

# V-Tap VoIP 3

## Manual

v3.30



# Contents

<b>1</b>	<b>Introduction.....</b>	<b>5</b>
<b>2</b>	<b>Getting started.....</b>	<b>6</b>
2.1	Hardware installation.....	6
2.1.1	Connection at Home example .....	7
2.1.2	Connection at the Office example .....	7
2.2	Software installation.....	8
2.2.1	Call Recorder Apresa.....	8
2.2.2	V-Archive software on a PC.....	9
2.3	Checklist for Tunnel connection .....	10
<b>3</b>	<b>Web interface and Settings .....</b>	<b>11</b>
3.1	Access & IP address .....	11
3.2	Web interface.....	12
3.3	Settings.....	14
3.3.1	General Network settings.....	14
3.3.2	Tunnel settings.....	16
3.3.3	Secure Connection with TLS .....	19
3.3.4	Special Tunnel & Network settings.....	20
3.3.5	Login settings for Web access & FTP.....	23
3.3.6	NTP and Date+Time settings .....	24
3.3.7	Proxy settings.....	25
3.3.8	Button Mode setting.....	33
3.3.9	Special Settings & Commands .....	34
3.3.10	Licenses & Versions .....	36

<b>4</b>	<b>LED's</b>	<b>37</b>
4.1	Red Error LED	37
4.2	Green Link LED	38
4.3	Blue Data LED	39
4.4	Amber SD-Power LED	39
<b>5</b>	<b>Button functions</b>	<b>40</b>
5.1	Start & Stop recording	40
5.2	Remove SD card safely	40
5.3	Disable DHCP temporary	41
5.4	Show IP address	41
5.5	Copy Settings from SD card	42
5.6	Factory settings	42
5.7	Format SD card	42
5.8	Default IP address	42
5.9	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>Special Modes of Operation</b>	<b>49</b>
7.1	Default Switch mode	49
7.2	Single-Proxy mode	50
7.3	Multi-Proxy mode	50
7.4	Proxy Public Access	51
7.5	FRITZ!Box recording with the V-Tap VoIP-3	52

<b>8</b>	<b>TLS on the V-Tap VoIP-3.....</b>	<b>62</b>
8.1	Tunnel over TLS.....	62
8.1.1	TLS with certificate verification .....	62
8.1.2	TLS without certificate verification.....	63
8.2	Tunnel protocol to V-Archive with TLS.....	63
8.3	Tunnel protocol to Apresa with TLS.....	64
8.3.1	Tunnel-TLS with a certificate from Apresa .....	64
8.3.2	Tunnel-TLS with a Let's Encrypt certificate .....	67
8.3.3	Tunnel-TLS with a certificate from another CA.....	69
8.4	Web interface over HTTPS .....	70
8.4.1	HTTPS with a self-signed certificate .....	70
8.4.2	HTTPS with own certificate .....	72
8.5	TLS specification.....	73
<b>9</b>	<b>Telnet connection.....</b>	<b>74</b>
<b>10</b>	<b>Technical Specifications.....</b>	<b>75</b>
<b>11</b>	<b>Revision History.....</b>	<b>76</b>
<b>12</b>	<b>Acknowledgements.....</b>	<b>77</b>
12.1	Privacy.....	77
12.2	Liability .....	77

# 1 Introduction

The V-Tap VoIP is a hardware and software solution for the recording of telephone calls that are transported over an IP network. The supplied hardware unit filters the network traffic, wraps the sniffed data into a special tunnel-format and stores it onto an SD card. The V-Tap VoIP can operate therefore stand-alone. The captured data can then be sent back over the network to an external server, which can be a [Call Recorder Apresa](#) (running on Linux) or the [V-Archive software](#) (running on a Windows PC). The 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.

By default, the V-Tap VoIP functions as a normal switch that allows 2 Ethernet connections. This makes it possible to connect a VoIP trunk directly and use one port for connection to the network. The VoIP trunk can be the connection to a VoIP PBX or an output of another switch with VoIP traffic. Port mirroring is done internally.

In the case that no SD card is inserted, the sniffed data is sent live over the network to the Apresa recorder or V-Archive software (streaming). With an SD card inserted, the sniffed data is stored as files 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. By using the SD card (FAT32 formatted), the V-Tap VoIP can operate completely stand-alone and can store data for weeks or even months, depending on the capacity of the card.

The internal settings of the V-Tap can be accessed through a web interface by any browser.

There are three models, the V-Tap VoIP-1/2/3. The VoIP-1 and VoIP-2 have 100 Mbps Ethernet ports, the VoIP-3 has 1000 Mbps (Gigabit) ports. The VoIP-2 and VoIP-3 further have extra Proxy modes and can make a secure connection with TLS. The VoIP-3 is the only one that can be powered by PoE and has built-in hardware filtering for IP addresses.

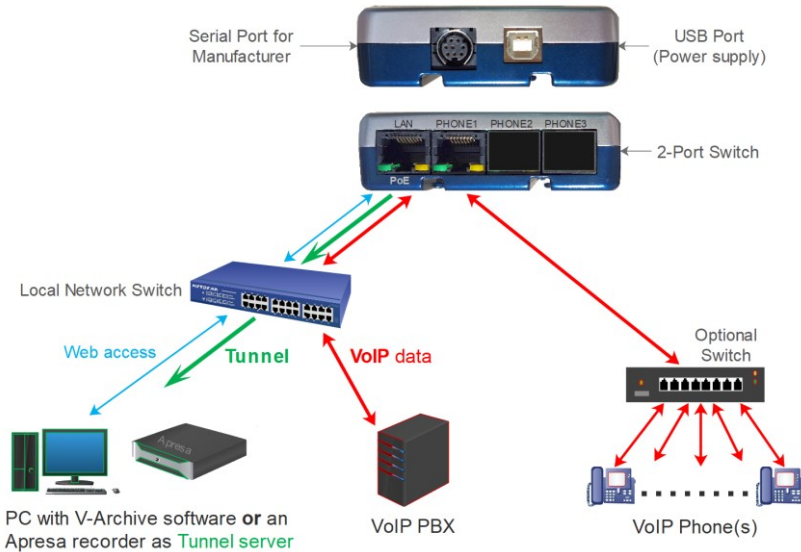
The V-Tap VoIP is a member of a family of compatible products that can be used to create all sorts of Call Recording solutions. There are V-Taps for VoIP, Analog, Audio and ISDN telephony and there is a V-App for mobile recording. All of these products will communicate with the Apresa Corporate or Apresa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

## 2 Getting started

### 2.1 Hardware installation

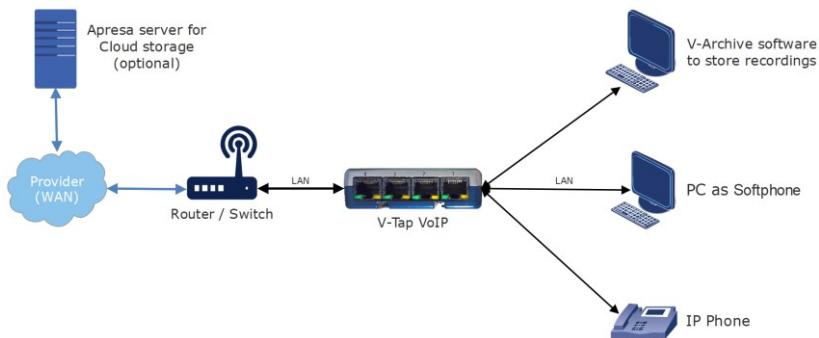
The V-Tap VoIP 3 is easy to setup. The following steps are involved:

- Connect the local network to the LAN port on the V-Tap VoIP 3.
- Connect the VoIP traffic to the PHONE1 port on the V-Tap VoIP 3.
- Connect the USB for power supply or use PoE on the LAN port.
- Insert an SD card (optional but recommended).
- Access the settings in the web interface by using a browser.

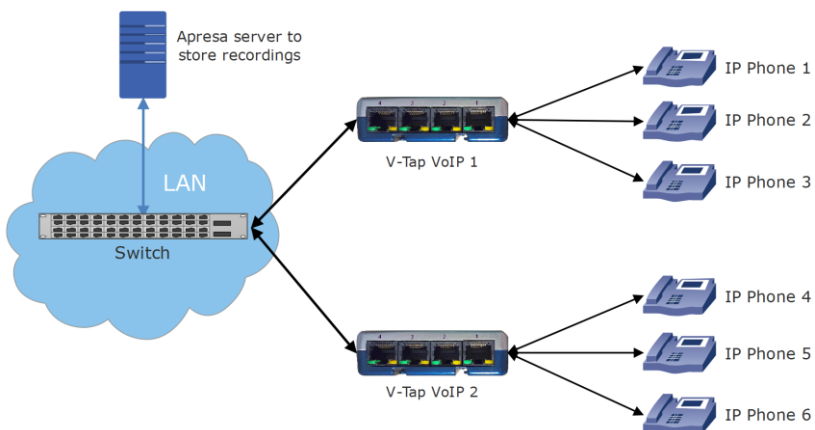


By default, the V-Tap VoIP 3 functions as a normal 2-port switch.

## 2.1.1 Connection at Home example



## 2.1.2 Connection at the Office example



## 2.2 Software installation

External software is needed to extract the recorded calls from the Tunnel data that is produced by the V-Tap VoIP. Also, when the data is 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 channel license, before the Apresa or V-Archive software can record your calls. Recording multiple calls simultaneously needs more licenses.

### 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 the files 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. The settings are as follows:

- 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]

MAC address	Encryption password	Tenant	Name	Delete
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.

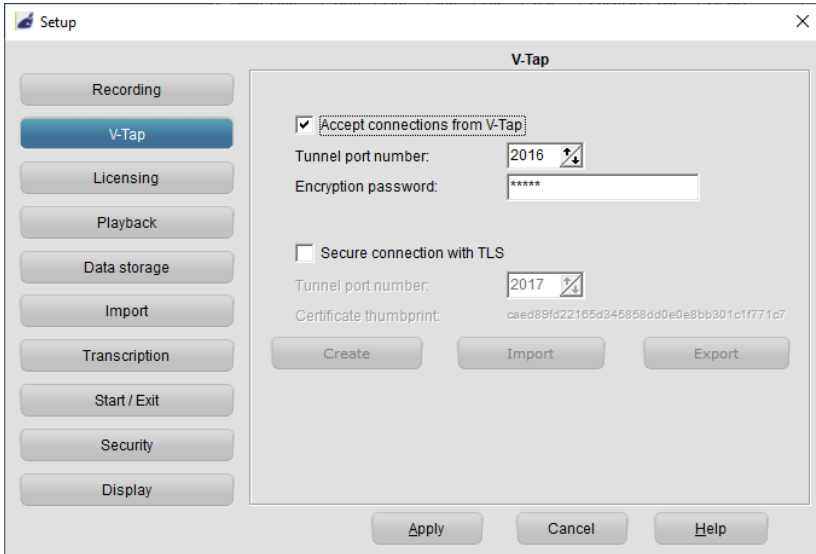
**NOTE2:** Be sure the Encryption password is the same as in the V-Tap unit.



## 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 VoIP, 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 needs to be open only when Tunnel-TLS is used.

The installer tries to open these ports automatically in Windows.

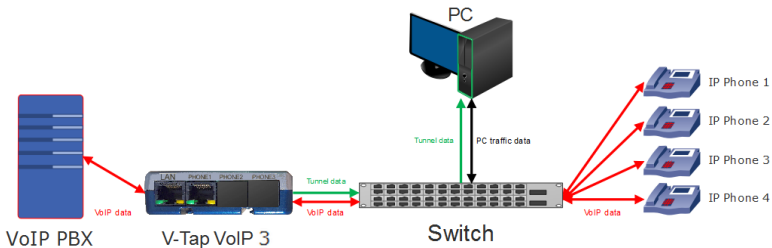
**NOTE3:** Be sure the Encryption password is the same as the "Encryption Password" in the V-Tap.

**NOTE4:** In the recording tab, enter the IP address(es) of the recorded VoIP phone(s) to get the right direction of the telephone calls.

**NOTE5:** 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 into a user accessible database. This checklist can be used to setup the Tunnel:

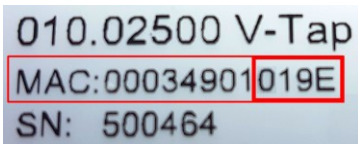
- 1) Install the [Hardware](#) and be sure that the VoIP data passes the V-Tap.
- 2) Install [Apresa](#) or [V-Archive](#) PC software and enable V-Tap connections.
- 3) Open the [Settings page](#) of the V-Tap in a browser by entering <http://vtapXXXX.local> , in which XXXX are the last 4 digits of the MAC address, found on the bottom of the unit.  
*It may take up to a minute after first connect, before this local name is known to the PC.*
- 4) The IP address of Apresa or PC with V-Archive must be entered as the "[Tunnel Server Address](#)".
- 5) Any **firewall** must be open for TCP port **2016**, which is 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 on the PC during installation of V-Archive, if permitted.*
- 6) The Tunnel connection is stable when the **GREEN LED is steady**, not blinking!  
*When using V-Archive, the V-Tap must be shown with its MAC address in the status line.*
- 7) For first tests, better turn off "[Tunnel Encryption](#)".  
*Otherwise, be sure that the Encryption password is the same in both V-Tap and Tunnel server.*
- 8) The V-Tap stores only data that passes the "[Tunnel TCP/SIP Port Filter](#)".  
*In case of an unknown port or for test, this filter can be set to zero to store **all** TCP/IP traffic.*
- 9) When data is stored during a call, the **BLUE LED blinks fast**.
- 10) To see if the Apresa or PC receives something from the V-Tap, it is possible to make a network trace for test. In V-Archive, go to menu Actions and select 'Network trace', press Start, make a call, press Stop and then Save. From the zip, 'tunneltrace.pcap' can be analyzed with Wireshark.
- 11) The SD card in the V-Tap should contain ".TUN" files when data is captured.  
The SD card can be read by the V-Archive PC software in menu File and 'Import from V-Tap'.
- 12) When the V-Tap is connected to a trunk, then it sees all calls that are passing. The V-Tap can only filter those calls on IP address, set with the "[Tunnel IP Address Filter](#)".

## 3 Web interface and Settings

The first step to access the web interface of the V-Tap VoIP is to connect a network cable to any of the 4 LAN ports on the unit. The other side of the cable can be connected to a LAN switch or directly to a PC.

### 3.1 Access & IP address

By default, the V-Tap has DHCP enabled and can be accessed with any browser by entering the address <http://vtapXXXX.local>, in which **XXXX** are the last 4 digits of the MAC address, found on the bottom:



For this V-Tap:

Default address:	<a href="http://vtap019e.local">http://vtap019e.local</a>
Default Username:	admin
Default Password:	admin

If no DHCP is available, 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 **192.168.55.66**  
See also [Disable DHCP temporary](#) and [Show IP address](#).

It is also possible to set a new fixed IP address by using an SD card:

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

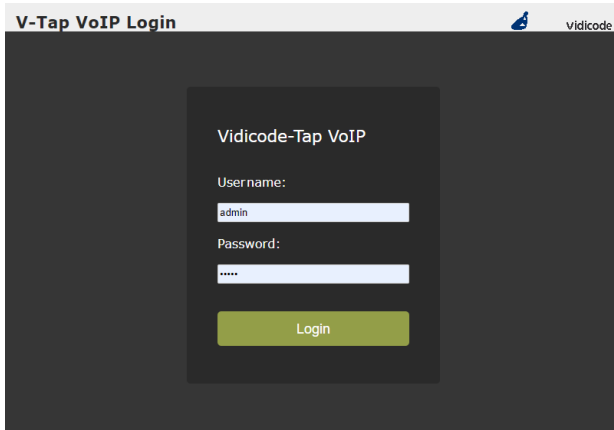


- . Create the text file "IP" on your PC.
- . The first line in this file must hold the IP address.
- . The second line is optional and can hold the IP mask.
- . Copy "IP.TXT" to the root directory of an SD card.
- . Insert the SD card into the V-Tap unit.
- . The IP address has now changed and can be 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:



The screenshot shows a web browser window titled "V-Tap VoIP Login" with a "vidicode" logo in the top right corner. The main content area is dark gray and contains a white login form. The form is titled "Vidicode-Tap VoIP" and includes the following fields and elements:

- A label "Username:" followed by a text input field containing the text "admin".
- A label "Password:" followed by a password input field containing four asterisks "\*\*\*\*".
- A green "Login" button positioned below the password field.

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 VoIP 3 Settings** 02-02-24 14:59:06 Vidicode

<p>Name of this V-Tap <input style="width: 80%;" type="text" value="V-Tap_VoIP_FEDC21"/> ⓘ</p> <p>DHCP Server <input checked="" type="checkbox"/> ⓘ</p> <p>V-Tap IP Address <input style="width: 80%;" type="text" value="192.168.0.32"/> ⓘ</p> <p>Subnet Mask <input style="width: 80%;" type="text" value="255.255.255.0"/> ⓘ</p> <p>Gateway Address <input style="width: 80%;" type="text" value="192.168.0.5"/> ⓘ</p> <p>DNS Server Address <input style="width: 80%;" type="text" value="8.8.8.8"/> ⓘ</p> <p>Tunnel Server Address <input style="width: 80%;" type="text" value="recording.vidicode.com"/> ⓘ</p> <p>Tunnel Destination Port <input style="width: 80%;" type="text" value="2016"/> ⓘ</p> <p>Tunnel IP Address Filter <input style="width: 80%;" type="text"/> ⓘ</p> <p>Tunnel TCP/SIP Port Filter <input style="width: 80%;" type="text" value="5060"/> ⓘ</p> <p>Tunnel UDP/RTP Port Filter <input style="width: 80%;" type="text" value="0"/> ⓘ</p> <p>Tunnel Encryption <input type="checkbox"/> ⓘ</p> <p>Encryption Password <input style="width: 80%;" type="text"/> ⓘ</p> <p>Secure Connection with TLS <input style="width: 80%;" type="text" value="0"/> ⓘ</p> <p>Button Mode <input style="width: 80%;" type="text" value="0"/> ⓘ</p> <p>Special Settings &amp; Commands <input style="width: 80%;" type="text"/> ⓘ</p>	<p>Login Username <input style="width: 80%;" type="text" value="admin"/> ⓘ</p> <p>Login Password <input style="width: 80%;" type="password"/> ⓘ</p> <p>NTP Server Address <input style="width: 80%;" type="text" value="pool.ntp.org"/> ⓘ</p> <p>GMT Minutes Correction <input style="width: 80%;" type="text" value="60"/> ⓘ</p> <p>New Date (DD-MM-YYYY) <input style="width: 80%;" type="text"/> ⓘ</p> <p>New Time (HH:MM:SS) <input style="width: 80%;" type="text"/> ⓘ</p> <p>Proxy Server V-Tap IP Address <input style="width: 80%;" type="text"/> ⓘ</p> <p>Proxy Source IP Address <input style="width: 80%;" type="text"/> ⓘ</p> <p>Proxy Destination Address <input style="width: 80%;" type="text"/> ⓘ</p> <p>Proxy Notify &amp; Record Options <input style="width: 80%;" type="text" value="0 /B0"/> ⓘ</p> <p>Proxy DTMF Start/Stop Options <input style="width: 80%;" type="text" value="0 /S1 /P0"/> ⓘ</p> <p>Licenses Apresa/PC/Proxy/S&amp;U <input style="width: 80%;" type="text" value="5 / 5 / 5 / 05-05-2055"/> ⓘ</p> <p>New License Key <input style="width: 80%;" type="text"/> ⓘ</p> <p><a href="#">License Activation</a></p> <p>V-Tap VoIP 3 OS Version <input style="width: 80%;" type="text" value="3.2.7 14-06-2023"/> ⓘ</p> <p>V-Tap VoIP 3 App Version <input style="width: 80%;" type="text" value="3.2.7 03-08-2023"/> ⓘ</p> <p>Serial Number / MAC Address <input style="width: 80%;" type="text" value="501234 / 000349FEDC21"/> ⓘ</p>
---	--

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 on the Settings page, 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> , in which **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](#).

#### V-Tap IP Address

As part of the local network, the V-Tap VoIP 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 VoIP 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 active, the gateway 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. The DNS address is NOT automatically obtained when DHCP is active.

---

## Setup for VLAN tagging (IEEE 802.1Q)

To setup the V-Tap to take part of a Virtual LAN, the network cable must be connected to port 4, marked 'LAN'.

Also, the following option must be added to the IP Address:

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

The IP Address is then for example: **192.168.0.12 /VLAN256 /PRIO1**

All web access and the Tunnel connection on port 4 are then sent with VLAN tags inserted, and the system only answers to packets with the same VID inside their tags.

The other 3 ports can still be used to access the V-Tap without tags. In VLAN mode, all network ports will still pass unchanged packets with or without VLAN tags between each other, as a switch normally does.

VoIP packets are stored for recording with the VLAN tags included. To remove the VLAN tags from the packets for storage, add **".RT"** to the [Special Settings & Commands](#) field.

Additional 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 VoIP. Leaving this field empty will disable the Tunnel function all together, in which case the V-Tap unit can only store data onto an 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

This is only possible with an SD card inserted, because 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 that comes by using an unknown port 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 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 also used for the encryption of the Tunnel data. 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 !

## Tunnel IP Address Filter

This filter acts as a Whitelist for IP addresses by default, meaning that only the addresses within the filter are recorded.

When this field starts with the letter 'B' the filter acts as a Blacklist, meaning that all addresses within the filter are NOT recorded and all other addresses are recorded.

When the field is left empty, the filter is disabled and all IP addresses are stored for recording.

Maximum 16 IP addresses and/or IP ranges can be entered, separated by a plus sign. An IP range can be set by defining a mask with the "/bits" notation behind the address.

Examples:

192.168.0.0/24 : Record only IP addresses that start with 192.168.0.x

10.247.0.0/16 : Record only IP addresses that start with 10.247.x.x

192.168.1.12 + 192.168.1.177 : Record these two IP addresses only

192.168.33.66 + 10.0.0.0/8 : Record an IP address and an IP range

B10.240.230.1+10.240.230.2 : Do not record these two IP addresses

B10.16.4.0/24 : Do not record IP addresses that start with 10.16.4.x

## Tunnel TCP/SIP Port Filter

The VoIP protocol packets that are recorded (sniffed) from the local network must pass this filter, else they are discarded.

The TCP/SIP Port Filter set to 0 (zero) disables the filter function. Then all TCP over IP packets are recorded, including most internet traffic, downloads and streaming media. The receiving Tunnel server can still pick out the VoIP calls, but on a busy local network this is not advised to do, because the V-Tap VoIP probably gets overloaded.

Disabling the filter is therefore only useful when the V-Tap is connected to one or more VoIP phones, not a trunk or network with other data traffic.

To store the SIP protocol only, the port filter must be set to 5060.

The Unify HFA protocol uses port 4060. Cisco SCCP uses port 2000.

It is also possible to enter two ports; for example "5060+2000".

## Tunnel UDP/RTP Port Filter

UDP packets, coming from the local network, can be filtered in the same way as TCP packets. The SIP protocol uses most of the time UDP with a random higher port number to transport the voice data, the so called RTP stream.

With standard SIP on the local network, this filter can be set to 0 (zero) to allow the V-Tap unit to take all UDP packets.

When the RTP stream is known, it is possible to enter a range of ports; for example "40000-44000" or "8000-12000".

**Note:** All UDP packets that have the same port number as the entered "Tunnel TCP/SIP Port Filter" are also stored.

### 3.3.3 Secure Connection with TLS

A secure network connection with the Transport Layer Security cryptographic protocol (TLS) is only available on the V-Tap VoIP-3. 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 VoIP 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.

The timeout is added for (yet) unknown situations where it is not allowed to have an open TCP connection for a long time.

 **.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.

 **.TL<leng> = Tunnel Minimum Packet Length (default 60)**

Tunnel Packets are network packets sniffed by the V-Tap VoIP. These are the wanted VoIP packets coming from your phone and local network. After they passed the internal filters and match the minimum size, they are sent with the Tunnel protocol to the server or stored onto SD card.

The default minimum size of 60 bytes is also the minimum standard Ethernet packet size. This means that packets of all sizes are taken. There may be situations where it is handy to increase the size, to minimize the overhead of stored packets. For example, when the size is set to 61 all ACK-packets from the TCP protocol are discarded.

 **.DB = Disable Tunnel Filter for Broadcast & ARP packets**

This filter sees that not too much packets are taken from the local network for storage. Many LAN's at the office have a lot of overhead from packets that are not relevant for recording VoIP calls. Therefore, all Broadcast and ARP packets are standard discarded, reducing the size of the stored Tunnel data.

**.DF = Disable Type Filter (default IP & ARP packets only)**

This hardware filter is very fast and looks at two bytes in all Ethernet packets, called the EtherType. Active by default, only two protocols are let through, namely Internet Protocol version 4 (IPv4) and the Address Resolution Protocol (ARP). Both are always needed for normal operation. All other protocols from the Internet Layer are not needed when recording normal VoIP calls.

Disabling this filter will increase the amount of stored redundant data a lot, when the V-Tap is connected to a PC LAN or trunk.

**.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.

There is probably no need to ever change this parameter when the Tunnel is sending on a normal LAN, but 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.

**.LH = Force Half Duplex on all ports**

**.LM = Force 10 Mbps on all ports**

**.LG = Force 100 Mbps on all ports**

These settings will result in much slower network operation. It may be used for test purposes.

Default, the ports are on Full Duplex operation with 1000 Mbps.

### 3.3.5 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 “.FP0” 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 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 !

The default password is “admin”.

### 3.3.6 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 zone 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**.



### 3.3.7 Proxy settings

Proxy mode is only available on the V-Tap VoIP-3 with a Proxy license.

The V-Tap VoIP-3 can act as one or more proxy servers for VoIP devices that are using the SIP protocol, like a SIP telephone or PBX. When setup right, all calls will pass the V-Tap and are recorded.

The big advantage of using the Proxy mode is, that a notification message can be played, and that the user can start and stop recording by pressing a key on his telephone (record-on-demand with DTMF).

The V-Tap forwards the SIP and RTP packets from the source VoIP device (client) to the destination VoIP provider and vice versa. In this way the SIP registration is still handled by the VoIP device itself and the V-Tap does not need to know the user's account information.

All other sniffing rules still apply when Proxy mode is active. So, the "IP Address Filter" and "SIP/RTP Port Filters" are still used to decide whether a packet must be stored onto the SD card or not.

One or more VoIP devices can be recorded by using the V-Tap as its proxy server; see **Single-** and **Multi-Proxy mode** further on.

There are three main settings involved to setup Proxy mode:

#### Proxy Server V-Tap IP Address

This is the IP address of the V-Tap as proxy server and must be the same as the proxy address that you have entered in your VoIP device (sometimes also called Outbound Proxy).

In case that more devices must be recorded, each using its own proxy, an IP range can be entered with a hyphen or minus sign between two IP addresses. See **Multi-Proxy mode** further on.

The entered IP for the proxy server is normally a private address that is part of the local network. However, it is also possible to enter a public address (WAN IP), directly accessible from the internet.

In some situations, it might be needed to use a different gateway to access the proxy destination. Another gateway IP address can be entered by adding the option **/Gx.x.x.x** behind the proxy server.

A special case is, when the V-Tap proxy server is on a local network, but the SIP client (proxy source) is on the internet somewhere. Then, the public IP address of your router must be entered by adding the option **/Rx.x.x.x** behind. See **Proxy Public Access** further on.

## Proxy Source IP Address

This is the IP address of the VoIP device that must be recorded. In case that more devices must be recorded, an IP range has to be entered with a hyphen or minus sign in between two IP addresses, or the field must be left empty.

A protocol port number can be added with the **:<port>** notation behind the IP address(es). For example **192.168.5.212:6077** to use port 6077 for the SIP protocol on the source side. Default, the port is on 5060 for standard SIP.

When left empty or when only a port number is entered, it is the same as entering the range **0.0.0.1 - 255.255.255.254**. This means that all IP addresses are taken as a source. Leaving the source empty can be done for all cases actually, even in Multi-Proxy mode, but may lead to unstable connections and is not tested for all situations.

When left empty and the proxy server has a public IP address, and is therefore directly accessible from the internet, the V-Tap automatically locks onto the source IP address of a client that is successfully registering at the destination provider. The registration is not checked when the proxy server has a private IP address. Checking the registration can be forced by adding the option **/E** and can be disabled for all situation with the option **/D**. See **Proxy Public Access** further on.

## Proxy Destination Address

This is the IP address or hostname of your VoIP provider or other VoIP PBX. The V-Tap needs to know this address, so it can forward all packets coming from the VoIP device(s) to this provider.

A protocol port number can be added with the **:<port>** notation behind the address. For example **sip.provider.com:7123** to use port 7123 for the SIP protocol on the destination side. Default, the port is on 5060 for standard SIP.

## Single-Proxy mode

Just a single IP address must be entered in the Proxy Server and Proxy Source fields. The Proxy Destination is always only one IP address or host name. Also, at least one Proxy license is needed. For example:

Proxy Server V-Tap IP Address = 192.168.0.244  
Proxy Source IP Address = 192.168.0.12  
Proxy Destination Address = sip.voip-provider.com

For a drawn scheme, see [Single-Proxy mode](#).

It is also possible to leave the Proxy Source field empty, in which case all SIP clients are accepted as a source, until the maximum Proxy licenses.

In combination with a **FRITZ!Box**, the Single-Proxy mode can be used to record all your phone calls, even those from the cordless DECT handsets. This special case is described in chapter [FRITZ!Box recording...](#)

## Multi-Proxy mode

To setup Multi-Proxy mode, an IP range must be entered in the Proxy Server and Proxy Source fields. The V-Tap then acts as multiple proxy servers. For example:

Proxy Server V-Tap IP Address = 192.168.0.**231** - 192.168.0.**235**  
Proxy Source IP Address = 192.168.0.**10** - 192.168.0.**60**  
Proxy Destination Address = sip.voip-provider.com

The above means that 5 devices can use the V-Tap as proxy and can therefore be recorded at the same time. For this to work, at least 5 Proxy licenses must be available inside the V-Tap.

The source devices must have an IP address that lies between the entered range and each source device must use a different proxy IP.

The 5 devices (IP phones) can then be filled in as follows:

1. IP phone 192.168.0.**12** uses V-Tap proxy 192.168.0.**231**
2. IP phone 192.168.0.**27** uses V-Tap proxy 192.168.0.**232**
3. IP phone 192.168.0.**41** uses V-Tap proxy 192.168.0.**233**
4. IP phone 192.168.0.**48** uses V-Tap proxy 192.168.0.**234**
5. IP phone 192.168.0.**56** uses V-Tap proxy 192.168.0.**235**

For a drawn scheme, see [Multi-Proxy mode](#).

It is recommended that the SIP phones are set to static IP addresses.

## Proxy Public Access, using a direct WAN IP address

The V-Tap can be given a public (WAN) IP address itself, and therefore becomes directly accessible from the internet by any SIP client on your mobile telephone.

Note, that the web settings page of the V-Tap can also become available on the internet in this case (1<sup>st</sup> example). A secure username and password must be selected therefore (see [Login Username/Password](#)).

For the proxy function, it is also safer to select a non-standard port number for the SIP protocol. The internet is full of ‘bots’ trying to abuse SIP on port 5060. The V-Tap proxy does therefore have a built-in safety, that looks at a successful registration by the SIP client at the VoIP provider and then locks onto that client’s IP address.

Example 1 for WAN IP **46.55.102.89** and port **6077** for SIP:

**V-Tap:** V-Tap IP Address = **46.55.102.89** (*on public IP*)  
Gateway Address = **46.55.102.1** (*ask provider*)  
Proxy Server V-Tap IP Address = **46.55.102.89**  
Proxy Source IP Address = **:6077**  
Proxy Destination Address = sip.voip-provider.com

**Client:** Outbound Proxy Server = **46.55.102.89:6077**

Example 2 for WAN IP **46.55.102.89** and port **6077** for SIP:

**V-Tap:** V-Tap IP Address = 192.168.0.23 (*on private IP*)  
Gateway Address = 192.168.0.1  
Proxy Server V-Tap IP Address = **46.55.102.89**  
Proxy Source IP Address = **:6077**  
Proxy Destination Address = sip.voip-provider.com

**Client:** Outbound Proxy Server = **46.55.102.89:6077**

(When the standard SIP port 5060 is used, then :6077 can be left out.)

For a drawn scheme, see [Proxy Public Access](#).

**Note** that some VoIP providers must be aware of the used WAN IP, and do not accept connections when accessed from any other IP address.

## Proxy Public Access, using a Router and Port Forwarding

When the V-Tap is connected to your LAN and must record all calls from a SIP client that is running on your mobile telephone, for example, then these points must be met:

- Your router must be open for the SIP protocol port AND for the used RTP ports that carry the audio of the calls. The default SIP protocol port 5060 is known, but the used RTP ports can be anything between 2000 and 65353. Most SIP clients have some setting to define the RTP port range and use port numbers above 10000 for RTP. Therefore, it is needed to setup Port Forwarding in your router and let the router send all the wanted ports to the V-Tap proxy server. It might be easier to enable the DMZ Host function in your router (when available) and let that send to the IP of the proxy server.
- The public IP address of your router (WAN IP) must be entered with the **/R** option in the 'Proxy Server V-Tap IP Address' setting.
- The public IP address of your router must be entered as the 'Outbound Proxy Server' in the settings of your SIP client.
- The 'Proxy Source IP Address' in the V-Tap must be left empty, or only a port number must be entered, when not using port 5060. This is, because the source IP address is unknown in advance when you are on a GSM or Wi-Fi network somewhere. But, if the public IP address of the used SIP client is known and is always the same, then it is better to enter that IP as the source.

Example for a router on WAN IP **46.55.102.89** and port **6077** for SIP:

**V-Tap:** V-Tap IP Address = 192.168.0.23 or 192.168.0.212  
Gateway Address = 192.168.0.1  
Proxy Server V-Tap IP Address = **192.168.0.212 /R46.55.102.89**  
Proxy Source IP Address = **:6077**  
Proxy Destination Address = sip.voip-provider.com

**Router:** Port Forwarding or DMZ Host = **192.168.0.212**

**Client:** Outbound Proxy Server = **46.55.102.89:6077**

(When the standard SIP port 5060 is used, then :6077 can be left out.)

**Note** that the V-Tap IP Address and the Proxy Server V-Tap IP Address can be the same address. For a drawn scheme, see [Proxy Public Access](#).

## Proxy Notify & Record Options

In Proxy mode, the V-Tap VoIP-3 can insert a notification message into the SIP RTP stream. The audio of the used message is stored inside the V-Tap, in a file called “**NOTIFY.WAV**”.

The format of this file must be G.711-Alaw, 8KHz, Mono (64kbps).

A new customized message can be placed easily into the system by putting NOTIFY.WAV onto an SD card and inserting the card into the V-Tap. The file is then automatically copied and removed from the card (see also WAV files on page 25).

There is a default message available on the system for test purposes.

To enable the notification message and/or set some recording options, a numeric value must be entered:

- +1** : Enable the notification message for incoming calls.
- +2** : Enable the notification message for outgoing calls.
- +4** : Record outgoing calls only (disable recording in-calls).
- +8** : Record incoming calls only (disable recording out-calls).
- +16** : Record audio from local side only (disable remote side).
- +32** : Record audio from remote side only (disable local side).
- +64** : Playback the message to local side only.
- +128** : Playback the message to remote side only.

For example, when only incoming calls must be recorded with notification, then the value **9** must be entered (+1+8).

### **Notification Beep**

The system can also produce a notification beep with a user defined interval. Both message and beep can be activated separately or work simultaneously.

The audio of the beep is also stored inside the V-Tap in a file called “**NBEEP.WAV**” and also in the format G.711-Alaw, 8KHz, Mono.

To enable the beep, add behind the Proxy Notify & Record Options:

**/B<sec>** : Enable the notification beep with interval <sec>.

When both the message and beep are needed, then enter: **3 /B15**

When only the beep is needed and no message, then enter: **0 /B12**

When no beep is needed, then **/B0** can be added or removed.

A new customized beep can be placed into the system by putting NBEEP.WAV onto an SD card and inserting the card into the V-Tap.

**Proxy Note 1 (STUN):**

When the SIP connection is using a STUN server to route the RTP stream, the notification message or beep may not work.

**Proxy Note 2 (SIP codec's):**

The audio data in the RTP stream is replaced by the V-Tap during playback, but this is not always possible when the used audio codec is unknown or irreplaceable. The G.722 and G.729 codecs are disabled by the V-Tap in the SIP protocol when a message is used, but the safest way of operation is to put the PCMA codec (G.711-ALaw) on top of the codec-list in your VoIP system.

Forcing PCMA by the V-Tap is done by adding the option **/C** behind the value in 'Proxy Notify & Record Options'.

**Proxy Note 3 (silence):**

Silence Compression or Comfort Noise must be disabled on the IP phone (SIP client), else the notification message may not work properly.

**Proxy Note 4 (message & recording):**

In case the notification message is not part of the recording or only one side of the conversation is recorded, you may first try the option **/X** behind the value in 'Proxy Notify & Record Options'. If still not working, try the option **/S**.

## Proxy DTMF Start/Stop Options

In Proxy mode, the V-Tap VoIP-3 can detect DTMF codes in the RTP stream (RFC 2833 / 4733) and inside SIP INFO messages.

To enable DTMF detection, a numeric value must be entered:

- +1** : Enable DTMF detection for remote side.
- +2** : Enable DTMF detection for local side.
- +4** : Start/Stop recording the audio of remote side only.
- +8** : Start/Stop recording the audio of local side only.
- +16** : Disable detection of DTMF-start.
- +32** : Disable detection of DTMF-stop.

For example, when the value 3 is entered, then both remote and local side can press DTMF to start and stop recording the audio of both sides. The value 7 sees that only the audio of the remote side is recorded or not (local side keeps on recording then).

By default, DTMF "1" is used to start recording and DTMF "0" is used to stop recording. To change the used digits, add the following options behind the numeric value:

- /Sx** : Define DTMF digit to Start recording: **x** = 0 till 9 or \* or #.
- /Px** : Define DTMF digit to Stop recording: **x** = 0 till 9 or \* or #.

To acknowledge the start and stop actions, the system plays back an audio file. The used files are called "**START.WAV**" and "**STOP.WAV**". These files are stored inside the V-Tap and heard directly after detecting DTMF-start or DTMF-stop.

About one second delay is needed before the actual sound starts, because some phones are silent during the tone generation. This delay must be part of the WAV file, so inserted in front of the sound. The format of the WAV files must be G.711-Alaw, 8KHz, Mono. Changing the default available beeps is done as follows:

1. With an SD card:  
Put your WAV files in the root of an SD card. Insert the card into the V-Tap. The system will automatically copy the files to its internal memory and delete them from the card again. Then the system reboots and the new messages are used.
2. With FTP:  
Connect to the V-Tap with FTP and upload your WAV files. After that, a reboot is needed to activate the new messages.



### 3.3.8 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

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. This only works well in combination with an SD card!

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 the data. Non-saved calls are deleted from the SD card.

**3** = Start-Stop mode. The state of the Red LED does not change in between calls. After power, the Red LED is OFF, so the V-Tap is not recording calls.

**mode + 4** = When 4 is added to the mode, the V-Tap is in 'pre-recording' mode, meaning that the 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.



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



## 3.3.9 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 setting 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!

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

- ".SR" = Remove files from the card after sending to the Tunnel server.
- ".SA" = Disable Auto Delete when the card is (almost) full.
- ".SP" = Enable SD Power Save Mode (slow clock on card during idle).
- ".FC<cou>" = File Auto Close Packet Count (default 20).
- ".FT<sec>" = File Auto Close Timeout in seconds (default 3).
- ".FF<max>" = Maximum number of Files on the card (default 5000).
- ".FS<siz>" = Maximum File Size in MB (default 250).
- ".SI<mhZ>" = SD card Interface Speed in MHz (default 50).
- ".SS<start-stop>" = Set time period for sending files (HH:MM-HH:MM).
- ".CA" = Store files on the card in PCAP format for trace (no recording!).
- ".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 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).
- ".TL<leng>" = Tunnel Minimum Packet Length in bytes (default 60).
- ".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.
- ".DF" = Disable EtherType Filter (default IP & ARP packets only)!
- ".DB" = Disable Tunnel Filter for Broadcast & ARP packets.
- ".LD" = Disable disconnecting the Tunnel when a Full-error is detected.
- ".LH" = Force Half Duplex on all ports, except a split or mirror port.
- ".LM" = Force 10 Mbps on all ports, except a split or mirror port.
- ".LG" = Force 100 Mbps on all ports, except split or mirror (VoIP-3 only).
- ".RT" = VLAN Tags are removed from the Tunnel data and Mirror Port.
- ".LT" = VLAN Tags are removed from the Mirror Port.

## **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.
- ".LN" = Disable Summer Time correction in the NTP function.
- ".LR" = When DHCP is enabled, a daily reset is done at 03:00.
- ".VT" = Enable the VLAN table in the switch chip (VoIP-3 only).
- ".DW" = Disable Workarounds for the switch chip (VoIP-3 only).
- ".LW<reg>=<val>" = Write a register in the switch chip with a value.
- ".MAC<hhhh>" = MAC Configuration bits (4 hex digits, default C254).
- ".I2C<num>" = I2C interface speed 160/8\*num (default 50 = 400 KHz).
- ".XO" = Debug mode enabled. Output to the serial port (57600,n81).
- ".XF" = Open debug trace file. The file is closed after a new login. Then  
".XF" must be removed again and the settings saved. The file  
TRACE.TXT can be downloaded with ftp or read from the card.

### 3.3.10 Licenses & Versions

#### Licenses Apresa/PC/Proxy/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.

More licenses are needed in the case that more calls can be busy simultaneously.

For example, when two VoIP calls are busy at the same time and the V-Tap has only one license, then the second call will be discarded by the Tunnel server and cannot be recovered anymore later.

For the V-Tap VoIP-3 there also exists a value for the Proxy-mode licenses. The amount of Proxy licenses is the amount of SIP devices that can make use of the V-Tap as a proxy server.

The end-date is the last day that the user can ask for support or update the firmware on the unit.

Adding new licenses or extending the S&U date is explained in the separate quick guide about [V-Taps and Licenses](#).

#### V-Tap VoIP OS Version

#### V-Tap VoIP App Version

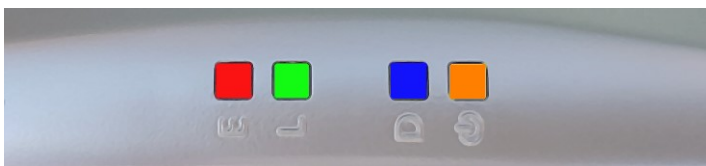
Firmware versions are shown for information purposes and cannot be changed.

#### 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.

The Blue LED may always blink a little when the network is connected, meaning that data is received by the V-Tap VoIP. The status of the V-Tap must be read from the Red, Green and Amber LED's.

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 per LED below.

### 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 Green LED and Amber LED blinking opposite.*  
This is the factory default and means that no Tunnel server is defined **and** no SD card is inserted, so no data is stored or sent. Entering an address for the Tunnel server and/or inserting an SD card solves the situation.
- *Red LED steady ON plus Green LED blinking slow.*  
The V-Tap unit tries to connect to the Tunnel server.

- *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. Then it is also recommended to check 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. See also [Remove SD Card safely](#).
- *Red LED blinking fast.*  
This indicates that data was lost. The internal buffer was overflowed, because the connection to the Tunnel server was lost or writing to the SD card failed. This situation can solve itself after connection to the Tunnel server has been restored.
- *Red LED blinking fast, together with all other LED's.*  
This happens after a fatal error in the system. The firmware must be updated.

## 4.2 Green Link LED

The Green LED shows the status of the link to the Tunnel server.

- *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 this takes longer, then 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.
- *Green LED OFF.*  
The only normal situation with the Green LED OFF is, when **no** Tunnel server is defined and an SD card is inserted.

### 4.3 Blue Data LED

The Blue LED shows the reception of data from the network.

- *Blue LED blinking.*  
The Blue LED blinks when data is received from the local network. Only the packets that have passed the filters will activate a blink.
- *Blue LED steady ON.*  
The Mirror function in the V-Tap VoIP is active. See [Mirror modes](#).

### 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 writing data to a file or 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 with the button is further explained in [Button setting](#).

### 5.2 Remove SD card safely

Directly after inserting an SD card, a file on the card is opened for writing. This is done to gain speed when data must be written. The file remains open for writing until it is closed automatically, after which a new file is opened immediately.

See for further explanation the chapter [SD card usage](#).

In the case the SD card is taken out without precaution, the current 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.**

**NOTE:** The above procedure does not work when the Button Mode is set, in which case the SD card can be just 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.VTV 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. Another way is to enter "FORMAT CARD" in [Special Settings & Commands](#).

## 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 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 VTAP.ROM and/or VTAP.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 , VTAP.ROM and VTAP.CPY must be on the card. The files SAVECONF, DELCONF and CLEARROM are optional.

## 6 SD card usage

Without an SD card inserted, the V-Tap VoIP will stream the sniffed data live to the Tunnel server (Apresa or V-Archive software).

The SD card is used to store the recorded VoIP data. The system writes the data to files in the Tunnel format, which is the same as the format sent to a Tunnel server. The files on the SD card are opened and closed automatically, depending on some parameters. The SD card must be FAT32 formatted and can be seen as a big cyclic memory buffer for the system; older files are automatically deleted when the card gets full.

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 then, but after a data-timeout 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 Tunnel files can be read and interpreted by the V-Archive software on a PC.

Files are not deleted from the card by the system. New files are created 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.

Without an SD card, the system has only little buffering capabilities. Any disturbance in the Tunnel connection would then lead to the loss of data. Another function for the SD card is to define a fixed IP address for the V-Tap unit; 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.

### **.FC<cou> = File Auto Close Packet Count (default 20)**

### **.FT<sec> = File Auto Close Timeout in seconds (default 3)**

These two parameters are used by the system to close files on the SD card automatically. As soon as you insert an SD card, a file is opened, and recorded data is written into the file. Stored packets are counted each second again and when the installed threshold is reached, the timeout becomes active. When the Packet Count is under the threshold for the duration of the installed timeout, the current open file is closed. A new file is opened immediately after that. One normal VoIP call produces about 100 packets per second for the duration of the call. After the call, a few or no packets are received. In this way, the Auto Close function can be seen as an active-idle detector. In the case that only one VoIP phone is connected, the files on SD card will then contain complete calls. With more phones/calls

active at the same time, the files can also contain multiple calls.

### **.FF<max> = Maximum Files on the card (default 5000)**

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 5000 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 sent to the Tunnel server, if that function is enabled. The name counter is incremented at the same time and a new file is opened. An uncompressed VoIP call produces roughly 26 Kbytes per second. This means a little less than 90 Mbytes per hour. The default of 250 is therefore enough for more than 2 hours of recording. A call that takes longer will continue in the next file, without loss of data.

### **.SS<start/stop> = Tunnel Send Start/Stop Time**

Sending files via the Tunnel can be scheduled into a timeframe. If lots of data has been received by the V-Tap and therefor also lots of data must be send to the Tunnel server, it might be useful to delay the sending to save bandwidth on the network. Sending data is then only done between the given start and stop times. The entered format must be "HH:MM / HH:MM". For example: ".SS22:00/08:15" means; send between 10.00 in the evening and 8.15 in the morning.

### **.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.


## .CA = Store files on the card in PCAP format

Enabling this option sets the V-Tap unit in a completely different mode. The format of the stored packets in the files on the SD card changes to the PCAP format. The files on the card are given the extension .CAP and are directly readable by PC tools like Wireshark. The Tunnel function itself is disabled, but packets still must pass the filters before they are stored.

This mode can be used for network debugging or tracing.

## .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=500 D=1**

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

Meaning, that there are 500 files on the card (file 501 is open now), that file 499 was sent successfully to the Tunnel server (next file to send is 500), and that no file was automatically deleted yet.

When the connection to the Tunnel server is right, then the read-counter is always the same as 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.

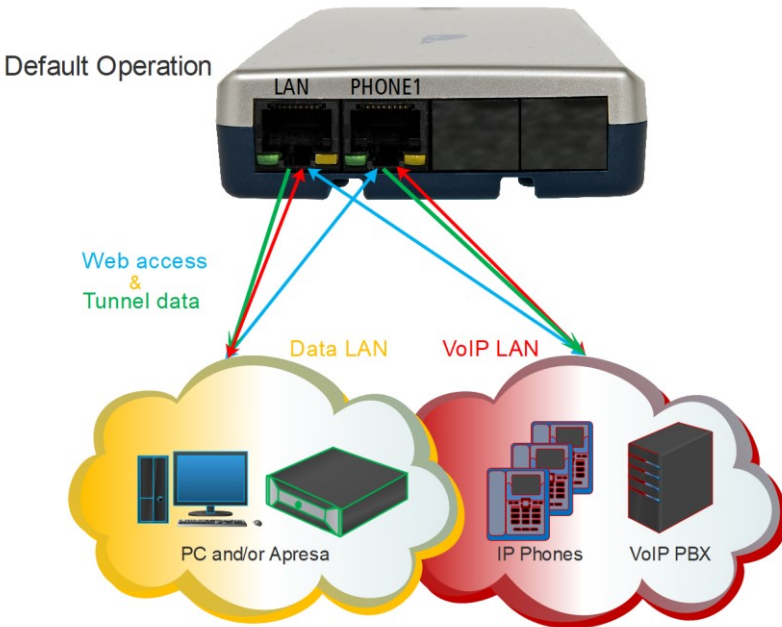


# 7 Special Modes of Operation

In the following paragraphs, the connection schemes for some situations are shown in a drawing. The settings to change these different modes of operation are also described.

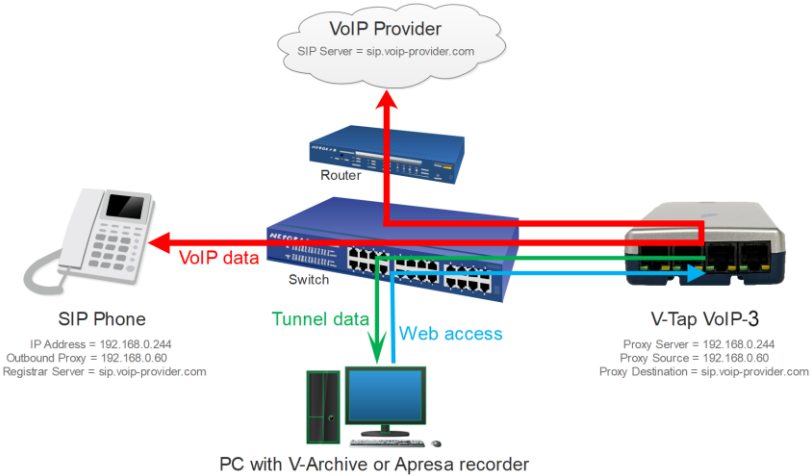
## 7.1 Default Switch mode

This is the default startup situation of the V-Tap VoIP. The unit functions as a normal 2-port switch; both ports can be used for web access, Tunnel connection and VoIP data.



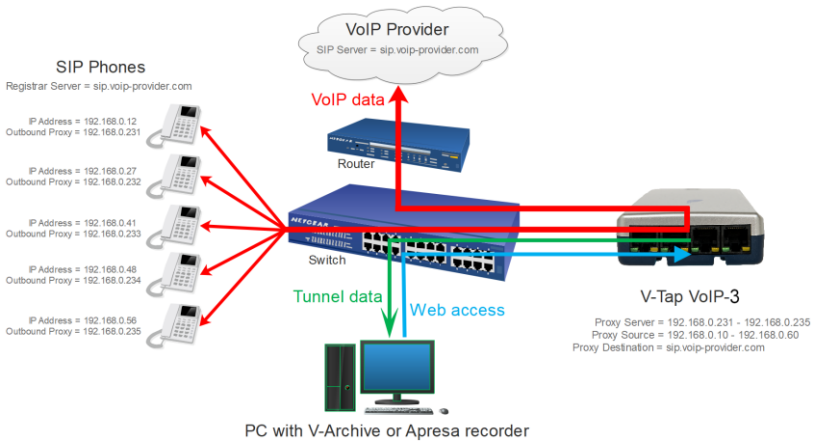
## 7.2 Single-Proxy mode

Proxy mode is available on the V-Tap VoIP-3 with a Proxy license.



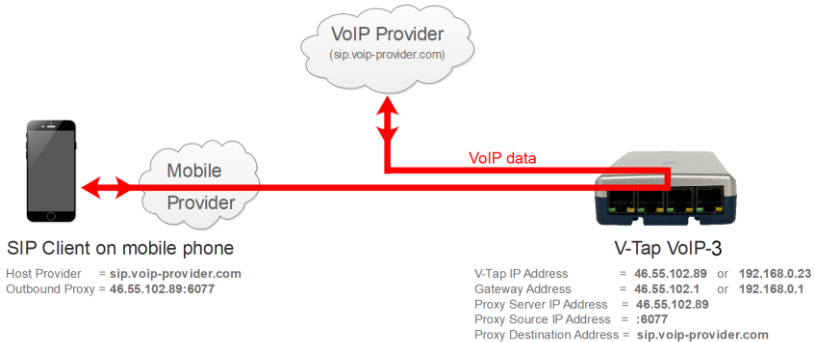
## 7.3 Multi-Proxy mode

In the example below, the V-Tap VoIP-3 needs at least 5 Proxy licenses.



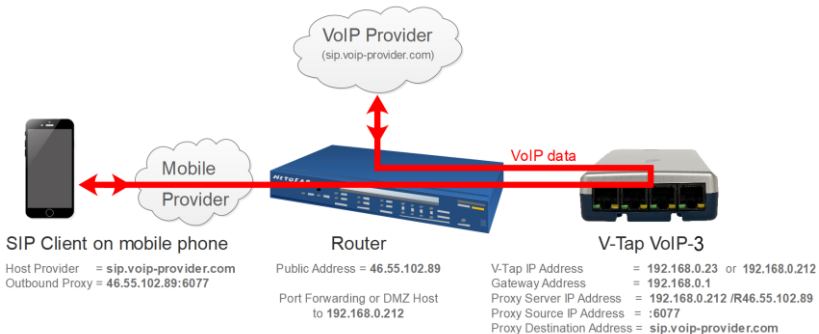
## 7.4 Proxy Public Access

### V-Tap VoIP-3 public proxy, using a direct WAN IP address:



Note that the 'V-Tap IP Address' can be set to a public or a local address. The Gateway Address must be set accordingly.

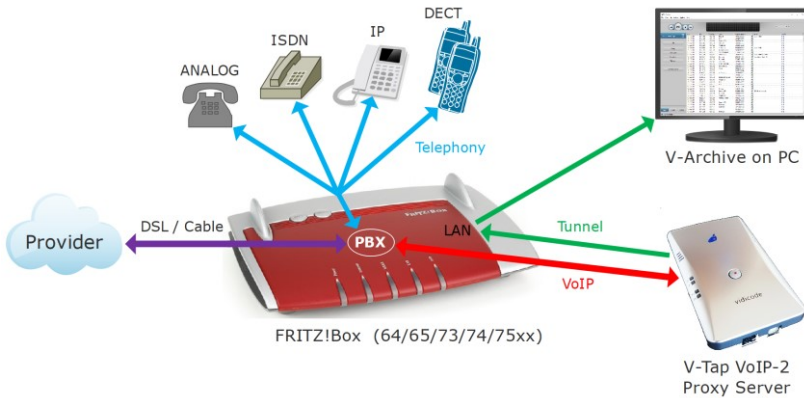
### V-Tap VoIP-3 public proxy, using a router and port forwarding:



Note that the 'V-Tap IP Address' also can be the same as the 'Proxy Server V-Tap IP Address', which is 192.168.0.212 in the example above.

(When the standard SIP port 5060 is used, then :6077 can be left out.)

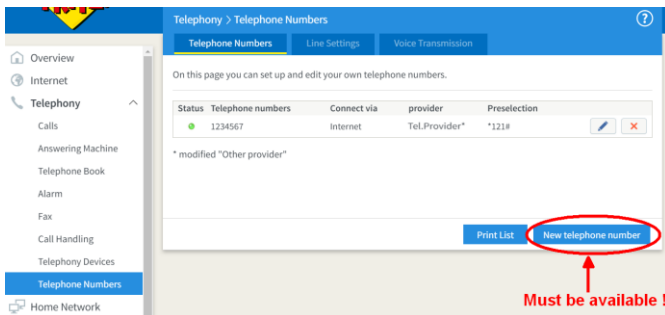
## 7.5 FRITZ!Box recording with the V-Tap VoIP-3



The Proxy mode in the V-Tap VoIP-3 can be setup in a special way to record the calls from all telephones that are connected to a FRITZ!Box. The telephones can be Analog, ISDN, IP and DECT. The FRITZ!Box model can be the 63xx, 64xx, 65xx, 66xx, 73xx, 74xx or 75xx. (As long as the VoIP PBX function is built-in, which is mostly standard.)

Mandatory for recording is, that the FRITZ!Box must have a telephony account with a provider, and there must be an option to add a new telephony account (this option is sometimes missing in pre-installed models). To find out, do the following:

Enter [fritz.box](http://fritz.box) or [192.168.178.1](http://192.168.178.1) in the address line of your browser. Login and select menu **Telephony** and then **Telephone Numbers**:






The FRITZ!Box must have at least one telephony account on this page, AND the option **New telephone number** must be available. Now you can continue the installation, which starts on the next page.

## Configuration of the V-Tap for FRITZ!Box recording

By default, the FRITZ!Box has the IP address 192.168.178.1.

In some installations, where the FRITZ!Box is placed behind a router in an existing LAN, the IP address is 192.168.188.1. In that case, all the addresses 192.168.178.xxx must be replaced by 192.168.188.xxx in the following examples.

The IP address 192.168.178.222 is chosen as the proxy server address for the V-Tap. The Proxy settings in the V-Tap web interface must then look like this:

Proxy Server V-Tap IP Address	<input type="text" value="192.168.178.222"/>	
Proxy Source IP Address	<input type="text" value="192.168.178.1"/>	
Proxy Destination Address	<input type="text" value="192.168.178.1"/>	

**NOTE 1:**

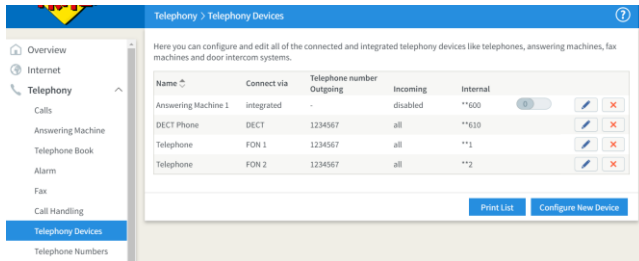
The V-Tap VoIP-3 needs a Proxy license ! (see also Notes at the end)

**NOTE 2:**

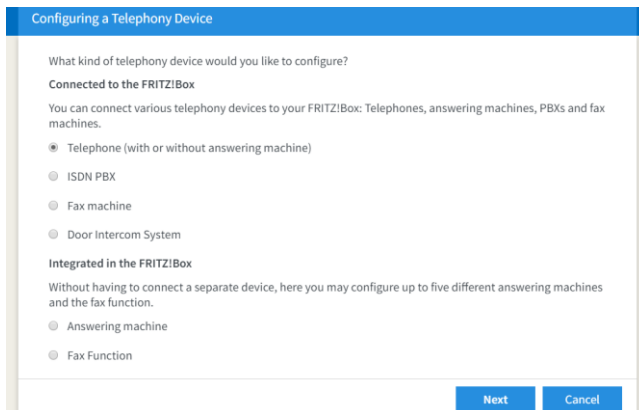
When using the V-Archive software, the "Tunnel Server Address" in the V-Tap must be set to the IP address of the PC.

# Configuration of the FRITZ!Box

Connect to the FRITZ!Box with a web browser and login.  
Select menu **Telephony** and then **Telephony Devices**



Press **Configure New Device**



Select **Telephone** and press **Next**

**Connect a telephone**

1. Connect the telephone to a suitable FON socket on the FRITZ!Box or keep your cordless (DECT) or IP phone ready.
2. Select the interface to which you connected the telephone.
  - FON 1 (analog telephone) - busy
  - FON 2 (analog telephone) - busy
  - FON S0 (ISDN telephone)
  - Cordless (DECT) telephone
  - LAN/WLAN (IP telephone)
3. Enter a name for the telephone, for example "living room" or "Anna's phone":

Select **LAN/WLAN (IP telephone)**, fill in a name and press **Next**

**Apply Settings to the IP Telephone**

1. Note the following account information to register your IP telephone after configuration with the FRITZ!Box.
2. Do this using the specified registrar, as well as the user name and a password you define yourself.

Registrar	fritz.box or 192.168.178.1
User name	<input type="text" value="V-Tap&amp;Fritz"/>
Password	<input type="password" value="v-tap&amp;fritz"/> good

Enter an easy to remember username and password and press **Next**  
*This account is only used internally and needed below during config.*

**Configure a telephone for outgoing calls**

Select which number should be used to conduct the calls.

1234567

Press **Next**

**Configure telephone settings for incoming calls**

Specify whether the telephone should accept all calls or only react to certain telephone numbers.

accept all calls  
 accept calls for the following numbers only:
 

- 1234567 (number for outgoing calls)

Back Next Cancel

Press **Next**

**Apply Settings**

The IP telephone is being configured with the following settings.

Telephony device	IP telephone
Name	V-Tap VoIP-2 Proxy
connected to/via	LAN/WLAN (IP telephone)
Number for outgoing calls	1234567
Numbers for incoming calls	all incoming calls

To save the settings in the FRITZ!Box, please click "Apply".

Back Apply Cancel

Press **Apply**

**Confirm**

The procedure requires extra confirmation.

- Pick up a telephone connected to the FRITZ!Box.
- Enter: \*17270
- Confirm your entries with the call key.
- Wait for the acknowledgment tone and hang up.

No telephone? Confirm with FRITZ!Box button ▲

**Confirm with FRITZ!Box button:**

- Briefly press any button on the FRITZ!Box.
- The LEDs on the FRITZ!Box flash once to confirm the procedure.

**Disable confirmation:**

The option "Extra confirmation of certain settings and functions" can be edited in the "System > FRITZ!Box Users > Login to the Home Network" area.

Cancel

See instructions above or press a button on the FRITZ!Box.

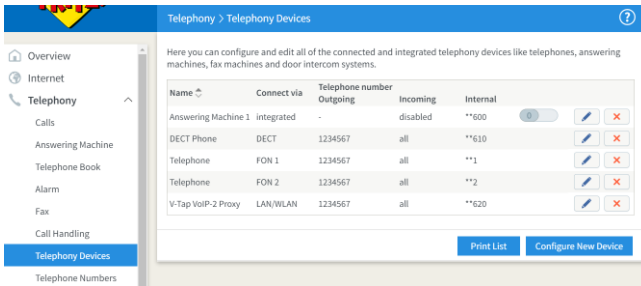
✔ Procedure confirmed

Click on "OK" to conclude the procedure.

OK Cancel

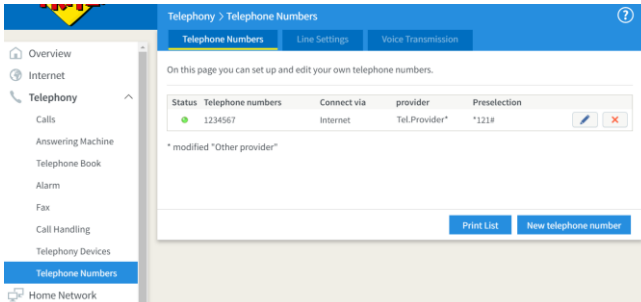


The list of Telephony Devices now looks as follows:

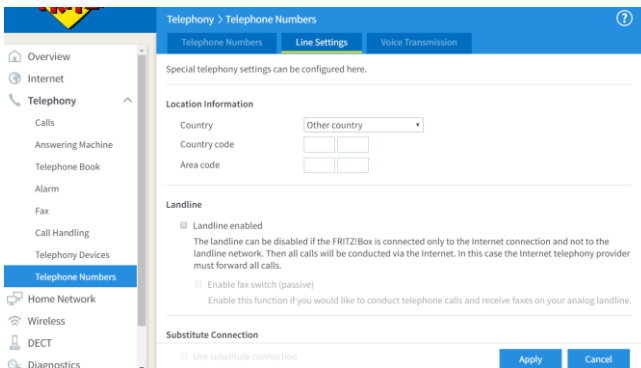


In menu **Telephony** on the left, select **Telephone Numbers**

*The following 2 steps may be skipped, but then some FRITZ!Box models might not be able to dial international numbers (test this yourself)!*



Select **Line Settings** on top



Empty the **Country code** and **Area code** fields and leave "Landline enabled" as it is, then press **Apply**

## New telephone number

In **Telephony > Telephone Numbers**, press **New telephone number**

**Entering telephone number**

Select your telephone provider and enter the telephone number and the registration data sent to you.

**Authentication Data**

Telephone provider:

---

Telephone Number for Registration\*:  Internal Telephone Number in the FRITZ!Box\*:

**\*Telephone Number for Registration**  
Please enter in this column the telephone number for registration. You received this telephone number from your provider. Different providers may call it by a different name. Please enter the telephone number exactly as you received it from the provider, including any special characters it may include.

**\*Internal Telephone Number in the FRITZ!Box**  
Now enter your telephone number without an area code and without special characters.

**Other Telephone Numbers**  
Under "Other Telephone Numbers" you can create additional telephone numbers, as long as they have same account information (user name and password) as the first telephone number. Telephone numbers with other account information can be configured later using the "New Telephone Numbers" button under "Telephone Numbers".

---

**Account Information**

User name:

Password:

Registrar:

Proxy server:

---

**Additional Settings**

DTMF transmission:

Fill in as is shown above, then press **Next**

*The number 222 is just used as an example and can be any number, as long as it is the same as used later on in this configuration.*

**Saving telephone numbers**

You entered the following registration information for the new internet telephone number:

provider	Other provider
Internet Telephone Number	222
User name	V-Tap&Fritz
Registrar	192.168.178.1
Proxy server	192.168.178.222

In the next step the registration data will be saved in the FRITZ!Box. Then a check will be performed to make sure that the configuration was completed successfully and that the configured telephone number now can be used to make telephone calls.

Check configuration of the telephone number after "Apply" has been clicked

Press **Next**

*Be sure the V-Tap VoIP-3 is connected to the LAN of the FRITZ!Box and has the right Proxy IP addresses.*

**Checking telephone numbers**

You entered the following registration information for the new internet telephone number:

provider	192.168.178.1*
Internet Telephone Number	222
User name	V-Tap&Fritz
Registrar	192.168.178.1
Proxy server	192.168.178.222

The registration information has been saved.

The telephony check was successful.

Press **Next**

**Telephony > Telephone Numbers**

On this page you can set up and edit your own telephone numbers.

Status	Telephone numbers	Connect via	provider	Preselection
<span style="color: green;">●</span>	1234567	Internet	*Tel.Provider*	**121#
<span style="color: red;">●</span>	222	Internet	192.168.178.1*	**122#

\* modified "Other provider"

Select **Telephony Devices** on the left.

**Telephony > Telephony Devices**

Here you can configure and edit all of the connected and integrated telephony devices like telephones, answering machines, fax machines and door intercom systems.

Name	Connect via	Telephone number Outgoing	Incoming	Internal
Answering Machine 1	Integrated	-	disabled	**600
DECT Phone	DECT	1234567	all	**610
Telephone	FON 1	1234567	all	**1
Telephone	FON 2	1234567	all	**2
V-Tap VoIP-2 Proxy	LAN/WLAN	1234567	all	**620

Press the **Edit/Pencil** button behind **"V-Tap VoIP Proxy"**

**Telephone Device on the "LAN/WLAN" Port**

**IP telephone** | Account information

The number you enter in the "Outgoing calls" field specifies the default connection type and the outgoing number of the IP telephone.

Name: V-Tap VoIP-2 Proxy

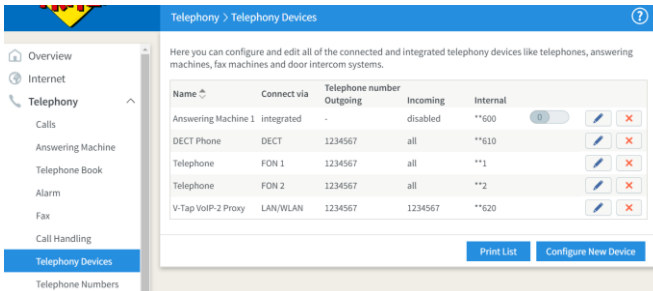
Outgoing Calls: 1234567

Note: This telephone may only make outgoing calls to numbers within the country. Change

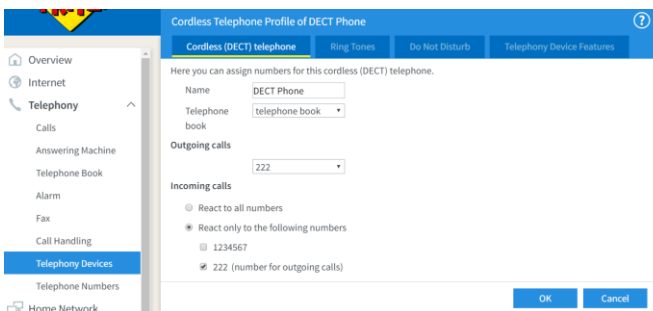
Incoming calls:

- React to all numbers
- React only to the following numbers
  - 1234567 (number for outgoing calls)
  - 222

Select the provider number for both out and in calls and in calls and allow international calls if applicable, then press **OK**



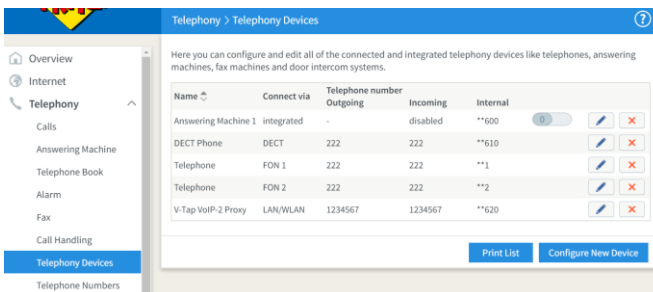
Press the **Edit/Pencil** button behind the **DECT Phone** device, or other telephony device that has to be recorded with the V-Tap.



Select number **222** for both Outgoing and Incoming calls, then press **OK**

*This step must be repeated for all telephony devices that have to be recorded with the V-Tap.*

The list of Telephony Devices then finally looks like this:

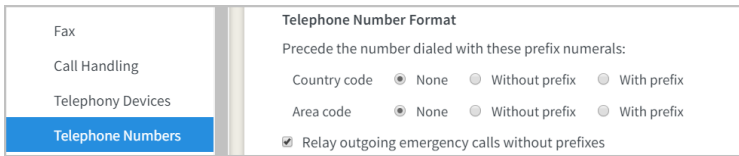


Recording the telephone calls should now work!

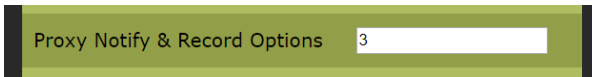
*Please also read the notes on the next page.*

## Notes for FRITZ!Box recording:

- DECT phones sometimes have to re-register before the newly programmed numbers start to work.
- For ISDN phones, the number 222 (from this example) must be programmed as MSN in the telephone itself.
- To be sure that dialling all number formats will work, better disable all prefixes by editing all entries in menu **Telephone Numbers**:



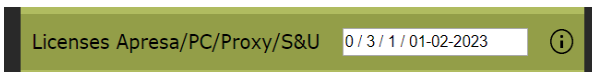
- To test if recording works in all cases, it might be handy to enable the notification message on the V-Tap, as is shown here:



At the start of each call a message is heard now, indicating that the call has passed the V-Tap.

Also, the **Blue LED** must blink fast during the call, indicating that recording the voice data works.

- The number of calls that can be recorded simultaneously depends on the FRITZ!Box model and can be 1 (73xx) or 2 (74xx) or 3 (75xx).
- To record 2 or 3 calls simultaneously, the V-Tap needs at least 2 or 3 PC licenses to get all recordings into V-Archive.  
The V-Tap also needs 1 Proxy license for FRITZ!Box recording:



- To get the direction of the call right in V-Archive (in-out), the name "fritzbox" must be entered in the field 'Local telephone numbers' in V-Archive > Options > Setup > Recording tab > Advanced settings.  
However, this name may differ per Fritz!BOX.

\*\*\* end of FRITZ!Box recording \*\*\*

## 8 TLS on the V-Tap VoIP-3

TLS mode is only available on the V-Tap VoIP-3.

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

### 8.1 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.

#### 8.1.1 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.

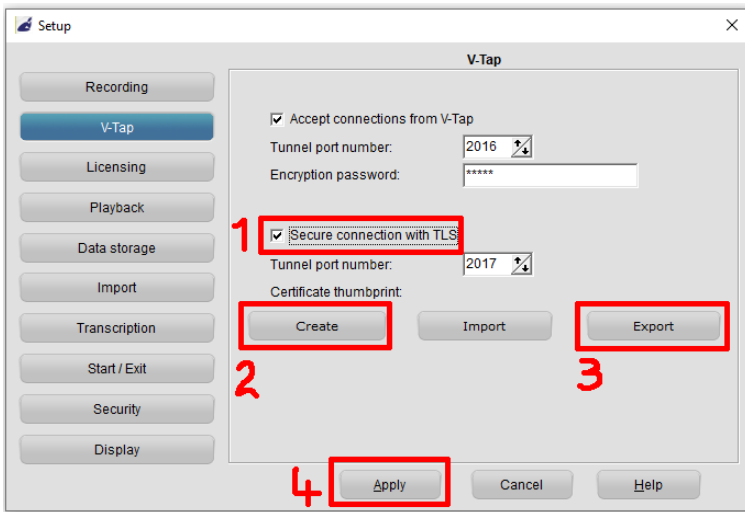
The V-Tap must also have it's time configured correctly, so that it falls between the "Not before" and "Not after" dates of the certificate. These dates are also determined during certificate generation. If a certificate expires, the V-Tap will no longer accept it.

## 8.1.2 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.

## 8.2 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".

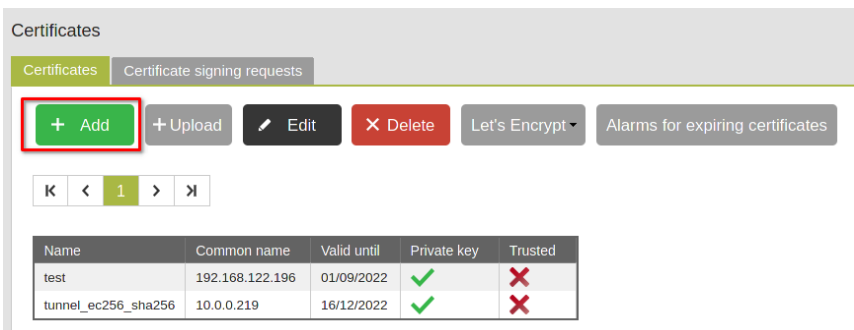
## 8.3 Tunnel protocol to Apresa with TLS

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

### 8.3.1 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**.

Certificate

Name: Tunnel Certificate

Common name: recording.vidicode.com

Trusted:

Private key:

Web server access to the private key:  (SAML)

Show certificate information:

Download

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.

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.v...)

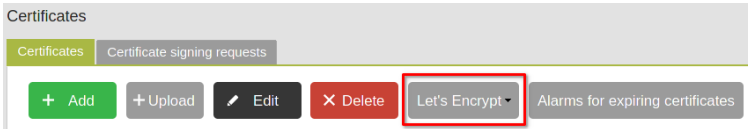
5. Insert the SD-card with the **TUNNEL.CRT** file into the V-Tap. The file is automatically copied to internal memory and then removed from the card. If everything has been done correctly, the V-Tap will connect to the Apresa via TLS if it is configured to so with the "[Secure Connection](#)" option. 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 <input type="button" value="="/>
Tunnel Status (TLS)	Listening on port: 2017	OK <input type="button" value="="/>
000349FEDC22	Connected (TLS)	OK <input type="button" value="="/>

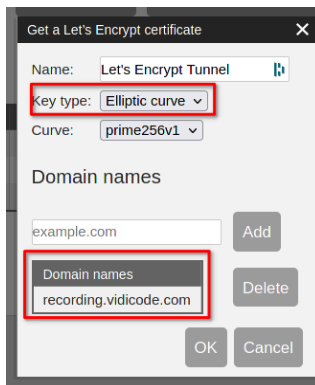
## 8.3.2 Tunnel-TLS with a Let's Encrypt certificate

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

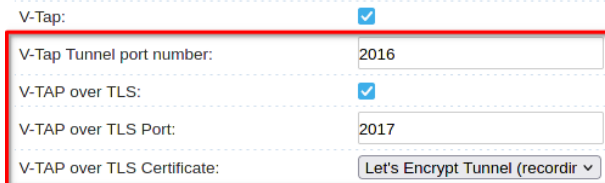
1. Go to Tools > Certificates. Select the Let's Encrypt menu. Register first from this menu if not done so already.



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	—

### 8.3.3 Tunnel-TLS with a certificate from another CA

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
Tunnel Status (TLS)	Listening on port: 2017	OK
000349FEDC22	Connected (TLS)	OK

## 8.4 Web interface over HTTPS

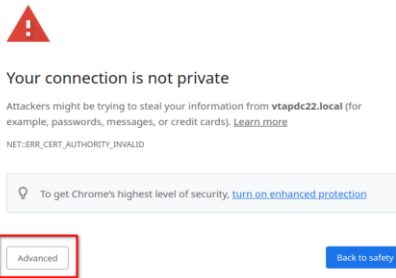
If HTTPS for the web interface is enabled, it will become available through `https://vtapXXXX.local` or `https://<ip-address>`. All communication with the web interface will then be encrypted.

### 8.4.1 HTTPS with a self-signed certificate

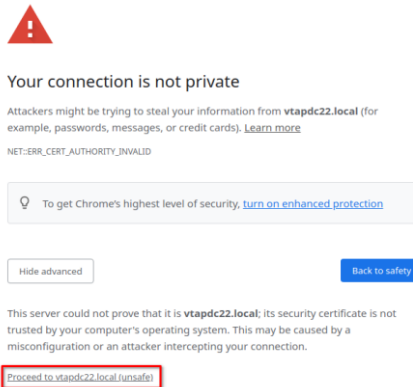
A self-signed certificate is generated by the V-Tap unit once https is enabled. Because the certificate is self-signed, web browsers are unable to validate it and might give a warning that the certificate is untrusted when first accessing the web interface through https. Usually there is a way to make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

#### Chrome browser

1. Click advanced



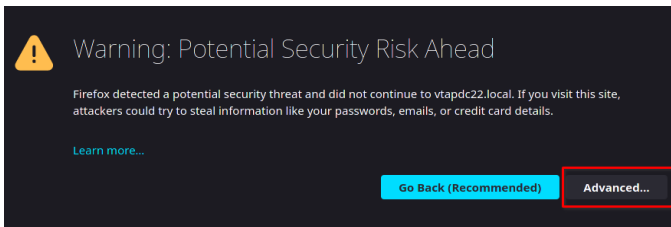
2. Click proceed to .....



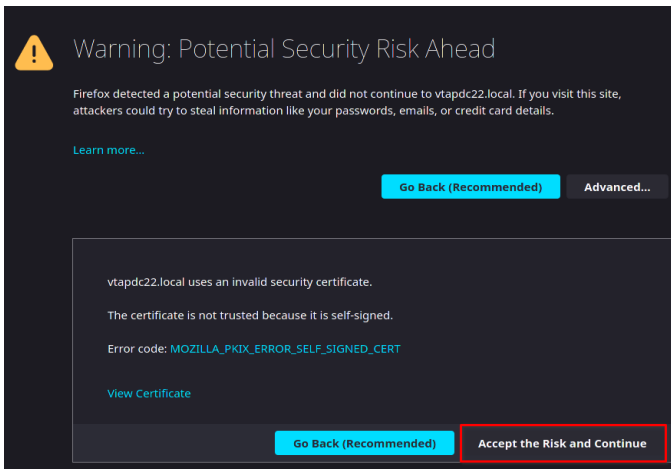
If no such options is shown, trying typing "thisisunsafe" (without the quotes).

## Firefox browser

### 1. Click advanced



### 2. Click Accept the Risk and Continue



## 8.4.2 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.



## 8.5 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

## 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 VoIP.

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 Technical Specifications

LAN port	: RJ45, Ethernet 10/100/1000 BASE-T, Full Duplex
PHONE1 port	: RJ45, Ethernet 10/100/1000 BASE-T, Full Duplex
Port Status LED's	: Link active & Rx/Tx activity blinking on all 4 Ethernet ports.
Switching	: L2 switching on all Ethernet ports.
PoE Bridge	: PoE is passively bridged from LAN to PHONE1, IEEE 802.3af. So, if the cable carries PoE, it is bridged to the other port. Note that the V-Tap VoIP itself does not generate PoE.
SD Card type	: Best to use SDHC/XC Ultra with a minimum speed of 40 MB/s.
SD Card size	: 8, 16 or 32 GB. Bigger is possible but must be FAT32 formatted.
SD Card storage	: Depends on the used VoIP codec and other network traffic. For normal G.711 VoIP calls, it is about 12 hours per 1 GB. For normal G.729 VoIP calls, it is about 24 hours per 1 GB.
USB Version	: V2.0 High Speed (480Mbps)
USB Profile	: Generic HID ( <b>VID_0DE1</b> & <b>PID_5101</b> or <b>PID_5102</b> )
USB Current	: 5V @300mA (Max. 2W)
USB Connector	: Full size 'B'- type
Button	: Function as described here: <a href="#">Button functions</a>
LED's (4x)	: Function as described here: <a href="#">LED's</a>
Size ( L x B x H )	: 137 x 81 x 30 mm
Housing material	: Blue bottom with Silver top, 4 pcs soft rubber footpads.
Weight	: 150 Gram
Temperature Range	: 0 – 40 °C
Humidity Range	: 10 – 90 %, non-condensing
EMC	: EN 55022:2010 / AC:2011 Class B , EN 55024:2010
Safety	: EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011
RoHS	: EN 50581:2012 (RoHS2) , RoHS Directive 2011/65/EU

# 11 Revision History

## v3.30 April 2024

- First release, based on the manual for the V-Tap VoIP 1 & 2.

## **12 Acknowledgements**

### **12.1 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.

### **12.2 Liability**

Correct functioning of the V-Tap VoIP 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 VoIP.