



## ***IOTA 10 CORE+***

*USER MANUAL*

IOTA software version: v6.0.7

If you have any questions, visit our Knowledge Base:

**<https://kb.profitap.com/>**

You can also contact us through our website:

**<https://www.profitap.com/contact-us/>**

Or directly 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. Product Overview</b>	<b>5</b>
1.1. Hardware Overview	5
1.2. Package Contents	5
1.3. Specifications	6
1.4. Interfaces & LED Behavior	7
1.4.1. Front	7
1.4.2. Rear	8
<b>2. Getting Started</b>	<b>9</b>
2.1. Power	9
2.2. Accessing IOTA Over the Network	9
2.2.1. Initial setup over serial connection	9
2.2.2. Accessing the IOTA GUI	10
2.3. Capture Interfaces	11
<b>3. IOTA Configuration</b>	<b>12</b>
3.1. Administration	12
3.1.1. Time & NTP Configuration	12
3.1.2. Network Configuration	13
3.1.3. HTTPS Certificate	14
3.1.4. ZeroTier	14
3.1.5. System Control	15
3.1.6. Firmware	15
3.1.7. License	15
3.1.8. Logs	16
3.2. Authentication	18
3.2.1. Local Users	18
3.2.2. TACACS+	19
3.2.3. RADIUS	20
3.2.4. LDAP and LDAPS	21
3.2.5. Custom Authentication Configuration	22
3.3. Device Reset	22
3.3.1. Network Configuration	22
3.3.2. Factory Reset	22
3.4. Device Recovery CLI	22
3.4.1. Accessing the CLI	23
3.4.2. Using the CLI	23
<b>4. Capture Management</b>	<b>25</b>
4.1. Capture Interfaces	25
4.2. Traffic Analysis	26
4.3. Data Storage	28
4.3.1. Storage Management	28
4.3.2. Packet Capture Statistics	28
4.3.3. Packet Capture Filters	29
<b>5. Analysis Dashboards</b>	<b>31</b>

5.1. Network Overview	32
5.2. TCP Traffic Overview	35
5.3. DNS Traffic Overview	36
5.4. HTTP Traffic Overview	37
5.5. RTP Traffic Overview	38
5.6. Top Applications Overview, Top DNS Queries Overview	39
5.7. Global Traffic Overview	40
5.8. Data Details	41
5.8.1. Filters	41
5.8.2. Table	43
5.8.3. Time graphs	44
<b>Legal</b>	<b>48</b>
Disclaimer	48
Copyright	48
Trademarks	48

# 1. Product Overview

## 1.1. Hardware Overview

IOTA 10 CORE+ is a high-speed packet capture and analysis solution for core networks, large branches, and data centers.

IOTA allows you to capture network traffic and get detailed real-time and historical insights into critical applications and data. IOTA helps quickly resolve network issues like performance and application problems through complete packet and metadata analysis.



## 1.2. Package Contents

Carefully unpack all the supplied items and retain the packaging for later use.

- 1 x IOTA 10 CORE+ main unit
- 1 x power adapter (100–240 VAC to 24 VDC, 5 A, 120 W)
- 1 x C13 AC power cord
- 1 x GPS/GLONASS antenna
- 1 x RJ45 Ethernet cable
- 1 x USB to RJ45 cable
- 1 x carry case

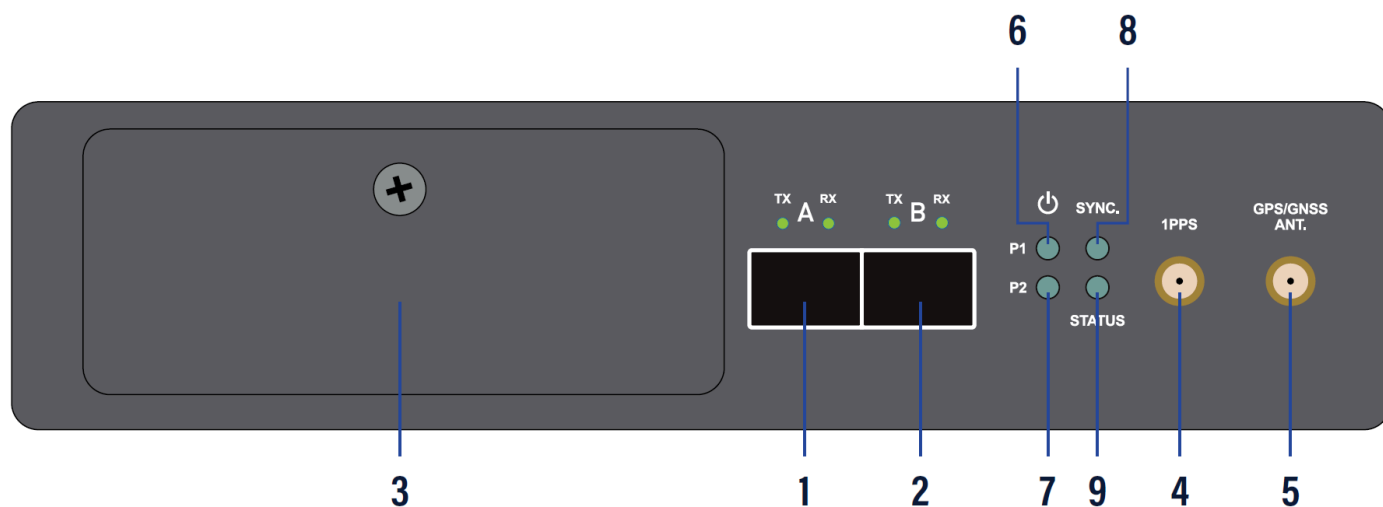
**Note:** Please contact the supplier if any part is missing or damaged.

### 1.3. Specifications

	<b>IOTA 10 CORE+</b>
Capture Interfaces	2 x 10G SFP+
Capture Mode	In-line and out-of-band
Supported Capture Speed	10G
Internal Storage	3, 15, or 30 TB high-performance solid-state storage
Power Inputs	2 x 24 VDC barrel jack (redundant)
Power Adapter	100–240 VAC, 50-60 Hz, 1.5 A to 24 VDC, 5 A, 120 W
Management Interfaces	1 x SFP+ Ethernet 10G 1 x RJ45 Ethernet 2.5GBASE-T 1 x RJ45 RS232 serial
Management Service	HTTPS (server) SSH (recovery CLI)
Timing Connectors	1 x SMA female (PPS) 1 x SMA female (GPS) 1 x RJ45 2.5G PTPv2
Additional Functions Interfaces	1 x USB 3.0
Dimensions (WxDxH)	165 x 255 x 50 mm 6.5 x 10 x 2 in
Weight	2.4 kg 5.3 lb

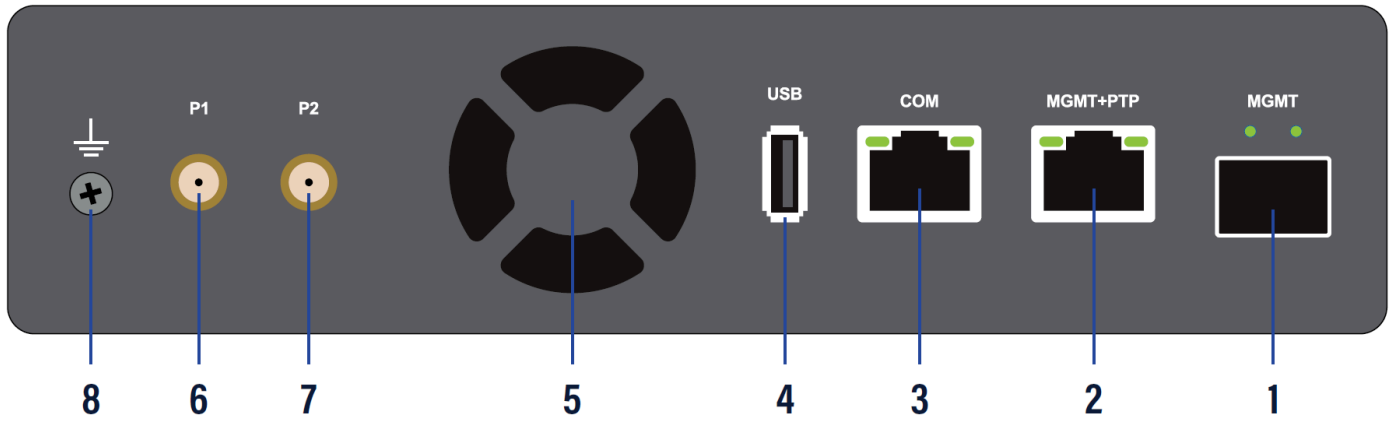
## 1.4. Interfaces & LED Behavior

### 1.4.1. Front



1	Capture port A, SFP+ 10G
2	Capture port B, SFP+ 10G
3	Removable SSD
4	SMA female connector (PPS in)
5	SMA female connector (GPS/GLONASS antenna)
6	Power 1 status LED <b>Green:</b> Power input 1 connected and receiving power. <b>Orange:</b> Power input 1 not receiving power. <b>Orange blinking:</b> System booting. <b>Red:</b> Error. <b>Off:</b> System shutting down or no power.
7	Power 2 status LED <b>Green:</b> Power input 2 connected and receiving power. <b>Orange:</b> Power input 2 not receiving power. <b>Orange blinking:</b> System booting. <b>Red:</b> Error. <b>Off:</b> System shutting down or no power.
8	Sync LED <b>Green blinking:</b> Internal timestamp synchronized with the configured time system (GPS, PTPv2, etc.) with an accuracy of $\pm 10$ ns.
9	Status LED <b>Green:</b> System operating normally. <b>Green blinking:</b> Capture in progress. <b>Orange blinking:</b> System booting. <b>Orange:</b> System shutdown initiated. <b>Orange+green blinking:</b> Updating OS. <b>Orange+magenta blinking:</b> Factory reset initiated. <b>Blue:</b> Capture interface state changing.

### 1.4.2. Rear



1	Management port 1, SFP+ Ethernet 10G
2	Management port 2 and PTPv2 port, RJ45 Ethernet 2.5GBASE-T
3	Serial management port, RJ45 RS232
4	USB 3.0 port
5	Fan
6	Power input 1, 24 VDC barrel jack
7	Power input 2, 24 VDC barrel jack
8	Grounding screw

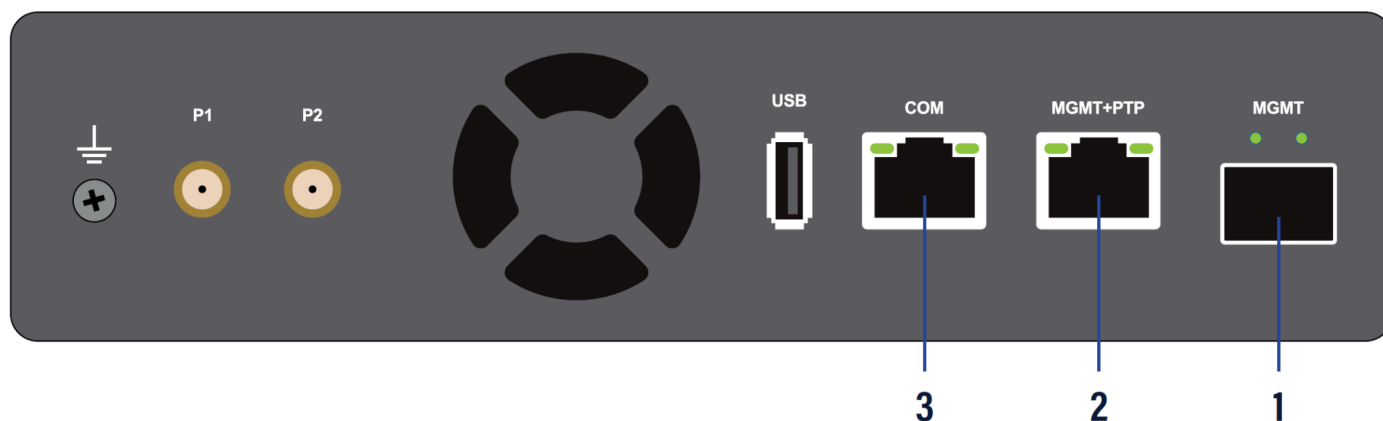
## 2. Getting Started

### 2.1. Power

Connect the power supply to one of the barrel jack power connectors at the rear of the unit, and connect it to the main power. IOTA boots automatically after a power connection is established. Its status can be observed via the activity LEDs.

The unit features redundant powering. If both power inputs are connected, redundant powering ensures continued operation in case either port were to be disconnected or unable to provide power.

### 2.2. Accessing IOTA Over the Network



Connect the MGMT or MGMT+PTP port (**1** and **2** in the image above) to the network used to access the unit. The management interface will attempt to get an IP address from a DHCP server.

The service tag located at the bottom of the unit provides the management interfaces' MAC addresses.

#### 2.2.1. Initial setup over serial connection

The network settings of the MGMT and MGMT+PTP management interfaces can be configured via the serial management port (**3** in the image above). If the unit is deployed on a network with a DHCP server, you can skip this step.

To connect to the serial management interface, use the supplied cable and adapters, and any terminal software, with the following connection settings: 115200 baud rate, 8 bit, no parity, 1 bit stop.

Log in, using the following default credentials:

Username: **admin**

Password: **admin**

To display the current configuration of the device's management interfaces, use the following command:

```
.netconfig.show
```

The following interfaces can be configured:

**Management 1:** MGMT SFP+ Ethernet 10G

**Management 2:** MGMT+PTP RJ45 Ethernet 2.5GBASE-T

To update the configuration of an interface, use the following command:

```
.netconfig.update
```

The following arguments are accepted:

- `--dhcp_enabled`  
true/yes/y to enable and false/no/n to disable.
- `--gateway`
- `--hostname`
- `--interface`  
number of the network interface to update. (default: 1)
- `--ip`
- `--nameserver`
- `--netmask`

For instance, to configure management interface '1' with static IP '2.2.2.2', netmask '255.255.255.0', and gateway '3.3.3.3', use the following command:

```
.netconfig.update --interface 1 --dhcp_enabled no --ip 2.2.2.2 --netmask  
255.255.255.0 --gateway 3.3.3.3
```

### 2.2.2. Accessing the IOTA GUI

To access the IOTA over the network, connect to the HTTPS interface by browsing to the device IP of your IOTA.

The full URL should be: `https://<ip_addr>`

DHCP mode is enabled by default.

Network settings can be modified via the IOTA GUI (see [Network Configuration](#)) or the recovery CLI (see [Device Recovery CLI](#)).

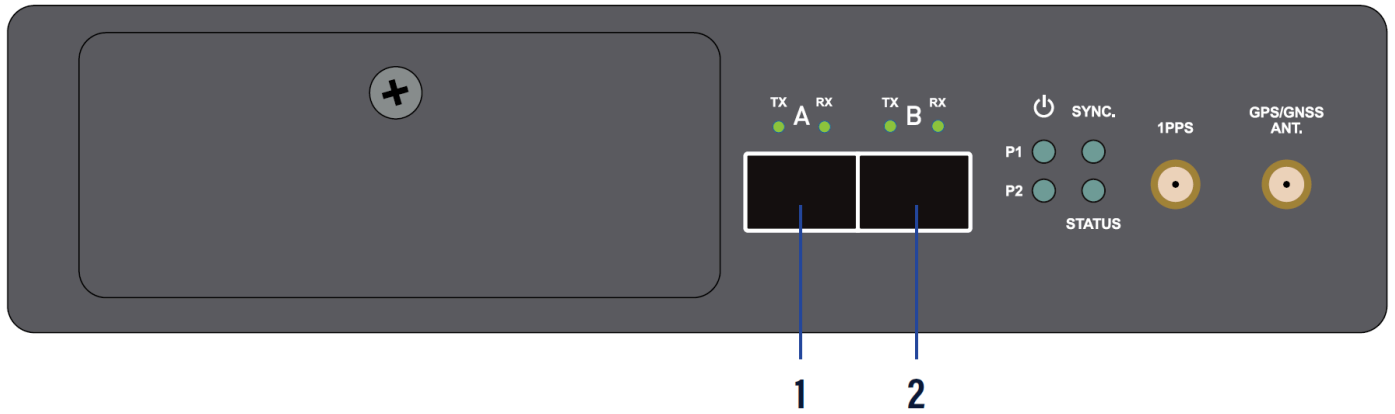
To log in, use the following initial credentials:

Default username: **admin**

Default password: **admin**

**Note:** Make sure to change the default credentials as soon as possible.

## 2.3. Capture Interfaces



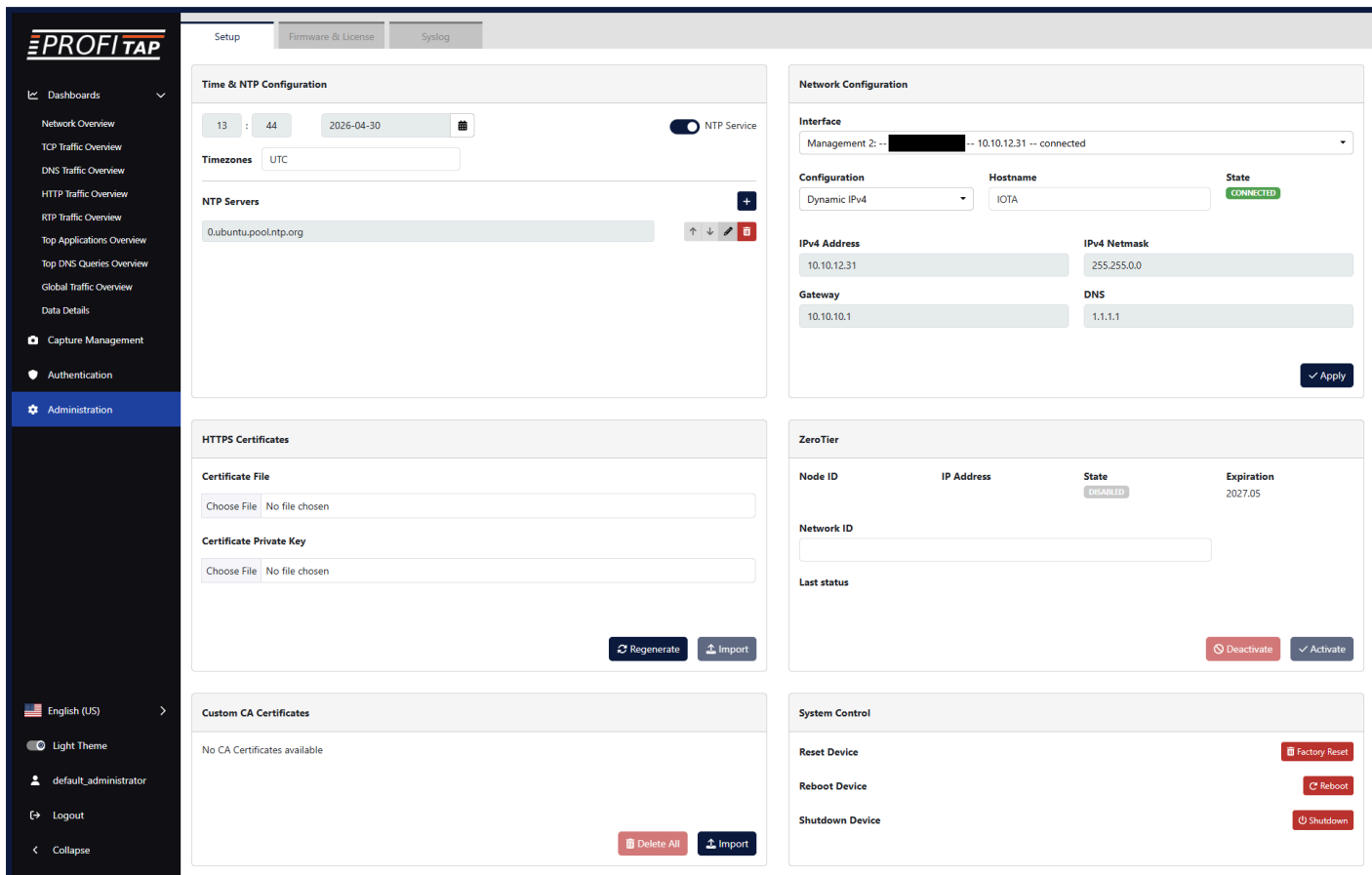
Connect cables and transceivers from the line(s) from which to capture traffic to the SFP+ capture port(s) (**1** and **2** in the image above).

For more information, see [Interfaces](#) and [Capture Interfaces](#).

# 3. IOTA Configuration

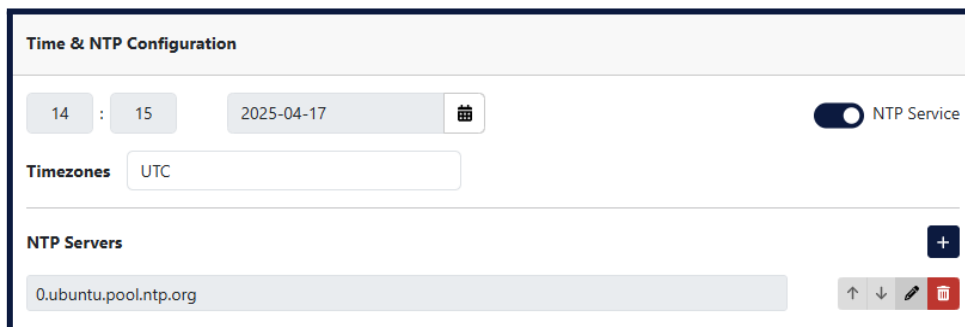
## 3.1. Administration

The **Administration** page, accessed from the main menu, allows users with administrator privileges to change system-related settings.



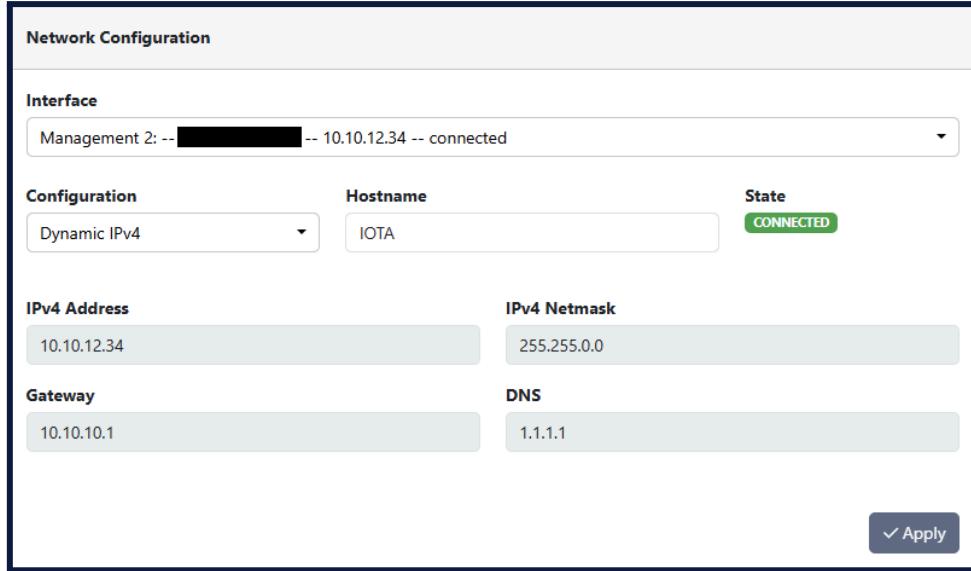
### 3.1.1. Time & NTP Configuration

The **Time & NTP Configuration** section of the **Administration > Setup** page allows the configuration of the system date, time, time zone, and NTP service. The NTP service is enabled by default, and can be disabled or enabled on this page. NTP servers can be added, modified, or removed. The appropriate time zone should be set manually, whether or not the NTP service is enabled.



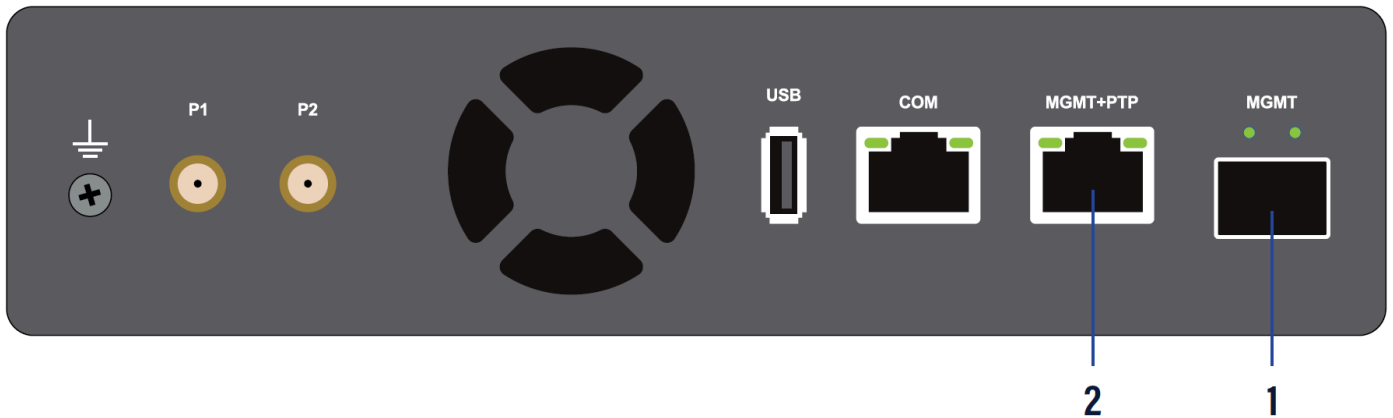
### 3.1.2. Network Configuration

The **Network Configuration** section of the **Administration > Setup** page allows the configuration of the network settings for each of the device's management interfaces. Select a network interface from the *Interface* drop-down menu to display its settings. If *Configuration* is set to *Static IPv4*, the IP address, network mask, gateway and DNS server can be set manually. If *Configuration* is set to *Dynamic IPv4*, IOTA will attempt to receive network settings from a DHCP server. The hostname can be defined in either case.



The following interfaces can be configured:

- **Management 1:** MGMT SFP+ Ethernet 10G
- **Management 2:** MGMT+PTP RJ45 Ethernet 2.5GBASE-T



### 3.1.3. HTTPS Certificate

The **HTTPS Certificate** section of the **Administration > Setup** page allows the configuration of the HTTPS certificate and key for connection to the IOTA management interface.

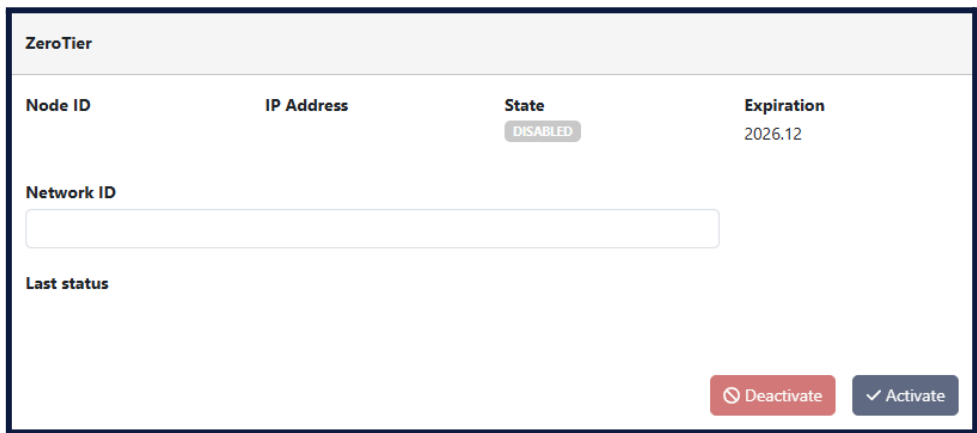


The screenshot shows a web interface titled "HTTPS Certificates". It contains two sections: "Certificate File" and "Certificate Private Key". Each section has a "Choose File" button and a text field displaying "No file chosen". At the bottom right, there are two buttons: "Regenerate" (with a circular arrow icon) and "Import" (with an upload icon).

Click the *Regenerate* button to generate a new self-signed certificate and key. Alternatively, a certificate and certificate key can be imported by clicking the *Choose File* buttons, selecting the appropriate files, and clicking the *Import* button. Note that the imported HTTPS certificate must include the EKU and SAN fields, and shouldn't be password-protected.

### 3.1.4. ZeroTier

The **ZeroTier** section of the **Administration > Setup** page allows the configuration of the ZeroTier feature.



The screenshot shows a web interface titled "ZeroTier". It features a table with the following data:

Node ID	IP Address	State	Expiration
		DISABLED	2026.12

Below the table, there is a "Network ID" input field and a "Last status" label. At the bottom right, there are two buttons: "Deactivate" (with a power-off icon) and "Activate" (with a checkmark icon).

ZeroTier provides an easy way to remotely access the device via a P2P VPN and manage virtual networks on a cloud application. Visit [www.zerotier.com](http://www.zerotier.com) for more information.

**Note:** ZeroTier is a licensed feature. The *Expiration* section shows the service expiration date of the current ZeroTier license.

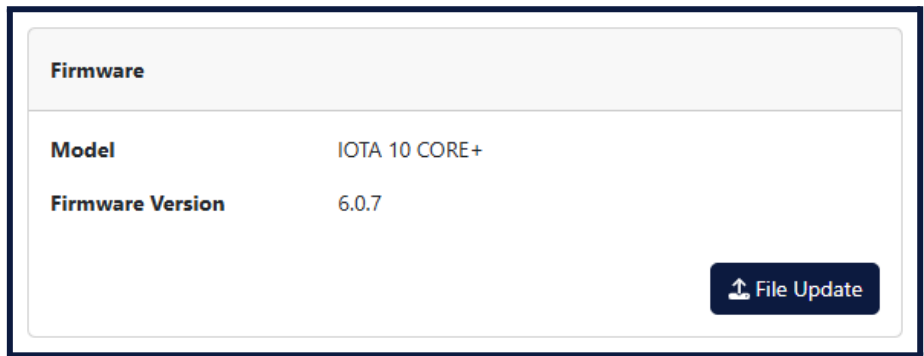
### 3.1.5. System Control

IOTA can be restarted, shut down, or reset to factory settings, via these buttons. Factory reset is only possible if no capture is currently in progress (capture can be stopped on the *Capture Management* page).



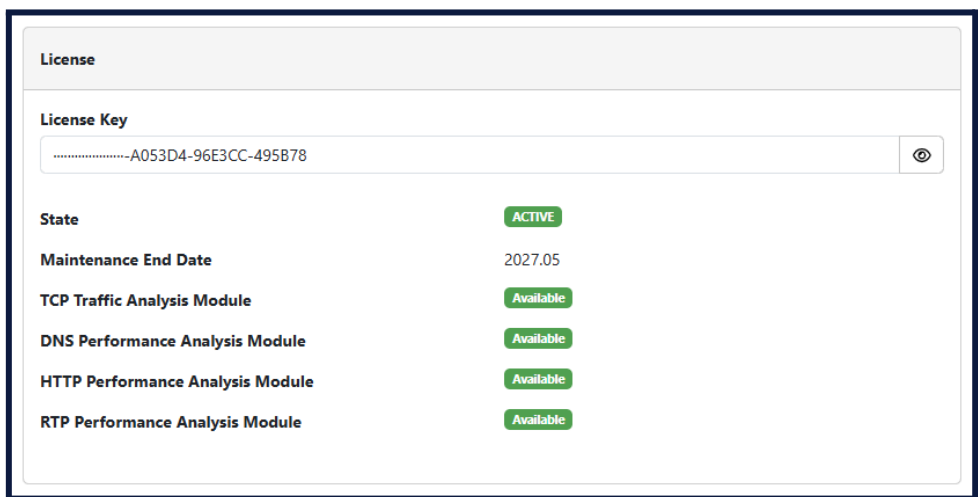
### 3.1.6. Firmware

The **Firmware** section of the **Administration > Firmware & License** page displays the currently-installed firmware version, and provides the ability to update it by uploading a new firmware file.



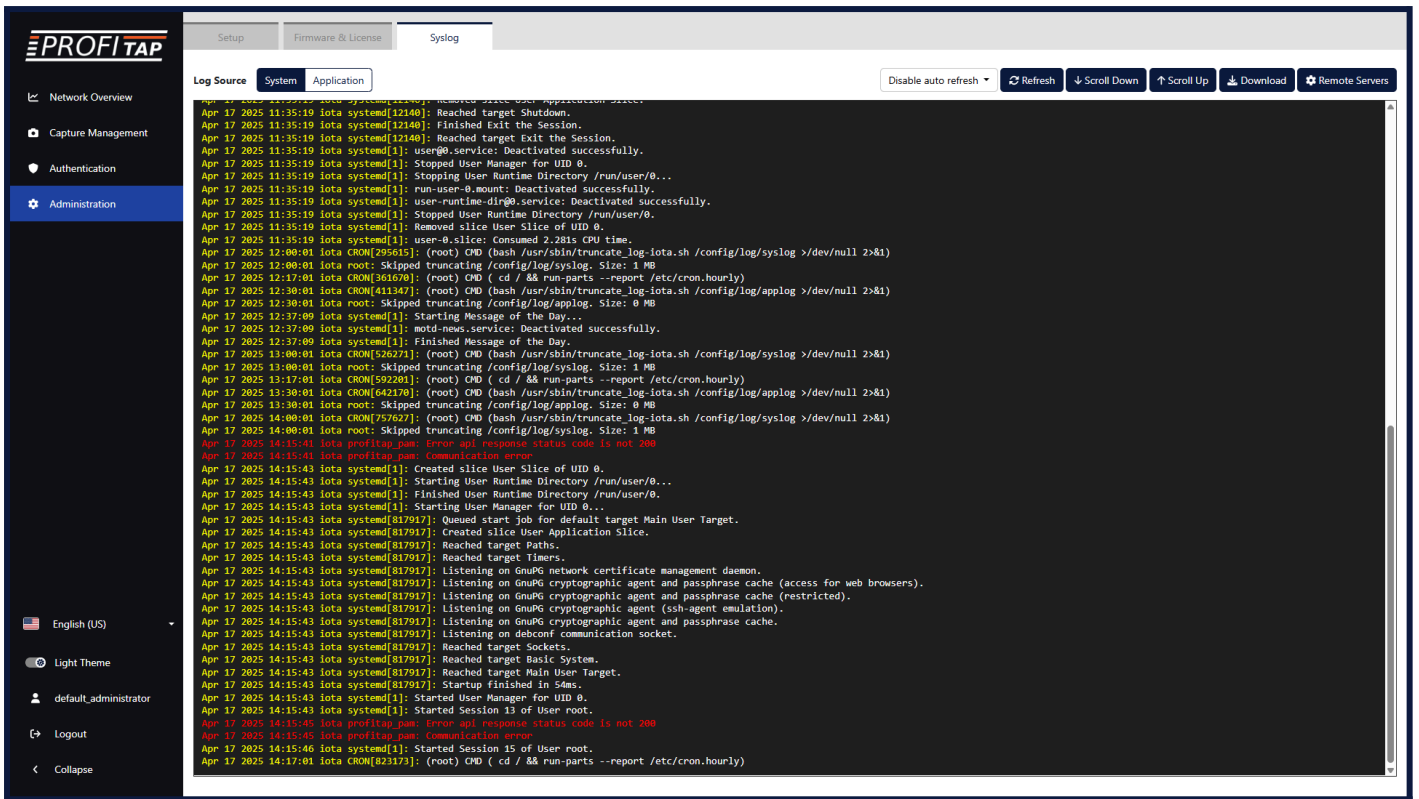
### 3.1.7. License

The **License** section of the **Administration > Firmware & License** page provides information about the current license. The license concerns the availability of advanced traffic analysis modules, and the ability of the device to install new firmware updates. *Maintenance End Date* displays the expiration date of the license. A device with an expired license can be used indefinitely with the currently-installed firmware version.

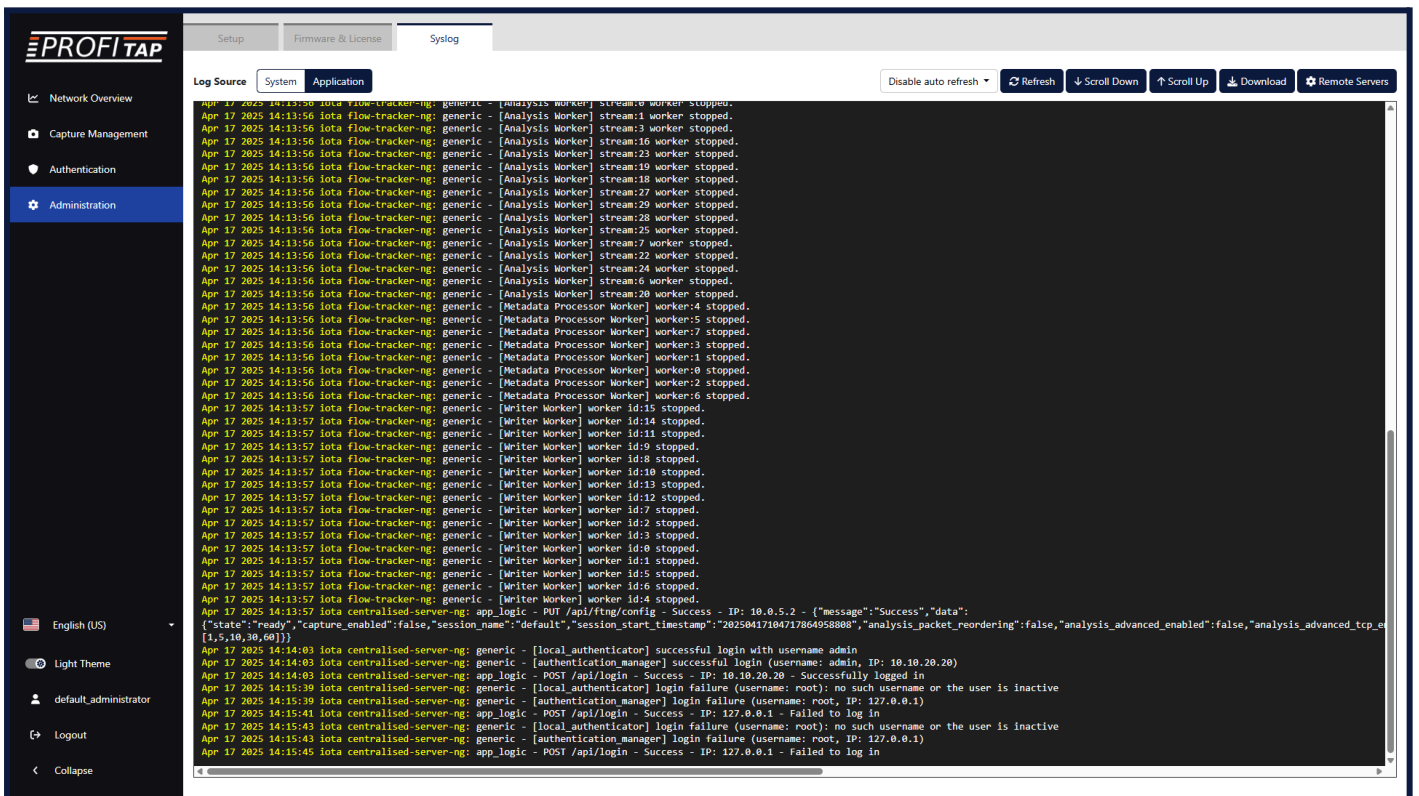


### 3.1.8. Logs

The Administration > Syslog page displays the logs of the IOTA system and application.



The displayed logs can be selected between *System* and *Application* in the top left corner of the page. *System* logs contain all of the embedded OS activity. *Application* logs contain the activity of the IOTA-specific software.





## 3.2. Authentication

The **Authentication** page can be accessed via the *Authentication* menu item by users with **Administrator** role.

### 3.2.1. Local Users

The **Local Users** tab allows administrators to add new users or edit existing users and their privilege levels. Depending on the selected role, the user has the following rights:

- **administrator**: full control, limitless administration and system update;
- **user**: create and set rules, aggregate and filter traffic, and port configuration;
- **viewer**: view only: settings, statistics, active rules.

The minimum requirements for the passwords are as follows:

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

The screenshot shows a web form titled "Add User" with a close button (X) in the top right corner. The form contains the following fields and elements:

- Name**: A text input field.
- E-mail**: A text input field.
- Username**: A text input field.
- Role**: A dropdown menu currently set to "Viewer".
- Active**: A toggle switch currently turned on.
- Password**: A text input field with a strength indicator on the right showing four red error messages:
  - × 8 characters
  - × One letter uppercase
  - × One letter lowercase
  - × One digit
- Confirm Password**: A text input field with a strength indicator on the right showing one red error message:
  - × Password match

At the bottom right of the form, there are two buttons: "Close" and "Confirm".

### 3.2.2. 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 3 seconds);
- privilege mapping (translates the 15 privilege levels from TACACS+ into those of the viewers, users and admins; can be configured).

**Edit TACACS+ Server**

Hostname:  Port:  Priority: 1  Timeout:

Login Type: Login  Secret:

**Privilege Mapping**

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Viewer Privilege Level [ 0 - 4 ]      User Privilege Level [ 5 - 10 ]      Admin Privilege Level [ 10 - 15 ]

### 3.2.3. 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 3 seconds);
- privilege mappings count (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).

#### Edit RADIUS server ✕

Hostname	Port	Priority	Timeout
<input type="text"/>	<input type="text"/>	<input type="text" value="1"/> ▾	<input type="text"/>
Fallback Role	Secret		
<input type="text" value="None"/> ▾	<input type="text" value="..."/>		

---

Privilege Mapping Count +

Name	Type	Comparison	Value	Role
------	------	------------	-------	------

✕ Cancel ✓ Confirm

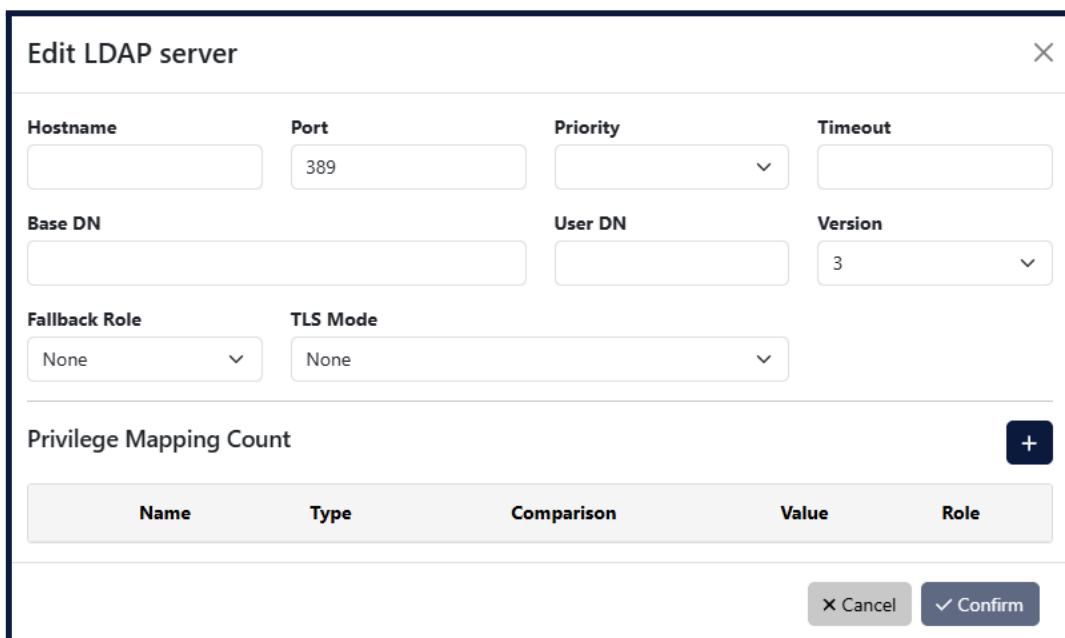
### 3.2.4. LDAP and LDAPS

The **LDAP** tab offers the possibility to configure one or more LDAP servers for user authentication. In order to set up the LDAP access, the following settings are required:

- server hostname or address;
- server port: (default 389 for LDAP and 636 for LDAPS);
- 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);
- timeout (waiting time for response from the LDAP server, can be set between 1 and 3 seconds);
- base DN (base distinguished name): this is the base DN used to query the LDAP servers for its information (example: ou=people, dc=example, dc=com);
- user DN (user distinguished name): DN parameter used to query for the usernames. (example: uid);
- LDAP version: it is possible to configure both LDAP Version 2 and Version 3 servers;
- privilege mappings count (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);
- TLS mode: the user can select whether the server requires TLS (for LDAPS), and if they wish to enforce strict TLS session validation. Note that if this option is set to "strict", the user will likely need to import a private CA certificate into IOTA (*Administration > Setup GUI page*).



**Edit LDAP server** ✕

Hostname	Port	Priority	Timeout
<input type="text"/>	389	<input type="text" value=""/>	<input type="text"/>
Base DN	User DN	Version	
<input type="text"/>	<input type="text"/>	3	<input type="text" value=""/>
Fallback Role	TLS Mode		
None	None		

Privilege Mapping Count +

Name	Type	Comparison	Value	Role
------	------	------------	-------	------

✕ Cancel ✓ Confirm

### 3.2.5. Custom Authentication Configuration

IOTA allows users to not only define multiple authentication methods, but also to configure how the different methods are used by the system. Clicking the *Configure Authentication* button on either the *Users*, *TACACS+*, *RADIUS*, or *LDAP* 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, LDAP, or TACACS+ methods, this means that no server is responding (or no server is programmed). If only one of the registered LDAP/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.



## 3.3. Device Reset

### 3.3.1. Network Configuration

The management ports' network configuration can be modified via the IOTA GUI (see [Network Configuration](#)) or the recovery CLI (see [Device Recovery CLI](#)).

### 3.3.2. Factory Reset

The device can be reset to factory settings via the *Factory Reset* button on the [Administration > Setup](#) page.

## 3.4. Device Recovery CLI

The recovery command-line interface (CLI) can be used to modify the network settings of the management interfaces, and to reboot the device.

### 3.4.1. Accessing the CLI

The recovery CLI can be accessed by users with **administrator** privileges (both local users and AAA, see [Authentication](#)) either via SSH through the MGMT and MGMT+PTP ports, or via the COM port (serial RS323).

To connect to the device via SSH, perform the following command (where **USERNAME** is the username and **IOTA\_IP** is the IP address of the device), and submit the password when prompted:

```
ssh USERNAME@IOTA_IP
```

For example:

```
→ ~ ssh recovery@10.10.12.98  
recovery@10.10.12.98's password: 
```

The other way of accessing the CLI is via the COM port. To connect to the serial management interface, use the supplied cable and adapters, and any terminal software, with the following connection settings: 115200 baud rate, 8 bit, no parity, 1 bit stop. Log in using the credentials of a user account with administrator privileges in the appearing shell.

The first method will work if the IOTA device has correctly configured network settings. The second method will always work.

### 3.4.2. Using the CLI

Once logged in with the appropriate credentials, the CLI prompt appears.

Useful commands to navigate the console:

- `ls` or `help` to list available commands (or by hitting TAB from keyboards)
- `.` returns to the initial branch
- `..` returns to the previous branch

```
.> help  
  
Possible commands:  
  netconfig      manage network configuration.  
  reboot        reboot the device.
```

The `netconfig` command branch is used to configure the network settings of the device's management interfaces. In the `netconfig` command branch, the `show` and `update` commands are available.

```

.> netconfig
.netconfig.> help
Possible commands:
  show
      show current network configuration.

  --interface
      number of the network interface to show. (when unspecified, shows all interfaces)

  update
      update the network configuration.

  --dhcp_enabled
      true/yes/y to enable and false/no/n to disable.

  --gateway
  --hostname
  --interface
      number of the network interface to update. (default: 0)

  --ip
  --nameserver
  --netmask

```

The `show` command (or `.netconfig.show`) displays the current configuration of all of the device's management interfaces.

The `update` command (or `.netconfig.update`) is used to update the configuration of any of the interfaces. The accepted arguments for the `update` command can be displayed with the `help` command (or `.netconfig.update.help`). For instance, in order to configure the management interface with ID 3 to have a static IP, netmask and gateway, the following command can be executed:

```

.netconfig.> update --interface 3 --dhcp_enabled no --ip 2.2.2.2 --netmask 255.255.255.0 --gateway 3.3.3.3
Successfully updated the network configuration.
STATE: disconnected
DHCP: disabled
MAC: 7c:c2:55:25:1d:f5
IP: 2.2.2.2
HOSTNAME: [null]
GATEWAY: 3.3.3.3
NETMASK: 255.255.255.0
NAMESERVER: [null]

```

The following interfaces can be configured:

- **Management 1:** MGMT SFP+ Ethernet 10G
- **Management 2:** MGMT+PTP RJ45 Ethernet 2.5GBASE-T

The `reboot` command (or `.reboot`) reboots the device immediately after confirmation:

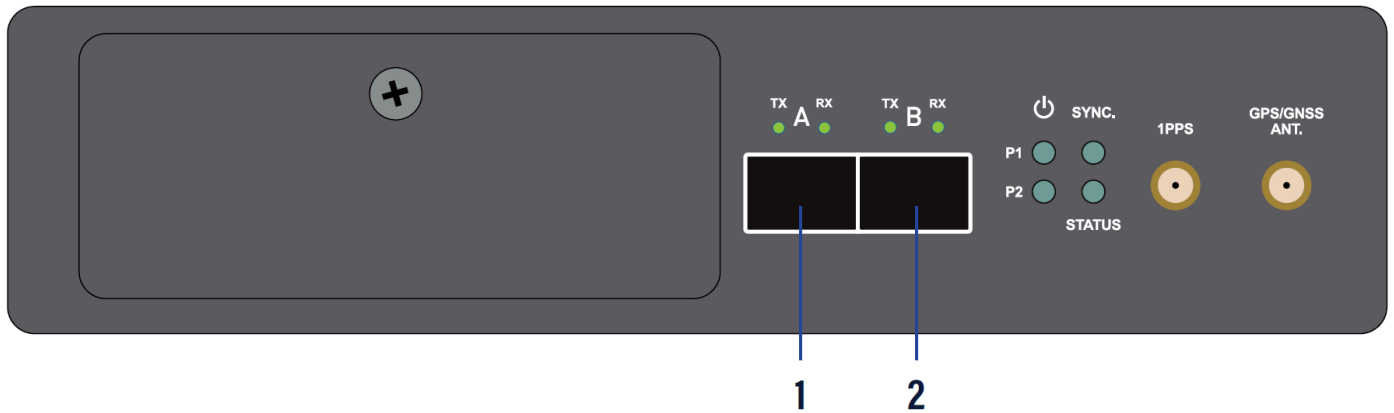
```

.> reboot
Are you sure you want to reboot the device? (yes/no)

```

# 4. Capture Management

## 4.1. Capture Interfaces



IOTA 10 CORE+ features two 10G SFP+ capture interfaces (1 and 2 in the image above), and can capture 10G traffic from both of these interfaces at the same time, either in in-line mode or out-of-band.

The screenshot shows the PROFITAP web interface. On the left is a dark sidebar with a menu including 'Dashboards', 'Network Overview', 'TCP Traffic Overview', 'DNS Traffic Overview', 'HTTP Traffic Overview', 'RTP Traffic Overview', 'Top Applications Overview', 'Top DNS Queries Overview', 'Global Traffic Overview', 'Data Details', 'Capture Management' (highlighted), 'Authentication', and 'Administration'. The main content area is divided into several sections. At the top, there are three summary cards: 'Capture Interfaces' (Port A: Down, Port B: Down, RX: 0 bps), 'Traffic Analysis' (State: Ready, Analyzed Packets: 0), and 'Data Storage' (Packet Capture: 0 B/s, Total Storage Usage: 0%). Below these is a 'Port Statistics' table. The table has columns for 'Ports', 'Port A', 'Port B', and 'Total'. The rows include Status (Link Down), Bandwidth (0 bps), Packet Rate (0 pps), Good Frames (0), Good Octets (0), Bad Frames (0), Discarded Frames (0), Dropped Frames (0), and Dropped Octets (0). A 'Reset Statistics' button is at the bottom right of the table. Below the table are two configuration sections: 'Capture Interface Configuration' (Capture Mode: Span) and 'Timestamp Synchronization' (Current Source: PTP, Last Sync Time: 2026-04-29 16:31:19, Capture Time Source: GPS Time, Synchronization Sources: 1. PTP, 2. GPS, 3. External PPS, PTP State: Locked, GrandMaster ID: d0a4b1.ffe.00104d, Last Offset: -54ns, GPS State: Locked, Fix Quality: DGPS, Fix Satellites: 20, Last Sync Time: 2026-04-29 16:31:20, External PPS State: Unlocked). An 'Apply' button is at the bottom of the configuration sections.

The **Capture Interfaces** tab displays the state and statistics of the capture interfaces.

The **Capture Interface Configuration** section allows you to change the mode of the capture interfaces between in-line and out-of-band (SPAN).

- In **in-line** mode, traffic is transmitted between both capture ports: devices connected through ports A and B can communicate, and traffic will be captured in both directions.
- In **SPAN** mode, the connection between ports A and B is severed: traffic is only received (and captured), on either or both ports.

The **Timestamp Synchronization** section provides information and controls for timestamping.

- **Current Source:** Time source currently used for timestamp synchronization.
- **Last Sync Time:** Snapshot of the timestamping time (UTC).
- **Capture Time Source:** Time source used to initialize the capture time. If *System Time* is selected, the settings on the *Administration > Setup* page will be used, unless the device is receiving time information on the PTP port, in which case PTP will supercede other time sources. If *GPS Time* is selected, the system will wait for a lock before starting the capture.
- **Synchronization Source:** Priority system to select the order in which the device will check the time sources to use for the timestamp clock synchronization (clock disciplining). Each source can be enabled or disabled. When disabled, the source will be ignored for clock synchronization.

The right side of the *Timestamp Synchronization* section displays the current state of the different time synchronization sources. These are updated independently from the priority configuration and provide an overview about their state.

**Note:** For the best results, the GPS antenna should be set up outside, or near a window. Other factors can affect results, such as weather, cloudiness, and geographical location in regards to satellite availability.

## 4.2. Traffic Analysis

The screenshot displays the PROFITAP Traffic Analysis dashboard. On the left is a sidebar with navigation options: Dashboards, Network Overview, TCP Traffic Overview, DNS Traffic Overview, HTTP Traffic Overview, RTP Traffic Overview, Top Applications Overview, Top DNS Queries Overview, Global Traffic Overview, Data Details, Capture Management (highlighted), Authentication, and Administration. The main content area is divided into several sections:

- Capture Interfaces:** Port 1: 100G (RX: 1.02 Gbps), Port 2: Down (RX: 0 bps).
- Traffic Analysis:** State: Active, Analyzed Packets: 19,28.
- Data Storage:** Packet Capture: 0 B/s, Total Storage Usage: 69.65%.
- Analysis Session:** State: Active (with Stop button), Session Name: default, Session Identifier: 2026040211203122648606. Statistics: Received Packets: 19,204,984,690, Pending Packets: 0, Ignored Packets: 403,293, Detected Flows: 219,358,359, Pending Flows: 32,677. (with Reset Statistics button).
- Traffic Analysis Settings:** Flows Time Sampling Period: 1 Second, TCP Performance Analysis (off), VLAN/MPLS Correlation (off), Packet Re-ordering (off), RTP Performance Analysis (off), DNS Performance Analysis (off), HTTP Performance Analysis (on).
- Hostnames:** Filter hostnames... + Add. Table with columns Hostname and IP Address: google.com (8.8.8.8), test.com (10.0.0.45).
- Host Groups:** Filter groups... + Add. Table with columns Group and IP Addresses: eg (8.8.8.8).
- Custom Applications:** Filter applications... + Add. Table with columns Application, Server Address, Protocol, Port: da (111.11.11.11, TCP, 0).

The **Traffic Analysis** tab provides controls for the capture and analysis of traffic.

The **Analysis Session** section displays the capture state and statistics, and allows you to start and stop the capture via the *Start Capture/Stop Capture* button. The *Session Name* field allows you to change the name of the capture session. When a capture is in progress, the *Session Identifier* displays an identifier for the current capture session, based on the start time of the capture.

The use of capture sessions will allow to join traffic incoming from different sources in a single metadata domain, enabling the use of the device at the core of your visibility infrastructure. Metadata on certain analysis dashboards will be able to be filtered based on capture session name and capture session start time.

The **Traffic Analysis Settings** section allows you to configure the following traffic analysis options:

- **Flows Time Sampling Period:** Sampling period used to create traffic metadata entries in the device storage. Lower values allow more detailed traffic analysis but it will increase storage usage.
- **VLAN/MPLS Correlation:** If enabled, VLAN tags and MPLS labels will be used to identify traffic flows. If disabled, they will be ignored.
- **Packet Re-ordering:** Enabling TCP packets reordering will improve application detection but it may impact traffic timing and metrics evaluation.
- **TCP Performance Analysis:** When enabled, the analysis engine will generate TCP performance metrics. This may impact analysis performance.
- **DNS Performance Analysis:** When enabled, the analysis engine will generate DNS performance metrics. This may impact analysis performance.
- **HTTP Performance Analysis:** When enabled, the analysis engine will generate HTTP performance metrics. This may impact analysis performance.
- **RTP Performance Analysis:** When enabled, the analysis engine will generate RTP performance metrics. This may impact analysis performance.

The **Hostnames**, **Host Groups** and **Custom Applications** sections allow you to define custom resolutions to be displayed in the analysis dashboards.

- **Hostnames:** Resolves singular IP addresses to a hostname.
- **Host Groups:** Tags any IP address within a subnet with the specified group name.
- **Custom Applications:** Tags flows matching a destination IP, protocol and port number with the specified application name.

**Note:** Hostnames and Host Groups are resolved at query time (i.e. when using the analysis dashboards), while Custom Applications are resolved at analysis time (i.e. when the traffic is first analyzed).

## 4.3. Data Storage

The screenshot displays the PROFITAP Storage Management interface. On the left is a navigation sidebar with options like Dashboards, Network Overview, and Capture Management. The main content area is titled 'Storage Management' and includes a 'Storage Overview' section with a storage allocation slider and cleanup controls. Below that is the 'Packet Capture Filtering' section, which contains 'Packet Capture Statistics' and 'Packet Capture Filters'.

The **Data Storage** tab provides controls for the filtering and storage of captured traffic.

### 4.3.1. Storage Management

The **Storage Management** section allows you to define the allocation of storage for *Metadata* (extracted from observed traffic and used in the analysis dashboards) and *Packet Capture* (raw captured data), and to control the cleanup of stored data.

Click and drag the slider to change the storage allocation. The used and total allocated storage for metadata and for packet capture are displayed below the slider, on the left and right respectively. Further below, a time estimation of the available storage when capturing is displayed when available.

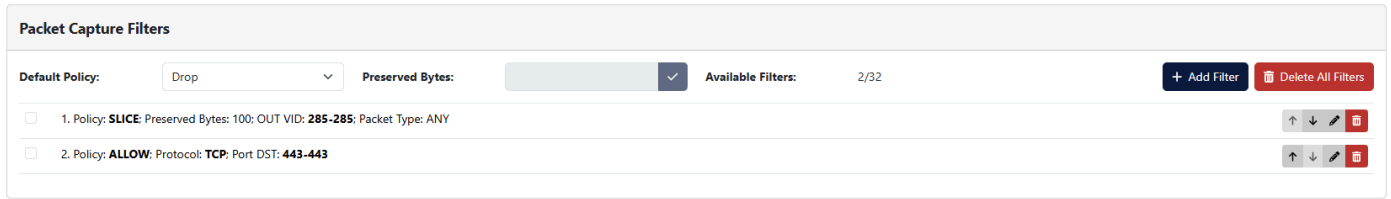
The cleanup of previously captured data is done by defining a start time and end time for the data to delete, then clicking the *Delete Metadata* button to remove metadata extracted from captured traffic, the *Delete Packet Capture* button to remove raw captured data, or the *Delete All Data* button to remove both.

### 4.3.2. Packet Capture Statistics

The **Packet Capture Statistics** section provides statistics about the packet capture, with *Stored Packets* referring to packets allowed to be captured by the defined filters, *Removed Packets* to packets filtered out, and *Dropped Packets* packets dropped by the capture interfaces. The *Reset Statistics* button resets these statistics.

### 4.3.3. Packet Capture Filters

The **Packet Capture Filters** section allows you to define filters for traffic capture. This only affects the capture of raw data and has no effect on the metadata used for the analysis dashboards.

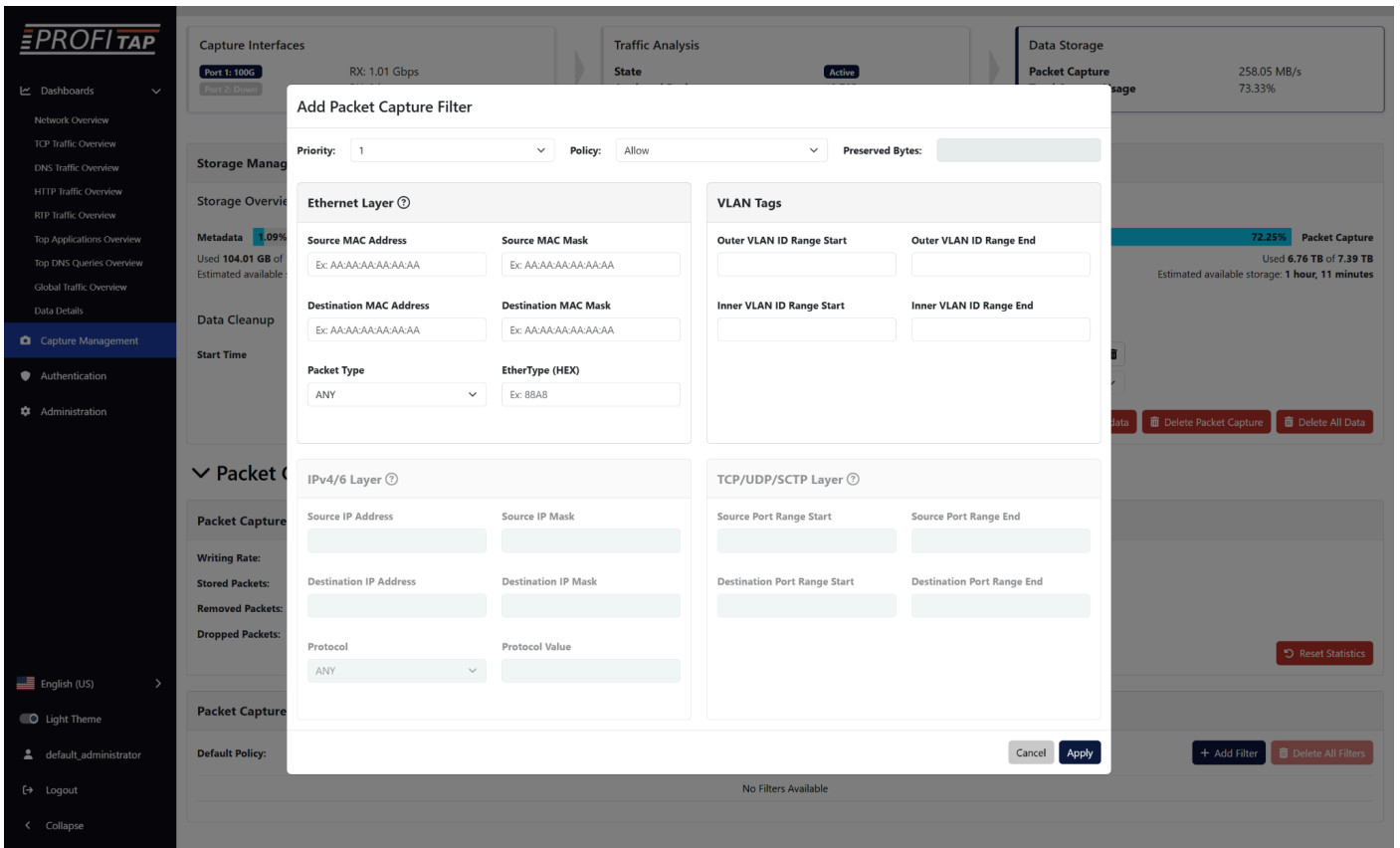


The *Default Policy* can be set to **Allow**, **Drop**, or **Slice**:

- **Allow** will capture all traffic by default, in which case **Drop** filters can be used to filter out specific traffic.
- **Drop** will not capture any traffic by default, in which case **Allow** filters should be defined to capture specific traffic.
- **Slice** will capture packets truncated to the size specified in the **Preserved Bytes** field.

Each filter has its own policy, and can be set as an **Allow**, **Drop**, or **Slice** filter, to capture, filter out, or packet slice traffic matching that filter.

Filter priority can be defined on the filter window, or by clicking the up and down arrows in the list of filters, with a lower number corresponding to a higher priority. This can be used to create exception cases within drop or allow filters.



The possible filtering options are as follows:

- **Ethernet Layer**

Only frames matching MAC details configured in this section will be targeted (Source/Destination MAC Address, Source/Destination MAC Mask), with the possibility to select the **Packet Type** (ARP, IPv4, IPv6, TCP (IPv4/6), UDP (IPv4/6), SCTP (IPv4/6), Custom Protocol (IPv4/6), or any).

- **IPv4/IPv6 Layer**

When IPv4/IPv6 is selected, the system will filter for any packet of those types. In order to filter for the IPv4/IPv6 details, the user needs to fill in the related fields (Source/Destination IP Address, Source/Destination IP Mask). The **Protocol** setting is only configurable for IPv4/IPv6, allowing the user to restrict the traffic to a specific type of L4 header (TCP, UDP, SCTP, ICMP, IGMP). *Any* allows entering a custom protocol value or setting no filter for L3 headers.

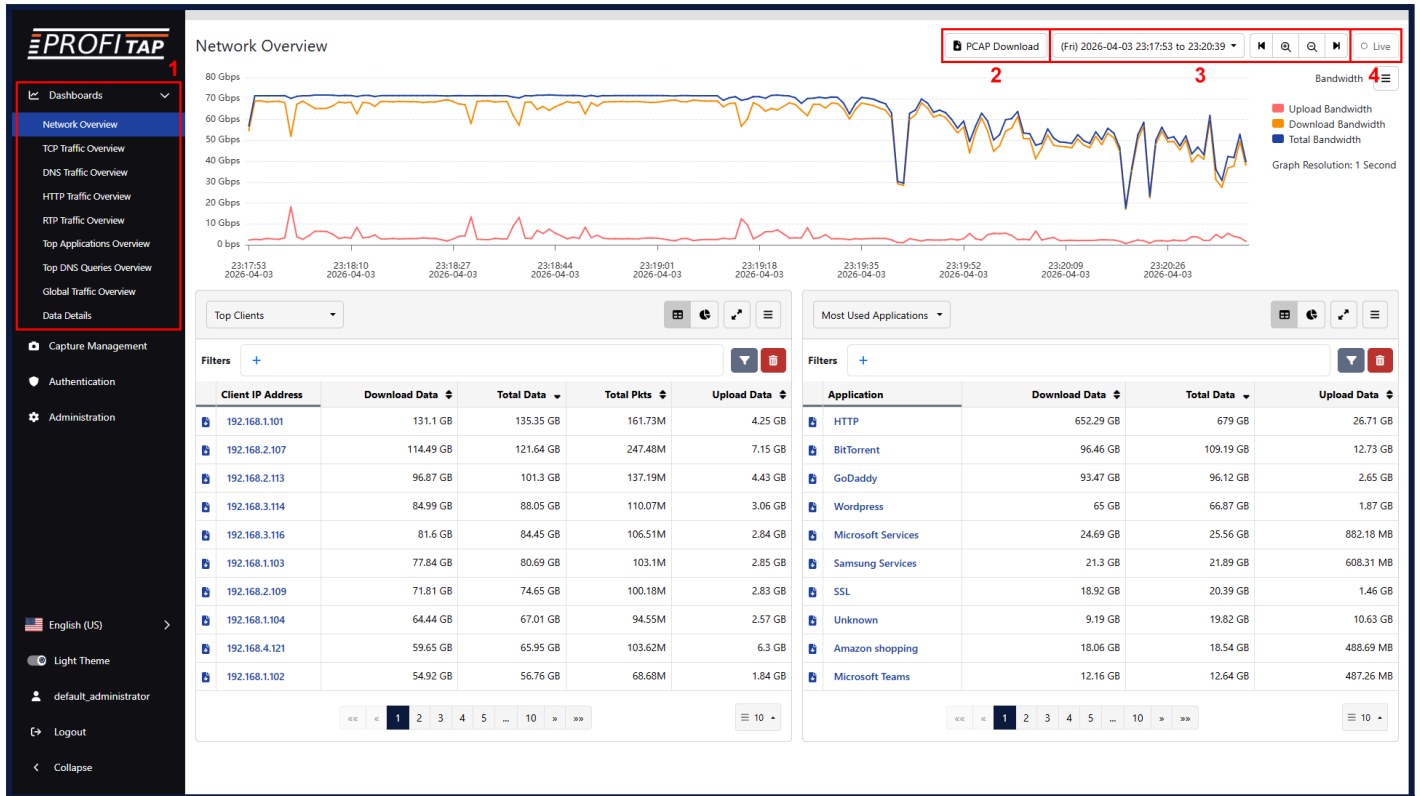
- **TCP/UDP/SCTP Layer**

When TCP/UDP/SCTP is selected in **Packet Type** or **Protocol**, a range of source and destination ports can be defined in this section.

- **VLAN Tags**

Can be used for filtering on outer/inner VLAN by defining a range of inner and outer VLAN IDs. Both ranges cannot overlap.

## 5. Analysis Dashboards

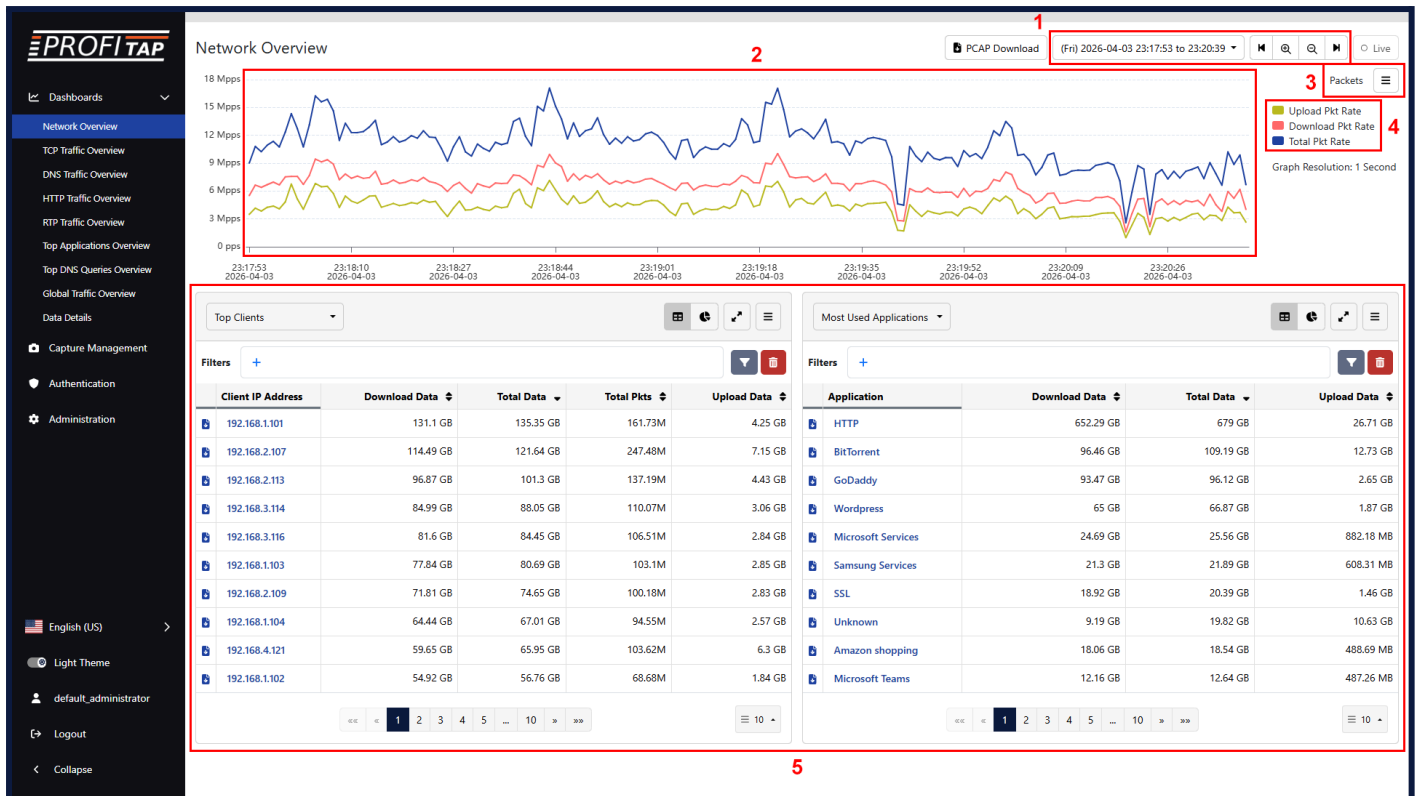


Network Overview dashboard - Bandwidth view

IOTA's analysis dashboards allow you to explore metadata extracted from captured traffic.

- [1] The main menu allows you to navigate between the different dashboards.
- [2] The *PCAP Download* button allows you to download the raw data for the selected time range and filters in PCAPNG file format.
- [3] The time range can be selected in the top-right corner of the screen.
- [4] The *Live* button allows you to enable or disable the automatic refreshing of the dashboard with new captured data.

## 5.1. Network Overview



Network Overview dashboard - Packets view

The **Network Overview** dashboard displays a time graph giving an overview of bandwidth usage and number of packets over time for the selected time range.

[1] You can select the time range in the top-right corner of the screen.

[2] You can also click and drag on the time graph itself to create a selection for a specific time range. You can click and drag this selection to move it along the time graph, and click and drag the edges of this selection to adjust its start and end time. The contents of the sections below are automatically updated based on this selection. Right-click the selection to open its context menu, allowing you to zoom in on it, reset the zoom, or clear the selection.

[3] The time graph can be changed between *Capture Bandwidth*, *Capture Packets*, *Analysis Bandwidth*, and *Analysis Packets* in the top-right corner of the screen, below the time range controls.

[4] Click the rectangle next to each metric name to show or hide the corresponding line on the time graph.

[5] The sections below the time graph display metadata for the top entries in the selected time range for the selected categories.

	Download Data	Total Data	Total Pkts	Upload Data
Most Used Applications	131.1 GB	135.35 GB	161.73M	4.25 GB
Top Server Countries	114.49 GB	121.64 GB	247.48M	7.15 GB
Top VLANs	96.87 GB	101.3 GB	137.19M	4.43 GB
Top HTTP Servers	84.99 GB	88.05 GB	110.07M	3.06 GB
Top HTTP Endpoints	84.99 GB	88.05 GB	110.07M	3.06 GB
Top HTTP User Agents	84.99 GB	88.05 GB	110.07M	3.06 GB
Top RTP Clients	81.6 GB	84.45 GB	106.51M	2.84 GB
Top RTP Servers	77.84 GB	80.69 GB	103.1M	2.85 GB
Top IP Connections	71.81 GB	74.65 GB	100.18M	2.83 GB

[6] The categories can be changed using the drop-down menu in the top-left corner of each section.

Client IP Address	Download Data	Total Data	Total Pkts	Upload Data
192.168.1.101	131.1 GB	135.35 GB	161.73M	4.25 GB
192.168.2.107	114.49 GB	121.64 GB	247.48M	7.15 GB
192.168.2.113	96.87 GB	101.3 GB	137.19M	4.43 GB
192.168.3.114	84.99 GB	88.05 GB	110.07M	3.06 GB
192.168.3.116	81.6 GB	84.45 GB	106.51M	2.84 GB
192.168.1.103	77.84 GB	80.69 GB	103.1M	2.85 GB
192.168.2.109	71.81 GB	74.65 GB	100.18M	2.83 GB
192.168.1.104	64.44 GB	67.01 GB	94.55M	2.57 GB
192.168.4.121	59.65 GB	65.95 GB	103.62M	6.3 GB
192.168.1.102	54.92 GB	56.76 GB	68.68M	1.84 GB

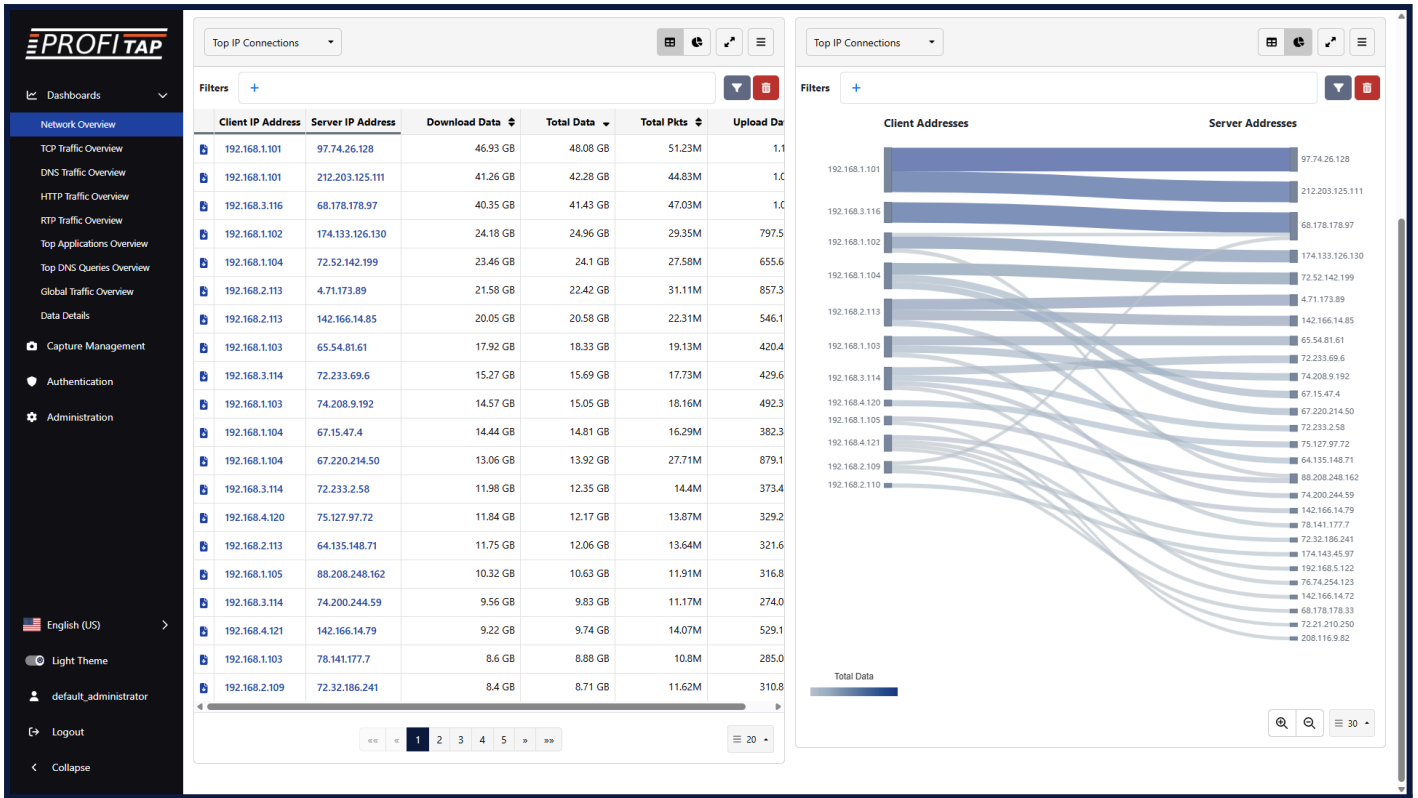
[7] In the top-right corner of each section, the view can be changed between table view and diagram view using the two leftmost buttons. The *Expand/Collapse* button toggles the width of the section between half-width and full-width. The rightmost button open a menu for selecting the metrics to display. In the table view, this menu allows you to show or hide specific metrics columns. The entries in the table can be sorted using the metrics columns that are displayed. In the diagram view, this menu allows you select which metric diagram to display.

[8] Display filters can be defined here. After defining filters, press the *Apply Filter* button to update the view. Press the *Reset* button to reset the display filters.

[9] In both the table view and diagram view, clicking a value and selecting *View Details* will navigate to the *Details* page with a pre-filled filter for this value (see **Data Details** below). In the table view, clicking a value also allows you to add it to the display filters as an *include* or *exclude* filter. A *Download traffic PCAP* button is present next to each table entry. Clicking this button downloads the traffic relevant to this entry in PCAPNG format.

[10] The navigation at the bottom of a table allows you navigate between pages.

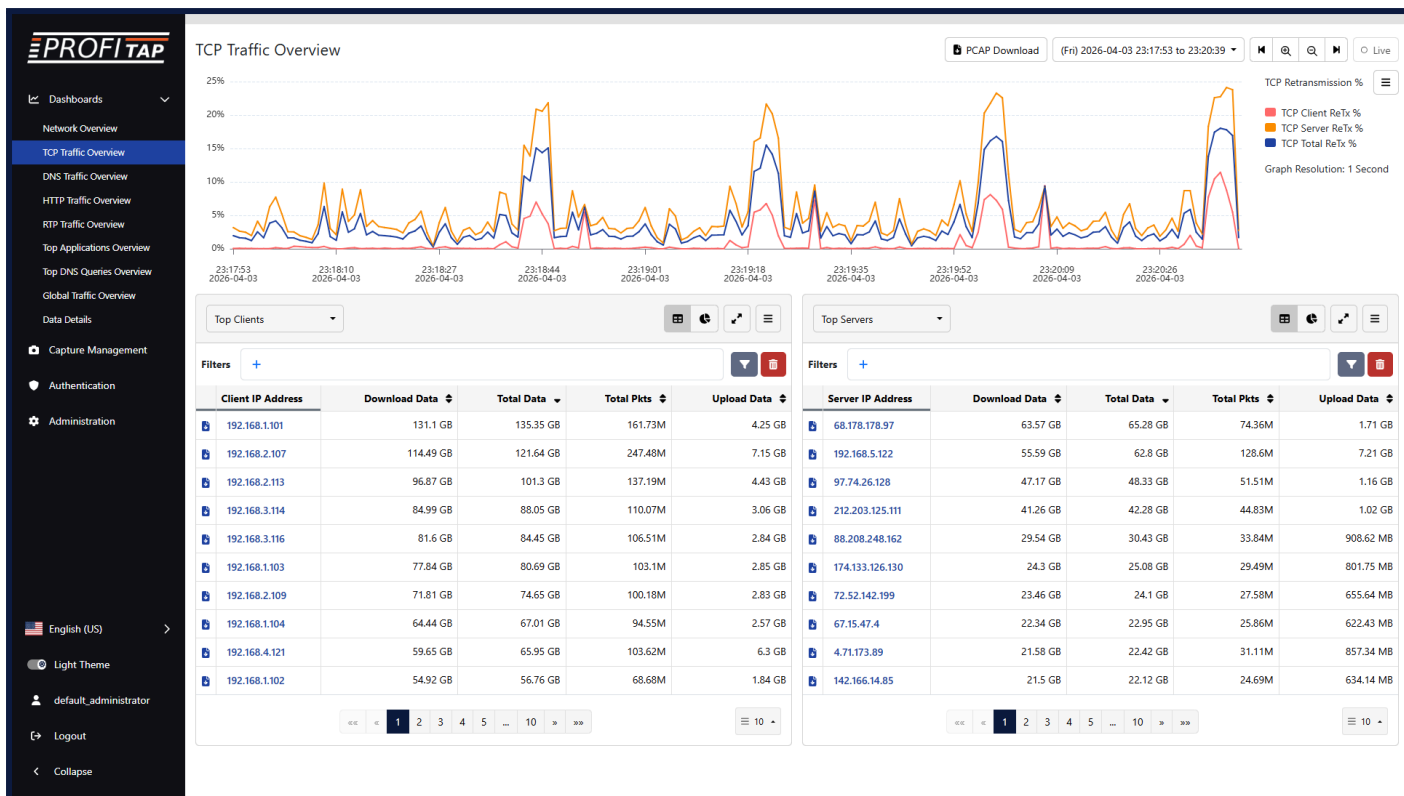
[11] The number of entries displayed on each page of the table can be selected in the bottom-right corner.



Network Overview dashboard - Top IP Connections

In the example above, we are displaying the top client-server IP connections in both sections. The left section is set to a table view, with entries sorted by *Total Data*. The right section is set to a diagram view, with *Total Data* selected as the metric to display. The type of diagram will depend on the selected metric; in this case, a Sankey diagram.

## 5.2. TCP Traffic Overview



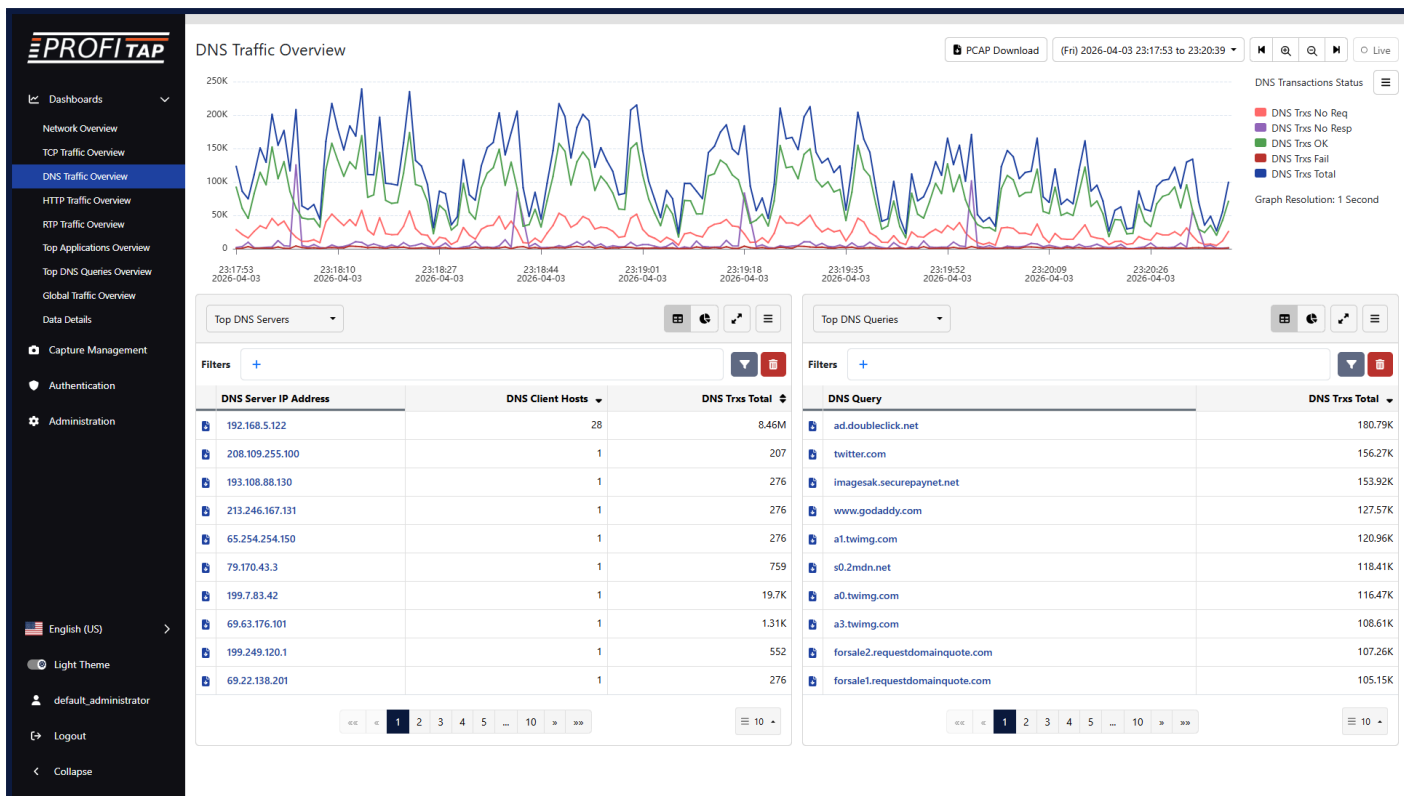
TCP Traffic Overview dashboard

The **TCP Traffic Overview** dashboard displays a time graph giving an overview of measured TCP iRTT, latency, retransmissions, and out-of-order packets over time for the selected time range.

The time graph can be changed between *TCP iRTT*, *TCP Latency*, *TCP Retransmission Packets*, *TCP Retransmissions %*, *TCP Out of Order Packets*, and *TCP Out of Order %* in the top-right corner of the screen, below the time range controls.

Other controls are the same as the **Network Overview** dashboard.

## 5.3. DNS Traffic Overview



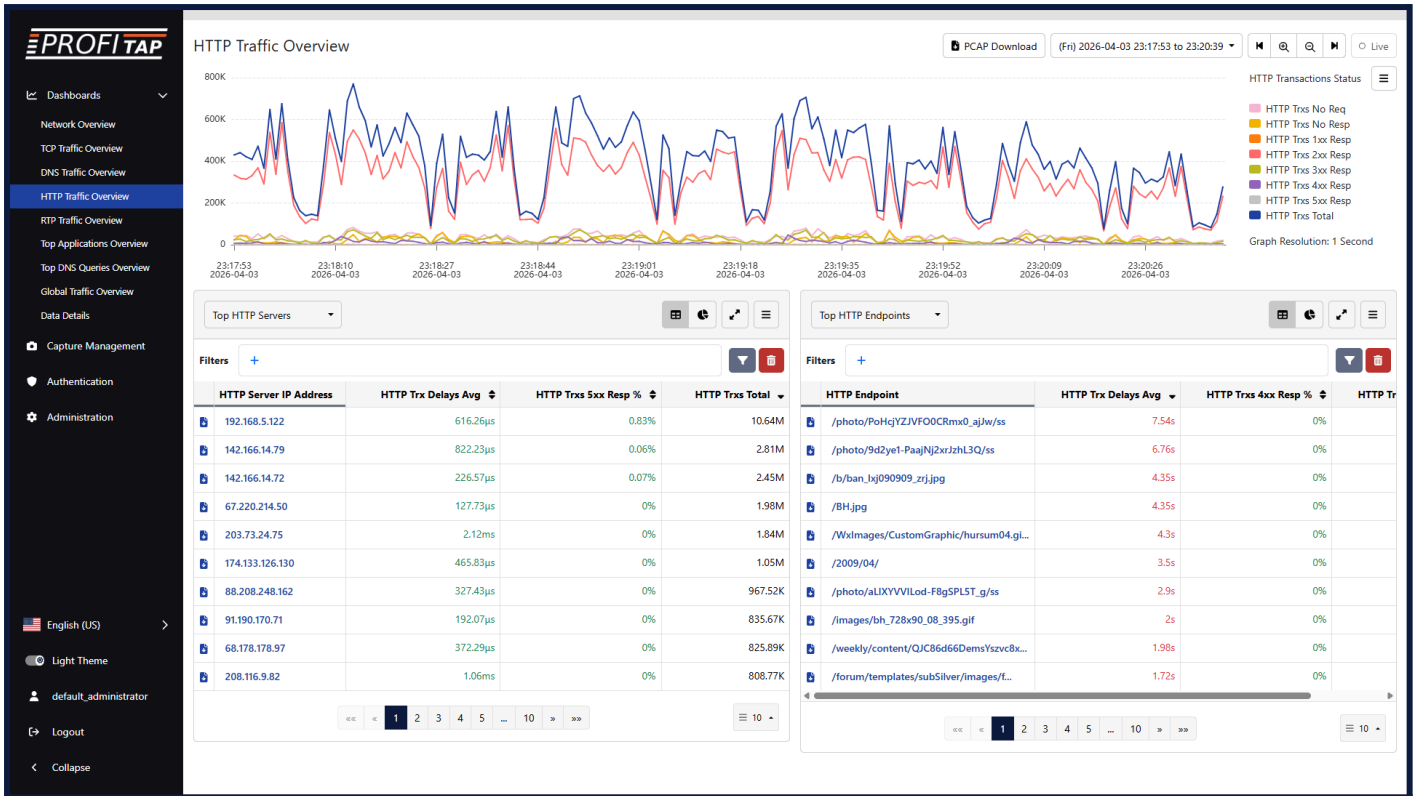
DNS Traffic Overview dashboard

The **DNS Traffic Overview** dashboard displays a time graph giving an overview of DNS functionality and performance over time for the selected time range.

The time graph can be changed between *Transactions Delays*, *Transactions Status*, *Transactions Status %*, *Transactions Performance Success*, *Transactions Performance Success %*, *Transactions Performance Failed*, *Transactions Performance Failed %*, *Transactions Performance Total*, and *Transactions Performance Total %* in the top-right corner of the screen, below the time range controls.

Other controls are the same as the **Network Overview** dashboard.

## 5.4. HTTP Traffic Overview



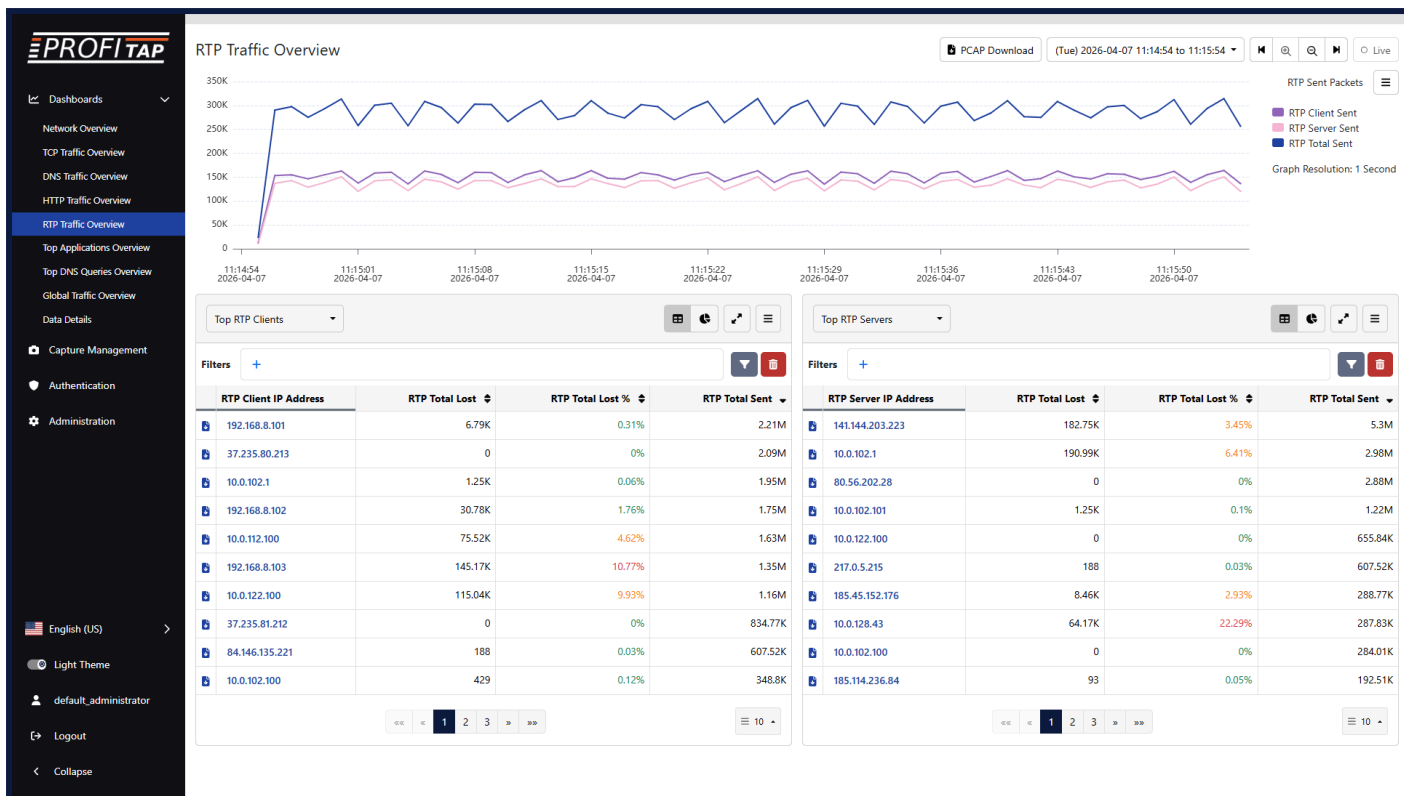
HTTP Traffic Overview dashboard

The **HTTP Traffic Overview** dashboard displays a time graph giving an overview of HTTP functionality and performance over time for the selected time range.

The time graph can be changed between *Transactions Delays*, *Transactions Status*, *Transactions Status %*, *Transactions Performance Success*, *Transactions Performance Success %*, *Transactions Performance Failed*, *Transactions Performance Failed %*, *Transactions Performance Total*, and *Transactions Performance Total %* in the top-right corner of the screen, below the time range controls.

Other controls are the same as the **Network Overview** dashboard.

## 5.5. RTP Traffic Overview



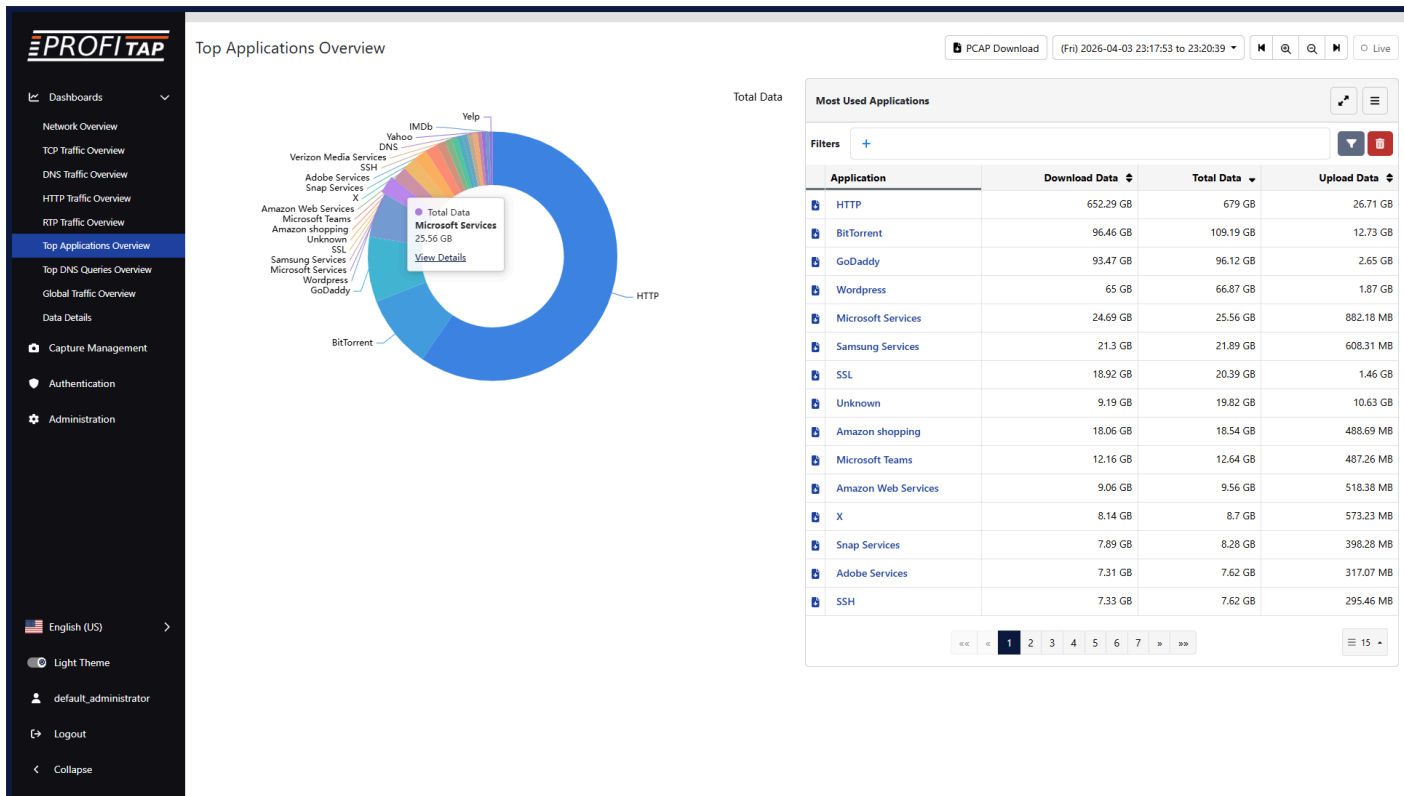
RTP Traffic Overview dashboard

The **RTP Traffic Overview** dashboard displays a time graph giving an overview of RTP functionality and performance over time for the selected time range.

The time graph can be changed between *Sent Packets*, *Lost Packets*, *Lost Packets %*, *Overhead Packets*, *Overhead Packets %*, *Out of Order Packets*, *Out of Order Packets %*, *Duplicate Packets*, *Duplicate Packets %*, *Jitter*, and *MOS Estimation* in the top-right corner of the screen, below the time range controls.

Other controls are the same as the **Network Overview** dashboard.

## 5.6. Top Applications Overview, Top DNS Queries Overview



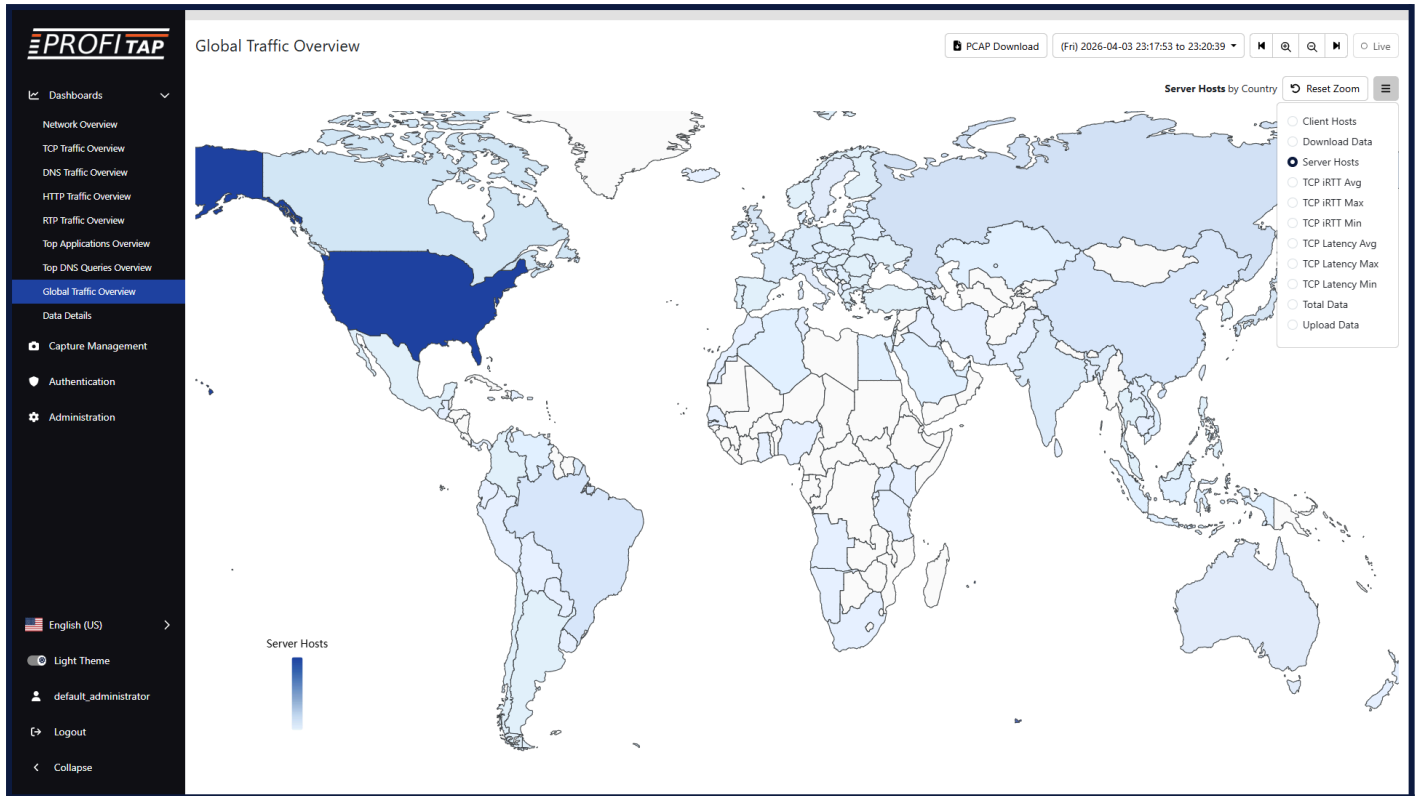
*Top Applications Overview dashboard*

The **Top Applications Overview** and **Top DNS Queries Overview** dashboards display a chart and a table giving an overview of the top applications and DNS queries respectively for the selected time range.

The controls are similar to the **Network Overview** dashboard.

The menu in the top-right corner of the table allows you to show or hide specific metrics columns. The entries in the table can be sorted using the metrics columns that are displayed. Sorting by a metric will also update the chart accordingly. The type of chart displayed will depend on the selected metric.

## 5.7. Global Traffic Overview



*Global Traffic Overview dashboard*

The **Global Traffic Overview** dashboard displays a world map providing an overview of traffic based on country, with each country colored depending on the selected metric, for the selected time range.

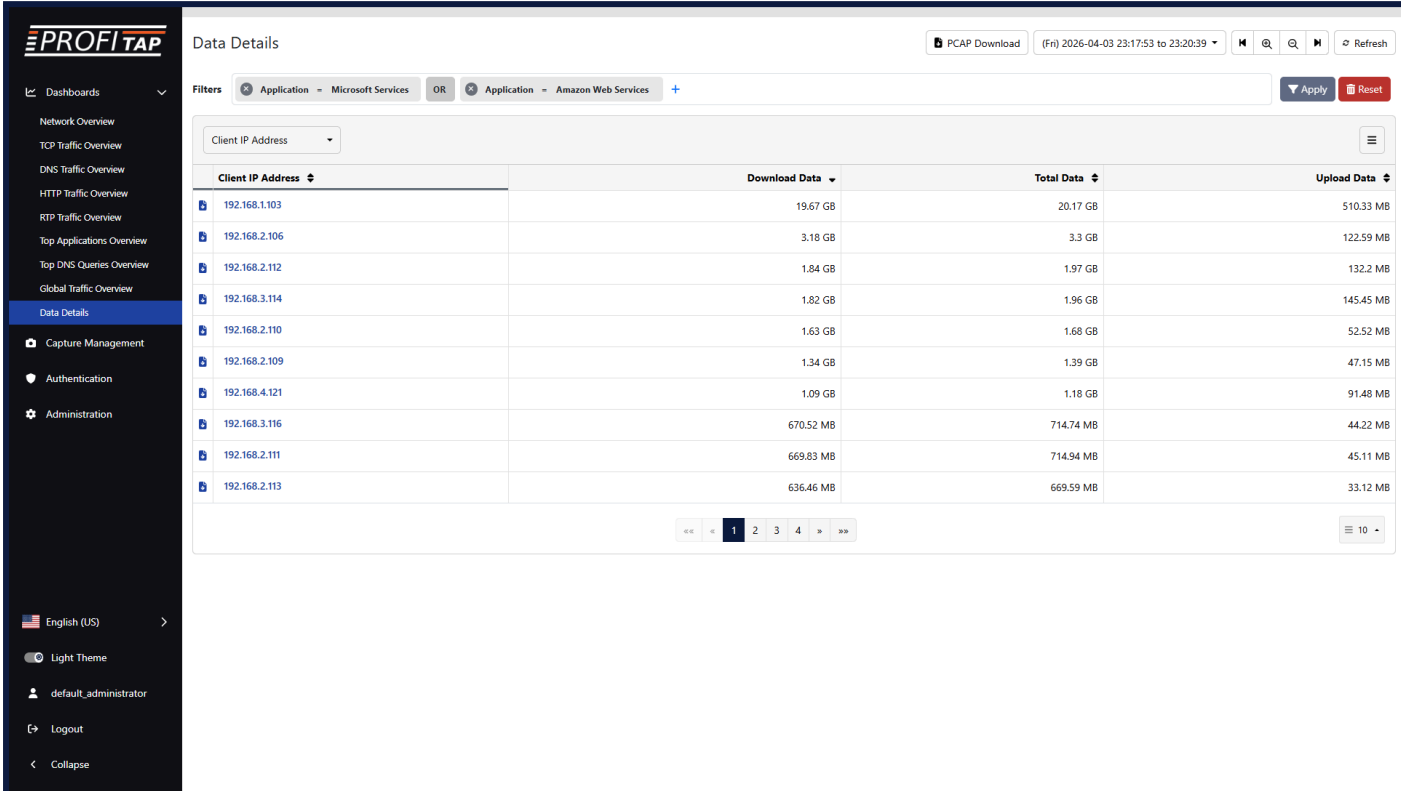
The metric to target can be changed using the menu in the top-right corner of the map.

Clicking a country and then *View Details* will navigate to its *Details* page (see **Data Details** below).

## 5.8. Data Details

The **Data Details** dashboard allows you to display and dive into accumulated data for the selected time range and filters.

In the other dashboards, selecting *View Details* for a value will navigate to a *Details* page with a pre-filled filter for the selected value and a *back* arrow for navigating to the previous dashboard. This *Details* page and the *Data Details* dashboard are functionally the same.



The screenshot shows the 'Data Details' dashboard in PROFITAP. The dashboard is titled 'Data Details' and includes a top navigation bar with a 'PCAP Download' button, a time range selector '(Fri) 2026-04-03 23:17:53 to 23:20:39', and search and refresh icons. Below the top bar is a 'Filters' section with two active filters: 'Application - Microsoft Services' and 'Application - Amazon Web Services'. A 'Client IP Address' dropdown menu is visible. The main content area is a table with the following columns: 'Client IP Address', 'Download Data', 'Total Data', and 'Upload Data'. The table contains 12 rows of data. At the bottom of the table is a pagination control showing page 1 of 10.

Client IP Address	Download Data	Total Data	Upload Data
192.168.1.103	19.67 GB	20.17 GB	510.33 MB
192.168.2.106	3.18 GB	3.3 GB	122.59 MB
192.168.2.112	1.84 GB	1.97 GB	132.2 MB
192.168.3.114	1.82 GB	1.96 GB	145.45 MB
192.168.2.110	1.63 GB	1.68 GB	52.52 MB
192.168.2.109	1.34 GB	1.39 GB	47.15 MB
192.168.4.121	1.09 GB	1.18 GB	91.48 MB
192.168.3.116	670.52 MB	714.74 MB	44.22 MB
192.168.2.111	669.83 MB	714.94 MB	45.11 MB
192.168.2.113	636.46 MB	669.59 MB	33.12 MB

*Data Details dashboard*

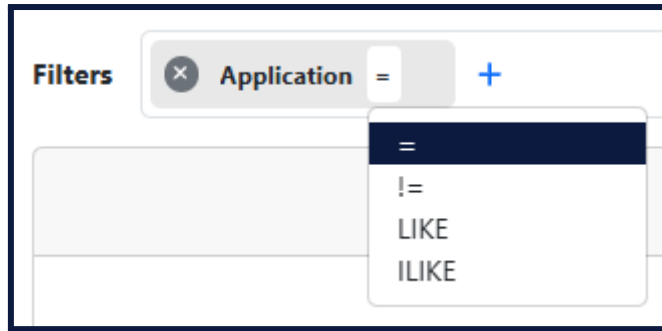
### 5.8.1. Filters

Filters can be managed in the *Filters* section at the top of the dashboard.

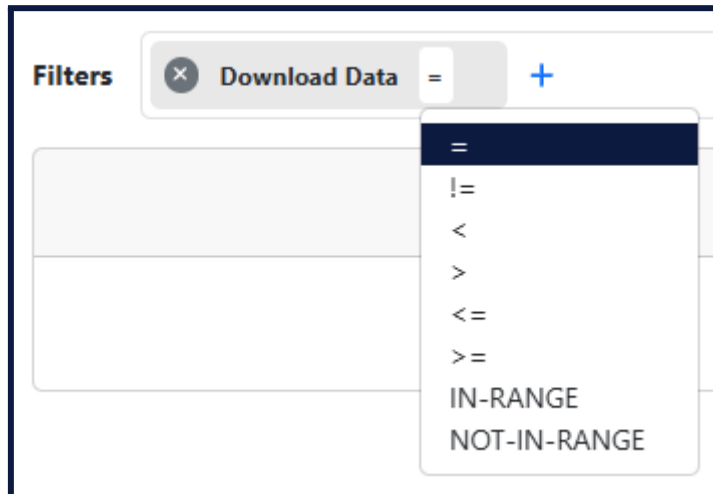
To add a filter, click the + button and select a filter parameter from the list, after which a list of possible values to choose from will be displayed (this can take a few seconds to appear depending on the amount of data). Select a value from the list or type one in.

Clicking the equals sign (=) allows you to change the filter operator. The available operators will depend on the selected filter parameter. All filter parameters provide the *equal-to* and *not-equal-to* operators.

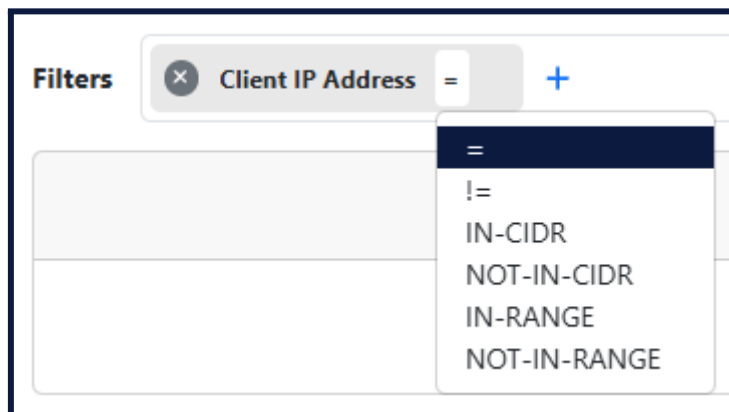
Alphanumeric filter parameters provide the *LIKE* operator for case-sensitive matching and *ILIKE* for case-insensitive matching.



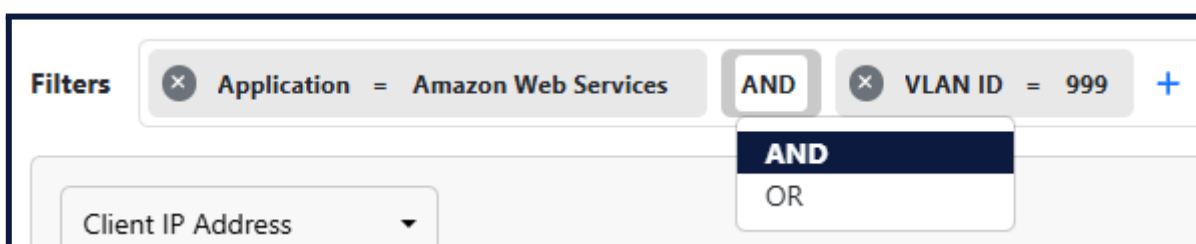
Numeric filter parameters provide the *less-than*, *greater-than*, *less-than-or-equal-to*, *greater-than-or-equal-to*, *IN-RANGE*, and *NOT-IN-RANGE* operators.



IP address filter parameters provide the *IN-CIDR*, *NOT-IN-CIDR*, *IN-RANGE*, and *NOT-IN-RANGE* operators.

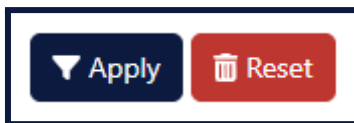


When adding more than one filter, the operator between filters can be changed between *AND* and *OR*.

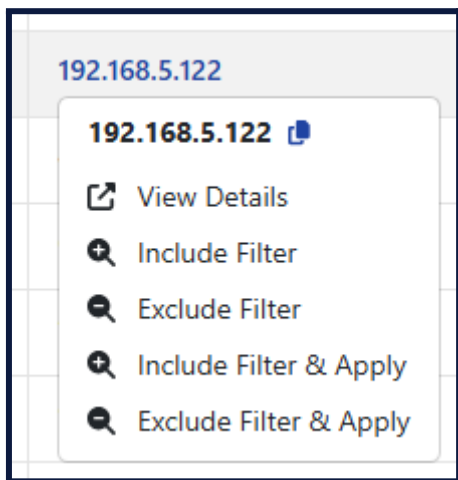


These filters are applied both to the dashboard display and to the *Download PCAP* feature.

Click the *Apply* button to query the database and display data matching the selected filters and time range. Click the *Reset* button to clear the filters.

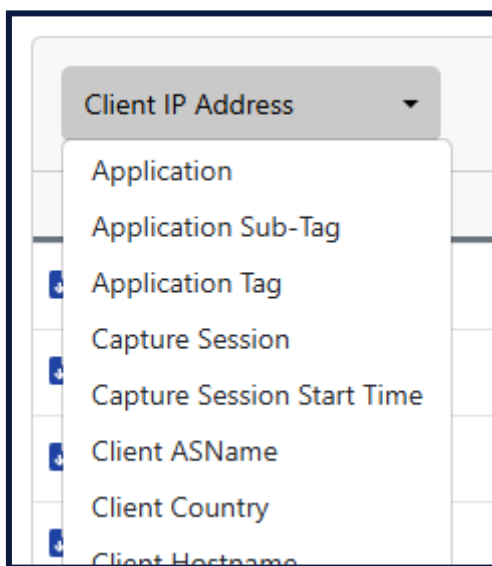


Clicking certain values in the table allows you to add an *include* or *exclude* filter to the query for this value, using the *Include Filter* and *Exclude Filter* options, or to create a new query with an *include* filter for this value, using the *View Details* option.

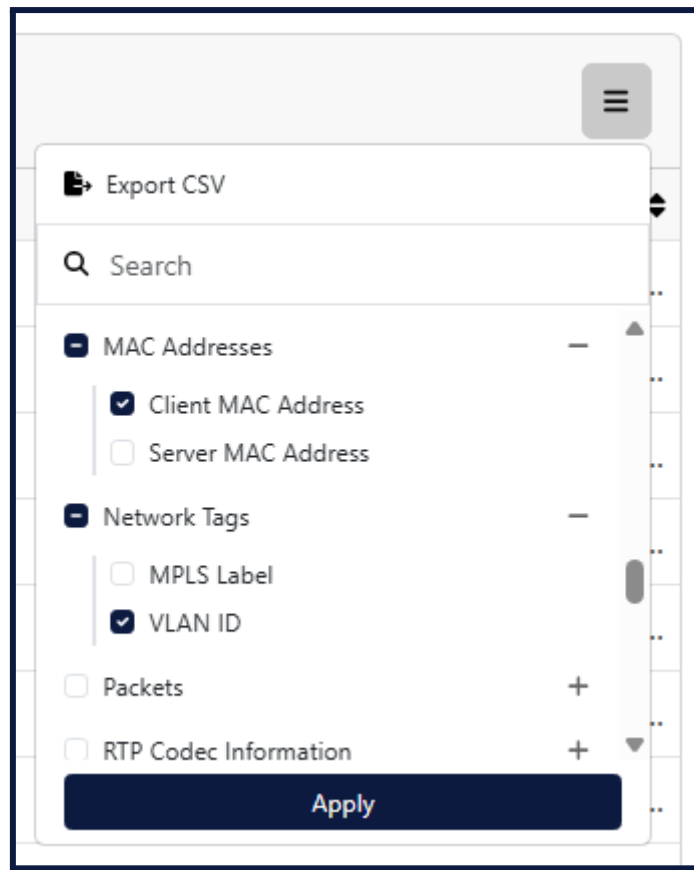


### 5.8.2. Table

In the table displaying entries of accumulated data, the primary parameter can be changed using the drop-down menu in the top-left corner.



The button in the top-right corner of the table opens a menu for selecting which metrics columns to display or hide. Available metrics are categorized, and the search field can be used to look for specific metrics. An *Export CSV* button is also available in this menu for downloading the table as a CSV file.



The entries in the table can be sorted using the metrics columns that are displayed by clicking the column header.

The navigation at the bottom of a table allows you to navigate between pages.

The number of entries displayed on each page of the table can be selected in the bottom-right corner.

The *Download traffic PCAP* button on the left of each table entry allows you to download the accumulated traffic for this entry.

The *PCAP Download* button in the top-right corner of the page allows you to download the accumulated traffic for all displayed entries in the selected time range.

### 5.8.3. Time graphs

Hovering certain values in the table gives the option to create a time graph for tracking the selected metric over time for the selected primary parameter entry. Up to 3 time graphs can be created, for 3 different metrics.

**PROFITAP**

Data Details PCAP Download (Fri) 2026-04-03 23:17:53 to 23:20:39 Refresh

Filters: Total Data > 0 Bytes Apply Reset

Client IP Address

Client IP Address	Download Data	Total Data	Upload Data
192.168.1.101	131.73 GB	136 GB	4.27 GB
192.168.2.107	114.78 GB	121.94 GB	7.16 GB
192.168.3.114	102.32 GB	105.96 GB	3.64 GB
192.168.2.113	96.99 GB	101.42 GB	4.44 GB
192.168.1.103	83.47 GB	86.53 GB	3.06 GB
192.168.3.116	80.33 GB	83.15 GB	2.82 GB
192.168.2.109	76.29 GB	79.26 GB	2.97 GB
192.168.4.121	63.01 GB	69.05 GB	6.05 GB
192.168.1.104	64.66 GB	67.18 GB	2.52 GB
192.168.1.102	61.85 GB	63.9 GB	2.05 GB

« 1 2 3 4 5 ... 10 »

With a time graph created for a metric, hovering the value of a different entry for that same metric allows you to add a line in the time graph for tracking that metric for that entry. Up to 5 lines can be created.

**PROFITAP**

Data Details PCAP Download (Fri) 2026-04-03 23:17:53 to 23:20:39 Refresh

Filters: Total Data > 0 Bytes Apply Reset

Client IP Address

6.52 GB  
5.59 GB  
4.66 GB  
3.73 GB  
2.79 GB  
1.86 GB  
953.67 MB  
0 Bytes

23:17:53 2026-04-03 23:18:10 2026-04-03 23:18:27 2026-04-03 23:18:44 2026-04-03 23:19:01 2026-04-03 23:19:18 2026-04-03 23:19:35 2026-04-03 23:19:52 2026-04-03 23:20:09 2026-04-03 23:20:26 2026-04-03

Total Data

- 192.168.1.101 Client IP Address
- 192.168.2.107 Client IP Address
- 192.168.3.114 Client IP Address
- 192.168.2.113 Client IP Address

Client IP Address	Download Data	Total Data	Upload Data
192.168.1.101	131.73 GB	136 GB	4.27 GB
192.168.2.107	114.78 GB	121.94 GB	7.16 GB
192.168.3.114	102.32 GB	105.96 GB	3.64 GB
192.168.2.113	96.99 GB	101.42 GB	4.44 GB
192.168.1.103	83.47 GB	86.53 GB	3.06 GB
192.168.3.116	80.33 GB	83.15 GB	2.82 GB
192.168.2.109	76.29 GB	79.26 GB	2.97 GB
192.168.4.121	63.01 GB	69.05 GB	6.05 GB
192.168.1.104	64.66 GB	67.18 GB	2.52 GB
192.168.1.102	61.85 GB	63.9 GB	2.05 GB

« 1 2 3 4 5 ... 10 »

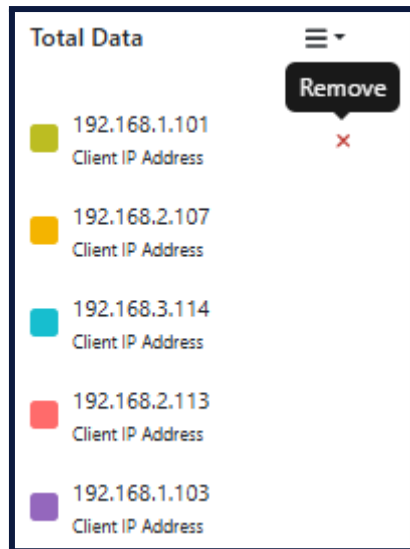


Click the square next to each parameter to show or hide the corresponding line on the time graph.

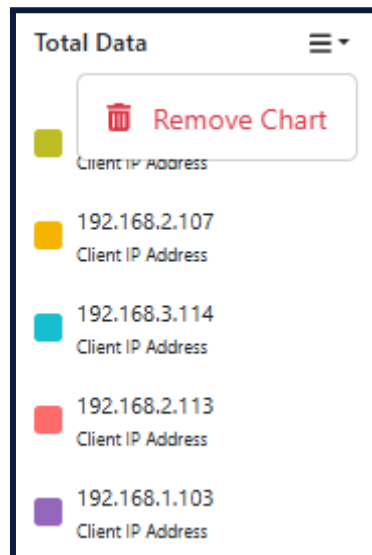
The close-up shows the legend for the 'Total Data' graph. It lists five client IP addresses with their corresponding traffic volumes. A 'Hide' button is visible next to the first IP address, 192.168.1.101, indicating that the user can toggle the visibility of each data series.

Client IP Address	Traffic Volume
192.168.1.101	3.41 GB
192.168.2.107	362.56 MB
192.168.3.114	43.18 KB
192.168.2.113	2.21 GB
192.168.1.103	75.51 MB

Hover over a parameter and click the *Remove* cross to remove it from the time graph.



Click the button in the top-right corner of a time graph and select *Remove Chart* to remove it.



# ***Legal***

## ***Disclaimer***

The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranty 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 HQ B.V.  
High Tech Campus 84  
5656AG Eindhoven  
The Netherlands  
sales@profitap.com  
[www.profitap.com](http://www.profitap.com)

© 2026 Profitap — v1.4