	White	D1
D0	Green	D0
GND	Black	GND
+12V	Red	PWR+

Nortech CRC400

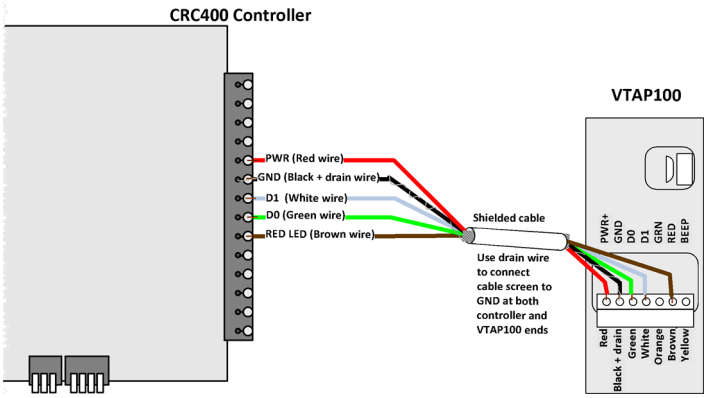


Figure 2-9 Connection between VTAP100-PAC-W v4a or v5 and Nortech CRC400 access controller

Nortech CRC400 Controller Signal Name	Wire colour (typical)	VTAP100 Signal Name (v4a or v5 hardware)
LED	Brown	RED
Data/D1	White	D1
Data/D0	Green	D0
0 Volts	Black	GND
+VE	Red	PWR+

Nortech Dataquest

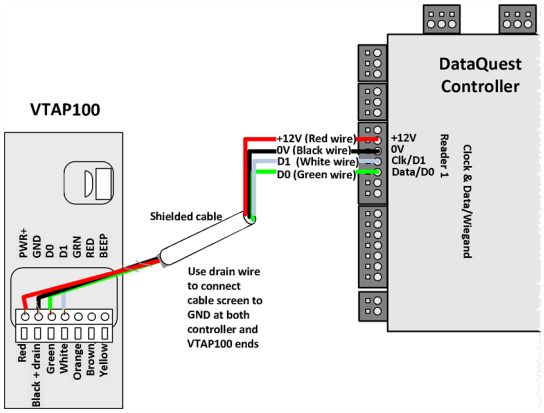


Figure 2-10 Connection between VTAP100-PAC-W v4a or v5 and Nortech Dataquest access controller

Nortech Dataquest Controller Signal Name	Wire colour (typical)	VTAP100 Signal Name (v4a or v5 hardware)
Clk/D1	White	D1
Data/D0	Green	D0
0V	Black	GND
+12V	Red	PWR+

Paxton Net2

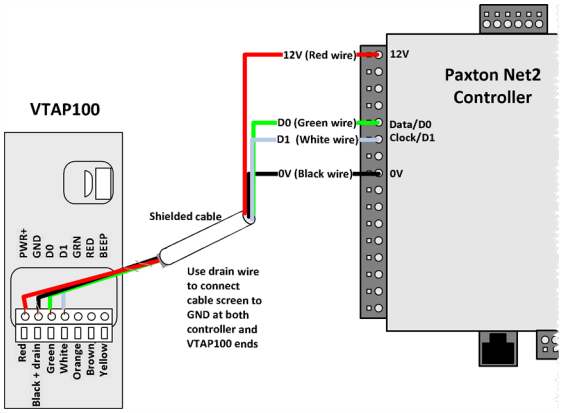


Figure 2-11 Connection between VTAP100-PAC-W v4a or v5 and Paxton Net2 access controller

Paxton Net2 Controller Signal Name	Wire colour (typical)	VTAP100 Signal Name (v4a or v5 hardware)
Clock/D1	White	D1
Data/D0	Green	D0
0V	Black	GND
12V	Red	PWR+

HID Mercury MR52-S3B

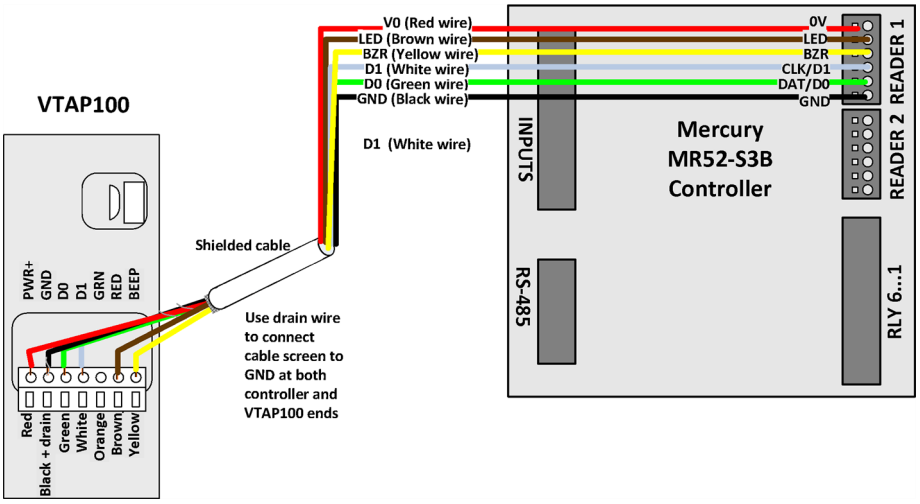


Figure 2-12 Connection between VTAP100-PAC-W v4a or v5 and HID Mercury access controller (MR52-S3B)

Connections are shown for Reader 1 on the controller, but Reader 2 connections are equivalent.

HID Mercury Controller Signal Name	Wire colour (typical)	VTAP100 Signal Name (v4a or v5 hardware)
D0/DAT/TR-	Green	D0
D1/CLK/TR+	White	D1
GND	Black	GND
V0	Red	PWR+
BZR	Yellow	BEEP
LED	Orange	RED (or GRN)

3 Choose a location for your VTAP reader

Position the VTAP100-PAC-W so that users can easily tap their smartphone against the label, on top of the device, and also to allow a suitable wired connection (cable run) between the VTAP100 and associated access controller, to make both power and data connections.

CAUTION: Never allow a metal surface between the VTAP100 and the user's phone or card.

The square case for a VTAP100-PAC-W is 86mm x 86mm and 25.5mm deep.

Figure 3-1 VTAP100 -SQ square case

The compact case for a VTAP100 is 97mm x 49mm and 40mm deep.

Figure 3-2 VTAP100-CC compact case

The VTAP reader must be stored and operated under the following conditions:

- Ambient temperature -25 to +70°C (-13 to 158°F)
- Humidity 0 to 95% RH non-condensing
- Pressure 86-106kPa

The -SQ square case models are for indoor use only, where -CC compact case models can be used indoors or outdoors.

When using the -CC model outdoors, install the VTAP reader in a wallmount (vertical) orientation, in as sheltered a location as possible. The case is not sealed because the design allows for water ingress and egress. Do not block the drain holes in the case. The PCBs for this model are conformally coated to protect the electronics.

The compact case separates into two pieces, which clip together around the PCB. After deciding where you will use your VTAP100, you may want to alter the assembly to suit the location.

You may have to remove a small label on the end of the VTAP reader, to uncover the screw that holds the pieces together. To do this in a way that will keep the label in good condition to reapply later, apply pressure directly down on the label and slide it gently towards the edge of the case.

Figure 3-3 Where to apply pressure to slide label off case

The case can be changed from an ergonomic desktop reader design to one suited for wall mounting, simply by rotating the PCB and the case front through 180°, keeping the LED and LED window aligned. Mount the PCB in the case, then engage the hooks at the LED window edge of the case to form a hinge, lower the cover and secure with a screw at the opposite end.

Figure 3-4 Wallmount or desktop assembly

The cable can be routed directly out of the back of the reader, if preferred, to hide the wire completely from view or prevent access. The back label includes a circular pre-cut section that can be pushed out to allow the cable to be passed though.

4 Obtain a custom label for the case

We can design and affix your own branded label to the unit.

If you would like to brand your VTAP readers do contact **vtap-support@dotorigin.com**.

We can take your CMYK, vector format images and design and supply labels manufactured to high standards using an advanced production method, where the printing is protected by a thick layer of clear plastic, making them scratchproof, waterproof and UV-proof.

Apple guidelines require the standard contactless logo to be used, and so our standard label template includes this along with a design that highlights the location of the VTAP antenna, as that is the target location for a user to tap their phone.

The size of the label recess on a square (-SQ) case is 72mm x 72mm (2.85in x 2.85in) with 4mm (0.16in) radius rounded corners as shown below.

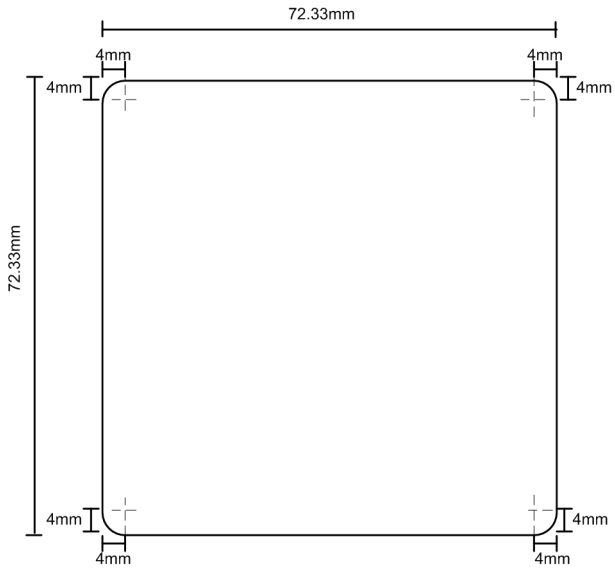


Figure 4-1 Dimensions of label recess in -SQ square case

The size of the label recess on a compact case (-CC) is 41mm x 57mm with 2mm radius rounded corners as shown below.

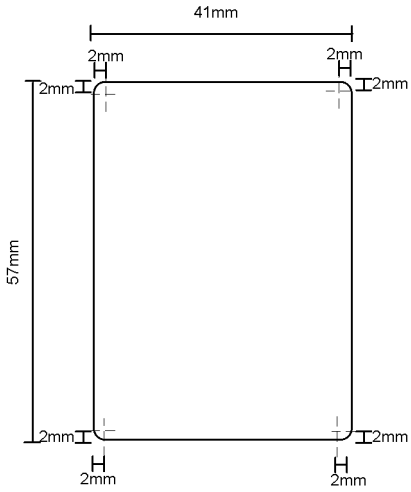


Figure 4-2 Dimensions of label recess in -CC compact case

5 Mount a VTAP reader

The square case has mounting holes, in case you want to fix the device in place. The case separates into two pieces, which clip together around the PCB. The following diagram shows the location of mounting holes in the square case base plate:

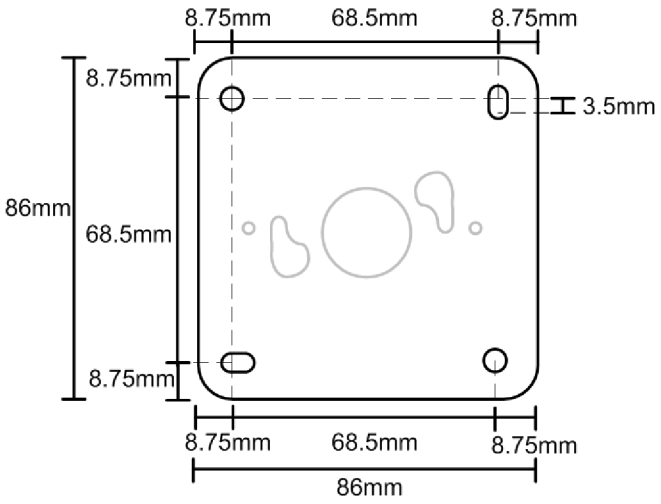


Figure 5-1 Mounting holes in the -SQ square case base plate

The compact case has mounting holes, in case you want to fix the device in place. The case separates into two pieces, which clip together around the PCB. The following diagram shows the location of mounting holes in the compact case base plate:

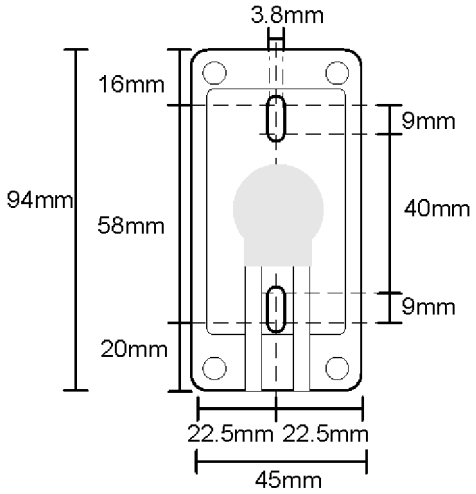


Figure 5-2 Mounting holes in the -CC compact case base plate

The VTAP reader is rated at 5V DC (typ. 110mA, max 150mA) for power over USB. When powered over Wiegand it is rated at 8V-16V DC @ 30 to 100mA

The wires for power and data connection to an access controller all come through the large hole in the base plate of the reader.

We recommend that you complete and test your configuration before the VTAP reader is mounted. Detailed help is in the VTAP Configuration Guide.

6 Hardware lock to disable USB mass storage device

You can lock the VTAP reader so that its firmware and configuration cannot be changed. You can either do this in software, or simply disable the mass storage device in hardware. If you have a boxed VTAP or VTAP100-PAC-W it is strongly recommended that you use the software lock option, which is described in the VTAP Configuration Guide.

A software lock prevents changes but leaves the file system readable. A hardware lock means that the VTAP reader will no longer be detected as a USB mass storage device. (It will still behave as an HID keyboard device and, if enabled, the virtual COM port will behave as a composite USB device consisting of HID keyboard and USB virtual COM port.)

Users of a VTAP100-PAC-W will need to open the case to locate the jumper labelled LOCK (close to the MicroUSB connector) on the PCB.

If you have a compact (CC) case you need to remove the screw from the case (which may be either a security screw or Phillips head screw).

Connect a jumper across LOCK on the PCB to lock the device, preventing firmware or configuration changes via the mass storage device. (You may still update firmware or configuration via command interfaces, virtual COM port or serial ports, if they are enabled.)

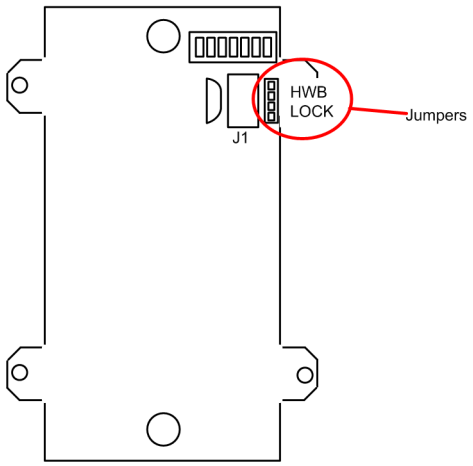


Figure 6-1 Jumper positions on VTAP100 PCB v4a or v5 hardware

Note: If you have a VTAP100 PCB version 3a or earlier the connections will be different, please **contact us** for manuals specific to your hardware. (If you are not sure which version PCB you have, just follow the instructions in **Find your hardware version**.)

If your VTAP100 board has a daughter board on top, as is the case for a VTAP100-PAC-W, you will need to lift the daughter board off, to reach these jumpers.

When you start the VTAP100, the presence of this jumper means the connected PC will not detect a USB mass storage device, only a keyboard (or keyboard and virtual COM port).

When you remove the jumper across LOCK and restart the VTAP100, it will be detected as a USB mass storage device and you can make firmware or configuration changes again.

7 Find your hardware version

If you need to report a problem with your VTAP100 or find the right reference diagram you will need to know your hardware version.

If you can connect your VTAP100 to a PC, you can easily check the BOOT.TXT file.

If you navigate to the VTAP100 in the computer's file system. It will appear as an attached mass storage device and list the files contained, including the `BOOT.TXT` file.

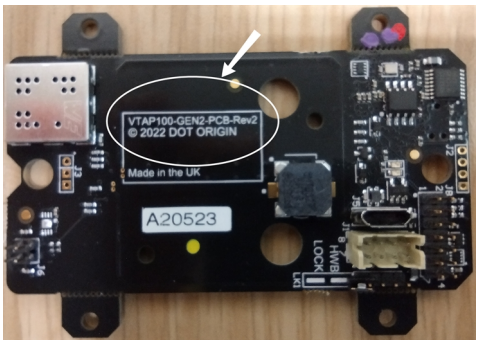
Inspecting `BOOT.TXT` you will find a number next to the word `Hardware:` such as `v5`. This is the Hardware version in use.

Alternatively, over a serial connection to the VTAP100, sending the `?b` command will return the `BOOT.TXT` information.

If you cannot power the VTAP100

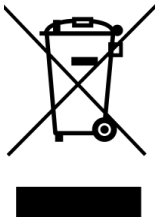
Open the case, by removing the end label and the security screw - at the opposite end of the reader to the LED window, on a compact case.

You will find the version number printed on the PCB, such as "VTAP100-PCB-V4a ©2021 DOT ORIGIN Ltd." which is VTAP100 v4a hardware. In the photo below is "VTAP100-GEN2-PCB-Rev2 © 2022 DOT ORIGIN" which is also known as VTAP100 v5 hardware.



8 Disposal

For safety and sustainability, it is the responsibility of the integrator to ensure that when equipment containing a VTAP100 reaches the end of its life, it is recycled in accordance with WEEE Regulations within the EU.



VTAP100 (PCB and cables) should not be disposed of in general waste. If you wish to discard electrical and electronic equipment (EEE), please contact your supplier for further information.