



# ***PROFITAP VTAP***

*USER MANUAL*

**PROFITAP**

[www.profitap.com](http://www.profitap.com)

If you have any questions, you can contact us through our website:

[www.profitap.com](http://www.profitap.com)

or by email:

[support@profitap.com](mailto:support@profitap.com)

For the latest documentation and software, visit our Resource Center:

<https://resources.profitap.com/>

# TABLE OF CONTENTS

<b>1. vTAP System Architecture</b>	<b>5</b>
1.1 Abbreviations	5
1.2 Overview	5
1.3 Prerequisites	5
1.4 Minimum Resource Requirements	5
<b>2. vTAP Deployment</b>	<b>6</b>
2.1 Select an OVF Template	7
2.2 Select a Name and Folder	7
2.3 Select a Compute Resource	8
2.4 Review Details	8
2.5 Select Storage	9
2.6 Select Networks	9
2.7 Customize Template	10
2.8 Ready to Complete	10
2.9 Adjust Network Settings	11
2.10 IP Address	12
<b>3. vTAP Manager Configuration</b>	<b>13</b>
3.1 Login	13
3.2 Dashboard	13
3.3 Virtual Environments	14
3.3.1 VCSA Access	14
3.3.2 Virtual Machines	17
3.3.3 Virtual Distributed Switches	17
3.4 Statistics	18
3.4.1 Global Statistics	18
3.4.2 Active Rule Set	19
3.5 Traffic Management	19
3.5.1 Active Rule Set	19
3.5.2 Rule Sets	20
3.5.2.1 Rule Set Configuration	22
3.5.2.2 Rule Configuration	22
3.5.3 Interface Groups	29
3.6 Authentication	30
3.6.1 Users	30
3.6.2 TACACS+	30
3.6.3 RADIUS	31
3.6.4 Custom Authentication Configuration	31
3.7 Administration	32
3.7.1 License Information	32
3.7.2 Configuration Backup and Restore	32
3.7.3 Network	33
3.7.4 CA Certificates	33

3.7.5 Syslog	33
3.7.6 Support	33

**Legal** **34**

Disclaimer	34
------------	----

Copyright	34
-----------	----

Trademarks	34
------------	----

# 1. vTAP System Architecture

## 1.1 Abbreviations

<b>VDS</b>	Virtual Distributed Switch
<b>VCSA</b>	vCenter Server Appliance
<b>vNPB</b>	Virtual Network Packet Broker
<b>VM</b>	Virtual Machine

## 1.2 Overview

Profitap vTAP consists of two components: the **vTAP Manager**, and the **vNPB** (or vBroker).

The vTAP Manager is an orchestrator for the virtual TAPs and filtering machines (vNPB). It has complete visibility over the entire virtual environment: VMs, VDS, hosts, and VCSA.

The vNPB must be deployed on the same host as the tapped VMs, while the vTAP Manager can be deployed on any host having a constant connection to the VCSA.

## 1.3 Prerequisites

vSphere 6.5 or 7  
Virtual Distributed Switch  
vCenter Server Appliance

## 1.4 Minimum Resource Requirements

**vTAP Manager:** 1 vCPU, Memory 2 GB, Hard Drive 12 GB  
**vNPB:** 1 vCPU, Memory 2 GB, Hard Drive 12 GB

## 2. vTAP Deployment

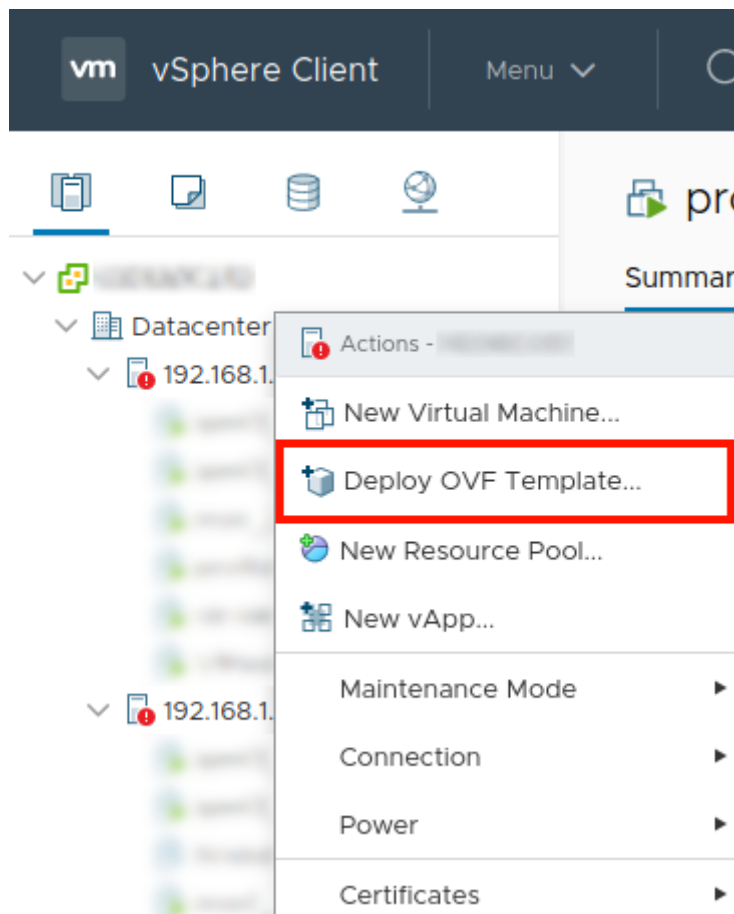
Deploying the vTAP on a host will deploy the vTAP Manager. vNPB deployment is done automatically by the vTAP Manager on any host on which it is required by the filter rules (see [Rule Sets](#) section).

The Profitap vTAP release consists of the following files:

**profitap\_vtap.ovf**

**profitap\_vtap.vmdk**

To deploy the vTAP, connect to your vSphere client, select *Deploy OVF Template* on the desired ESXi host, and follow the wizard.



## 2.1 Select an OVF Template

The screenshot shows the 'Deploy OVF Template' wizard at step 1, 'Select an OVF template'. The left sidebar lists the steps: 1. Select an OVF template (highlighted), 2. Select a name and folder, 3. Select a compute resource, 4. Review details, 5. Select storage, and 6. Ready to complete. The main area is titled 'Select an OVF template' and contains the instruction 'Select an OVF template from remote URL or local file system'. Below this, there is a text input field with the placeholder 'http | https://remoteserver-address/filetodeploy.ovf|.ova'. There are two radio button options: 'URL' (unselected) and 'Local file' (selected). Under 'Local file', there is a 'Browse...' button and the text '2 files selected.'. At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'.

- Select *Local file*
- Click *Browse*
- Navigate to the location of the vTAP files
- Select **both** files (OVF and VMDK)
- Click *Next*

**Note:** It is important to select both the OVF and VMDK file. To select multiple files, use CTRL on PC, and CMD on Mac.

## 2.2 Select a Name and Folder

The screenshot shows the 'Deploy OVF Template' wizard at step 2, 'Select a name and folder'. The left sidebar lists the steps: 1. Select an OVF template (checked), 2. Select a name and folder (highlighted), 3. Select a compute resource, 4. Review details, 5. Select storage, and 6. Ready to complete. The main area is titled 'Select a name and folder' and contains the instruction 'Specify a unique name and target location'. Below this, there is a text input field for 'Virtual machine name:' with the value 'profitap\_vtap'. Underneath, there is a section titled 'Select a location for the virtual machine.' which contains a tree view with a root folder 'Datacenter' and a sub-folder 'Datacenter 1'. At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'.

- Enter a VM name
- The appropriate VM location should already be selected, but a different one can be selected if desired
- Click *Next*

## 2.3 Select a Compute Resource

The screenshot shows the 'Deploy OVF Template' wizard at step 3, 'Select a compute resource'. The progress bar on the left indicates that steps 1, 2, and 3 are completed. The main area is titled 'Select a compute resource' and contains the instruction 'Select the destination compute resource for this operation'. Below this is a tree view showing a 'Datacenter' folder expanded to show two compute resources, each with a red error icon. A 'Compatibility' section below shows a green checkmark and the text 'Compatibility checks succeeded.' At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'.

- The appropriate compute resource should already be selected, but a different one can be selected if desired
- Click *Next*

## 2.4 Review Details

The screenshot shows the 'Deploy OVF Template' wizard at step 4, 'Review details'. The progress bar on the left indicates that steps 1, 2, and 3 are completed, and step 4 is the current step. The main area is titled 'Review details' and contains the instruction 'Verify the template details.' Below this is a table with the following data:

Publisher	No certificate present
Download size	Unknown
Size on disk	Unknown (thin provisioned)
	8.0 GB (thick provisioned)

At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'.

- Verify the template details
- Click *Next*



## 2.5 Select Storage

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- 5 Select storage**
- 6 Customize template
- 7 Ready to complete

**Select storage**  
Select the storage for the configuration and disk files

Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed

VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Type
datastore1	458.25 GB	475.56 GB	351.88 GB	VM

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

- Select the storage for the configuration and disk files
- Click *Next*

## 2.6 Select Networks

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- 6 Select networks**
- 7 Customize template
- 8 Ready to complete

**Select networks**  
Select a destination network for each source network.

Source Network	Destination Network
vTapNetwork	VM Network

1 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL BACK NEXT

- Select the network for the vTAP Manager VM to connect to. The network must be reachable by the user (via HTTPS), by the VCSA, and by the ESXi hosts where vNPBs will be deployed.
- Click *Next*

## 2.7 Customize Template

Deploy OVF Template

✓ 1 Select an OVF template  
✓ 2 Select a name and folder  
✓ 3 Select a compute resource  
✓ 4 Review details  
✓ 5 Select storage  
**6 Customize template**  
7 Ready to complete

✓ All properties have valid values

Configuration parameters 6 settings

Use DHCP	If turned off, 'IPv4', 'Netmask' and 'Gateway' fields are mandatory to be filled in; if one or more of them have incorrect or empty values, while DHCP is off, the machine will try to use fallback values: 169.254.1.1 and 255.255.0.0 for 'IPv4' and 'Netmask' in respect
IPv4	If DHCP is off 192.168.1.1
Netmask	If DHCP is off 255.255.255.0
Gateway	If DHCP is off
Nameserver	IP address of the nameserver
Hostname	Hostname of the machine

CANCEL BACK NEXT

Configure network settings for the vTAP Manager on this window.

If *Use DHCP* is enabled, the vTAP Manager will attempt to get network settings from a DHCP server. If the vTAP Manager cannot receive network settings from a DHCP server (no DHCP server available, or no allocatable IP addresses available), it will use *169.254.1.1* as fallback IP and *255.255.0.0* as netmask. The *IPv4*, *Netmask*, and *Gateway* fields are ignored.

If *Use DHCP* is disabled, the *IPv4* and *Netmask* fields are required. If these fields are empty, or filled but malformed, the vTAP Manager will use *169.254.1.1* as fallback IP and *255.255.0.0* as netmask.

## 2.8 Ready to Complete

Deploy OVF Template

✓ 1 Select an OVF template  
✓ 2 Select a name and folder  
✓ 3 Select a compute resource  
✓ 4 Review details  
✓ 5 Select storage  
✓ 6 Customize template  
**7 Ready to complete**

Ready to complete  
Click Finish to start creation.

Provisioning type	Deploy from template
Name	profitap_vtap
Template name	profitap_vtap
Download size	Unknown
Size on disk	8.0 GB
Folder	Datacenter
Resource	
Storage mapping	1
All disks	Datastore: datastore1; Format: Thick provision lazy zeroed
Network mapping	0

CANCEL BACK FINISH

Review the template deployment summary and click *Finish*.

## 2.9 Adjust Network Settings

The screenshot shows the configuration interface for vApp Options. The top navigation bar includes Summary, Monitor, Configure (selected), Permissions, Datastores, Networks, and Updates. The left sidebar lists Settings (vApp Options selected), More, Alarm Definitions, Scheduled Tasks, Policies, and Guest User Mappings. The main content area shows 'vApp Options are enabled' with an 'EDIT...' button. Below this is the 'IP Allocation' section with expandable 'Authoring' and 'Deployment' options. The 'OVF Settings' section includes a 'VIEW OVF ENVIRONMENT' button and a table with two rows: 'OVF environment transport' (VMware Tools) and 'Installation boot' (Disabled). The 'Properties' section has buttons for ADD, EDIT, SET VALUE, and DELETE, followed by a table of configuration parameters.

	Key	Label	Value	Default Value	Category	Type
<input checked="" type="radio"/>	enable_dhcp	Use DHCP	True	True	Configuration parameters	boolean
<input type="radio"/>	ipv4	IPv4			Configuration parameters	string
<input type="radio"/>	netmask	Netmask			Configuration parameters	string
<input type="radio"/>	gateway	Gateway			Configuration parameters	string
<input type="radio"/>	nameserver	Nameserver			Configuration parameters	string
<input type="radio"/>	hostname	Hostname			Configuration parameters	string

Network settings can be adjusted in the vTAP Manager VM's properties.

With the vTAP Manager VM turned off, navigate to **Configure > Settings > vApp Options > Properties**, and adjust these properties as needed.

The *Use DHCP* option can be enabled or disabled in this window.

If *Use DHCP* is enabled, the *IPv4*, *Netmask*, and *Gateway* properties are ignored.

If *Use DHCP* is disabled, the *IPv4* and *Netmask* properties are required.

The vTAP Manager VM checks these properties when it is booted, and uses them if they have been changed since the last boot. Modifying the VM's network settings can also be done from within the vTAP Manager's user interface, in which case these displayed properties will not be updated, although they can still be modified, which will update the VM's network settings the next time it is booted.

**NOTE:** If the vTAP Manager is migrated (either manually, or during a VMware environment upgrade) the vApp options will need to be recreated.

With the vTAP Manager VM turned off, navigate to **Configure > Settings > vApp Options > Properties**, and recreate these properties as needed (see image above).

Additionally, the *VMware Tools* option **needs to be enabled**. To do so, click the *EDIT* button at the top right corner of the *vApp Options* page, navigate to the *OVF Details* tab, and tick the *VMware Tools* checkbox.

Edit vApp Options | profitap\_vtap\_051

Enable vApp options

IP Allocation | **OVF Details** | Details

OVF environment transport

ISO image ⓘ

VMware Tools ⓘ

Installation boot ⓘ

Enable

Delay (s) 0 ⓘ

## 2.10 IP Address

The vTAP Manager VM's IP address will appear in *IP Addresses* on the VM's *Summary* page. Note that it may take 1-2 minutes to appear after the VM has been turned on.

## 3. vTAP Manager Configuration

### 3.1 Login

Open a web browser and enter the vTAP Manager's IP address in the address bar.

Login, using the appropriate account credentials.

The initial credentials are as follows:

- Username: **admin**
- Password: **admin**

**Note:** It is strongly recommended to change the default administrator password when first accessing the vTAP Manager.

To change the default password, click the *Admin* link at the bottom left of the screen and enter a new password in the Edit User window.

### 3.2 Dashboard

The screenshot displays the vTAP Manager Dashboard. It is divided into three main sections: State Information, Total Traffic Statistics, and ESXi Hosts.

**State Information:**

Platform:	vmware	Total VCSAs:	1
Product ID:	vtap	Total VMs:	13
Software version:	fb917ba	Total VDSes:	1
Time:	15/09/2020 15:15	ESXi Hosts:	2
Uptime:	23:36:45		

**Total Traffic Statistics:**

Rx Bandwidth:	196 kbps	Tx Bandwidth:	196 kbps
Rx Bytes:	4 Mbps	Tx Bytes:	4 Mbps
Rx Packets:	948,186	Tx Packets:	948,186
Rx Error Packets:	712,786	Tx Error Packets:	712,786
Rx Dropped Packets:	1,348,604	Tx Dropped Packets:	1,348,604
Filter Dropped Packets:	91,607,968	Filter Dropped Bytes:	86 bps

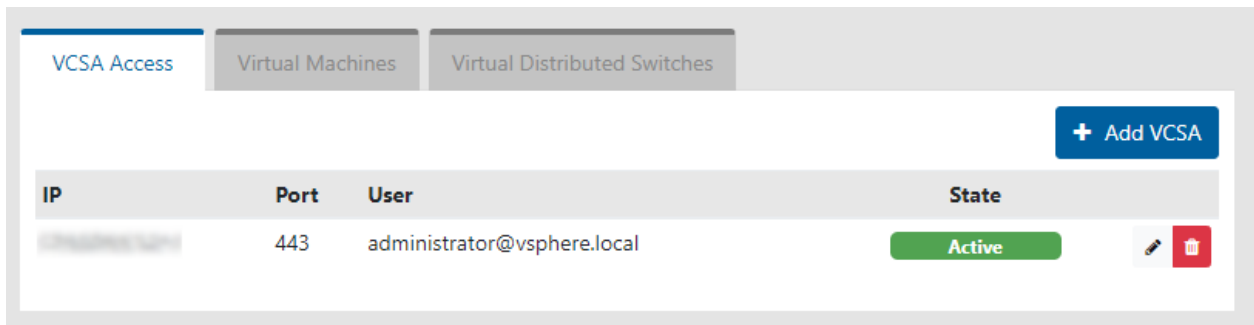
**ESXi Hosts:**

Connected	Model	IP address	CPU usage	Memory usage	Storage usage	Uptime	VMs number
✓			0.22 %	0.62 %	0.02 %	28d - 2m - 33s	6
✓			0.19 %	0.79 %	0.23 %	29d - 4h - 15m - 0s	7

The Dashboard page contains general information and statistics about the vTAP software and the network(s) it is connected to.

## 3.3 Virtual Environments

### 3.3.1 VCSA Access



The VCSA Access page lists VCSAs that the vTAP has been configured to connect to, and their current status (*Active, Loading, Wrong Credentials, or Unavailable*).

The permissions on this page for the different user roles are as follows:

Role	Permissions
Admin	Add, edit, remove VCSAs
Operator	Read-only
Viewer	Read-only

### Add VCSA ✕

VCSA Credentials  VCSA Networks

**Insert VCSA Credentials**


<b>IP</b>	<input type="text" value="192.168.1.100"/>	<b>Port</b>	<input type="text" value="443"/>
<b>User</b>	<input type="text" value="administrator@vsphere.local"/>	<b>Password</b>	<input type="password" value="....."/>




## Setup VCSA Networks

Host IP	Network	DHCP	IP	Netmask	Gateway
192.168.1.1	VM Network	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
192.168.1.2	VM Network	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

To add a VCSA, click the *Add VCSA* button. The *Add VCSA* window will appear. Fill in the fields: IP, Port, User, and Password. Click the *Next* button. If the vTAP is able to connect using the provided information, the next page will appear. Select the network and network settings for each ESXi host, then click *Done*. The VCSA will be added to the list.

To edit a current VCSA entry, click the *edit* button  on the line of the VCSA entry you would like to edit. The *Edit VCSA* window will appear. The process is the same as when adding a VCSA.

To remove a VCSA, click the *remove* button  on the line of the VCSA entry you would like to remove.

The following permissions are required on the vSphere account used to connect to a VCSA:

- **dvPort group**
  - Create
  - Delete
  - Modify
- **Distributed switch**
  - VSPAN operation
- **Datastore**
  - Allocate space
  - Remove file
  - Update virtual machine files
  - Update virtual machine metadata
- **Global**
  - Cancel task
- **Host**
  - Local operations
    - Create virtual machine
    - Delete virtual machine
    - Reconfigure virtual machine
- **Network**
  - Assign network
  - Configure
  - Remove
- **Virtual machine**
  - Change Configuration
    - Add new disk
    - Add or remove device
    - Modify device settings
    - Rename
    - Reset guest information
  - Edit Inventory
    - Create new
    - Remove
  - Interaction
    - Console interaction
    - Guest operating system management by VIX API
    - Power off
    - Power on
  - Provisioning
    - Deploy template
- **vAPP**

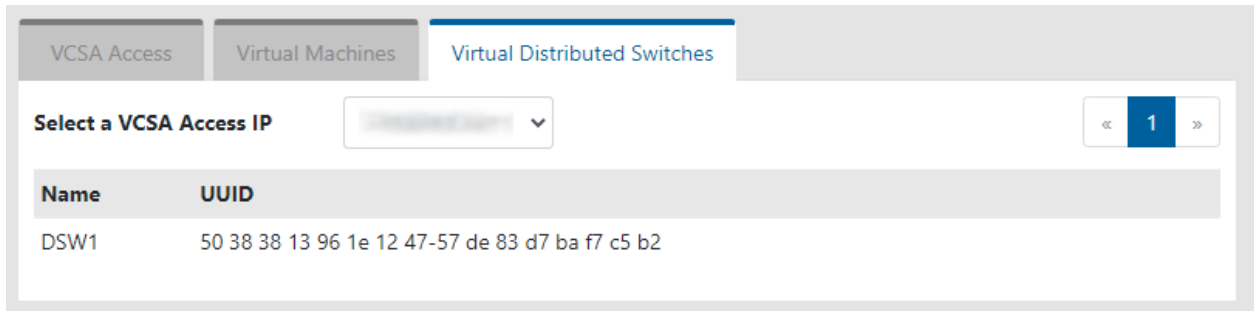


### 3.3.2 Virtual Machines

The Virtual Machines page lists all VMs on the currently-selected VCSA, providing their name, ESXi host on which they are present, UUID, number of NICs, and IP address(es) of each NIC.

To select a different VCSA, use the *Select a VCSA Access IP* drop-down menu.

### 3.3.3 Virtual Distributed Switches



The Virtual Distributed Switches page lists all VDSes on the currently-selected VCSA, providing their name and UUID.

To select a different VCSA, use the *Select a VCSA Access IP* drop-down menu.

## 3.4 Statistics

### 3.4.1 Global Statistics

Global Statistics		Active Rule Set			
<b>vTAP Processed Traffic Statistics</b>					
Received ▾	host1	host2			
Bandwidth	294 kbps	294 kbps			
Good packets	1,422,279	1,422,279			
Error packets	1,069,179	1,069,179			
vNIC drop packets	2,022,906	2,022,906			
All octets	5,542,962	5,542,962			
Transmitted ▾	host1	host2			
Bandwidth	294 kbps	294 kbps			
Good packets	1,422,279	1,422,279			
Error packets	1,069,179	1,069,179			
vNIC drop packets	2,022,906	2,022,906			
All octets	5,542,962	5,542,962			
Filtered					
Not-matching packets	137411952	137411952			
Not-matching octets	129	129			
<hr/>					
<b>Destination Statistics</b>					
IP	Type	Bytes	Passed	Error	Dropped
10.10.10.1	erspan2	691,356	1,975,308	1,378,152	173,752
10.10.10.1	erspan2	9,200,616	137,598,662	6,911,102	174,400

The vTAP Processed Traffic Statistics section provides aggregated statistics for all the hosts that are visible to the vTAP.

The Destination Statistics section provides traffic statistics for each of the interfaces set as destination in the active rule set.

### 3.4.2 Active Rule Set

Name	Passed packets	Dropped packets
rule_1	11,272,870	1,169,148
rule_2	1,759,752	1,612
rule_3	196	179,780

The Active Rule Set page provides statistics for each of the rules in the active rule set.

## 3.5 Traffic Management

Traffic management is done via Rule Sets. A rule set can contain any number of rules, with each rule containing any number of filters. Multiple different rule sets can be created to fit different needs and requirements, with only one being active at a time.

Each rule within a rule set defines one or more tapping points, the destination for the tapped traffic, and the filters applied to that traffic. Rules operate independently from each other.













Each filter within a rule defines which part of the traffic will be allowed or dropped. Filters within a rule operate in conjunction with each other, allowing for precise targeting of the desired traffic.

### 3.5.1 Active Rule Set

Name	rule_set_1	Description	Rule Set 1	Created By	admin
<b>Created Date</b>	15/09/2020	<b>Modified Date</b>	15/09/2020		
<b>Rules</b>					
Name	Sources	# of allowed filters	# of dropped filters	Destination	
rule_1	iperf3_1_215	1	0	2.2.2.2	

The Active Rule Set page provides information about the currently active rule set, and about the rules it contains.

### 3.5.2 Rule Sets

Name	Description	Created By	Created Date	Modified Date	
rule_set_1	Rule Set 1	admin	15/09/2020	15/09/2020	   
rule_set_2	Rule Set 2	admin	15/09/2020	15/09/2020	   
rule_set_3	Rule Set 3	admin	15/09/2020	15/09/2020	   

The Rule Sets page lists the existing rule sets, highlights the current active rule set, and provides the ability to add, rename, configure, duplicate, activate, and remove rule sets.

A rule set can contain multiple rules. Each rule defines which traffic will be tapped, and the destination the tapped traffic will be sent to.

**Note:** Only one rule set can be active at a time. The current active rule set is highlighted in blue in the rule set list.

**Note:** Modifications to the active rule set require the rule set to be applied again to take effect.

## Create Rule Set



Name

rule\_set\_1


Description


Rule Set 1

Save


Cancel

To add a rule set, click the *Create Rule Set* button. The *Create Rule Set* window will appear. Give the rule set a name by filling in the *Name* field. A description can also be given to the rule set by filling in the *Description* field. Click the *Save* button. An empty rule set will be created, to which rules can now be added (see [Rule Set Configuration](#) section).

To rename a rule set, click the *edit* button  on the line of the rule set you would like to rename. The *Edit Rule Set* window will appear. The process is the same as when adding a rule set.

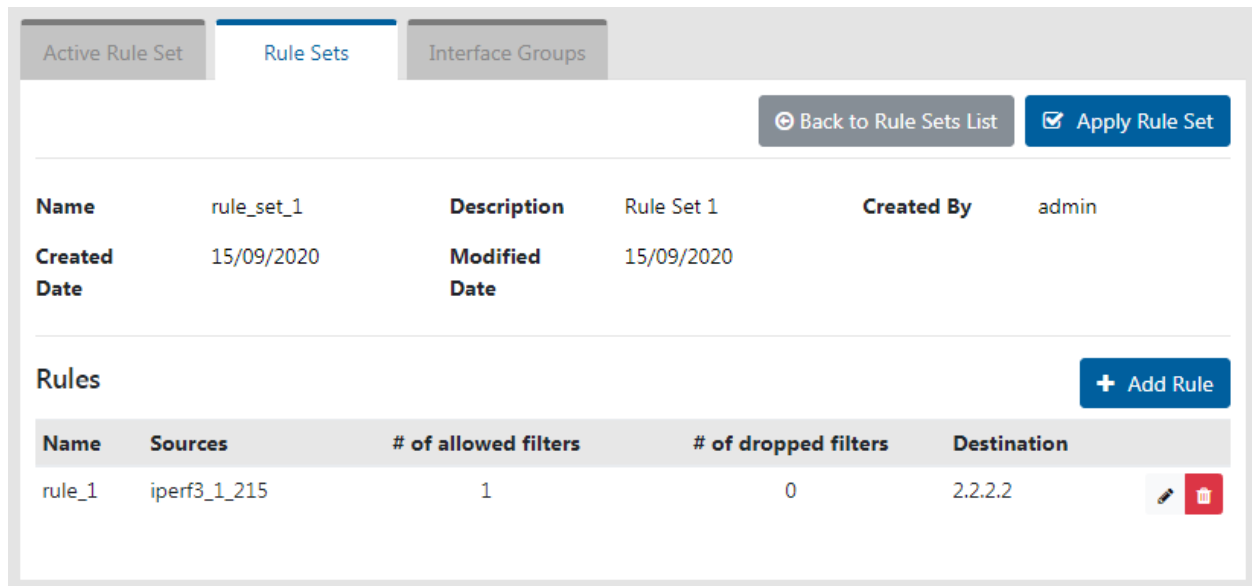
To configure a rule set, click the *configure* button  on the line of the rule set you would like to configure. Refer to the [Rule Set Configuration](#) section for more information.

To duplicate a rule set, click the *duplicate* button on the line of the rule set you would like to duplicate.

To activate a rule set, click the *apply* button  on the line of the rule set you would like to activate.

To remove a rule set, click the *remove* button  on the line of the rule set you would like to remove.

### 3.5.2.1 Rule Set Configuration



Name	Sources	# of allowed filters	# of dropped filters	Destination
rule_1	iperf3_1_215	1	0	2.2.2.2

The Rule Set Configuration page provides information about the rule set, and lists the rules it contains. It provides the ability to add, edit, duplicate, and remove rules, to activate the rule set, and to go back to the list of rule sets.

To activate the rule set, click the *Apply Rule Set* button.

To go back to the list of rule sets without activating the rule set, click the *Back to Rule Sets List* button.


### 3.5.2.2 Rule Configuration

Rules are processed independently from each other. Each rule can contain complex filters for targeting specific traffic.

Each rule defines the following:

- the interface(s) and/or group(s) of interfaces
- the direction of the traffic for each interface and/or group of interfaces
- the filter(s) that will be applied to the tapped traffic
- the destination for the tapped traffic

To add a rule to the rule set, click the *Add Rule* button. The *Create Rule* window will appear. Refer to the Create Rule section for information about the rule creation process.

To edit a rule, click the *edit* button  on the line of the rule you would like to edit. The *Edit Rule* window will appear. The process is the same as when creating a rule.

To duplicate a rule, click the *duplicate* button on the line of the rule you would like to duplicate.

To remove a rule, click the *remove* button  on the line of the rule you would like to remove.

### 3.5.2.3 Create Rule — Interfaces

Create Rule ✕

Interfaces Interface Groups Filters Destination

Name  Allow multicast/ broadcast traffic

Select Interfaces ✕ Deselect All

VM	State	Port	VDS	Host	TAP Direction
<input checked="" type="checkbox"/>	Active	50	DSW1		Inbound
<input type="checkbox"/>	Active	51	DSW1		Inbound
<input type="checkbox"/>	Active	52	DSW1		Inbound
<input type="checkbox"/>	Active	53	DSW1		Inbound
<input type="checkbox"/>	Active	54	DSW1		Inbound
<input type="checkbox"/>	Active	55	DSW1		Inbound
<input type="checkbox"/>	Inactive	56	DSW1		Inbound
<input type="checkbox"/>	Active	57	DSW1		Inbound
<input type="checkbox"/>	Inactive	58	DSW1		Inbound
<input type="checkbox"/>	Inactive	59	DSW1		Inbound
<input type="checkbox"/>	Inactive	100	DSW1		Inbound

Fill in the *Name* field to name the rule. If empty, a rule name will be automatically created.

Click the *Allow multicast/broadcast traffic* switch to include multicast and broadcast traffic in the tapped traffic.

Select the interfaces you would like to tap by ticking their checkbox. For each of the selected interfaces, select whether you would like to tap inbound traffic, outbound traffic, or both, in the *TAP Direction* drop-down menu.

Clicking the icon above the checkboxes reorders the list so that all currently selected interfaces appear at the top of the list, for a better overview of selected interfaces.

**Note:** Selecting interfaces on this page is not required. However, at least one interface or interface group must be selected to complete the rule creation process. Interface groups can be selected on the next page.

### 3.5.2.4 Create Rule — Interface Groups

Create Rule ×

Progress: Interfaces  — Interface Groups  — Filters  — Destination

Select Groups ✕ Deselect All

<input checked="" type="checkbox"/>	ID	Name	TAP Direction
<input type="checkbox"/>	1	group_1	<div style="border: 1px solid #ccc; padding: 2px;"><span>Inbound</span> ▾ Inbound Outbound Both</div>

Back Next Done

Select the interface groups you would like to tap by ticking their checkbox. For each of the selected interface groups, select whether you would like to tap inbound traffic, outbound traffic, or both, in the *TAP Direction* drop-down menu.

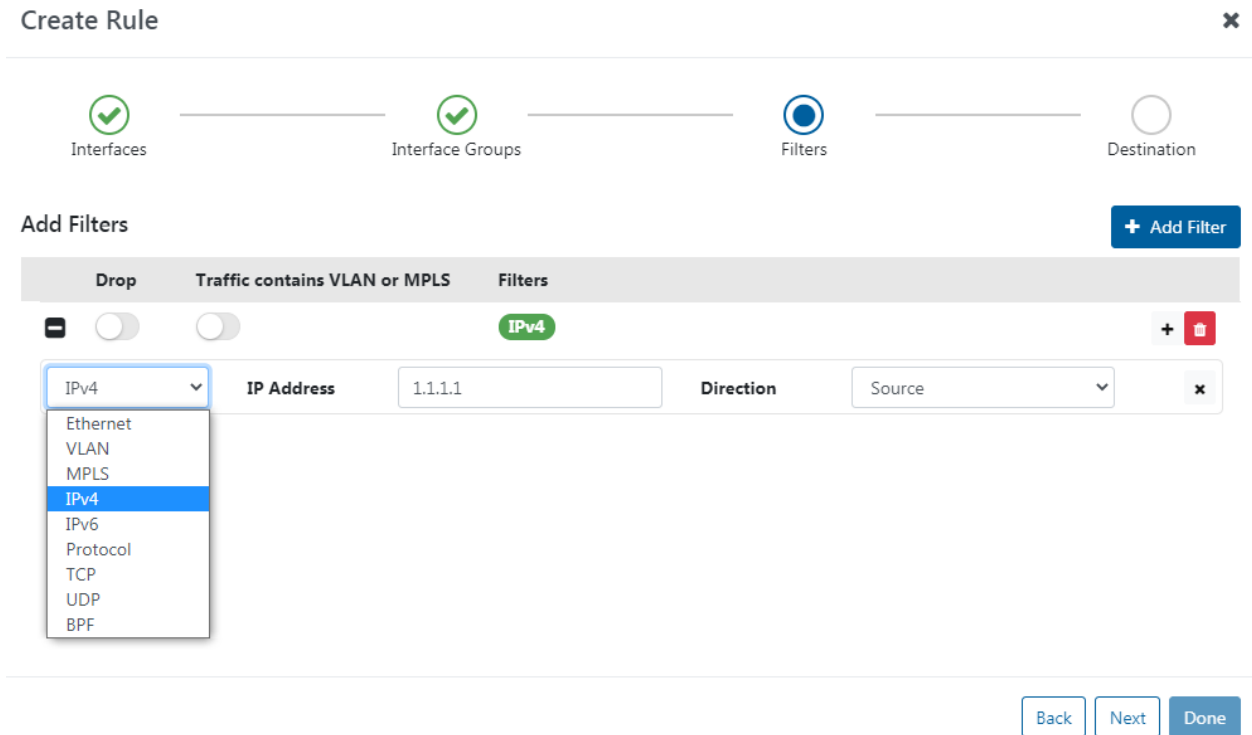
**Note:** Selecting interface groups on this page is not required. However, at least one interface or interface group must be selected to complete the rule creation process. Individual interfaces can be selected on the previous page.

**Note:** The *TAP Direction* setting of individually selected interfaces supersedes that of the selected group(s) they are part of.




**Note:** For interfaces that are present in two or more of the selected groups, the *TAP Direction* setting of those groups are merged (i.e. *Inbound + Outbound*, *Inbound + Both*, and *Outbound + Both* are treated as *Both*).



### 3.5.2.5 Create Rule — Filters



Multiple filter rows can be created, and each filter row can contain one or more statements.

To add a filter row, click the *Add Filter* button. A filter row with one statement will be created. To add more statements to a filter row, click the *add statement* button  of that specific filter row. To remove a statement from a filter row, click the *remove statement* button  of that specific statement. To remove a filter row, click the *remove* button  of that specific filter row.

#### No filters

If no filter rows are present, all traffic for the selected interfaces and their selected TAP direction will be tapped and sent to the destination.

#### "Allow" filter rows (Drop option off)

"Allow" filter rows are logically disjunctive (OR), and thus any traffic matching any "allow" filter row will be tapped and sent to the destination, except for the parts of that traffic that match "drop" filter rows.

#### "Drop" filter rows (Drop option on)

"Drop" filter rows are logically disjunctive (OR), and thus any traffic matching any "drop" filter row will be dropped.

If only "drop" filter rows are set, all traffic will be tapped and sent to the destination, except for traffic that matches any of these "drop" filters.

## Traffic contains VLAN or MPLS

When enabled on a filter row, this feature includes VLAN- and MPLS-tagged traffic for this filter row (up to 2 layers of encapsulation).

### Filter statements

Statements within a filter row are logically conjunctive (AND), and thus each filter row only applies to traffic which matches all of the statements within that filter row.

### Filter types

The **Filters** column of each filter row provides an overview of the filter types of all statements present in the filter row.

The leftmost drop-down menu of each statement allows the selection of the type of filter for this statement. The rest of the fields and drop-down menus in that statement will depend on the selected filter type.

### Ethernet

MAC Address: specify a MAC address.

Direction: select whether the targeted traffic should match the specified MAC address as Source, Destination, or both.

### VLAN

VLAN ID: specify the VLAN ID that the targeted traffic should match.

### MPLS

MPLS Label: specify the MPLS label that the targeted traffic should match.

### IPv4

IP Address: specify an IPv4 address.

Direction: select whether the targeted traffic should match the specified IPv4 address as Source, Destination, or both.

### IPv6

IP Address: specify an IPv6 address.

Direction: select whether the targeted traffic should match the specified IPv6 address as Source, Destination, or both.

### Protocol

Select the protocol that the targeted traffic should match.

## **TCP**

Select whether the targeted traffic should match a specific TCP port (*Single*) or a range of TCP ports (*Range*).

If *Single* is selected, type in the TCP port in the *Port* field.

If *Range* is selected, type in the first TCP port of the port range in the *Begin* field, and the last TCP port of the port range in the *End* field.

Direction: select whether the targeted traffic should match the specified TCP port or TCP port range as Source, Destination, or both.

## **UDP**

Select whether the targeted traffic should match a specific UDP port (*Single*) or a range of UDP ports (*Range*).

If *Single* is selected, type in the UDP port in the *Port* field.

If *Range* is selected, type in the first UDP port of the port range in the *Begin* field, and the last UDP port of the port range in the *End* field.

Direction: select whether the targeted traffic should match the specified UDP port or UDP port range as Source, Destination, or both.

## **BPF**

BPF allows the input of expressions using the Berkeley Packet Filter syntax.

### 3.5.2.6 Create Rule — Destination

#### Create Rule ×

---

✓  
Interfaces

✓  
Interface Groups

✓  
Filters

○  
Destination

#### Setup Destination

Tunnel Type	<input type="text" value="GRE"/>
IP Address	<input type="text" value="2.2.2.2"/>
Force MTU ⓘ	<input checked="" type="checkbox"/>
MTU	<input type="text" value="1500"/>

Specify the destination to which the traffic will be sent, and which tunneling protocol to use.

The supported tunneling protocols are GRE and ERSPANv2.

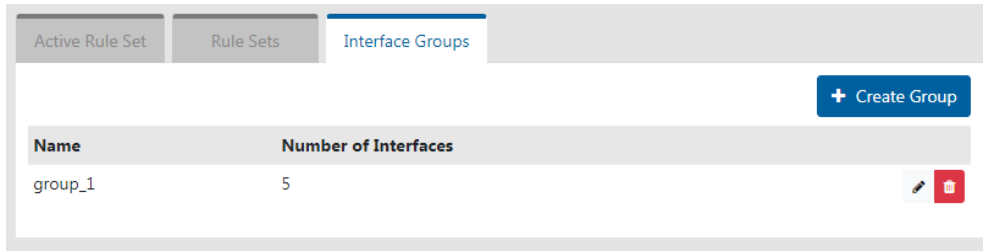
Select a protocol, and type in the destination IP address in the *IP Address* field. If ERSPANv2 is selected, a tunnel ID must also be provided in the *Tunnel ID* field.

**Note:** The destination must be reachable from the vNPB in order for it to receive the traffic.

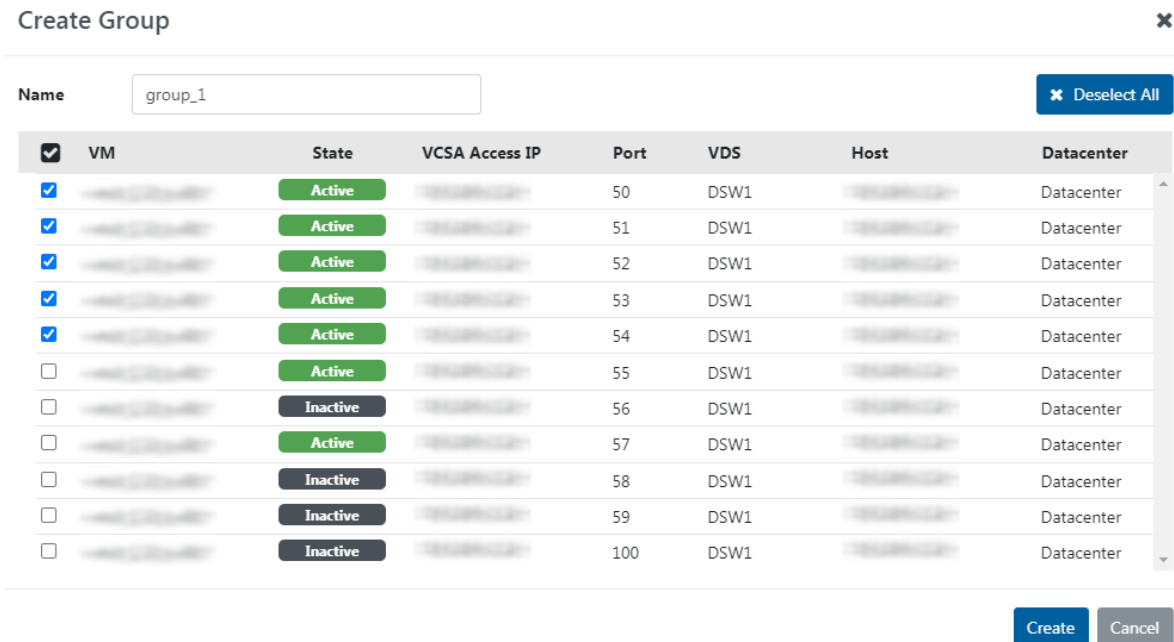
If *Force MTU* is disabled, the packets can be larger than the MTU of the network, which would lead such packets to be dropped. If the user is certain that the packets will always be smaller than the MTU (for example, VoIP packets are usually ~500 bytes), this setting can be disabled, leading to increased performance of the virtual broker.

If *Force MTU* is enabled, the final size of the packets can be controlled with the corresponding setting (in bytes).

### 3.5.3 Interface Groups




The Interface Groups page lists the existing interface groups, and provides the ability to add, edit, and remove interface groups.



To add an interface group, click the *Create Group* button. The *Create Group* window will appear. Give the group a name by filling in the *Name* field, then select the interfaces you would like to include in the group. Click the *Create* button.

Clicking the icon above the checkboxes reorders the list so that all currently selected interfaces appear at the top of the list, for a better overview of selected interfaces.

To edit an interface group, click the *edit* button  on the line of the group you would like to edit. The *Edit Group* window will appear. The process is the same as when adding a group.

**Note:** The list of interfaces only shows interfaces which can be tapped.

To remove an interface group, click the *remove* button  on the line of the group you would like to remove.

## 3.6 Authentication

### 3.6.1 Users

The **Users** tab allows users logged in as administrators to add new users or edit existing users and their privilege levels.

The user permissions for each Role are as follows:

Role	Permissions
Admin	Full access
Operator	Full access, except: - VCSA Access page read-only - Users page inaccessible - Administration page inaccessible
Viewer	- All pages read-only - Users page inaccessible - Administration page inaccessible

The minimum requirements for the passwords are as follows:

- 8 characters;
- one letter uppercase;
- one letter lowercase;
- one digit.



### 3.6.2 TACACS+

The **TACACS+** tab allows adding one or more TACACS+ servers, and configuring the following details:

- priority (sets the order in which the servers will be taken into account, if more are added, with a lower number corresponding to a higher priority);
- login type (chap, login, pap);
- server hostname;
- port;
- secret key;
- timeout (waiting time for response from the TACACS+ server, can be set between 1 and 15 seconds);
- privilege mapping (translates the 15 privilege levels from TACACS+ into those of the viewers, users and admins; can be configured).

### 3.6.3 RADIUS

The **RADIUS** tab allows adding one or more RADIUS servers, and configuring the following details:

- priority (sets the order in which the servers will be taken into account, if more are added, with a lower number corresponding to a higher priority);
- server hostname;
- port;
- secret key;
- timeout (waiting time for response from the RADIUS server, can be set between 1 and 15 seconds);
- privilege level mappings (allows adding one or more rules for users. These rules are integer or string **type** attributes, requiring a **name** and a **value**. During authentication, the system checks if a user matches the rules. If there is a match between a user and a rule, then a **role** is applied for the user);  
**Note:** To add a new rule, click the  button. To apply the rule, click the  button.
- fallback role (comes into place when there isn't a match between a user and a rule, with the 'none' option denying authentication access to *any* user).

### 3.6.4 Custom Authentication Configuration

vTAP Manager allows users to not only define multiple authentication methods, but also to configure how the different methods are used. Clicking the *Configure Authentication* button on either the *Users*, *TACACS+*, or *RADIUS* page allows users to see the list of available authentication methods and change their priority and activation strategy.

For each method, one of the following strategies can be selected:

- **Enable:** The method is activated and will be used to authenticate users;
- **Disable:** The method is not active and its configuration will be ignored;
- **Restrict:** A restricted authentication method is activated only if all higher priority methods are failing access. In the case of RADIUS or TACACS+ methods, this means that no server is responding (or no server is programmed). If only one of the registered RADIUS/TACACS+ servers replies with a rejection, the following restricted methods will be skipped. Note that *Local Users* are always available, meaning that any *restrict* method after that will never be activated.



## 3.7 Administration

### 3.7.1 License Information

The **License Information** section of the **Setup** tab provides information about the current vTAP license, and the ability to activate a license, and edit or deactivate the current license.

State: displays the current state of the license. The possible states and their meaning are as follows:

License State	Meaning
Inactive	No licence has been activated. The maximum amount of licensed taps is 10, and the license state will change to <i>Expired</i> after 6 hours.
Active	A license is currently active. The maximum amount of licensed taps and the expiration date are defined by the type of license.
Expired	The license has expired. The vTAP is disabled until a valid license is activated.
Suspended	The license has been suspended. The vTAP is disabled.
Grace period over	The vTAP was unable to verify the license for a certain amount of time. The vTAP is disabled until the license can be verified.
Error	An internal error. Please review system logs and contact support.

License Key: shows the current license key. To enter a new license key, press the *edit* button  , enter the license key in the now-active field, then click the *activate license key* button  to activate the license.

Deactivate button: deactivates the license on the current vTAP instance. Can be used in order to be able to activate the license on a different vTAP instance. After successful deactivation, the current vTAP instance license state will switch to *license expired* after 10 minutes.

Licensed Taps: displays the amount of tap points in the active rule set, and the maximum amount of tap points for the current license.

### 3.7.2 Configuration Backup and Restore

The **Configuration Backup and Restore** section of the **Setup** tab allows the exporting and importing of the vTAP instance configuration. The data can be exported by inserting a passphrase, selecting the parts to be exported, and pressing the *Export* button. The system will generate an encrypted archive that can be safely stored as backup. This package can be imported back to the vTAP instance via a similar process: insert the passphrase, select the parts of the configuration you wish to import, press the *Import* button, and select the archived configuration file.

**Note:** The same passphrase as the one used for exporting the configuration file is required for importing it.



### 3.7.3 Network

Network

<b>Link state</b>	Connected
<b>Hostname</b>	<input type="text" value="ubuntu-minimal"/>
<b>Name server</b>	<input type="text" value="8.8.8.8"/>
<b>DHCP</b>	<input checked="" type="checkbox"/>
<b>IP</b>	<input type="text" value="192.168.1.1"/>
<b>Mask</b>	<input type="text" value="255.255.255.0"/>
<b>Gateway</b>	<input type="text" value="192.168.1.1"/>
<b>MAC</b>	<input type="text" value="08:00:27:00:00:00"/>

The Network section provides information about the vTAP network information, and the ability to edit it. The IP, Mask, and Gateway fields can be edited if DHCP is disabled.

### 3.7.4 CA Certificates

CA certificates can be added in this section.

This is necessary, for instance, in cases in which the environment the vTAP is installed in has its own certificate authority, which does not allow a secure access to the internet from inside the vTAP, and thus prevents connections to the Cryptlex server, which is necessary to activate and maintain the license.

### 3.7.5 Syslog

The **Syslog** tab displays the logs of the vTAP system. On this page, the system logs can be refreshed, downloaded, or reset. The Syslog tab can also be used to configure remote collectors for the system logs. This can be done by clicking the *Remote Servers* button and using the view that appears to configure the remote logging server details.

### 3.7.6 Support

The **Support** tab provides access to support files embedded in the vTAP instance: the user manual (this document), REST API documentation, and Ansible library.

# ***Legal***

## ***Disclaimer***

The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes in the content thereof without obligation of the manufacturer to notify any person of such revision or changes.

## ***Copyright***

This publication, including all photographs and illustrations, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of the author.

## ***Trademarks***

The trademarks mentioned in this manual are the sole property of their owners.



Profitap develops and manufactures Copper and Fiber Network TAPs, Network Packet Brokers and Portable Field Service Troubleshooters. These solutions are designed with the security, forensics, deep packet capture and network performance monitoring sectors in mind. Profitap network solutions help eliminate network downtime and add security to existing and new networks all over the world, assist in lawful interception applications and reduce network complexity. All of Profitap's network monitoring tools are highly performant, secure and user-friendly, and provide complete visibility and access to your network, 24/7. Learn more at [profitap.com](https://profitap.com)

PROFITAP HQ B.V.  
High Tech Campus 84  
5656AG Eindhoven  
The Netherlands

[sales@profitap.com](mailto:sales@profitap.com)  
[www.profitap.com](https://www.profitap.com)

© 2022 Profitap — v2.8