VTAP100

Installation Guide - VTAP100 RS-485/OSDP Reader

VTAP100-PAC-485

Revised February 2025 v1.22

DOT ORIGIN

If you need help to set up or use your VTAP reader, 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 VTAP reader or this documentation, then please contact our support team. The product is constantly being reviewed and improved and we value feedback about your experience.

Contents

Safety instructions

> ⚠️ **WARNING: INTENDED USE**
>
> The VTAP100-PAC-485 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-485 model to a PC or **alternatively** power the unit by connecting it to an access controller, using the RS-485 connector cable. If the VTAP100 is being powered through its RS-485 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-485 with the supplied cable.

1   Using this guide

This guide is for first-time users of the VTAP100-PAC-485.

Figure 1-1 VTAP100 in compact (-CC) case

It contains the information you need to install your VTAP reader.

Consult the VTAP Configuration Guide for more about custom configuration and maintenance features for any VTAP reader, including how to update the firmware on your VTAP100-PAC-485, 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-485 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-485 model only, is that it will support an RS-485 connection for transferring data or commands.

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-485 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-485 will be able to receive and respond to commands over RS-485 on default settings, but must be configured over USB from a PC, if it is to send pass data over the RS-485 interface. 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 VTAP reader.

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 VTAP reader to your PC, using a USB cable.

3. Open a text editor, such as Windows Notepad.

4. When you tap the OriginPass on the VTAP reader:

   - Pass contents will be displayed in the open text editor, through keyboard/barcode emulation.
   - The feedback LEDs on the VTAP reader 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 VTAP reader 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 VTAP reader

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 VTAP reader, which shows up in the file system of your PC as a mass storage device.
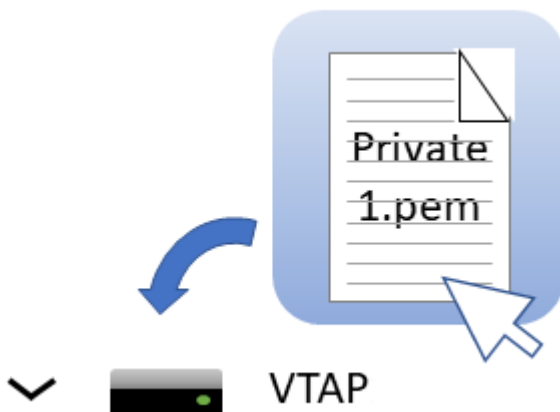
> **Note:** When you reboot the VTAP reader your key will have been stored in hardware, and will no longer be listed as a file on the device. You can confirm key file(s) have been loaded when you **Check status in Boot.txt**. If the key file does not disappear and there is an error in `Boot.txt`, check 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 VTAP reader 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 VTAP reader, but could help other people who need to edit the file. Start any comment lines in the `config.txt` file, that the VTAP reader 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 VTAP reader 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 VTAP reader, only if the pass does not require authentication by the terminal.

2.3 Check status in `BOOT.TXT`

If you navigate to the VTAP reader 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 VTAP reader 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 VTAP reader.

- 'VTAP label' (if set) - the assigned serial number for your VTAP reader, which matches that on its label. This will not show if not set.

- 'Firmware' - the VTAP reader core firmware version in use. You will find the latest firmware versions at **https://www.vtapnfc.com/download/**

- 'Hardware' - the VTAP reader 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 Using the RS-485 interface

The RS-485 interface on the VTAP reader can be used to send NFC mobile wallet pass payload straight to a control unit, such as an access control unit, just like sending data from any other card or pass reader. RS-485 is a half-duplex interface, which means that communication is only ever in one direction at any time. The hardware contains two data or signal lines (either A and B or + and −), which send balanced signals over the two lines. This means both lines contain the same signal but one is inverted with respect to the other. The RS-485 interface makes use of VTAP configuration settings starting `Serial2...`, described as the Serial2 interface.

The following steps will configure this interface (unless you will be **Using OSDP over RS-485**, see section **2.5**):

1. The Serial2 interface is enabled on the VTAP100 by default. Should you need to disable it, set `Serial2Mode=0` and/or `Serial2RS485=0` to disable the Serial2 interface and/or RS-485 transmission driver in the `config.txt` file.

2. By default, the VTAP reader is in active mode and any data read by the VTAP reader will be passed to the Serial2 interface, since `Serial2Source=A1`. To restrict this, so that only some types of data will be passed over RS-485, use another value for `Serial2Source` to suit your application. Refer to the VTAP Commands Reference Guide for options with this setting.

3. The Serial2 interface needs to be in passive mode to support uni-directional communications between the VTAP reader and the connected device. So use `PassiveInterfaces=4` in the `config.txt` to enable passive mode on the Serial2 interface.

4. When the VTAP reader is in passive mode, being polled for data by another system, it is important to realise that, by default, data is only retained for 3000 milliseconds after a pass, card or tag is read. After this period the data and information about this read can no longer be sent on any interface. Use the `InvalidDataCacheMS` setting if you need to change this to an amount of time that better suits your application.

5. The default port settings are 9600 baud rate, no parity, 8 data bits and 1 stop bit. If this does not match your RS-485 system, change these settings, using `Serial2Settings` in `config.txt`. Define the interface parameters in the sequence `<baud rate>, <parity>, <data bits>, <stop bits>,` as in the example `Serial2Settings=115200,n,8,1`.

6. If you only need a part of the full pass payload use `Serial2Pass...` settings to extract only that part. Refer to the VTAP Commands Reference Guide for more about these settings.

> **Example: Settings in Config.txt file to extract
> a part of the pass payload over RS-485 interface**
>
> ```
> VTAPConfig!
>
> PassiveInterfaces=4    ; Enable passive mode for RS-485 interface
>                        ; (Serial2)
> Serial2PassMode=1      ; Enable extracting part of the entire pass
>                        ; payload
> Serial2PassSeparator=| ; Set the separator character to divide the pass
>                        ; payload on the basis of
> Serial2PassSection=2   ; Sets the section of interest, based on the
>                        ; Serial2PassSeparator character (starts from 0)
> ```
>
> From a full pass payload of: `3|F6I53ZaPv2Ys2PAb|C699E142|Dot`
>
> This is the output which will result using the above settings: `C699E142`

7. Prefix and postfix characters can be added to the data being sent over the RS-485 interface. Use `Serial2Prefix` or `Serial2Postfix` to set these (max 16 characters). URL encoding is supported.

> **Example: Adding prefix and postfix on a Serial2 RS-485 interface
> for pass and card/tag payload**
>
> ```
> Serial2Prefix=UID:
>
> Serial2Postfix=%20Type:$t,Slot:$n
> ```
>
> This will result in Google pass output:
>
> `UID:3|F6I53ZaPv2Ys2PAb|Muhammad Faraz|Dot Type:G,Slot:16`
>
> or MIFARE Classic card output:
>
> `UID:0473816A831E80 Type:4,Slot:--`

After changing the `Serial2...` settings in `config.txt` and saving that file (if something other than default behaviour is required), you can start sending commands (queries) over the Serial2 RS-485 interface, to receive pass payloads in response.

The most commonly used commands are:

- `?r` to get the last read pass or card/tag payload (as long as it is within the `InvalidDataCacheMS` period).

- `?type` to get the pass or card type along with VAS merchant ID or ST Collector ID and ECC key slot.

Refer to the VTAP Commands Reference Guide for all the available commands for the Serial2 interface.

For more information about the VTAP100 RS-485 and other serial interfaces refer to the VTAP Serial Integration Guide.

2.5 Using OSDP over RS-485

OSDP defines a method for secure communication between an Access Control Unit (ACU) and all its Peripheral Devices (PDs). The VTAP reader RS-485 interface can be used for OSDP communications between the VTAP (PD) and an ACU, in an access control system.

The command interfaces on a VTAP reader are designed as human interfaces. Using the secure OSDP protocol on interfaces provides an ideal machine interface, with the necessary CRCs and integrity checks.

A VTAP reader will support basic and secure modes on OSDP.

Please refer to VTAP Application Notes about using OSDP over an RS-485 interface. If you need further support, please contact **vtap-support@dotorigin.com**.

2.6 RS-485 wiring (for model VTAP100-PAC-485 only)

Use the RS-485 connector supplied to make an RS-485 wiring connection to a configured VTAP100-PAC-485 reader from your access controller, like any other reader.

Use 24AWG twisted pair shielded cable for the connection between VTAP100-PAC-485 reader and controller (for example Belden 82842).

> **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.

To access the RS-485 connector on a VTAP reader you need to open the 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.

> ⚠️ **CAUTION:** We strongly recommend that power is disconnected from the installation cable before wiring the VTAP100 connector.

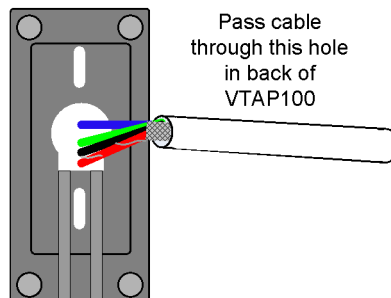Pass cable through this hole in back of VTAP100

Figure 2-2 Where to pass RS-485 cable into the compact case

Screw the back of the VTAP100 case to the wall before connecting the cable to the RS-485 connector.

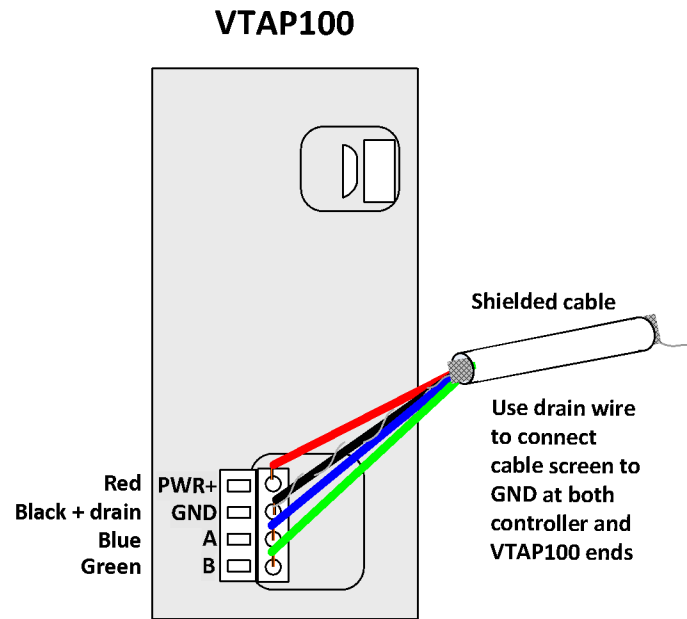Follow this figure and table to make the right connections in your access controller:

VTAP100

Figure 2-3 Connection to VTAP100-PAC-485 and access controller (for example)

Access Controller Signal Name (for example)	Wire colour (typical)	VTAP100 Signal Name (v5 hardware)
PWR+	Red	PWR+
GND	Black	GND
A	Blue	A
B	Green	B

Termination resistance is not required when connecting a VTAP reader over the RS4845 line, because it uses a low slew-rate RS-485 transceiver (commonly used in modern devices). The only scenario where termination resistance may be required is where impedance matching is required because a controller is using a termination resistance.

3 Choose a location for your VTAP reader

Position the VTAP100-PAC-485 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 VTAP reader and associated access controller, to make both power and data connections.

> **CAUTION:** Never allow a metal surface between the VTAP reader and the user's phone or card.

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

Figure 3-1 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 VTAP100-PAC-485 reader can be used indoors or outdoors.

When using the VTAP100-PAC-485 reader 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 VTAP reader, 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 3-2 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 180º, 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 3-3 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 compact case (-CC) is 41mm x 57mm with 2mm radius rounded corners as shown below.
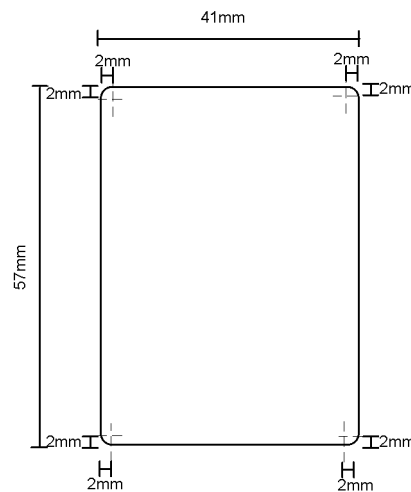

Figure 4-1 Dimensions of label recess in -CC compact case

5   Mount a VTAP reader

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:
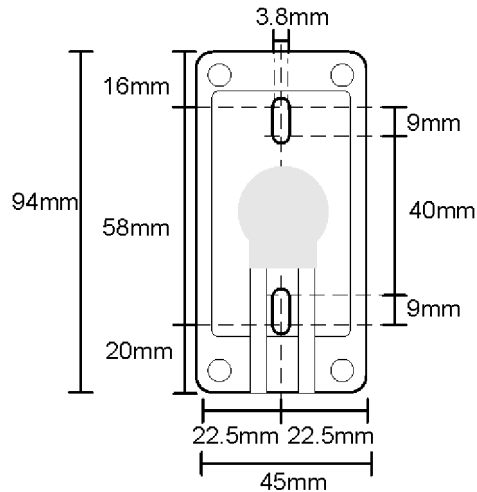

Figure 5-1 Mounting holes in the -CC compact case base plate

The VTAP reader is rated at 5V DC (typ. 110mA, max 150mA) for power over USB.

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-485 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-485 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.)
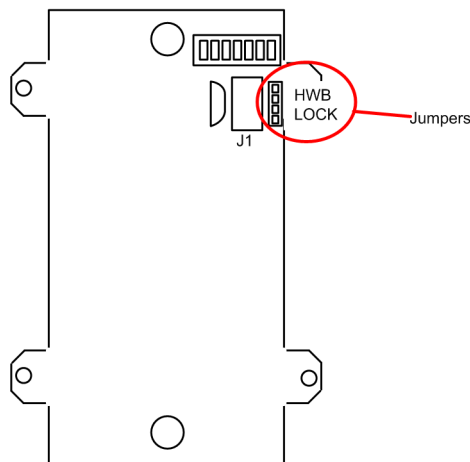
Figure 6-1 Jumper positions on VTAP100 PCB v5 hardware

If your VTAP reader board has a daughter board on top, as is the case for a VTAP100-PAC-485, you will need to lift the daughter board off, to reach these jumpers.

When you start the VTAP reader, 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 VTAP reader, 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 VTAP reader or find the right reference diagram you will need to know your hardware version.

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

If you navigate to the VTAP reader 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 VTAP reader, sending the `?b` command will return the `BOOT.TXT` information.

If you cannot power the VTAP reader

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.
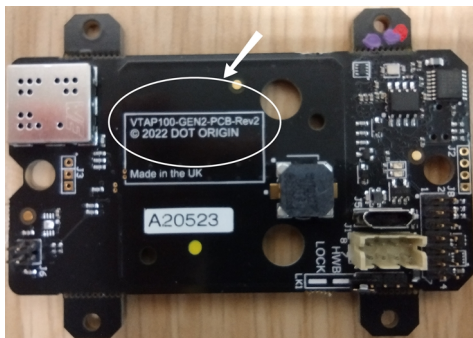
8 Disposal

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

VTAP reader (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.