

# V-Tap Analog 2

## Manual

v4.26



# Contents

<b>1</b>	<b>Introduction.....</b>	<b>5</b>
<b>2</b>	<b>Getting started.....</b>	<b>6</b>
2.1	<b>Hardware installation.....</b>	<b>6</b>
2.1.1	Line connection (Analog Phone) .....	7
2.1.2	Handset connection (Digital Phone) .....	7
2.1.3	Audio connection .....	8
2.2	<b>Software installation.....</b>	<b>9</b>
2.2.1	Call Recorder Apresa .....	9
2.2.2	V-Archive software on a PC.....	10
2.3	<b>Checklist for Tunnel connection .....</b>	<b>11</b>
<b>3</b>	<b>Web interface and Settings .....</b>	<b>12</b>
3.1	<b>Access &amp; IP address .....</b>	<b>12</b>
3.2	<b>Web interface.....</b>	<b>13</b>
3.3	<b>Settings.....</b>	<b>15</b>
3.3.1	General Network settings .....	15
3.3.2	Tunnel settings.....	17
3.3.3	Secure Connection with TLS .....	19
3.3.4	Special Tunnel & Network settings .....	20
3.3.5	Wi-Fi settings.....	22
3.3.6	Login settings for Web access & FTP.....	23
3.3.7	NTP and Date+Time settings .....	24
3.3.8	Local Phone Number .....	25
3.3.9	Audio Input setting .....	25
3.3.10	Stereo Recording & Recording Quality .....	26
3.3.11	Button Mode setting.....	27

3.3.12	Notification Message settings.....	28
3.3.13	Analog settings .....	29
3.3.14	Special Settings & Commands .....	32
3.3.15	Licenses & Versions .....	35
<b>4</b>	<b>LED's .....</b>	<b>36</b>
4.1	Red Error LED .....	36
4.2	Green Link LED.....	37
4.3	Blue Data LED.....	38
4.4	Amber SD-Power LED .....	38
<b>5</b>	<b>Button functions .....</b>	<b>39</b>
5.1	Start & Stop recording.....	39
5.2	Remove SD Card safely .....	39
5.3	Disable DHCP temporary .....	40
5.4	Show IP address .....	40
5.5	Copy Settings from SD card.....	41
5.6	Factory settings.....	41
5.7	Format SD card.....	41
5.8	Default IP address .....	41
5.9	Temporary access with Wi-Fi .....	42
5.10	Firmware update .....	43
<b>6</b>	<b>SD card usage.....</b>	<b>44</b>
6.1	Special SD card settings .....	45
<b>7</b>	<b>Notification &amp; System Messages.....</b>	<b>48</b>
<b>8</b>	<b>Number-list (Black- or White-list) .....</b>	<b>49</b>
<b>9</b>	<b>Telnet connection.....</b>	<b>50</b>

<b>10</b>	<b>TLS on the V-Tap.....</b>	<b>51</b>
10.1	Tunnel over TLS.....	51
10.1.1	TLS with certificate verification .....	51
10.1.2	TLS without certificate verification.....	52
10.2	Tunnel protocol to V-Archive with TLS .....	52
10.3	Tunnel protocol to Apresa with TLS.....	53
10.3.1	Tunnel-TLS with a certificate from Apresa .....	53
10.3.2	Tunnel-TLS with a Let's Encrypt certificate.....	56
10.3.3	Tunnel-TLS with another CA certificate .....	58
10.4	Web interface over HTTPS .....	59
10.4.1	HTTPS with a self-signed certificate.....	59
10.4.2	HTTPS with own certificate.....	61
10.5	TLS specification.....	62
<b>11</b>	<b>Using the RTR Call Monitoring Software.....</b>	<b>63</b>
<b>12</b>	<b>Technical Specifications.....</b>	<b>64</b>
<b>13</b>	<b>Revision History.....</b>	<b>65</b>
<b>14</b>	<b>Acknowledgements.....</b>	<b>66</b>
14.1	Privacy.....	66
14.2	Liability .....	66

# 1 Introduction

The V-Tap Analog 2 is a hardware and software solution for the recording of telephone calls. The supplied hardware unit can record the audio from an analog telephone line or any telephone that works with a cord-connected handset. The recorded calls are stored onto an SD card in WAV files, and therefore the V-Tap Analog can operate stand-alone. The content of the SD card can be sent optionally over the network, in which case the data is wrapped into a special Tunnel-format that can be received by the [Call Recorder Apresa](#) (running on Linux) or by a Windows PC running the [V-Archive software](#). The external Apresa recorder or V-Archive software can both interpret the tunnel-format and make playable audio files from it, together with the original date, time and call number information (meta data).

The use of an SD card is mandatory and must be FAT32 formatted. The recorded data is stored in WAV file format on the card. Depending on whether a Tunnel has been defined or not, the files are sent over the network or can be read later by the V-Archive software from the card. Note that, without a Channel License for Apresa or PC, the V-Tap Analog does not produce WAV files or store any data on the SD card.

The V-Tap Analog can operate completely stand-alone and when the capacity of the SD card is big enough, it can store data for weeks or even months.

Connection to the V-Tap Analog is made with a network cable or by using Wi-Fi, when available. The web interface can be accessed by using a browser. The LAN cable is connected to the Ethernet port (100 Mbps).

The V-Tap Analog 2 is a member of a family of compatible products that can be used to create all sorts of recording solutions. There are V-Taps for VoIP, Analog, Audio and ISDN telephony and there is a V-App for mobile recording. All of these products will communicate with the Apresa Corporate or Apresa Cloud-based recording solutions.

**NOTE 1:** The V-Tap Analog needs to be powered through USB with 500 mA and a FAT32 formatted SD card must be inserted.

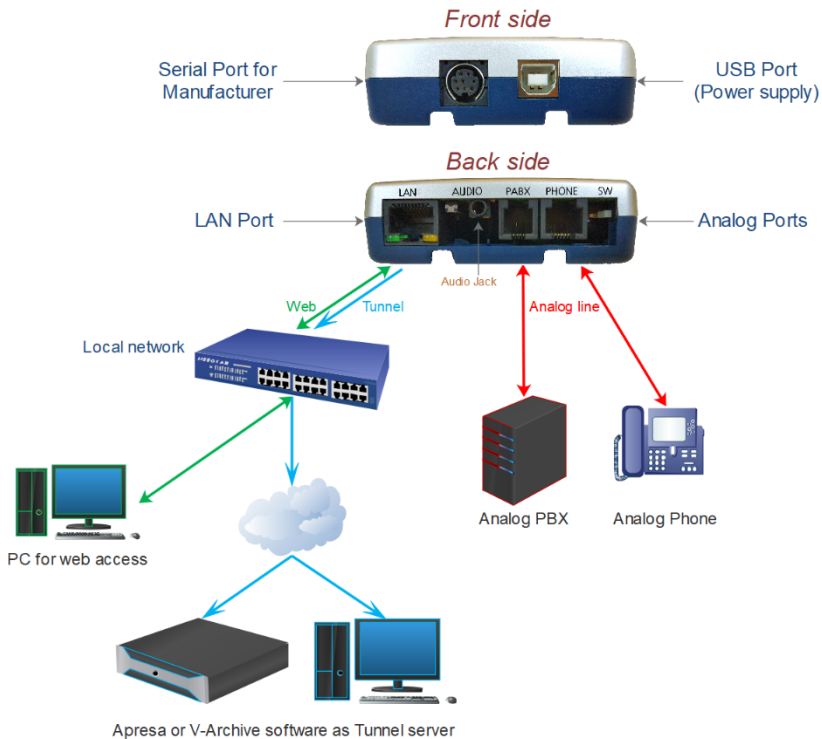
**NOTE 2:** The V-Tap Analog needs at least 1 Channel License for Apresa or PC, else no calls are stored on the SD card.

## 2 Getting started

### 2.1 Hardware installation

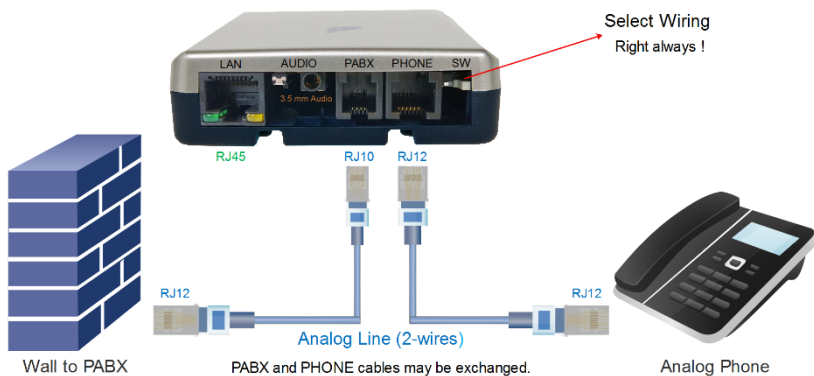
The V-Tap Analog is easy to setup. The following steps are involved:

- Connect the phone to the V-Tap Analog (see below & next page).
- Insert an SD card (up to 32 GB, FAT32 formatted).
- Connect the local network. Not needed when Wi-Fi is used.
- Connect USB to the V-Tap for power.
- Access the settings in the web interface by using a browser.



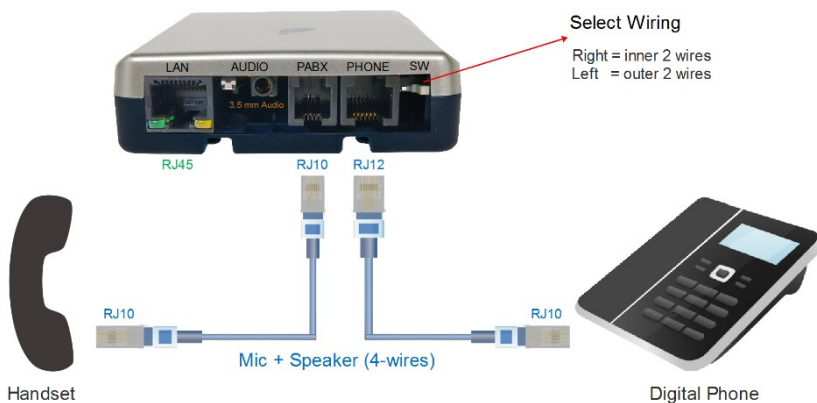
The two possible ways to connect the V-Tap Analog to the telephone system (line or handset) are shown in the next two schemes. The possibility to use the V-Tap Analog for audio recording is shown in the third scheme.

## 2.1.1 Line connection (Analog Phone)



The position of the wire-select switch is always to the right in this case.

## 2.1.2 Handset connection (Digital Phone)



The position of the wire-select switch can be to the left or to the right, depending on the wiring inside the handset-cable.

The setting [Audio Activated Recording](#) must be enabled to select this connection with 4-wires.

## 2.1.3 Audio connection



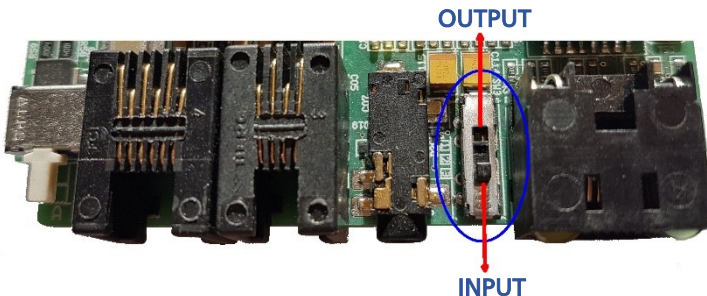
The 3.5 mm stereo audio plug can be used as an input or as an output.

### **Input (default)**

As an input, the web-setting "Record from Audio Input" must be set first before recording from the audio plug is possible; see [Audio Input](#).

### **Output**

The audio switch must be pushed to the inside of the case. Then the audio signal of the analog line becomes available on the plug. By connecting a headphone or multi-media speakers, the user can listen live to calls on the line. No further web-setting is needed for this feature.





## 2.2 Software installation

External software is needed to extract the recorded calls from the Tunnel data that is produced by the V-Tap Analog. Also, when the calls are first stored on an SD card, external software is needed to interpret this data from the card, especially when the data is encrypted.

The Tunnel data stream, coming directly from the V-Tap, can be sent to the [Call Recorder Apresa](#) or the [V-Archive software](#).

### NOTE:

The V-Tap needs at least one Apresa or PC upload-channel license key before the Apresa or V-Archive software can record your calls.

### 2.2.1 Call Recorder Apresa

The [Call Recorder Apresa](#) is recorder software running on the Linux Debian operating system. The Apresa can receive Tunnel data from the V-Tap, convert this data into audio files and store these into its own database.

The Apresa can receive multiple data streams from many V-Tap units simultaneously. In that case the recordings of different locations are centrally stored in one database.

To setup the Apresa to act as a Tunnel server for a V-Tap, go to System settings, Network tab and enable “V-Tap” as is shown below:

The screenshot shows a configuration form for V-Tap settings. The form includes the following fields and options:

- V-Tap:
- V-Tap Tunnel port number: 2016
- V-TAP over TLS:
- V-TAP over TLS Port: 2017
- V-TAP over TLS Certificate: None
- V-Tap Data separation:
- Accept only known V-Taps:
- Accept only encrypted V-Tap connections:
- Store V-Tap recordings in received format:
- V-Tap Encryption password: Default: [Empty field]
- Table with columns: MAC address, Encryption password, Tenant, Name, Delete. Row 1: None
- Buttons: Add, Delete
- Always generate an alarm when a V-Tap in the table is not connected:

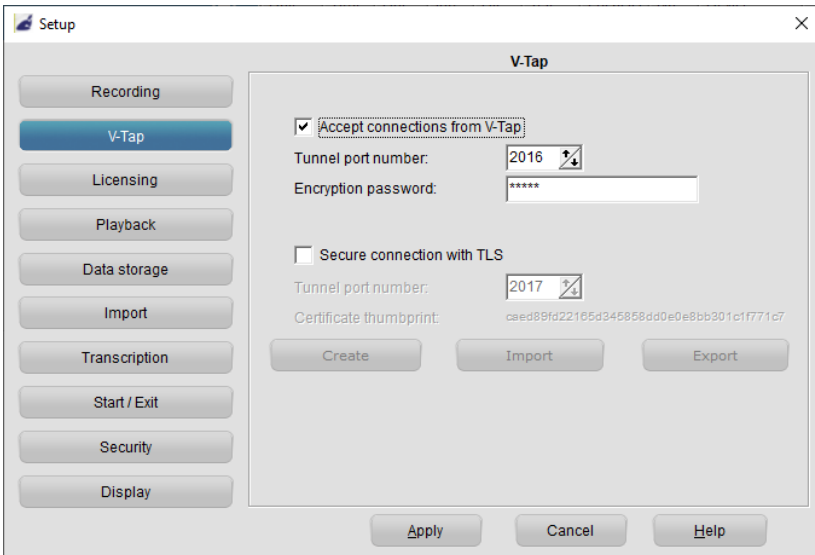
**NOTE1:** Apresa’s IP address is the “Tunnel Server Address” in the V-Tap.

**NOTE2:** Be sure the Encryption password is the same as in the V-Tap unit.

## 2.2.2 V-Archive software on a PC

The [V-Archive software](#) for the PC can, just as the Apresa, receive Tunnel data from the V-Tap Analog, convert this data into audio files and store the files into its own database. The V-Archive software can also receive multiple data streams from different V-Tap units simultaneously.

To setup the V-Archive software to accept connections from a V-Tap, go to Options, Setup, Recording tab and enable as is shown below:



**NOTE1:** The PC's IP address is the "Tunnel Server Address" in the V-Tap.

**NOTE2:** Be sure that the PC's firewall is open for TCP port 2016, the default "Tunnel Destination Port" in the V-Tap.

TCP port 2017 must be open when Tunnel-TLS is used.

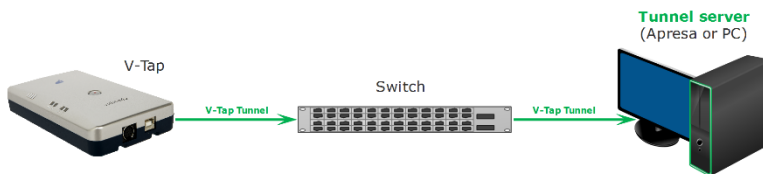
The installer tries to open these ports automatically in Windows.

**NOTE3:** Be sure the Encryption password is the same as the "Encryption Password" in the V-Tap.

**NOTE4:** The V-Archive software itself does not need any license to receive from the V-Tap. Licenses are inside the V-Tap.

*The V-Archive software for the PC is further not described in this manual; see for more details the [V-Archive manual](#).*

## 2.3 Checklist for Tunnel connection



A connection between V-Tap and Apresa or PC software is needed to get the recorded data automatically into a user accessible database.

The following checklist can be used to setup this Tunnel connection:

- 1) Install the [Hardware](#).
- 2) Install Apresa or V-Archive PC [Software](#) and enable V-Tap connections.
- 3) Open the [Settings page](#) of the V-Tap in a browser, <http://vtapXXXX.local>  
*XXXX* are the last 4 digits of the MAC address, found on the bottom.  
*It may take up to a minute after first connect, before this local name is known to the PC.*
- 4) On the Settings page, the IP address of the Apresa or the PC with V-Archive must be entered as the "[Tunnel Server Address](#)".
- 5) Any **firewall** must have a rule that makes it possible to receive from TCP port **2016**, the default "[Tunnel Destination Port](#)". If secure connection with TLS is used for the Tunnel, then also TCP port **2017** must be open.  
*These ports are automatically opened during installation of V-Archive, if permitted by the PC.*
- 6) The Tunnel connection is stable when the **GREEN LED is steady**, not blinking!  
The V-Tap must be shown with its MAC address in the status line of V-Archive.
- 7) For first tests, better turn off "Tunnel Data Encryption". Otherwise, be sure that the Encryption password is the same in both V-Tap and Apresa or PC.
- 8) When data is stored during a call, the **BLUE LED** blinks.
- 9) To see if the PC receives something from the V-Tap, it is possible to make a network trace for test purposes. In V-Archive, go to menu Actions and select 'Network trace', press Start, make a short call, wait 10 seconds, press Stop and then Save. From the zip file 'tunneltrace.pcap' can be analyzed with Wireshark.  
The Apresa recorder has a similar option to make a network trace in menu Tools, System.
- 10) The SD card in the V-Tap should contain ".WAV" files. This SD card can be read by the V-Archive software in menu File and 'Import from V-Tap'.

## 3 Web interface and Settings

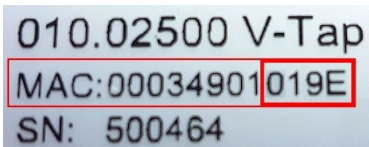
There are two ways to access the web interface of the V-Tap:

- 1) Connect a network cable to the LAN port on the unit. The other side of the cable can be connected to a LAN or directly to a PC.
- 2) When a Wi-Fi module is available it may not be enabled by default. To enable [temporary](#), power off and remove the SD card. Hold the button pressed during power on and keep pressed for about 12 seconds until only the Blue LED is on. Release the button, then Wi-Fi is available until the next reboot.

### 3.1 Access & IP address

In the case of using Wi-Fi, you need to enter the Wi-Fi access password first, which is the 12 digits MAC address of the V-Tap, also found on the bottom of the box. When connected (without internet), the IP address **192.168.55.66** must be entered in a browser. Remember to disabled mobile data on your phone (!), else this IP address is not found.

In the case of using a cable, DHCP is enabled and the V-Tap can be accessed with a browser by entering the address <http://vtapXXXX.local> In which **XXXX** are the last 4 digits of the MAC, as found on the bottom:




For this V-Tap:


Default cable address:	<b>http://vtap019e.local</b>
Default web Username:	<b>admin</b>
Default web Password:	<b>admin</b>
Default Wi-Fi Password:	<b>00034901019E</b> < <i>capitals here!</i>
Default Wi-Fi IP address:	<b>192.168.55.66</b>

<p>If no DHCP server is available on the cable, it can be disabled temporary by pressing the button for 1 second. The LED's will flash shortly and the V-Tap can be accessed on the IP address <b>192.168.55.66</b> See also <a href="#">Disable DHCP temporary</a> and <a href="#">Show IP address</a>.</p>
--

If still no access is possible, the easiest way to set a new fixed IP address is to use an SD card:



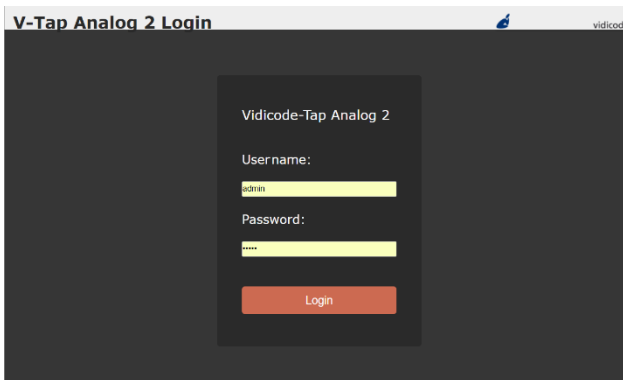
### Defining a fixed IP address with an SD card:



- . Create the text file “**IP**” on your PC.
- . The first line in this file must hold the IP address.
- . The second line is optional and can hold the IP mask.
- . Copy “**IP.TXT**” to the root directory of an SD card.
- . Insert the SD card into the V-Tap unit.
- . The IP address has now changed and can be accessed.
- . The file “**IP.TXT**” is deleted from the card by the V-Tap.
- . **Note:** The IP address **0.0.0.0** enables DHCP on the V-Tap.


## 3.2 Web interface

Entering the address in your browser will show the following screen:



Now enter “admin” for the Username and “admin” for the Password, then press the **Login** button and the Settings page appears:

*(The settings on the next page are not the default settings, but just an example.)*

**V-Tap Analog 2 Settings** 02-02-22 14:58:58  Vidicode

Name of this V-Tap	V-Tap_Analog_AAA401 <span>i</span>	Local Phone Number or Name	Alwin Line 1 <span>i</span>
DHCP Server	<input checked="" type="checkbox"/> <span>i</span>		
IP Address	192.168.0.31 <span>i</span>	Record from Audio Input	<input type="checkbox"/> <span>i</span>
Subnet Mask	255.255.255.0 <span>i</span>	Stereo Recording	<input type="checkbox"/> <span>i</span>
Gateway Address	192.168.0.5 <span>i</span>	Recording Quality	1 <span>i</span>
DNS Server Address	8.8.8.8 <span>i</span>	Button Mode	0 <span>i</span>
		Notification Message	<input type="checkbox"/> <span>i</span>
Tunnel Server Address	recording.vidicode.com <span>i</span>	Notification Volume	16 <span>i</span>
Tunnel Destination Port	2016 <span>i</span>	On/Off-Hook Level	90 <span>i</span>
Tunnel Data Encryption	<input type="checkbox"/> <span>i</span>	Caller ID Type	2 <span>i</span>
Encryption Password	<input type="password"/> <span>i</span>	Audio Activated Recording	<input type="checkbox"/> <span>i</span>
		Start Channel A (else B)	<input checked="" type="checkbox"/> <span>i</span>
Secure Connection with TLS	0 <span>i</span>	Audio Start/Stop Level	50 <span>i</span>
		Pre-Recording Time (100ms)	0 <span>i</span>
Wi-Fi Access Point	<input type="checkbox"/> <span>i</span>	Silence Timeout (sec)	7 <span>i</span>
Wi-Fi Tunnel AP Name	<input type="text"/> <span>i</span>	Automatic Level Control	<input checked="" type="checkbox"/> <span>i</span>
Wi-Fi Tunnel AP Password	<input type="password"/> <span>i</span>	Amplification Channel A	31 <span>i</span>
		Amplification Channel B	31 <span>i</span>
Login Username	admin <span>i</span>	Handset Amplification	<input type="checkbox"/> <span>i</span>
Login Password	<input type="password"/> <span>i</span>		
NTP Server Address	pool.ntp.org <span>i</span>	Licenses: Apresa / PC / S&U	1 / 1 / 02-22-2022 <span>i</span>
GMT Minutes Correction	60 <span>i</span>	New License Key	<input type="text"/> <span>i</span>
New Date (DD-MM-YYYY)	<input type="text"/> <span>i</span>	<a href="#">License Activation</a>	
New Time (HH:MM:SS)	<input type="text"/> <span>i</span>	V-Tap Analog 2 OS Version	1.0.30 02-02-2022 <span>i</span>
		V-Tap Analog 2 App Version	4.2.32 02-02-2022 <span>i</span>
Special Settings & Commands	<input type="text"/> <span>i</span>	Serial Number / MAC Address	501234 / 000349AAA401 <span>i</span>

Save & Logout
Cancel & Logout

Putting the mouse cursor on the ‘i’ behind a setting, will show extra information about that setting.

By pressing the **Save & Logout** button, the settings are sent to the V-Tap unit. Any ongoing recording is stopped, the file on SD card is closed, and after a few seconds the new settings are activated.

## 3.3 Settings

The settings are divided into groups that are described in the following paragraphs.

### 3.3.1 General Network settings

#### Name of this V-Tap

This field can be filled in with any name you like and is used for remote recognition of the V-Tap unit. The name is shown in the web interface and after connecting with ftp or telnet. The name is not used in the Tunnel protocol. The maximum length is 30 characters. The single and double quotation marks ( ' and " ) cannot be used !

#### DHCP Server

Default, DHCP is enabled and the V-Tap can be accessed with a browser by entering the address <http://vtapXXXX.local> XXXX are the last 4 digits of the MAC address, found on the bottom. When a DHCP server is available on the network, the IP address, Subnet mask, Gateway address and DNS address are automatically assigned. Without DHCP, they must all be entered manually. With default settings, DHCP can be disabled temporary by pressing the button for 1 second, see [Disable DHCP temporary](#). The DHCP setting is not used for Wi-Fi connections.

#### IP Address

As part of the local network, the V-Tap needs an IP address. In case DHCP is used, the DHCP server will assign the V-Tap an IP address. In case DHCP is not used, a static IP address must be filled in. The default address is 192.168.55.66 , see also [Access & IP Address](#). See the next page to setup for VLAN usage.

#### Subnet Mask

The subnet mask is used for so called 'subnetting', a way to logically divide one network into more networks. The logical AND of the IP address with the mask must be the same for the V-Tap and the computer connecting to it. The default mask is 255.255.255.0. In case DHCP is used, the mask is automatically obtained.

## Gateway Address

The Gateway address is used by the V-Tap unit when access outside the local network (LAN) is required. This sort of access can be needed by the Tunnel protocol for streaming to a remote computer and/or by the NTP feature for obtaining the current date and time. In case DHCP is used, the gateway address is automatically obtained.

## DNS Server Address

The Domain Name Service (DNS) is needed in case a name is entered instead of an IP address for the Tunnel server and/or the NTP server. The default DNS address 8.8.8.8 is the Google Public DNS, but the Gateway must be defined also before this address is reachable. In case DHCP is used, the DNS address is automatically obtained.

---

## Setup for VLAN tagging (IEEE 802.1Q)

To setup the V-Tap to take part of a Virtual LAN, the following option must be added to the IP Address:

**/MLAN<0-4095>** : Set the VID field and enable VLAN tagging.  
**/PRIO<0-7>** : Set the Priority field inside the VLAN tags.

The IP Address is then for example: **192.168.0.12 /MLAN256 /PRIO1**

All web access and the Tunnel connection on the LAN port are then sent with VLAN tags inserted, and the system only answers to packets with the same VID inside their tags.

Additional VLAN options can be added to the IP Address:

**/C** : VLAN tags in received packets are checked (default).  
**/X** : VLAN tags in received packets are NOT checked.

---



## 3.3.2 Tunnel settings

### Tunnel Server Address

Here you fill in the IP address or hostname of the Tunnel server that is going to receive the recordings coming from the V-Tap Analog. Leaving this field empty will disable the Tunnel function all together, in which case the V-Tap only stores recordings onto the SD card. The receiving server can be an Apresa recorder or a PC running the V-Archive software. In both cases, the V-Tap needs a license to allow Tunnel data to be uploaded/streamed to the Tunnel server.

It is also possible to send the recordings to two servers, by entering two addresses with a plus sign in between. For example:

192.168.0.38 + recording.vidicode.com

Recordings are sent to one server at the time; when finished with a file, it is sent to the other server.

**Without a license, the receiving server will discard the Tunnel data.**

### Tunnel Destination Port

The Tunnel protocol is based on the TCP protocol and that involves a Destination Port and a Source Port. Both are numbers from 0 till 65535 that are included in each packet and are very important for the receiving end of the Tunnel data. The receiving Tunnel server must be setup to look for the same port number as is installed in this Tunnel Destination Port.

Not all TCP port numbers are available for tunnelling, because some are officially used by other protocols. For example, port 80 is used for HTTP in all browsers to communicate over the World Wide Web.

A list of known port numbers can be found on the internet.

The default port number 2016 is not an official port and can be used safely for this Tunnel protocol. The only drawback of using an unknown port number is, that a firewall will block this port. For that reason, it is important that any firewall that is passed by the Tunnel stream must be setup right.

Add **/TLS<port>** to use a different port number for a Tunnel-TLS connection, default port 2017 is used by the system (normal port + 1).



**Firewalls must have a rule to let through TCP port 2016.**



## Tunnel Data Encryption

The data inside the Tunnel protocol is sent encrypted over the network. The used method is AES with a 256-bit Cryptographic Key. For privacy reasons it is advised to leave the encryption enabled.

## Encryption Password

This parameter is used for the encryption of the Tunnel data and the file on SD card (see below). The receiving side of the Tunnel data, the Apresa or V-Archive software, must use the same password. Leaving the password empty is still doing the encryption but is less secure. Comma's and single and double quotation marks cannot be used !

### 3.3.3 Secure Connection with TLS

Secure network connections with the Transport Layer Security cryptographic protocol (TLS) can be enabled here by adding together the following numbers:

- +1** enables TLS for the Tunnel connection
- +2** enables TLS for the web interface (HTTPS)
- +4** disables certificate verification for Tunnel-TLS

For example, to enable TLS for both the tunnel and the web interface, enter **3**.

Note that Tunnel Data Encryption and any TLS mode cannot be active at the same time, in which case TLS is preferred by the system.

The used port number for Tunnel-TLS can be changed in the Tunnel Destination Port setting, by adding the option **/TLS<port>**. For example:

Tunnel Destination Port = 2016 /TLS7871

Certificates for TLS connections can be added to the system with the following three files:

- TUNNEL.CRT** for the Tunnel-TLS certificate
- HTTPS.CRT** for the HTTPS certificate (optional)
- HTTPS.KEY** for the HTTPS private key (optional)

Put one or more of these files on an SD card and insert the card into the V-Tap. The files are then automatically copied to internal memory and removed from the card.

It is also possible to upload these files by using an FTP connection.

For Tunnel-TLS, the certificate can be downloaded from the Call Recorder Apresa or the V-Archive software on the PC.

For HTTPS, the certificate and private key are automatically generated, if they do not exist.

For more information about TLS, see the chapter: [TLS on the V-Tap](#).

### 3.3.4 Special Tunnel & Network settings

Next follows a description of some settings for the Tunnel and network, which must be entered in [Special Settings & Commands](#).

#### .TS<port> = Tunnel Source Port (default 0 = random)

The Source Port also has an important role in the Tunnel protocol. The default number 0 selects randomly a port number between 49152 and 65535. This range of port numbers is recommended by IANA to be used for dynamic ports.

Once a connection has been established between the V-Tap and the receiving Tunnel server, the chosen port number is kept active for the duration of the communication session. When connection is lost for some reason, a new source port is chosen for the next connection. This ensures fast reconnection, because the TCP protocol does not allow the same source port to be used again within a short time. After an OS specific timeout of normally a few minutes, the port numbers become available again for reuse.

It is therefore not recommended to select a fixed number for the Tunnel Source Port in cases where live streaming is done without using an SD card.

#### .TC<sec> = Tunnel Connect Timeout (default 22 seconds)

This timeout is used when the V-Tap tries to connect to the Tunnel server. The default 22 seconds is enough to send 4 requests. If no reply comes from the remote side within the timeout, the V-Tap starts trying again after a few seconds with a new source port number (see above). Storage onto SD card just continues and is not interrupted by any connection or disconnection of the Tunnel.

#### .TI<sec> = Tunnel Idle Timeout (def 0 = always connected)

This timeout is used to disconnect the active tunnel connection, only when no packets are received (sniffed) anymore from the local connected network. Default, the idle timeout is disabled and the tunnel stays connected forever.

 **.TK<sec> = Tunnel Keep-alive Timer (default 60 seconds)**

This timer is used to keep the connection alive between the V-Tap and the Tunnel server. Default, a dummy TCP packet is sent every 60 seconds by the V-Tap to the server.

 **.LX<size> = Maximum Data Size in packets (default 1024)**

This sets the maximum length of the data portion inside all communicated packets on the network for Tunnel, FTP and Web. The length excludes the Ethernet, IP and TCP headers, which are 54 bytes together. The maximum length of any packet on the network can be 1514 bytes, so that leaves max **1460** bytes for the data part. The default length is based on optimal performance when sending data from an SD card.

When sending directly on a WAN or very busy LAN, the length might be decreased for better performance (try **.LX512**).

 **.LS<num> = LAN System Service Timer (default 18 = fastest)**

The default value is for fastest network speed. When a lot of V-Tap units are sending to the same Tunnel server, it might be better to lower the speed to prevent an overload of streams.

The values 65 and 1 can be used for slow and slower sending.

The values 50 and 18 (same as 0) can be used for faster sending.

**NOTE:** When using the RTR Call Monitoring Software for the PC, the LAN Service Timer must be set to 1 to get a constant audio stream.

### 3.3.5 Wi-Fi settings

The Wi-Fi module in the V-Tap may not be enabled by default. To enable temporary do the following:

Power off and remove the SD card. Hold the button pressed during power on and keep pressed for about 12 seconds until only the Blue LED is on. Release the button, then Wi-Fi is available until the next reboot.

Once Wi-Fi is enabled, you can use your mobile phone or a laptop to connect to the V-Tap over the air to access the settings:

- Search for Wi-Fi apparatus on your smartphone or laptop, the V-Tap name "V-Tap\_Analog\_xxxxx" is then shown.
- Select it and when asked for a password, use the 12 digits MAC address of the unit, found on the bottom of the box. The first 6 digits of the MAC are always 000349 and the last 6 digits are also part of the Wi-Fi name.
- Disable mobile data on your phone (!), open a browser and enter the IP address 192.168.55.66. The web login page should appear. Login with username "admin" and password "admin".

The internal Wi-Fi works as an Access Point (AP) for web access and, at the same time, can act as a station to connect to an external AP for the tunnel function. DHCP is always enabled for Wi-Fi.

#### Wi-Fi Access Point

This enables or disables the web access using Wi-Fi permanently. The [temporary access](#) with the button is always available. The password to connect with Wi-Fi can be changed in the [Login Password](#) field.

#### Wi-Fi Tunnel AP Name

#### Wi-Fi Tunnel AP Password

To setup a tunnel connection over Wi-Fi, the V-Tap must connect to an external AP. In most of the cases this will be a router somewhere in the building. The AP's name and password must be filled in here.

The Wi-Fi module can be disabled completely by turning off the Wi-Fi Access Point option in the settings AND the Tunnel AP fields must be left empty. All further access must then be done through a LAN cable.

Sending tunnel data with Wi-Fi is slower than using a LAN cable. So, some delay must be considered before files are transferred.

### 3.3.6 Login settings for Web access & FTP

The internal web server can be accessed by entering the address of the V-Tap in the address bar of any browser. See also [Access & IP Address](#).

The V-Tap also has a built-in FTP (File Transfer Protocol) server that allows you to access the internal filing system. At this moment, this is only used for updating the firmware remotely; see [Firmware update](#).

FTP is disabled by entering ".FPO" in [Special Settings & Commands](#).

#### Login Username

Username to log in to the Web settings page and FTP.  
The username field can be maximum 30 characters long.  
Spaces, commas, the single and double quotation marks (' and " ),  
and the back- and forward-slashes (\ and / ) cannot be used !  
The default username is "admin".

#### Login Password

Password to log in to the Web settings page and FTP and [Telnet](#).  
The total password field can be maximum 30 characters long.  
Spaces, commas, the single and double quotation marks (' and " ),  
and the back- and forward-slashes (\ and / ) cannot be used as the  
password ! The default password is "admin".

The option **W<xxxxxxxx>** can be added to set the Wi-Fi password.  
This Wi-Fi password must be minimal 8 characters long.

### 3.3.7 NTP and Date+Time settings

NTP (Network Time Protocol) can be used to synchronize the internal clock with the world-clock. The V-Tap also has its own accurate internal clock and battery to keep the clock running when power fails, but it is safer when NTP is also used.

NTP gets the exact clock from the server and the internal clock is updated with this, which is important to get the date and time right for all recorded calls.

The V-Tap synchronizes the clock 6 times per day (each 4 hours).

The default port number for NTP is 123 and can be changed by entering “.NP<port>” in [Special Settings & Commands](#).

#### NTP Server Address

The IP address or the hostname of the NTP server. Default, the address is set to “pool.ntp.org”, but the Gateway and the DNS server must be defined also for this to work.

A second NTP server for backup can be added with a plus-sign in between. For example: pool.ntp.org + time.google.com

The option /X can be added behind the address(es) to disable the correction for the Daylight Saving Time (Summer Time).

Make this address field empty when no NTP is used.

#### GMT Minutes Correction

The time correction in minutes to the GMT (Greenwich Mean Time) zone. The number can start with the minus sign when needed.

For example, enter “-300” for Eastern Time (that is -5 hours for east-coast US & Canada).

#### New Date (DD-MM-YYYY)

#### New Time (HH:MM:SS)

The current date and time are shown on top of the page. A new date and/or time can be set with these parameters

For the date, the entered format must be day, month and year, separated by the minus-sign and always 10 characters long in total.

For the time, the entered format must be hour, minutes and seconds, separated by the colon-sign and always 8 characters long in total.

The new date and time are set after pressing **Save & Logout**.



### 3.3.8 Local Phone Number

#### Local Phone Number or Name

This number or name represents the recorded telephone of the local side. It is used to complete the meta data and for recognition of the calls later on in the Apresa or V-Archive database.

A number or name are both possible, up to a maximum of 15 characters. A name is shown in capitals in the database software.

The remote phone number is obtained from the dial process during outbound calls (received DTMF) or from the received Caller ID during inbound calls.

### 3.3.9 Audio Input setting

#### Record from Audio Input

The 3 mm audio plug at the back is taken as the audio source for recording when this setting is enabled. The audio switch at the back must also be set as 'input', which is the default position.

By default, this setting is off and the Phone and PABX jacks are taken as the input source.

The audio jack can record from microphone's or other audio sources, such as an audio output signal from a radio system.

Recording in this way can produce high quality recordings, especially when [Stereo Recording](#) is enabled and the Recording Quality is set to 2 or 3 (sample rate 16 or 32 KHz).

When recording from the audio plug, the start/stop method must also be changed to manually with the [Button Mode](#) or automatically with [Audio Activated Recording](#).

### 3.3.10 Stereo Recording & Recording Quality

#### Stereo Recording

Stereo recording can be of use when the V-Tap Analog is connected to a 4-wired handset on the line inputs. Then the audio of the speaker and microphone signals (remote and local sides of a call) are stored separately in the recorded files.

Recording from the audio input plug is also possible in stereo.

Note: Files will get twice as big when stereo is enabled.

#### Recording Quality

This value can be filled in as follows:

- 1 = Sample Rate 8 KHz (default)
- 2 = Sample Rate 16 KHz
- 3 = Sample Rate 32 KHz
- +4 = PCM 16-bits (else G.711 A-Law compression)
- +8 = Store Channel A samples only
- +16 = Store Channel B samples only for Local-side-recording!
- +32 = Disable Noise Gate for Auto Level Control

For normal analog lines, the bandwidth frequency is specified up till about 4000 Hz. A sample rate of 8 KHz is therefore enough to get good quality recordings.

Some lines have better bandwidth, and especially when recording from a handset, a sample rate of 16 KHz will give much nicer recordings. The files will get twice as big with 16 KHz.

Recording with a sample rate of 32 KHz is of no use for analog lines or phones. This can be used to make high quality recordings from the audio input. The files will get four times bigger with 32 KHz.

By default, each sample is compressed with G.711 A-Law to an 8-bit value. Adding 4 to the sample rate (thus enter 5, 6 or 7) will store each sample as an uncompressed 16-bit value. The uncompressed files will again get twice as big.

Storing one channel only in the file is only usable when recording from a 4-wired handset or the stereo audio input.

### 3.3.11 Button Mode setting

The button can be used to manually start and stop recording calls. Other special functions of the button are described in chapter [Button functions](#)

#### Button Mode: 1=Start 2=Stop

Manual recording with the button is enabled when this setting is other than zero. Manually starting and stopping is used when one phone is connected and the user can press the button on the V-Tap.

The following values can be entered:

**1 = Start mode.** Each call starts with the Red LED OFF (not recording).  
The user must press the button before or during the call to save the recorded data. Non-saved calls are deleted from the SD card.

**2 = Stop mode.** Each call starts with the Red LED ON (recording).  
The user must press the button before or during the call to cancel saving of the data. Non-saved calls are deleted from the SD card.

**3 = Manual Start-Stop mode.** Each time when the button is pressed during a call, a recorder file is opened or closed on the SD card. After power on, the Red LED is OFF, so the V-Tap is not recording.

**Mode + 4 =** When 4 is added to mode, the V-Tap is in 'pre-recording' mode, meaning that all audio of all calls is always stored, even after stopping with the button. Normally, the audio storage is stopped or started when the button is pressed. The decision to keep or delete the recording is made at the end of each call, depending on the state of the Red LED at that time. One advantage is, that the user can press the button in the middle of a call to 'start' it and then the complete call from the beginning is saved.

**Mode + 8 =** The non-saved calls are kept on the SD card, but are NOT sent to the Tunnel server. Keeping these files can be used for safety reasons, giving the possibility to retrieve them later. These files have a different file name and are only deleted from the card when overwritten or by the "SD Delete File after Sending" function.

**Mode + 128 =** Use an External Button on the Mini DIN8 pin2.

**Watch the Red LED: ON=Started (Recording) , OFF=Stopped**

## 3.3.12 Notification Message settings

### Notification Message

By enabling the notification message, a unique feature of the V-Tap Analog is activated. At the start of each recording a message is played on the line that can be heard by both local and remote caller. The message is stored onto the V-Tap in the file "NOTIFY.WAV", which can be changed by the user.

See further chapter [Notification & System Messages](#).

#### **Important Note:**

When off-hook detection is used on an analog line, the system knows the direction of the calls. Standard in this situation, outgoing calls are NOT recorded, when notification is enabled!

To enable the recording of outgoing calls in this case, add 32 to the Notification Volume (see below).

### Notification Volume

The playback volume of the notification message can be set from 0 till 20 (higher is louder) and is in steps of +3dB.

Other values can be added to set the following features:

+32 : Record outgoing calls when notification is enabled.

+64 : Include the notification message in the recordings.

#### **Note1:**

The default volume is too loud when the V-Tap is connected to the handset of a phone instead of an analog line. The value should be set about 7 steps lower in that case.

#### **Note2:**

The volume of the message, as heard on the line, strongly depends on the way how it was recorded earlier on another machine (louder audio in the file is better).

### 3.3.13 Analog settings

#### On/Off-Hook Level

This level is used to detect if the connected analog phone has taken the hook/handset or not. The V-Tap must be connected in between the phone and a normal analog line for this to work.

The value can be set from 0 till 255 and a lower value means a more sensitive off-hook detection (higher is a more sensitive on-hook detection). The level on 0 (zero) disables the hook detector.

The value 256 can be added to set a special feature; the dialling process for outgoing calls is not recorded then. Recording starts after dialling the last digit and after a timeout of 4 seconds. Another time can be set with the ".ID<sec>" in [Special Settings & Commands](#).

#### Caller ID Type

Caller ID is a feature of the connected analog line. The phone number of the caller is then passed to the called party. So, this works for inbound calls only. Not all lines do have Caller ID available, depending on the provider or PABX that serves the analog line. Only three values can be entered:

1 = DTMF type or 2 = FSK V.23 type or 3 = FSK Bell 202 type

#### Audio Activated Recording

Detecting the start and the end of a call can be done in two ways. Default, the hook method is active, meant to be used with analog telephones on a normal analog line, using the middle 2-wires on the jack. In that case, the On/Off-Hook Level is used to start and stop recording.

The second method uses an audio level detector and the Audio Start/Stop Level is used to start and stop recording. This method must be used when the V-Tap is connected to the handset of a telephone, using all 4-wires (2 for the microphone and 2 for the speaker).

Getting numbers with Caller ID and DTMF detection do not work in audio activated mode and the on/off-hook detector is disabled.

When connected to a handset, the Handset Amplification is normally also enabled, because the audio coming from a handset is much lower in volume than the audio coming from an analog line.

### Start Channel A (else B)

This setting is only used when Audio Activated Recording is enabled. The Start Channel is very important in the case recording is done from a handset, because a 4-wired handset produces two audio signals; one from its speaker and one from its microphone.

To determine the start of a call, the system can look at the audio of the selected channel A or B only (speaker or microphone).

The goal is to set the Start Channel to the speaker signal, because the microphone of most phones is still active when the phone is idle and therefore produces too much audio when the handset is on-hook. This would then result in constantly false detection of calls and audio files are created when the room is noisy.

Most of the time, also the speaker produces some audio when the phone is idle, but that level is much lower than the one produced by the microphone.

To start on both channels A+B, add 512 to the Pre-Recording Time.

### Audio Start/Stop Level

This value is only used when Audio Activated Recording is enabled. The start and stop level is a border for the system to decide if a call has started or stopped.

The value can be set from 0 till 255 and a lower value means a more sensitive detection of audio/voice.

Stop is detected when the audio is below the level for the duration of the Silence Timeout (see below).

The level on 0 (zero) disables the audio detector.

To set the sensitivity of the audio detector, a value can be added:

+ (1 till 127) x 256 : Debounce per 10 ms. The default is 200 ms.

For example; to set a debounce of 100 ms, add 2560 (10 x 256).

### Pre-Recording Time (per 100ms)

This value is only used when Audio Activated Recording is enabled.

The system continuously stores audio samples in a rotating buffer.

When the start of a call is detected, some time in front can be taken, so no word is missed.

The maximum is 240, which is 24 seconds when recording with a sample rate of 8 KHz in Mono mode.

The value 512 can be added to set a special feature; then both channels A and B are used to detect audio for start.

### Silence Timeout (per second)

This value is only used when Audio Activated Recording is enabled. The end of a call is detected when the audio level is below the Audio Start/Stop Level for the whole duration of the Silence Timeout. When the timeout is too short, calls are split into multiple recordings. When the timeout is too long, consecutive calls can be merged into one recording. The timeout on 0 (zero) is only useful in combination with the Button Mode set to start-stop.

### Automatic Level Control

The hardware can automatically control the amplification of the input signals when the volume of the audio is low. The result may be that the recording sounds less natural than a recording without ALC.

### Amplification Channel A

### Amplification Channel B

In the case Automatic Level Control is disabled, the amplification of the input signals can be set manually to a fixed value. In the other case that Automatic Level Control is enabled, the volumes are controlled by the hardware automatically and the amplification settings are unused, except the value 0. There are two channels A and B, because the input signals can come from a 4-wired handset cable (speaker and microphone signals) or from the stereo audio input plug. The amplification can be set from 1 till 63 (per +0.75 dB). The value **0** is a special case; the channel is disabled for recording.

Other values can be added to set the following features:

- +64 : Extra amplifier enabled for this channel only (20x boost).
- +128 : Automatic Level Control enabled for this channel only.
- +256 : Inject Notification enabled for this channel only.
- +512 : Boost the recorded signal on this channel by +13 dB.

### Handset Amplification

Extra amplifiers (20x) can be enabled when the audio signals have a very low volume. Activating this setting is almost always needed when the V-Tap is connected to the handset of a phone (4-wires).

## 3.3.14 Special Settings & Commands

### Special Settings & Commands

In this field extra settings can be entered, used to alter functionality or to setup alternative modes of operation.

All special settings start with a dot in front, followed by two letters.

Some of them also require a numeric value behind.

There are a few special commands, without the dot.

### Special Commands

- "SD" = Show free space on the card after each reboot; [more info](#).
- "FORMAT CARD" = Format the SD card. All data on the card will be deleted!
- "FACTORY" = Back to factory settings, except all licenses. IP is default!
- "FACTORY WIFI" = Factory settings AND enable Wi-Fi module & settings.
- "FACTORY NOWIFI" = Factory settings AND disable Wi-Fi module & settings.

### Special SD card Settings (see also [Special SD card settings](#))

- ".SR" = Remove files from the card after sending.
- ".SA" = Disable Auto Delete when the card is (almost) full.
- ".SP" = Enable SD Power Save Mode (slow clock during idle).
- ".FF<max>" = Maximum number of Files on the card (default 10000).
- ".FS<size>" = Maximum File Size in MB (default 250).
- ".SI<mhz>" = SD card Interface Speed in MHz (default 50).
- ".CS" = Show all current SD file-counters; [more info](#).
- ".CR<cou>" = Set Read file-counter.
- ".CW<cou>" = Set Write file-counter.
- ".CD<cou>" = Set Delete file-counter.

### Special Recording settings

- ".II" = Disable recording of Incoming calls.
- ".IO" = Disable recording of Outgoing calls.
- ".IM<sec>" = Set Minimum Call Duration in seconds (default=0).
- ".ID<sec>" = Set Dial DTMF Timeout in seconds (see On/Off-Hook Level).
- ".IR" = Record outgoing calls when notification is enabled.
- ".IN" = Include the notification message in the recorded files.
- ".IA" = Always play notification message, also when not recording.
- ".IB<sec>" = Notification Beep Interval in seconds, using "NBEEP.WAV".
- ".IW<sec>" = Notification Beep Interval in seconds, using Square Wave.
- ".IL<num>" = Notification Beep Length for Square Wave (default=62).
- ".IF<num>" = Notification Beep Frequency for Square Wave (default=2).



## Special Analog & Audio settings

".AS<num>"	= Set Audio detect Sensitivity 0-255 per 10ms (default=15)
".AH<num>"	= Set Hook detect Sensitivity 0-255 per 10ms (default=10)
".AA<num>"	= Set Audio to output 0-3; bit0=A (left) , bit1=B (right)
".AI<num>"	= Set Input to output 0-3; bit0=A (left) , bit1=B (right)
".AT<num>"	= Set ALC Target level 0-15 per 1.5dB (default=11= -6dB).
".AN<num>"	= Set Noise Gate Threshold 0-31 per 1.5dB (default=28= -6dB)
".AF0/1"	= High Pass Filter 0=off or 1=on (default=off)
".AR0/1"	= Ring detect line on 0/1
".GD<num>"	= Gain for DTMF detect 0-7 (default=3)
".GF<num>"	= Gain for FSK detect 0-7 (default=3)
".GH<num>"	= Gain for Hook level detect 0-3 (default=0)
".GV<num>"	= Gain for Voice level detect 0-3 (default=0)
".GI<num>"	= Gain for Chan A+B inputs 0-3 (default=0=0dB per +10dB)
".GA<num>"	= Gain for Channel A input only ( " " )
".GB<num>"	= Gain for Channel B input only ( " " )
".GR<num>"	= Gain for Recorded file 0-255 (default=177= -9dB per +0.5dB)
".VP<num>"	= Volume for Playback 0-255 (default=255= 0dB per +0.5dB)
".VD<num>"	= Volume for Detect output 0 or 1 (default=1=0dB , 0=-6dB)
".VO<num>"	= Volume for Audio outputs 0-127 (def.=121=0dB per +1dB)
".VL<num>"	= Volume for Audio output A only ( " " " )
".VR<num>"	= Volume for Audio output B only ( " " " )
".VI<num>"	= Volume for Chan A+B in2outs 0-7 (default=7=0dB per -3dB)
".VA<num>"	= Volume for Channel A in2out only ( " " " )
".VB<num>"	= Volume for Channel B in2out only ( " " " )
".OH<num>"	= Offset for Hook detect 0-2047 (default=508)
".OV<num>"	= Offset for Voice detect 0-2047 (default=0)
".OP<num>"	= Offset for Playback 0-65535 (default=32767)

## Special Wi-Fi settings

".LAN"	= Start with the LAN cable and fallback to Wi-Fi connection.
".WF"	= Disable Fallback from Wi-Fi to LAN cable.
".WW"	= Disable WPA2_PSK encryption (= Open Wi-Fi no password).
".WC<chan>"	= Set Wi-Fi Channel ID; 1 till 13.
".WR<pow>"	= Set Wi-Fi RF TX Power; 0 till 82 per 0.25 dBm (default 58).
".WD"	= Set the DNS server for Wi-Fi the same as the LAN cable.
".WN"	= Disable NTP from Wi-Fi.
".WI<ip>"	= Set IP address for web server access, default 192.168.55.66
".WH"	= Set DHCP range <ip>1 till <ip>9 when using .WI
".WL"	= Disable the web login page after Wi-Fi connection.
".WT<secs>"	= Set Timeout for the TCP web server (default 90).
".WK<secs>"	= Keep-alive timer for the Wi-Fi Tunnel connection (def 60).
".WUP"	= Try to update the Wi-Fi module.
".WZ1/0"	= Disable(WZ1)/Enable(WZ0) Wi-Fi module during recording.

## Special Tunnel & Network Settings (see also [Special Tunnel & Network](#))

- ".TS<port>" = Tunnel Source Port 0-32767 (default 0 = random).
- ".TC<secs>" = Tunnel Connect Timeout (default 22 seconds).
- ".TI<secs>" = Tunnel Idle Timeout (default 0 = stay always connected).
- ".TK<secs>" = Tunnel connection Keep-alive Timer value (default 60).
- ".TV<secs>" = Tunnel Encrypt Vector renewal Timer value (default 15).
- ".NP<port>" = NTP Port number 0-32767 (default 123, 0=NTP disabled).
- ".FP<port>" = FTP Port number 0-32767 (default 21, 0=FTP disabled).
- ".FT<secs>" = FTP Failure Timeout (default 30 seconds).
- ".LX<size>" = Maximum Data Size in network packets (default 1024).
- ".LS<byte>" = Internal network service timer (default 18).
- ".DT" = Disable Telnet connections.
- ".TF" = Disable EtherType Filter (default IP & ARP packets only)!
- ".LH" = Force Half Duplex on all LAN ports.
- ".LM" = Force 10 Mbps on all LAN ports.

## Other Special Settings (debug/test purposes)

- ".UD" = Disable USB function, so no HID recognition (saves power).
- ".UP" = Disable USB Pausing (no interrupts 10 minutes after power on).
- ".UF" = Flash Wait States on 4 (else default on 5).
- ".UC" = Disable CPU Cash Controller (much slower).
- ".UM" = Disable Memory Protect Unit (slower).
  
- ".LI" = Initialize the IP-stack each time after closing the tunnel.
- ".LB" = Initialize the IP-stack twice during boot-init.
- ".LU" = The time is always Summer Time in the NTP function (DST).
- ".LN" = Disable Summer Time correction in the NTP function.
- ".LR" = When DHCP is enabled, a daily reset is done at 03:00.
  
- ".I2C<num>" = Set I2C interface speed 160/8x<num> (default 50 = 400 KHz).
- ".DFC<num>" = Set SPI interface speed 160/<num> (default 40 = 4 MHz).
- ".MAC<hhhh>" = MAC Configuration bits (4 hex digits, default C250).
  
- ".AW<reg>=<val>" = Write a codec register with a value.
  
- ".XO" = Debug mode enabled. Output to the serial port (57600,n81).
  
- ".XF" = Open Debug Trace file. The file TRACE.TXT is closed again after web login. Then ".DT" must be removed again and the settings saved. TRACE.TXT can be read from the SD card or downloaded with ftp.

### 3.3.15 Licenses & Versions

#### Licenses: Apresa / PC / S&U

#### New License Key

The Channel Licenses for a Call Recorder Apresa and a PC running V-Archive, and the end-date for Support & Update are shown here. A Channel License (also called Recorder License) is the right to upload a recorded call via the Tunnel to the Tunnel server, which is the Apresa recorder or the V-Archive software on a PC. The end-date is the last day that the user can ask for support or update the firmware on the unit.

#### **NOTE:**

At least one Channel/Recorder License is needed before the system starts recording any calls. Adding new licenses is further described in a separate quick guide about [V-Taps and Licenses](#).

#### V-Tap Analog 2 OS Version

#### V-Tap Analog 2 App Version

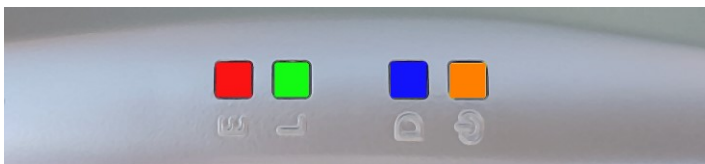
Firmware versions are shown for information purposes only and cannot be changed.

#### Serial Number / MAC Address

The Media Access Control (MAC) address of each device operating on an Ethernet network is a unique identifier that is needed to route the packets over the LAN.

The serial number and MAC address are both shown for information purposes only and cannot be changed.

## 4 LED's



E = Error (Red)  
L = Link (Green)  
D = Data (Blue)  
@ = SD-Power (Amber)

The 4 LED's are important for feedback to the user. Specially during first installation, the LED's can tell you if things are going wrong or right.

Situations with the LED's that are related to pressing the button are described in the next chapter [Button functions](#) .

The situations during normal operation are described below, per LED.

### 4.1 Red Error LED

The Red LED is used to indicate an error situation or to show the recording state when the button start/stop mode is configured.

- *Red LED steady ON plus Amber LED blinking.*  
This is the factory default and means that no SD card is inserted, so no data is stored. Inserting an SD card solves the situation.
- *Red LED steady ON plus Amber steady ON.*  
This can happen as soon as a call starts and the system has no Channel Licenses.
- *Red LED steady ON plus Amber LED blinking fast.*  
A read- or write-error happened on the SD card or the SD card is not usable by the system. This can only be solved by removing the card again. Check if the card lock-switch is on, else it is recommended to verify the card on an external PC.

- *Red LED steady ON and all other LED's OFF.*  
This situation can happen in two cases:  
Or the USB power supply does not generate enough current; try using a stronger USB port or power supply.  
Or the software in the system does not run at all, due to a hardware failure; contact your dealer.
- *Red LED steady ON with "Button Start/Stop" function.*  
If manual recording with the button is enabled, then the Red LED ON means that recording is active.
- *Red LED blinking plus Green LED blinking.*  
The system cannot connect to the Tunnel server.  
See also *Green LED blinking* below.
- *Red LED blinking once per second.*  
This happens when you take out the SD card while the system was still busy writing to it. So, an unclosed (0 bytes) file is now on the card. For more information, see [Remove SD Card safely](#).
- *Red LED blinking fast.*  
This indicates that the analog line is disconnected. It can only happen when on/off-hook detection is selected for start/stop.
- *Red LED blinking fast, together with all other LED's.*  
This happens after a fatal error in the application. The firmware must be updated.

## 4.2 Green Link LED

The Green LED shows the status of the link to the Tunnel server or the recording state when the button start/stop mode is configured without using the Tunnel. See also [Button Mode setting](#).

- *Green LED blinking.*  
The system tries to connect to the Tunnel server. This can last forever, but normally it should take a few seconds after reset. When longer, the Tunnel server could not be found, or the network connection is bad. The Red LED also starts blinking in that case. Check the **firewall** on the PC or switch!  
The Green LED goes to steady ON when the connection is made.

- *Green LED steady ON.*  
The link to the Tunnel server is OK.  
When start/stop with the button is selected and no Tunnel is configured, it means that recording is active.
- *Green LED OFF.*  
The only normal situation with the Green LED OFF is, when no Tunnel server is defined in the settings and an SD card is inserted.  
When start/stop with the button is selected and no Tunnel is configured, it means that recording is NOT active.

### 4.3 Blue Data LED

- *Blue LED blinking.*  
The Blue LED blinks to indicate that audio data is stored.  
In other words, recording is active; a file is opened on the SD card and data is written to it.  
Also during Wi-Fi initialization, the Blue LED can blink shortly.

### 4.4 Amber SD-Power LED

The Amber LED shows the status of the SD card and power.

- *Amber LED steady ON.*  
This indicates that an SD card is inserted and is ready to be used by the system.
- *Amber LED blinking short (Red LED OFF).*  
This indicates that an SD card is inserted, and the system is reading data from a file during sending with the Tunnel function.
- *Amber LED blinking fast (Red LED ON): SD card ERROR.*  
A read- or write-error happened on the SD card or the SD card is not usable by the system. The card must be removed and checked.

## 5 Button functions



The various button functions are described in the following paragraphs.

### 5.1 Start & Stop recording

When the “Start and Stop with Button” function is enabled, the Red LED indicates if recording is active or not. The Red LED OFF means that recording has stopped. The Red LED ON means that recording is active, and data is stored on SD card and sent to the Tunnel server. Manual recording is further explained in the [Button Mode setting](#).

### 5.2 Remove SD Card safely

In the case the SD card is taken out without precaution, a possibly open file is not closed properly and will have a content of zero bytes. The appearance in the directory remains. Also, there is a very small chance that the directory or some file gets corrupted by doing so. Therefore, to take out the card safely it is recommended to close all files first with the following procedure:

- **Press the button: All LED's are ON.**
- **Hold pressed for 2 seconds: Amber and Blue LED go OFF.**
- **Release the button: Amber LED starts flashing.**
- **Take out the SD card safely now.**

**NOTE1:** The above procedure does not work when the Button Mode is set, in which case the SD card can just be taken out.

**NOTE2:** When the Blue LED is not blinking, then no recording is busy, so no data is written, in which case the SD card can also be taken out.

## 5.3 Disable DHCP temporary

When running with default settings, there is a way to disable DHCP temporary. Then the settings can be reached through the web interface with the fixed IP address 192.168.55.66. If no settings are done, then DHCP is enabled again after reset.

- Press the button: All LED's are ON.
- Hold pressed for 1 second.
- Release the button: Red, Green and Blue LED's flash 3 times
- The web page is now reachable on IP address 192.168.55.66

**NOTE:** The IP address of your PC must lie in the range 192.168.55.0 till 192.168.55.255 and the IP mask should be 255.255.255.0.

## 5.4 Show IP address

The IP address of the V-Tap unit can get lost for some reason or is unknown, because a DHCP server is used and the name protocol does not work (MDNS). In other words, the user cannot reach the web interface anymore. There is a way to reset all settings to factory values (see next chapter), after which DHCP is enabled again.

If that is not desirable, then there is a way to show the IP address with the LED's (this does **not** work when the Button Mode is set):

- Press the button: All LED's are ON.
- Hold pressed for 5 seconds: All LED's go OFF.
- Release the button: Only the Green LED goes ON.
- Press the button now and the first digit is shown:
  - Green LED goes OFF,
  - Red LED blinks the first decimal digit (count!),
  - Green LED goes ON when finished.
- Repeat pressing the button for the next digits. For example: "192.168.0.10" needs the button to be pressed 12 times.
- The Blue LED blinks once to show there is a dot in the address.
- When Red or Blue is not blinking at all in between Green going OFF-ON, it means the zero digit.
- After the last digit, the system waits 5 seconds and then continues normal operation.



## 5.5 Copy Settings from SD card

The V-Tap automatically copies the settings files to the root of the SD card, directly after insertion (only if they do not exist already). The file CFG.VTH from the SD card can be edited with a text editor on the PC and then be copied back to internal memory. To do so, the SD card must be inserted while holding the button pressed on the V-Tap.

## 5.6 Factory settings

To reset all settings to factory default, the following must be done:

- Remove the SD card.
- Power Off the unit.
- Press the button.
- Power On and hold the button pressed; all LED's are ON.
- Release the button within 5 seconds; RGB LED's go OFF.
- Press the button 5 more times; RGB LED's blink fast.
- After 5 seconds, the system reboots automatically.

The procedure above is only possible when the system is running normal. With corrupted firmware, a special update must be done with an SD card (see [Firmware update](#)).

## 5.7 Format SD card

To format an SD card, insert the card somewhere during the factory settings procedure above, after the first release of the button. A second method is to enter "FORMAT CARD" in [Special Settings](#).

## 5.8 Default IP address

When the application does not seem to run at all anymore, then a reset to factory settings is not possible. Besides a special update with the SD card (see below), there is still a way to look with FTP in the filing system remotely. The following can be done:

- Remove the SD card.
- Power Off the unit.
- Press the button.
- Power On and hold the button pressed for 1 second.
- The IP address is now on the default value 192.168.55.66
- Only access with FTP is now possible (no web interface).

## 5.9 Temporary access with Wi-Fi

The V-Tap may have a built-in Wi-Fi module that is not enabled by default. To enable Wi-Fi temporary do the following:

- Power off and remove the SD card.
- Hold the button pressed during power on and keep pressed for about 12 seconds until only the BLUE LED is ON.
- Release the button; the BLUE LED goes off.
- Wi-Fi AP is now temporary active, until the next reboot.
- Connect with Wi-Fi your phone or laptop to "V-Tap.....".
- Enter the MAC address of the V-Tap as the Wi-Fi password.
- The MAC can be found on the bottom of the box.
- Disable mobile data on your phone, else the IP is not found!
- Open a browser and enter the IP address 192.168.55.66
- In the login page, enter "admin" and "admin".
- The settings page now appears.
- After Save & Logout, Wi-Fi is disabled again.
- To enable access permanently, enable [Wi-Fi Access Point](#).

## 5.10 Firmware update

When a firmware update must be applied, there are two possible states:

### I. The system is running normal.

When the system is accessible through FTP, the firmware can be updated with the PC tool 'vcUpdater'. This tool can be found on the Vidicode website in the menu Service and Support > Firmware.

Another way to update is by using an SD card as follows:

- The manufacturer must provide the necessary files first.
- Prepare an SD card with all unzipped files in the root directory.
- The V-Tap unit must run normal.
- Hold the button pressed while inserting the SD card.
- All LED's start flashing.
- Release the button, then update starts immediately.
- Normal operation resumes after maximal 30 seconds.

At least the files UPDATE.SD and HTAP.ROM and/or HTAP.CPY must be present on the card. The files SAVECONF, DELCONF and CLEARROM perform an action during update and are optional.

### II. The system is not running at all.

The following method is always valid to update or re-install the firmware (if the SD interface is still working):

- The manufacturer must provide the necessary files first.
- Prepare an SD card with all unzipped files in the root directory.
- Power Off the V-Tap unit.
- Insert the SD card.
- Hold the button pressed while applying power (insert USB cable).
- All LED's start flashing.
- Release the button, then update starts immediately.
- Normal operation resumes after maximal 30 seconds.

The files BOOT, UPDATE.SD , HTAP.ROM and HTAP.CPY must be on the card. The files SAVECONF, DELCONF and CLEARROM are optional.

## 6 SD card usage

The SD card is used to store the recorded calls. Without an SD card the recording of calls does not work. The V-Tap system stores the recorded data as a WAV file per call in the G.711 A-Law format. This takes 8000 bytes per second of storage space. The SD card must be FAT32 formatted and can be seen as a big cyclic memory buffer, because the oldest file is deleted automatically when the card is getting full.

The file names on the card are like "00000001.WAV", "00000002.WAV", etc. No call data can be extracted from the name, only the date and time of creation can be read from the directory list. The actual call data with phone number is enclosed inside the WAV header of each file and can be extracted by the Apresa or V-Archive software on the PC.

The WAV files are optionally encrypted, in which case they cannot be played directly by any media player (only noise is heard then).

In case of using a Tunnel server, the files are sent to the server as soon as they are closed. So, data is not sent live to the server, but only after the call has ended or after a file has reached its maximum size.

In the case that no Tunnel server is used, the files are just stored on the card until the user gets the card out. SD cards with recorded files on them can be read and interpreted by the V-Archive software on the PC.

Files are not deleted from the card by the system. Files are written until the card is full (error situation) or until the maximum number of files has been reached, in which case the oldest files are overwritten.

Another function for the SD card is to define a fixed IP address for the V-Tap; see [IP address](#). Yet another function is to [update the firmware](#).

Formatting an SD card is possible in two ways; see [Format SD card](#).



### Safely removal of the SD Card and Power Off.

- . Press the button for 2 seconds (Amber & Blue LED OFF).
- . Release the button (Amber LED flashing).
- . Take out the SD card or the USB cable (power off).



#### NOTE:

The procedure above does not work when start/stop with the button is set (see [Button Mode](#)). In that case, the SD card can just be taken out.

## 6.1 Special SD card settings

Next follows a description of some settings for the SD card, which must be entered in [Special Settings & Commands](#).

### **.SD = Show free space on the card after each reboot**

Enter “SD” as the first command in “Special Settings & Commands”. After each reboot and login, free space on the card is shown then. (A reboot is also done after pressing the ‘Save & Logout’ button.)

### **.SR = Remove files from the card after sending**

Normally, the files are kept on SD card and are not deleted by the system, except when the maximum number of files is reached, in which case the oldest files are overwritten automatically. It is an option to delete the files after the content was sent to a Tunnel server. A certain risk is taken then, because data cannot be recovered anymore after deletion.

### **.SA = Disable Auto Delete when the card is almost full**

When the card is almost full, the oldest files are deleted automatically by the system to create space. This process can be disabled, but new recordings will get lost in that case. When disabled, the user must replace the card on time.

### **.FY = Enable encryption of WAV files on the card**

By default, the WAV files on the SD card can be played by any media player. By enabling the file encryption, the files only produce noise. The file encryption uses the same Encryption Password as the Tunnel encryption.

### **.FF<max> = Maximum Files on the card (default 10000)**

The maximum number of files on the card has two purposes. First of all, it makes the directory on the card more manageable by the system and any PC. Too many files in one directory makes a slow system. The default number of 10000 is reasonable.

Secondly, a system can be built to use the card as an endless buffer, without the problem that the card is getting full. However, this must be calculated carefully and depends on the size of the card, the maximum file size (see below), the auto close function (see above) and the amount of recorded data (number of connected phones).

After the maximum number of files has been reached, the file write-counter is reset, and older files are overwritten automatically.

The maximum tested size of the SD card is 32 GB, and the card must be formatted with the FAT32 file system.

### **.FS<max> = Maximum File Size in MB (default 250)**

When a file on SD card reaches the maximum file size, the file is closed for further writing and then send to the Tunnel server, if that function is enabled. The name counter is incremented at the same time and a new file is opened.

Analog recording produces 8 Kbytes per second. This means a little less than 30 Mbytes per hour. The default of 250 Mbytes is therefore enough for more than 8 hours of recording. A call that takes longer will continue in the next file, without loss of data.

### **.SI<mh> = Card Interface Speed in MHz (default 50)**

This value must be changed only when there are problems with an SD card. The default is good for most of the cards on the market.

Valid speeds to enter: 1 till 12, 15, 17, 20, 24, 25, 30, 40, 50 and 60.

- 🔗 .CS = Show the card file counters after next login
- 🔗 .CR<cou> = Set new Read file counter
- 🔗 .CW<cou> = Set new Write file counter
- 🔗 .CD<cou> = Set new Delete file counter

Enter “.CS” in “Special Settings & Commands” (place at the end, if there are other settings). The next web login will then show the current file counters, used by the card filing system.

For example: **W=500 R=501 D=1**

This shows that the write-counter is on 500, the read-counter on 501 and the delete-counter on 1.

Meaning, that there are 500 files on the card (next file to open is 501), that file 500 was sent successfully to the Tunnel server (next file to send is 501), and that no file was automatically deleted yet.

When the connection to the Tunnel server is right, then the read-counter is always one above the write-counter.

The delete-counter only moves, when the SD card is full and old files are being deleted by the system.

The counters can have a maximum value, the same as the maximum number of files on the card, and can be changed by the “.FF” setting.

The read-counter can be set back to resend files. For example, “.CRO” will resend all recorder files from the card to the Tunnel server.

## 7 Notification & System Messages

The following audio files are used by the system:

- NOTIFY.WAV** : The Notification message. This file is played by the system when the notification is enabled and a recording starts. The message usually says something like: "Welcome.... this call will be recorded...". This message is also played when a recording is started by pressing the button.
- SBEEP.WAV** : Stop beep or message. This file is played when a Recording is stopped by pressing the button.
- NBEEP.WAV** : Notification beep. Used when ".IB<sec>" is entered in the [Special Settings & Commands](#). A short beep is heard by both parties during the whole conversation.
- BEEPS.WAV** : System error beeps. This file is played by the system when something is wrong, for example when no SD card is inserted.

### Format of the messages:

G.711 A-Law, 8 KHz sample rate, Mono.

### Other sample rates:

When the sample rate for recording is set to 16 KHz or 32 KHz, then "16" or "32" must be added to the file name (so "NOTIFY16.WAV") and the format of the message must also be accordingly.

### Putting the messages onto the system:

1. With an SD card:  
Put your .WAV file(s) in the root of an SD card.  
Insert the SD card into the V-Tap. The system will automatically copy the file(s) to its internal memory and delete the file(s) from the card.  
Then the system reboots and the new messages are used.
2. With FTP:  
Connect to the V-Tap with FTP and upload your .WAV file(s).



## 8 Number-list (Black- or White-list)

The V-Tap Analog can record the calls depending on the remote telephone number. A text file containing a list of numbers must then exist in the V-Tap with the following name:

**BLACK.TXT** : A black-list is used.  
**WHITE.TXT** : A white-list is used.

Only one of these two files can be active at the same time. If both exist, then BLACK.TXT is taken.

### When using a black-list:

If the number is found in the black-list, the call is not recorded. All other numbers/calls are recorded.

### When using a white-list:

If the number is found in the white-list, the call is recorded. All other numbers/calls are not recorded.

### Putting the number-list onto the system:

1. With an SD card:  
Put the file BLACK.TXT or WHITE.TXT in the root of an SD card. Insert the SD card into the V-Tap. The system will automatically copy the file to its internal memory and delete the file from the card. Then the system reboots and the new list is active.
2. With FTP:  
Connect to the V-Tap with FTP and upload BLACK.TXT or WHITE.TXT.

### Rules for the number-list:

- The black- or white-list can hold maximal 200 numbers.
- All numbers must be put on a separate line.
- Empty lines are not allowed in the list. They mark the end of the list.
- The numbers in the list must have the same format as on the line, but without preceding zero's (0793471001 becomes 793471001).
- It is also possible to enter the last (right-most) digits only of each number. But then, all entries must have the same length!
- The wildcard character "\*" can be used to denote a range (79347\*).

## 9 Telnet connection

The V-Tap can be accessed with the Telnet (Teletype Network) protocol. Telnet is an older protocol to access devices remotely with a simple terminal and then perform maintenance or change settings. Telnet also uses the TCP protocol with the fixed port number 23. Running a Telnet client program on the PC makes it possible to connect to the V-Tap.

After connecting, the V-Tap Name is shown, and some debug information is constantly sent; Opening and closing of the Tunnel connection and, when an SD card is used, the opening and closing of files on the card.

Further there are two commands that can be entered with Telnet:

The command **ATMENU** will first ask you to enter the Login Password, which is the same as the one used for web access (default "admin"), and then brings you in a remote maintenance menu. Once inside the menu, the tunnel function and SD card storage are stopped.

The menu gives the user the possibility to change the settings, reset the file counters on the SD card, reset to factory settings and change the clock. Normally, there is no need to use these functions over Telnet.

The command **ATDEBUG** is a toggle to enable and disable the output of more debug information. This is further not described in this manual.

Telnet is disabled by entering ".DT" in [Special Settings & Commands](#).

# 10 TLS on the V-Tap

The way to activate TLS is described in the settings chapter, see [Secure Connection with TLS](#).

## 10.1 Tunnel over TLS

The tunnel protocol can be send over TLS, which means that all data will be encrypted during transfer and that data is only readable by the receiver of the tunnel protocol. In the tunnel protocol, the V-Tap takes the role of the TLS client and the receiver the role of the TLS server. The TLS server sends it's certificate to the V-Tap during the setup of the TLS connection.

### 10.1.1 TLS with certificate verification

By default, the V-Tap will try to verify the certificate of the server and if this cannot be done, will refuse to setup the TLS connection.

The V-Tap will also check if the certificate has been signed by a certificate authority (CA) that is trusted.

This is done by checking if the certificate is signed by another certificate, either directly or through intermediates, that belongs to that authority. This is the root certificate. The V-Tap must have a copy of the root certificate in its own "truststore". The V-Tap comes with an empty truststore by default, so this must be configured before TLS connections can be used. The truststore can be seen as a list of root certificates that may be used for the purpose of certificate verification. It is configured by putting all root certificates in a file called **TUNNEL.CRT** on the SD-card. The certificates must be in PEM format. Once the SD-card is inserted, the file will be copied to the unit and used as the truststore.

See [Tunnel protocol to Apresa with TLS](#) below for several possible scenarios of what the exact contents of the file **TUNNEL.CRT** should be.

The V-Tap will also check if the certificate is issued for the name through which it tries to connect to the server. This is the Tunnel server address. So this name must be included in the certificate during creation.

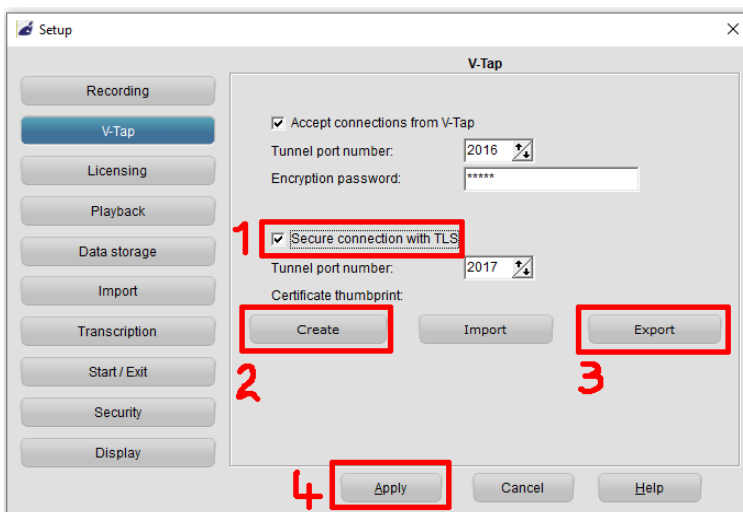
The V-Tap must also have it's time configured correctly, so that it falls between the "Not before" and "Not after" dates of the certificate. These dates are also determined during certificate generation. If a certificate expires, the V-Tap will no longer accept it.

## 10.1.2 TLS without certificate verification

The verification of certificates for the tunnel function can be disabled. This means that any certificate will be accepted. This is mainly useful for troubleshooting, but is also a security risk. While data will still be encrypted in transit, the identification of the receiving end cannot be confirmed anymore.

## 10.2 Tunnel protocol to V-Archive with TLS

In V-Archive go to menu Options > Setup > V-Tap:



1. Be sure TLS connection is enabled.
2. Create a certificate.
3. Export/Save the certificate file TUNNEL.CRT.
4. Be sure to press Apply.

Put the saved file TUNNEL.CRT onto an SD card and insert the card into the V-Tap. The file is automatically copied to internal memory and then removed from the card.

Be sure that the "[Secure Connection](#)" setting in the V-Tap is set to 1.

In V-Archive, the status line at the bottom must show:  
"V-Tap: 000349xxxxxx: TLS".

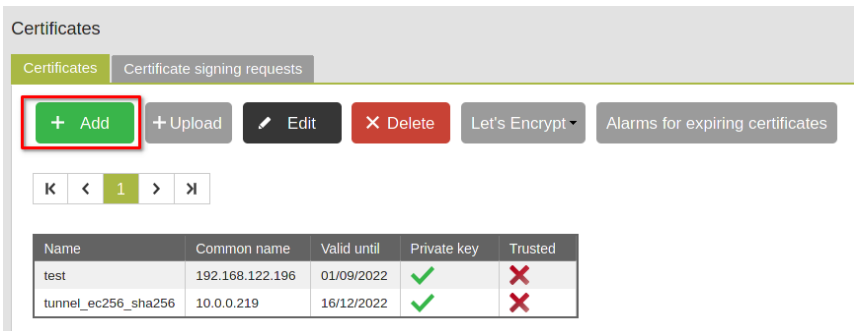
## 10.3 Tunnel protocol to Apresa with TLS

All following examples will use *recording.vidicode.com* as the tunnel server address.

### 10.3.1 Tunnel-TLS with a certificate from Apresa

A self-signed certificate from Apresa can be retrieved as follows:

1. Login to the Apresa and go to Tools > Certificates. It will show the page below. Click the "Add" button to create a new self-signed certificate.



Certificates

Certificates Certificate signing requests

+ Add + Upload Edit Delete Let's Encrypt Alarms for expiring certificates

K < 1 > X

Name	Common name	Valid until	Private key	Trusted
test	192.168.122.196	01/09/2022	✓	✗
tunnel_ec256_sha256	10.0.0.219	16/12/2022	✓	✗

2. Fill in the data. Only the fields name, days valid and IP Name or IP Adress are required. Note that the field "Name" can be anything. It has no meaning for the actual certificate itself. Here it is named "Tunnel Certificate". Then press OK.

Create a certificate

Name: Tunnel Certificate

Days valid: 365

IP Name or IP Address: recording.vidicode.com

Country Code: (2 letter code)

State or province name:

Locality (City):

Organization:

Organizational Unit:

E-mail Address:

Subject alternative name:

Copy common name to subject alternative name:

Add Delete

Type	Name
No subject alternative names	

On Apresa systems that use Debian 10 or higher as the OS, consider clicking the advanced button in the top right first, and selecting "Elliptic curve" as the key type, before clicking OK. This key type is more efficient than the default RSA key type, but cannot be created on older versions of the Debian OS.

Create a certificate

Name: Tunnel Certificate  Advanced

Days valid: 365

IP Name or IP Address: recording.vidicode.com

Country Code: (2 letter code)

State or province name:

Locality (City):

Organization:

Organizational Unit:

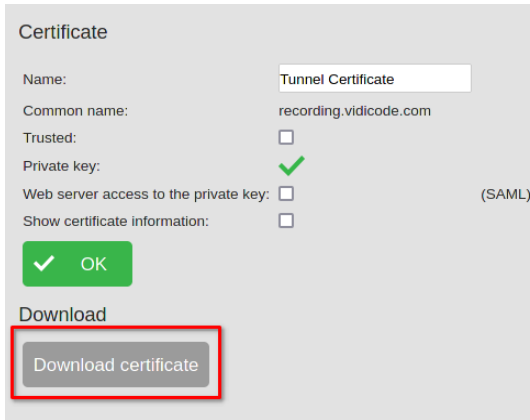
E-mail Address:

Private key

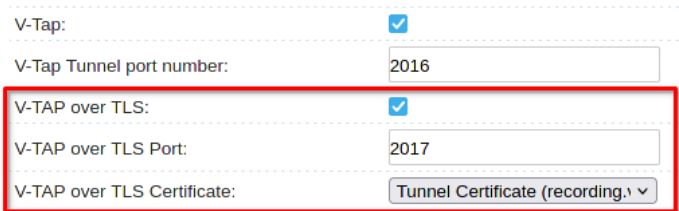
Key type: Elliptic curve

Curve: prime256v1

3. On the newly created certificate page, press download and store the certificate on the V-Tap SD-card in the file called **TUNNEL.CRT**.



4. Go to System settings > Network. From there, configure the Apresa to enable the tunnel protocol over TLS with the certificate that has just been created. Click apply and restart the recording component.



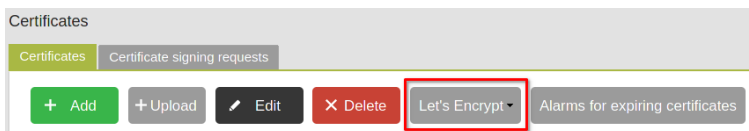
5. Insert the SD-card with the **TUNNEL.CRT** file into the V-Tap. The file is automatically copied to internal memory and then removed from the card. If everything has been done correctly, the V-Tap will connect to the Apresa via TLS if it is configured to so with the “[Secure Connection](#)” option. You can check this by going to Tools > System > System information. It should show the V-Tap ID and say Connected (TLS).

V-Tap Connections			
Tunnel Status	Listening on port: 2016	OK	⊞
Tunnel Status (TLS)	Listening on port: 2017	OK	⊞
000349FEDC22	Connected (TLS)	OK	⊞

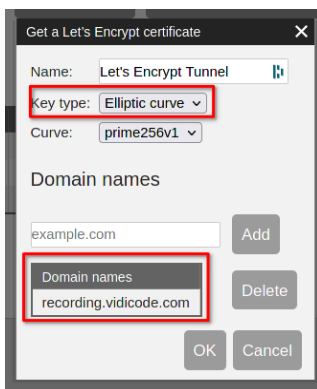
### 10.3.2 Tunnel-TLS with a Let's Encrypt certificate

If your Apresa is reachable via the public internet, it is possible to obtain a Let's Encrypt certificate for free.

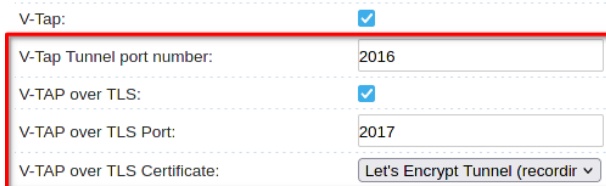
1. Go to Tools > Certificates. Select the Let's Encrypt menu. Register first from this menu if not done so already.



2. Once the Let's Encrypt registration is done, select "Get certificate" option from the menu and fill in the form. If the Apresa is running on Debian 10 or higher, consider selecting Elliptic curve as the private key type. Otherwise RSA is the only option. Press the OK button, and the Apresa will try to request a new certificate from Let's Encrypt.



3. Go to System settings > Network. From there, configure the Apresa to enable the tunnel protocol over TLS with the certificate that has just been created. Click apply and restart the recording component.





4. The V-Tap will need the Let's Encrypt root certificate in its truststore. It is available from here:

<https://letsencrypt.org/certificates/>

At the moment of writing, the ISRG ROOT X1 certificate, self-signed as PEM will be the correct root certificate. Download it and place it on the SD-card as **TUNNEL.CRT**.

5. Insert the SD-card with the **TUNNEL.CRT** file into the V-Tap. The file is automatically copied to internal memory and then removed from the card. If everything has been done correctly, the V-Tap will connect to the Apresa via TLS if it is configured to so with the "[Secure Connection](#)" option. You can check this by going to Tools > System > System information. It should show the V-Tap ID and say Connected (TLS).

V-Tap Connections			
Tunnel Status	Listening on port: 2016	OK	⊞
Tunnel Status (TLS)	Listening on port: 2017	OK	⊞
000349FEDC22	Connected (TLS)	OK	⊞

### 10.3.3 Tunnel-TLS with another CA certificate

1. If you already have a certificate from another Certificate Authority, go to Tools > Certificates and press upload. It is also possible to generate a certificate signing request on an Apresa. Go to Tools > Certificates and select the signing request tab. Click add and fill out the form. Once the request has been created, download it and send it to your certificate authority. Once the certificate has been obtained, go back to the certificate signing tab and select your signing request. From the upload the completed certificate.

2. Go to System settings > Network. From there, configure the Apresa to enable the tunnel protocol over TLS with the certificate that has just been created. Click apply and restart the recording component.

V-Tap:

V-Tap Tunnel port number: 2016

V-TAP over TLS:

V-TAP over TLS Port: 2017

V-TAP over TLS Certificate: Tunnel Certificate (recording) ▾

3. You will need to obtain the root certificate that has been used by your certificate authority for your certificate in PEM format. Store this certificate as **TUNNEL.CRT** on the SD-card.

4. Insert the SD-card with the **TUNNEL.CRT** file into the V-Tap. The file is automatically copied to internal memory and then removed from the card. If everything has been done correctly, the V-Tap will connect to the Apresa via TLS if it is configured to so with the "[Secure Connection](#)" option. You can check this by going to Tools > System > System information. It should show the V-Tap ID and say Connected (TLS).

V-Tap Connections		
Tunnel Status	Listening on port: 2016	OK <span>⊞</span>
Tunnel Status (TLS)	Listening on port: 2017	OK <span>⊞</span>
000349FEDC22	Connected (TLS)	OK <span>⊞</span>

## 10.4 Web interface over HTTPS

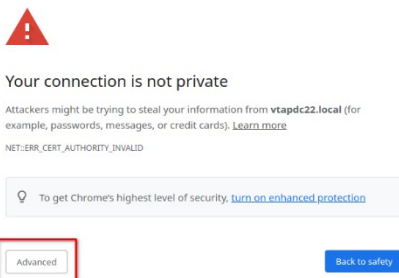
If HTTPS for the web interface is enabled, it will become available through `https://vtapXXXX.local` or `https://<ip-address>`. All communication with the web interface will then be encrypted.

### 10.4.1 HTTPS with a self-signed certificate

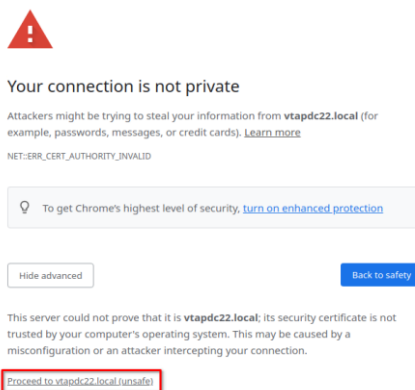
A self-signed certificate is generated by the V-Tap unit once https is enabled. Because the certificate is self-signed, web browsers are unable to validate it and might give a warning that the certificate is untrusted when first accessing the web interface through https. Usually there is a way to make an exception for a web page.

#### Chrome browser

1. Click advanced



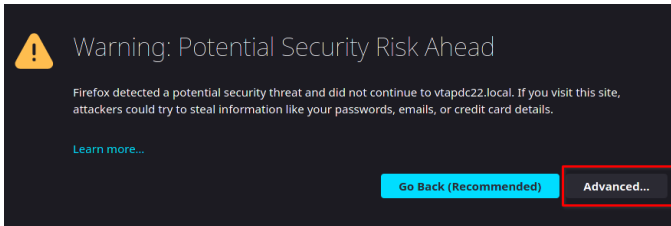
2. Click proceed to .....



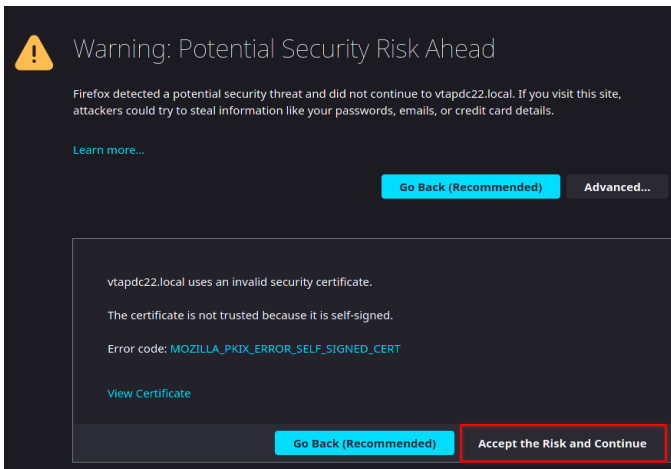
If no such options is shown, trying typing "thisisunsafe" (without the quotes).

## Firefox browser

### 1. Click advanced



### 2. Click Accept the Risk and Continue



## 10.4.2 HTTPS with own certificate

Instead of using the self-signed certificate generated by the V-TAP, it is also possible to supply a certificate and private key that you have generated yourself or that you have obtained from a certificate authority.

The certificate must be in PEM format. A certificate in PEM format will look like this if opened as a text file.

```
-----BEGIN CERTIFICATE-----  
    <Certificate Contents>  
-----END CERTIFICATE-----
```

The certificate should be stored on the SD-card in a file called **HTTPS.CRT**. Any intermediate certificates used to sign the certificate can also optionally be stored in the same file after the first certificate. So there may be more than one certificate in the **HTTPS.CRT** file, if this is the case.

The private key should be stored in another file and should also be in PEM file. The contents should look like this:

```
-----BEGIN PRIVATE KEY-----  
    <Private key contents>  
-----END PRIVATE KEY-----
```

Note that the "BEGIN PRIVATE KEY" and "END PRIVATE KEY" headers may look a little different depending on the type of private key that is used. The private key should also be stored on the SD-card as **HTTPS.KEY**.

Once the SD-card is inserted into the V-Tap, the files containing the certificate and private key will be copied to internal memory, then removed from the card, and used for the next HTTPS access.

Supported private key types are RSA with key sizes of 2048, 3072 and 4096 bits. Elliptic curve keypairs from the curves prime256v1 (NIST P-256) and secp384r1 (NIST P-384) are also supported. The signature algorithm of the certificate may use SHA-256 or SHA-384 as its hash algorithm. It is recommended to use an elliptic curve key based on prime256v1. This offers the best trade-off between resource usage and security.

## 10.5 TLS specification

**TLS versions:** TLS 1.3

**Cipher suites:** TLS\_AES\_128\_GCM\_SHA256

**Key exchange method:** ECDHE

**Elliptic curves:** prime256v1 (NIST P-256) , secp384r1 (NIST P-384)

**RSA private key sizes:** 2048 , 3072 , 4096 bits

**Signing algorithms:** RSA , ECDSA

**Hash algorithms:** SHA-256 , SHA-384

# 11 Using the RTR Call Monitoring Software

The V-Tap Analog can send information over the network using UDP packets. On the PC, the RTR Call Monitor Software can receive this information and will show in real time when a call is busy or not. It is even possible to listen live to the ongoing conversation (with some seconds delay).

Sending the UDP packets to the PC must be activated in the V-Tap:

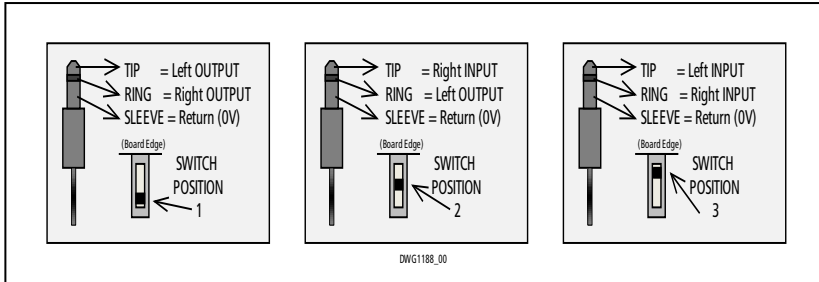
- On the PC edit a text file, called VMON.TXT
- On the first line of VMON.TXT enter the IP address of the PC running the RTR software.
- Optionally, the second and third lines can hold the UDP port numbers (destination and source). Default these are 1001 and 1001.
- The file VMON.TXT must be placed in the root of an SD card.
- The SD card must be inserted into the V-Tap; VMON.TXT is deleted and the V-Tap reboots.
- UDP is now automatically enabled and call information is sent to the defined IP address.

The file VMON.TXT can also be put onto the V-Tap using an FTP connection. A reboot is then needed after upload.

For more information, see the RTR software, or contact Vidicode.

# 12 Technical Specifications

Audio connector type : 3.5 mm circular TRS  
 Connector function set by switch : Stereo OUT, Mono IN+OUT, Stereo IN



Switch position#1 : Stereo OUTPUT  
 Switch position#2 : Mono INPUT+OUTPUT  
 Switch position#3 : Stereo INPUT

## Audio INPUT

Level : 1- 700 mV RMS (software setting)  
 Impedance : 2500 Ohm  
 Bandwidth : 4 or 8 or 16 KHz  
 Phantom power : 2.2V DC  
 AGC : Limiter range >40 dB with Noise Gate  
 Level detector range : Available, Range 0-250 mV RMS  
 Primary use : Electret Microphone

## Audio OUTPUT

Level : 50 – 2000 mV RMS (software setting)  
 Impedance : 150 Ohm  
 Bandwidth : 4 or 8 or 16 KHz  
 Primary use : Amplified Speaker

## USB Port

USB Version : V2.0 High Speed (480 Mbps)  
 USB Profile : Generic HID (VID: **0DE1** / PID: **5202**)  
 USB Current : 5V @ 500mA (Max. 3 W)  
 USB Connector : Full size 'B'- type



# 13 Revision History

## V4.26 September 2023

- Fixed settings page not showing.

## V4.25 June/October 2022

- Text for NTP server changed; new feature with 2 servers.

## V4.24 February-April 2022

- [Secure Connection with TLS](#) and new web settings page.

## V4.23 November 2021

- New procedure to enable Wi-Fi from default.

## V4.22 October/November 2021

- Wi-Fi description improved (disable mobile data!)
- Added a chapter about the RTR Call Monitor Software.
- Options added for VLAN usage & some corrections in the text.

## V4.21 May/June/August/September 2021

- The "Tunnel Server Address" can now hold two addresses.
- The login "User Name" is now called "Username".
- V-Archive installation does not need the V-Tap to be connected.

## V4.20 November/December 2020

- Settings page is much smaller! Removed settings are now in 'Special Settings'.

## V4.14 May/July/August 2020

- Introduction changed, added "Format SD card" and improved some text.

## V4.13 February 2020

- Changed scheme in 2.1 and added text about USB for V-Archive installation.

## V4.12 December 2019

- New chapter in Button function: "Copy Settings from SD card".

## V4.11 October 2019

- Picture of Audio Input/Output connector replaced.

## V4.10 October 2019

- Improved some text in General network settings.

## V4.9 October 2019

- Access description has changed because DHCP is default enabled now.

## V4.8 September 2019

- Help function in web settings added and text improvements.

## V4.7 August 2019

- USB information added and text improvements.

## V4.6 April 2019

- Changed settings text "Device Name" and "Device IP Address".

## V4.5 March 2019

- Replaced software name "Call Recorder VoIP" by "V-Archive".

## V4.4 December 2018

- Picture in [Audio connection](#) added.

## V4.3 November 2018

- New chapter: [Checklist for Tunnel connection](#).
- Picture in [Apresa install](#) replaced.

## V4.2 September 2018

- First release.

## **14 Acknowledgements**

### **14.1 Privacy**

When recording telephone conversations, the privacy of your conversation partner must be considered.

In some countries, there is an obligation to notify your conversation partner of the recording. Check your national legal obligations on this and other issues concerning the use of any Call Recorder.

Vidicode is not a source of official interpretation of laws of any country or state and shall not be construed as a source for making decisions whether to provide notification or not. Vidicode assumes no liability regarding incorrect notification of call recording.

### **14.2 Liability**

Correct functioning of the V-Tap Analog cannot be guaranteed under all conditions and thus we do not accept any liability for loss of information or other damages due to the use of the V-Tap Analog.