IOTA 100 CORE

USER MANUAL

IOTA software version: v6.1.0

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

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

https://resources.profitap.com/

TABLE OF CONTENTS

1. Product Overview **5**
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
2. Getting Started **9**
2.1. Rack Mounting 9
2.1.1. Installing the rails into a rack 9
2.1.2. Installing the unit into a rack 12
2.1.3. Removing the unit from a rack 13
2.1.4. Installing the unit into a telco rack 14
2.2. Power 15
2.3. Accessing IOTA Over the Network 15
2.4. Capture Interfaces 16
3. IOTA Configuration **17**
3.1. Administration 17
3.1.1. Time & NTP Configuration 17
3.1.2. Network Configuration 18
3.1.3. HTTPS Certificate 19
3.1.4. ZeroTier 19
3.1.5. System Control 20
3.1.6. Firmware 20
3.1.7. License 20
3.1.8. Logs 21
3.2. Authentication 23
3.2.1. Local Users 23
3.2.2. TACACS+ 24
3.2.3. RADIUS 25
3.2.4. LDAP and LDAPS 26
3.2.5. Custom Authentication Configuration 27
3.3. Device Reset 27
3.3.1. Network Configuration 27
3.3.2. Factory Reset 27
3.4. Device Recovery CLI 27
3.4.1. Accessing the CLI 28
3.4.2. Using the CLI 28
3.5. BMC IPMI Access 30
4. Capture Management **31**
4.1. Capture Interfaces 31
4.2. Traffic Analysis 33
4.3. Data Storage 34

4.3.1. Storage Management 34
4.3.2. Packet Capture Statistics 35
4.3.3. Packet Capture Filters 35
5. Analysis Dashboards **37**
5.1. Network Overview 38
5.2. TCP Traffic Overview 41
5.3. DNS Traffic Overview 42
5.4. HTTP Traffic Overview 43
5.5. RTP Traffic Overview 44
5.6. Top Applications Overview, Top DNS Queries Overview 45
5.7. Global Traffic Overview 46
5.8. Data Details 47
5.8.1. Filters 47
5.8.2. Table 49
5.8.3. Time graphs 50
Legal **54**
Disclaimer 54
Copyright 54
Trademarks 54

1. Product Overview

1.1. Hardware Overview

IOTA 100 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 100 CORE main unit
- 2 x C13 AC power cord
- 1 x rack mounting kit (rails, L brackets, screws)

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

1.3. Specifications

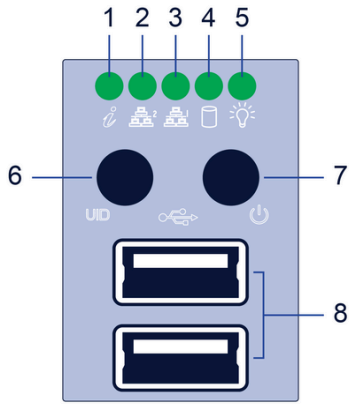
	IOTA 100 CORE
Capture Interfaces	2 x 40/100G QSFP28
Capture Mode	Out-of-band
Supported Capture Speed[1]	10G / 25G / 40G / 100G
Capture Performance[2]	100 Gbps / 16 M packets per second / 9 M flows per second
Internal Storage	32, 64, 128, or 307 TB high-performance solid-state storage The drives are set up in RAID 5 configuration.
Power Inputs	2 x C14 (redundant): 100–127 VAC, 9–7.5 A, 50–60 Hz, 800 W or 200–240 VAC, 6–4.5 A, 50–60 Hz, 860 W
Management Interfaces	2 x SFP+ Ethernet 1/10G 2 x RJ45 Ethernet 1/10G
Management Service	HTTPS (server) SSH (recovery CLI)
Additional Functions Interfaces	1 x RJ45 1G BMC IPMI 1 x RJ45 1G PTPv2 2 x USB 3.0 2 x USB 2.0 1 x VGA 1 x COM
Dimensions (WxDxH)	440 x 620 x 44 mm 17.3 x 24.4 x 1.7 in
Weight	11.3 kg 25 lb
Compliance	RoHS, CE, FCC, UKCA, TA

[1] 8 x 10G or 4 x 25G via breakout cables.

[2] Maximum performance in ideal conditions. Packet size may affect these values.

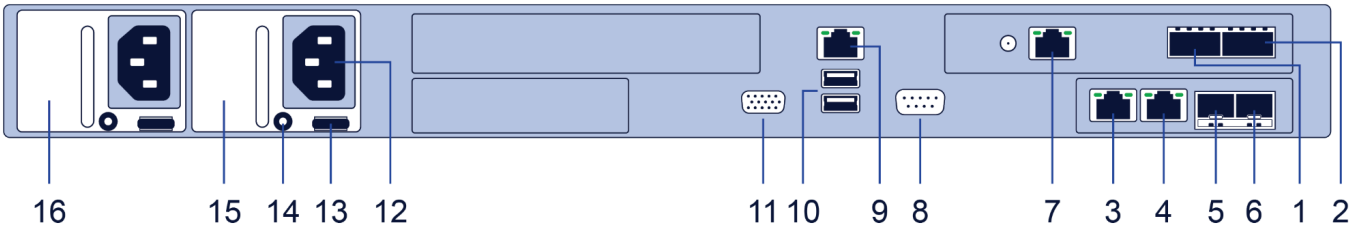
1.4. Interfaces & LED Behavior

1.4.1. Front



LEDs and buttons		State	Description
1	Information LED	Red, solid	An overheat condition has occurred.
		Red, blinking at 1 Hz	Fan failure, check for an inoperative fan.
		Red, blinking at 0.25 Hz	Power failure, check for a non-operational power supply.
		Red, solid, with Power LED blinking green	Fault detected.
		Blue and red, blinking at 10 Hz	Recovery mode.
		Blue, solid	UID has been activated locally to locate the server in a rack.
		Blue, blinking at 1Hz	UID has been activated using the BMC to locate the server in a rack.
		Blue, blinking at 2Hz	BMC is resetting.
		Blue, blinking at 4Hz	BMC is setting factory defaults.
		Blue, blinking at 10Hz with Power LED blinking green	BMC/BIOS firmware is updating.
2	NIC2 LED	Blinking	Network activity on LANs.
3	NIC1 LED		
4	Drive LED	Blinking	Activity on storage drives.
5	Power LED	Steady on	Power on.
		Blinking at 4 Hz	Checking BIOS/BMC integrity.
		Blinking at 4 Hz and "i" LED is blue	BIOS firmware updating.
		Two blinks at 4 Hz, one pause 2 Hz and "i" LED blue	BMC firmware updating.
		Blinking at 1 Hz and "i" LED red	Fault detected.
6	UID button, BMC reset		The unit identification (UID) button turns on or off the blue light function of the Information LED and a blue LED at the rear of the unit. This button can also be used to reset the BMC.
7	Power button		Applies or removes primary power from the power supply to the unit. Standby power is maintained. Shutting down the unit through the GUI is recommended.
8	USB 2.0 ports		

1.4.2. Rear



1		Capture port 1, QSFP28 40/100G
2		Capture port 2, QSFP28 40/100G
3		Management port 1, RJ45 1/10G
4		Management port 2, RJ45 1/10G
5		Management port 3, SFP+ 1/10G
6		Management port 4, SFP+ 1/10G
7		RJ45 1G PTPv2 port
8		COM port (serial)
9		RJ45 1G BMC IPMI port
10		USB 3.0 ports
11		VGA port
12		AC power connector
13		Power supply release tab
14		Power supply status LED
15, 16		Power supplies (redundant)

Power supply status LED	
LED color and state	**Description**
Solid green	Power supply is on.
Blinking green	Power supply is plugged in and turned off by the system.
Blinking amber	Power supply has a warning condition and continues to operate.
Solid amber	Power supply is plugged in and is in an abnormal state.
Off	No power.

2. Getting Started

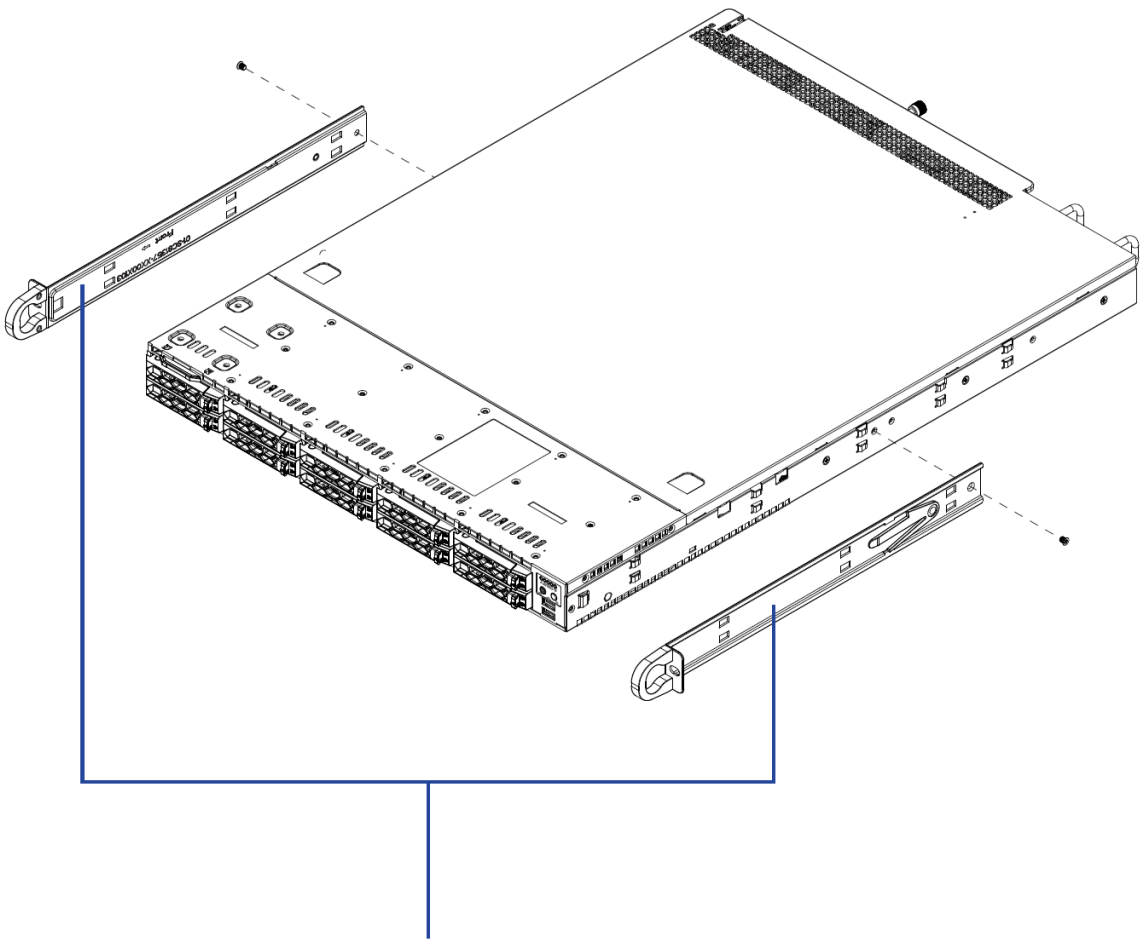
2.1. Rack Mounting

IOTA 100 CORE can be mounted in a rack of standard 19" width, using the provided rack mounting kit. The provided rail set fits a rack between 26" and 33.5" deep.

2.1.1. Installing the rails into a rack

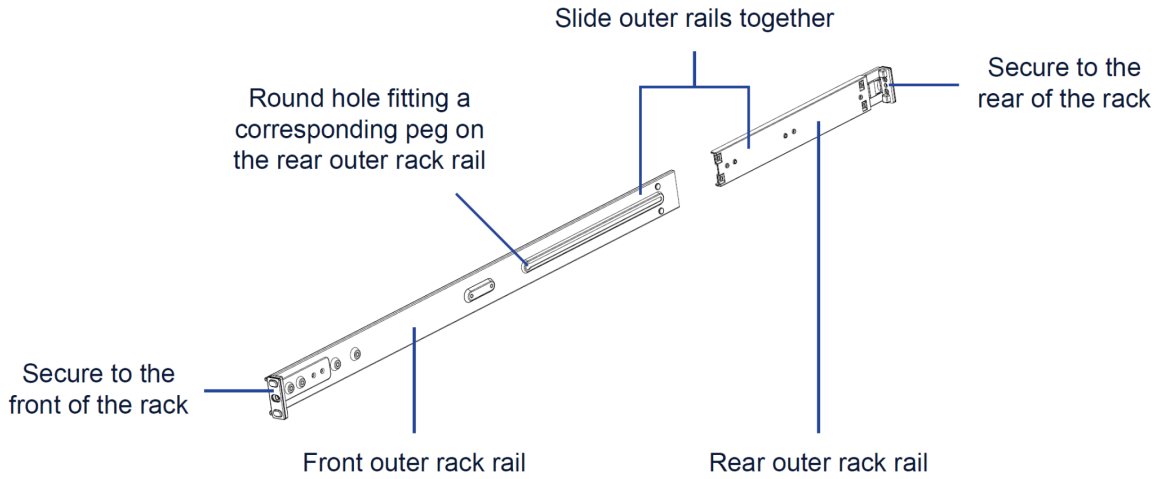
The chassis comes with two sets of rack rails, one for each side of the chassis. Each set consists of two sections: a two-part inner chassis rail that secures directly to the chassis, and a two-part outer rack rail that secures directly to the rack itself.

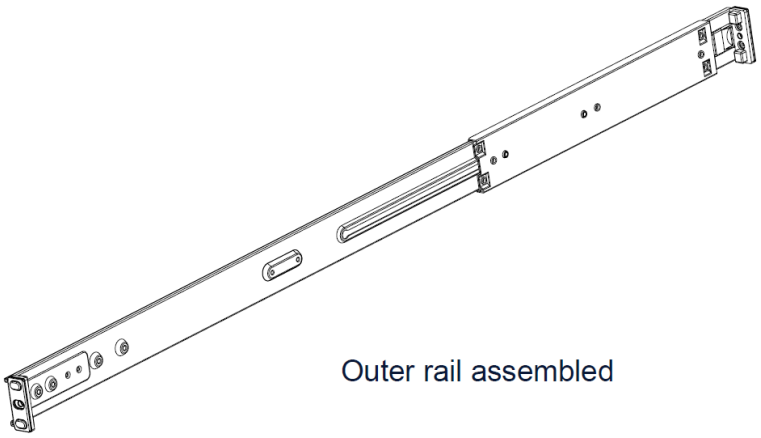
The front inner rails are pre-attached and do not interfere with normal use of the chassis if you decide not to use a server rack. The provided rear inner rails can be attached by sliding them on the sides of the chassis until the release tab is engaged, and securing them using the provided screws.



Front inner rack rails (pre-attached)

The outer rail can be assembled by aligning the round hole on the front outer rail with the peg on the rear outer rail, then sliding the rear rail such that the peg is secured in the track on the front rail.

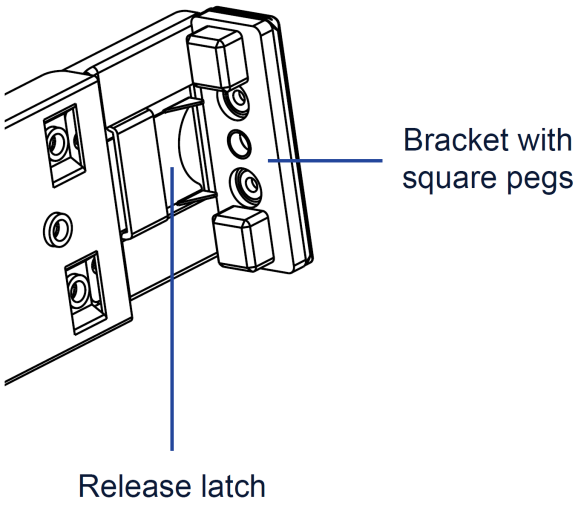




Note: Slide rail mounted equipment is not to be used as a shelf or a work space.

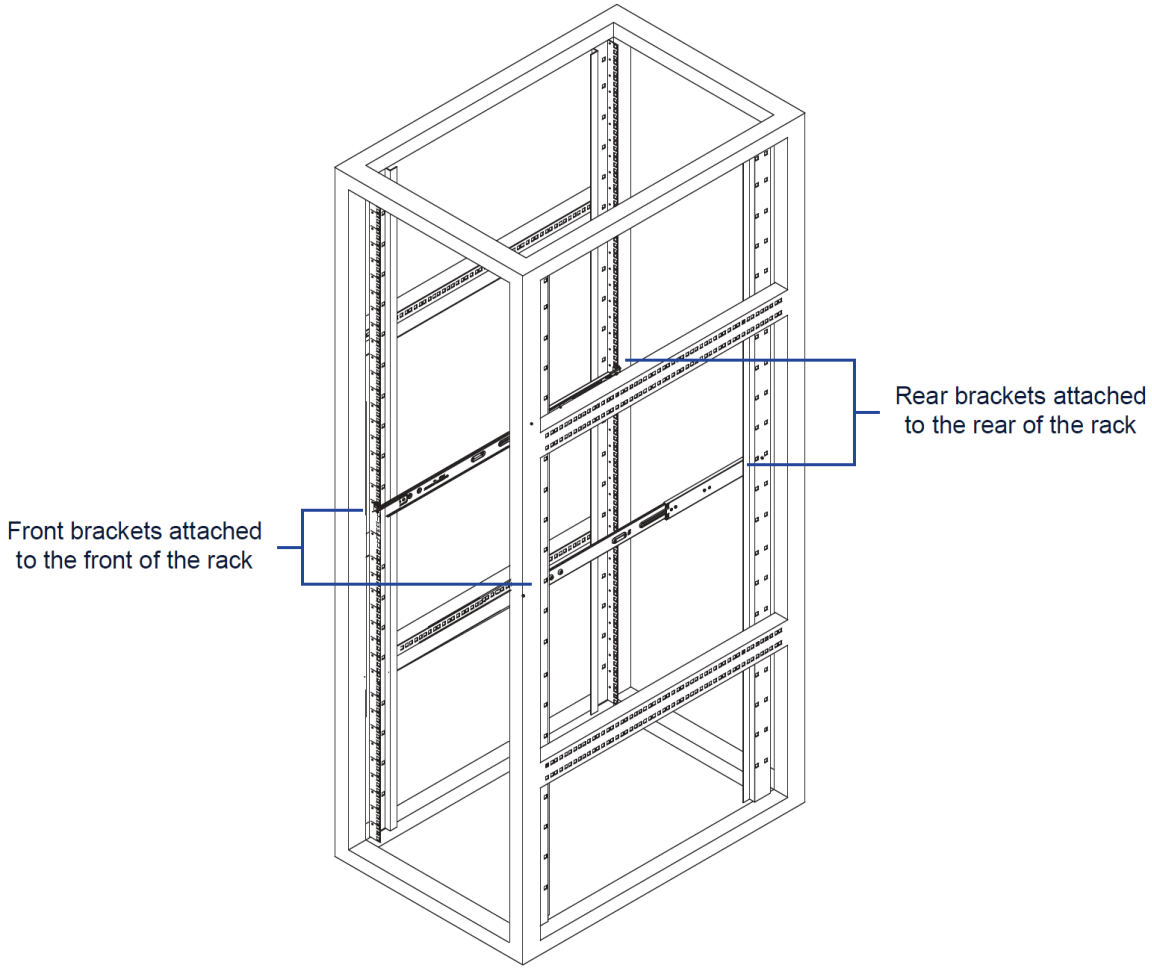
Warning: Do not pick up the server with the front handles. They are designed to pull the system from a rack only.

Each end of the assembled outer rail includes a bracket with square pegs to fit into the rack holes. If the rack holes are round, these brackets can be removed in order use screws to secure the rail to the rack instead.



Outer rail installation:

1. Align the square pegs on the front end of the rail with the square holes on the front of the rack. Push the rail into the rack until the release latch snaps into place, securing the rail to the rack. Keep the rail horizontal.
2. Adjust the rail to reach just past the full depth of your rack.
3. Align the square pegs on the rear end of the rail to the holes on the rack and push the rail into the rack until the release latch snaps into place, securing the rail to the rack.
4. Repeat the procedure for the other outer rail assembly.



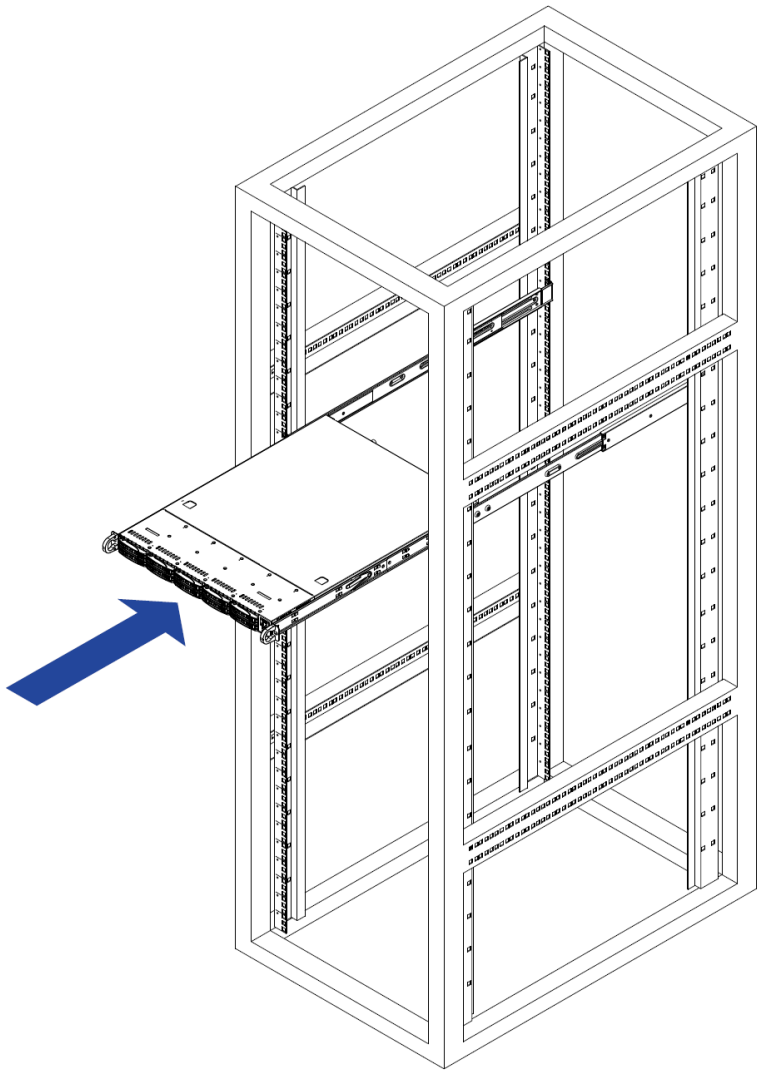
Note: Figure is for illustrative purposes only. Always install servers to the bottom of a rack first.

Warning: The rack stabilizing mechanism must be in place, or the rack must be bolted to the floor before sliding the unit out for servicing. Failure to stabilize the rack can cause the rack to tip over.

2.1.2. Installing the unit into a rack

Once the inner rails are attached to the chassis and outer rails to the rack, you can install the unit.

1. Align the rear of the chassis with the front of the outer rails on the rack.
2. Slide the chassis rails into the rack rails, keeping the pressure even on both sides (you may have to depress the locking tabs when inserting). When the unit has been pushed completely into the rack, you should hear the locking tabs click into position.
3. (Optional) Insert and tighten the thumbscrews that hold the front of the unit to the rack.

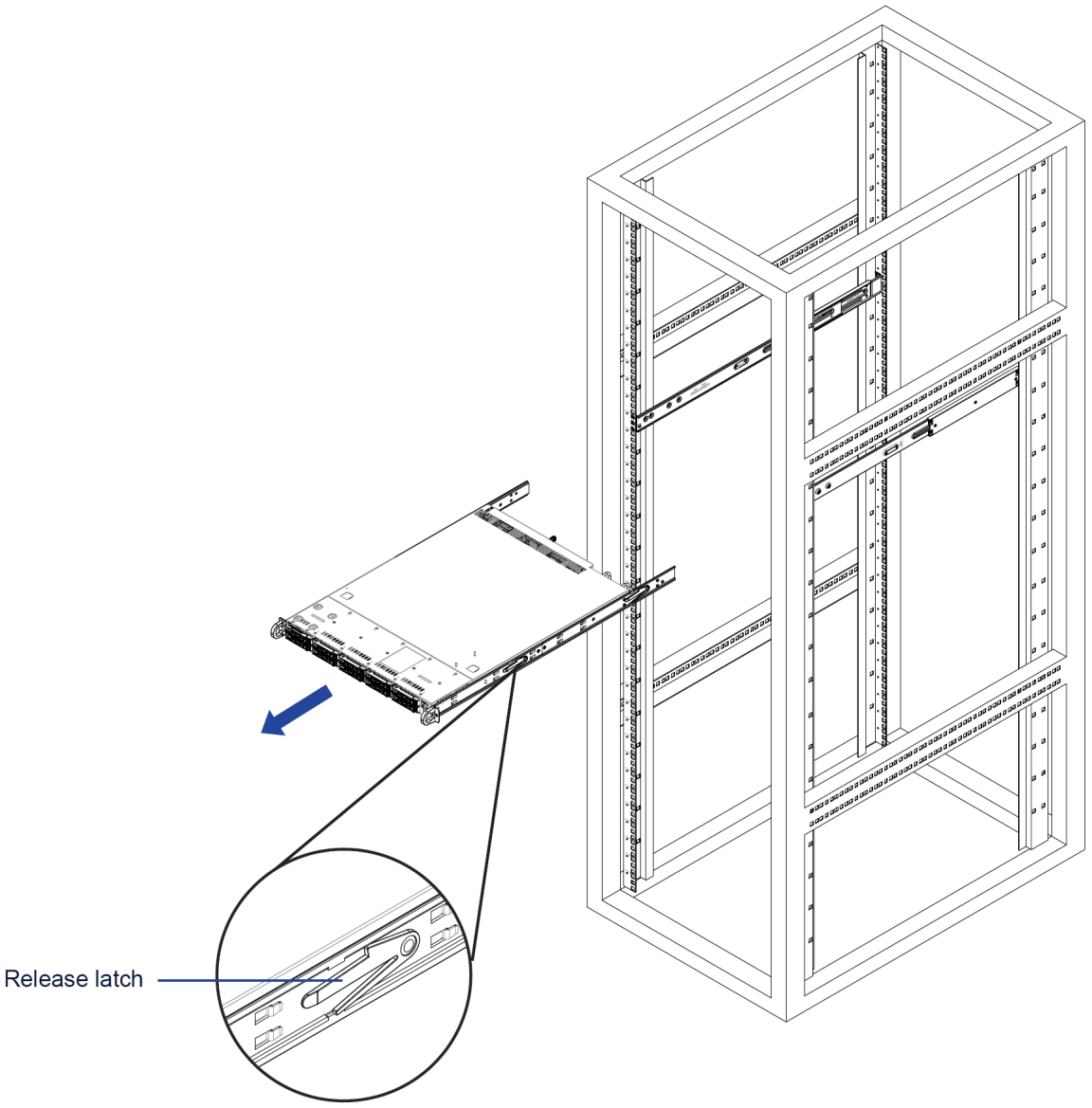


Installing the unit into the rack

2.1.3. Removing the unit from a rack

Caution! It is dangerous for a single person to off-load the heavy chassis from the rack without assistance. Be sure to have sufficient assistance supporting the chassis when removing it from the rack. Use a lift.

1. If necessary, loosen the thumb screws on the front of the chassis that hold it in the rack.
2. Pull the chassis forward out the front of the rack until it stops.
3. Press the release latches on each of the inner rails downward simultaneously and continue to pull the chassis forward and out of the rack.

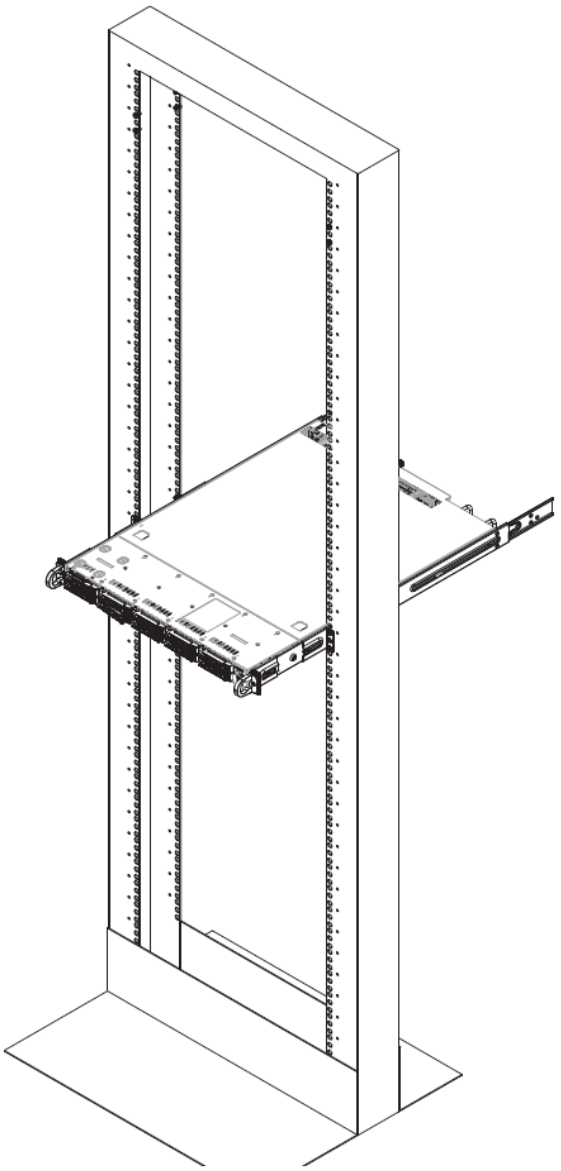


Removing the unit from the rack

2.1.4. Installing the unit into a telco rack

To install the server into a telco or post-style rack, use two L-shaped brackets on either side of the chassis (four in total).

1. Determine how far the server will extend out from the front of the rack. The chassis should be positioned so that the weight is balanced between front and back.
2. Attach the two front brackets to each side of the chassis, then the two rear brackets positioned with just enough space to accommodate the width of the rack.
3. Finish by sliding the chassis into the rack and tightening the brackets to the rack.



Installing the unit into a telco rack

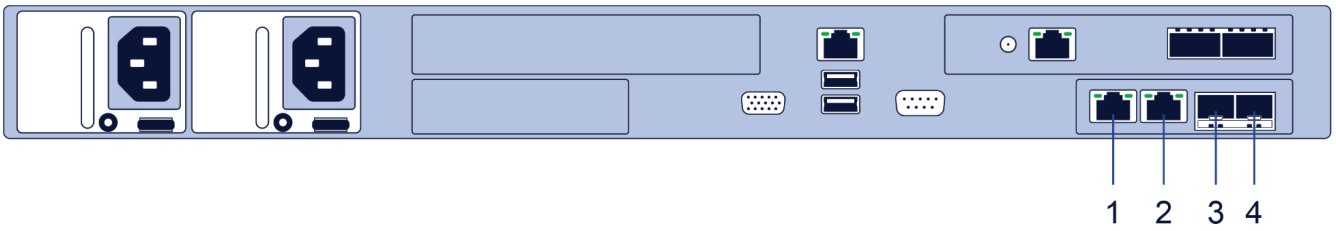
2.2. Power

Plug an AC cord into a power supply module at the rear of the unit, and connect it to the main power. Press the power button to turn on the unit.

The unit features redundant power supplies, and the system will continue to operate if one module fails. Connecting both power supplies is recommended to achieve maximum fail-safe operation at all times. The power supply modules are hot swappable, meaning they can be changed without powering down the system.

The power supplies are auto-switching capable, enabling them to automatically sense the input voltage and operate at 100–127 V or 200–240 V.

2.3. Accessing IOTA Over the Network



Connect one of the management ports (**1**, **2**, **3** and **4** 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 front of the unit provides the management interfaces' MAC addresses.

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.

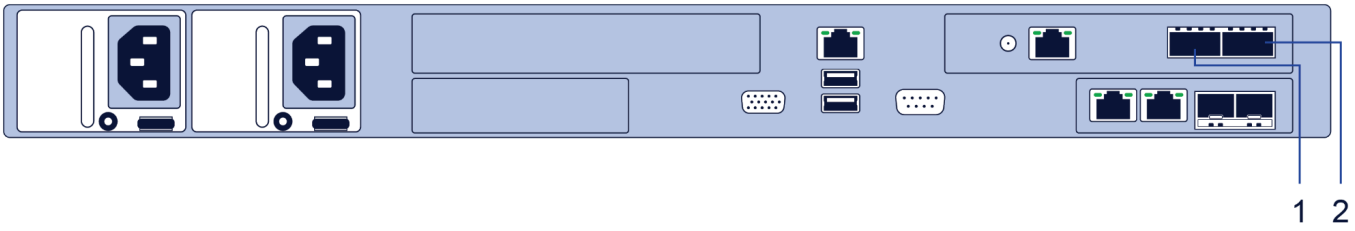
Network settings can be modified via the IOTA GUI (see Network Configuration) or the recovery CLI (see Device Recovery CLI).

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.

2.4. Capture Interfaces



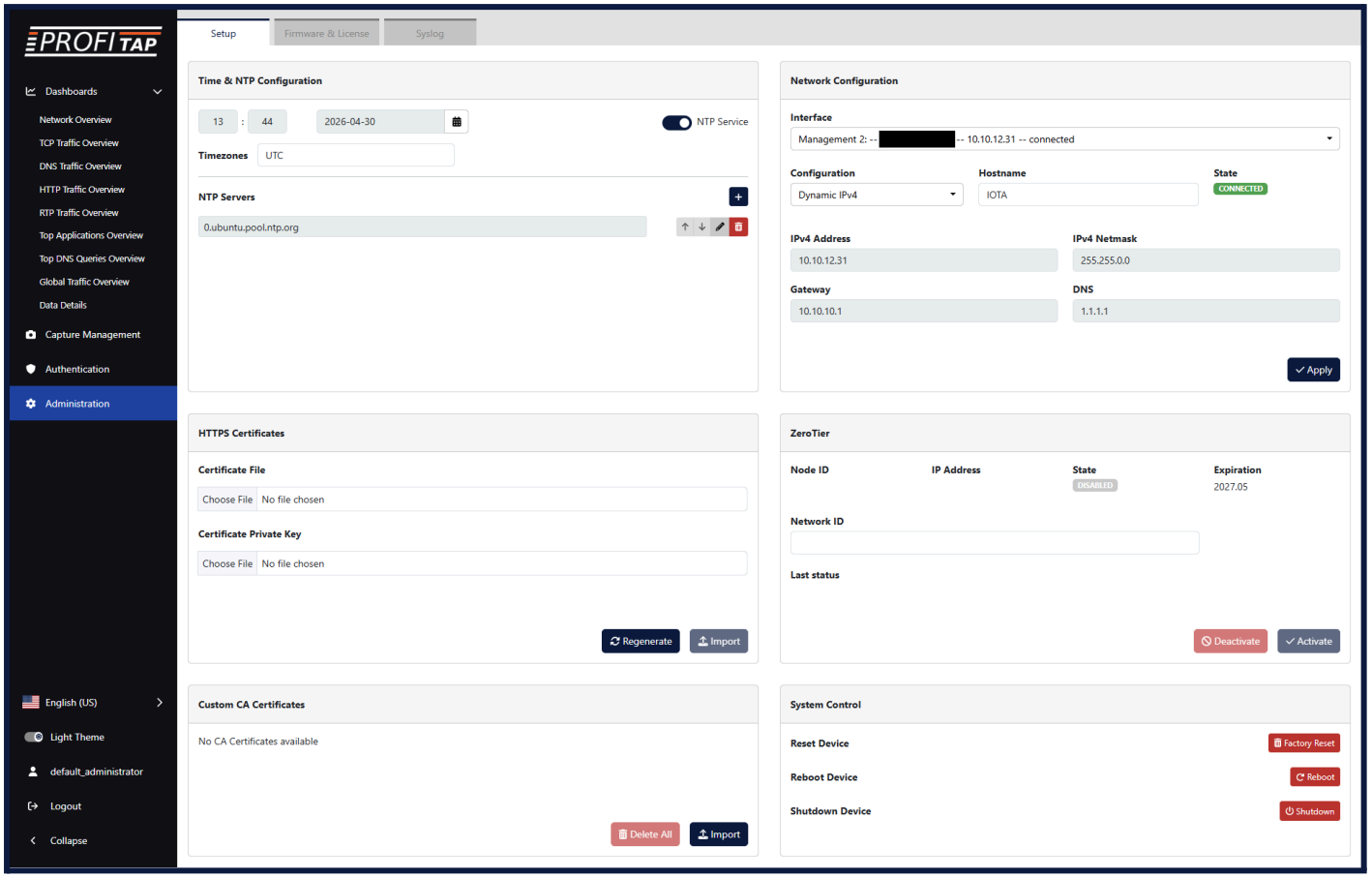
Connect cables and transceivers from the line(s) from which to capture traffic to the QSFP28 capture port(s) (**1** and **2** in the image above).

For more information, see Interfaces and Capture Interfaces.

3. IOTA Configuration

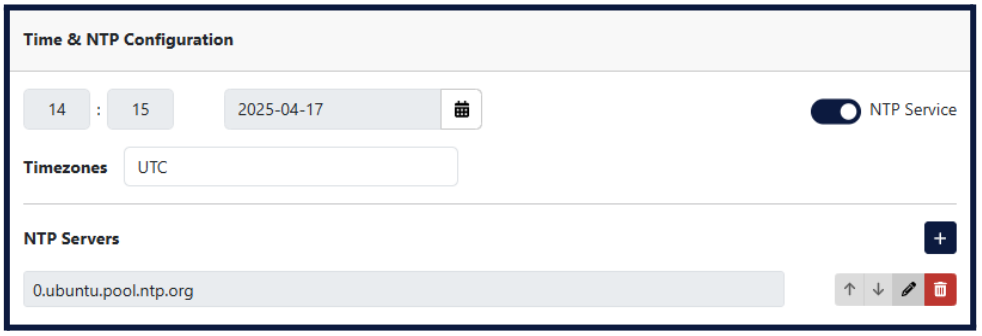
3.1. Administration

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



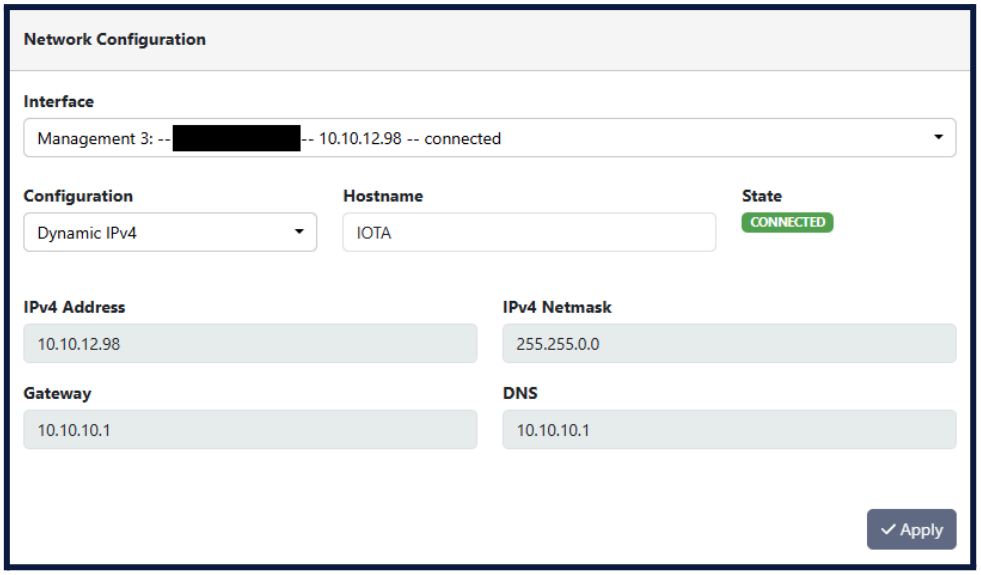
3.1.1. Time & NTP Configuration

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.



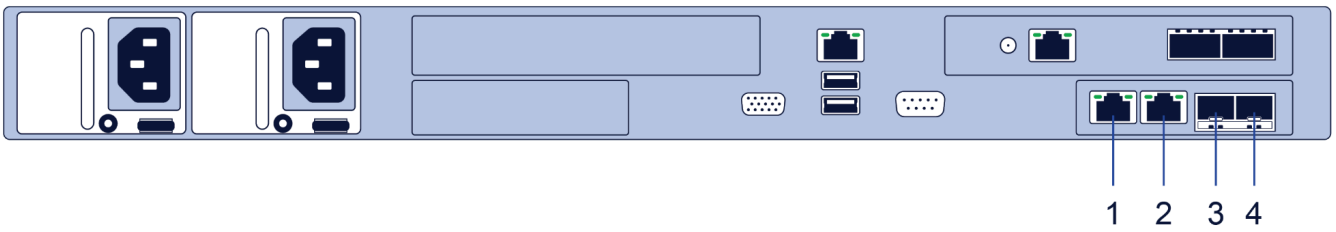
3.1.2. Network Configuration

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:** RJ45 1/10G
- **Management 2:** RJ45 1/10G
- **Management 3:** SFP+ 1/10G
- **Management 4:** SFP+ 1/10G



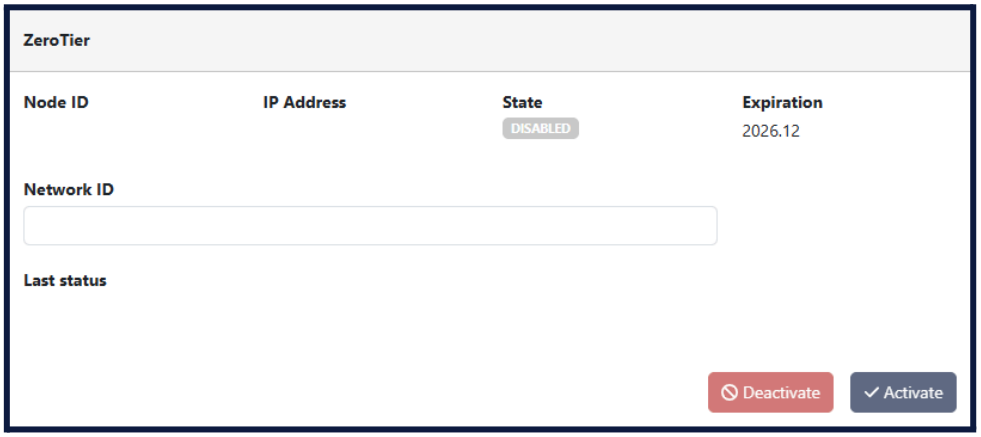
3.1.3. HTTPS Certificate

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.

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.



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 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

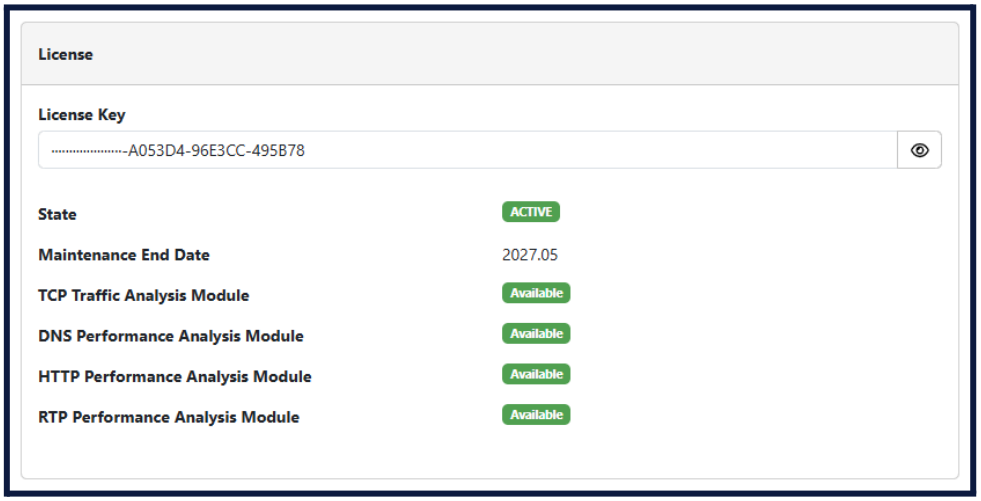
IOTA can be restarted, shut down, or reset to factory settings, via these buttons. Factory reset is only possible if no capture is currently in progress (capture can be stopped on the *Capture Management* page).

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.

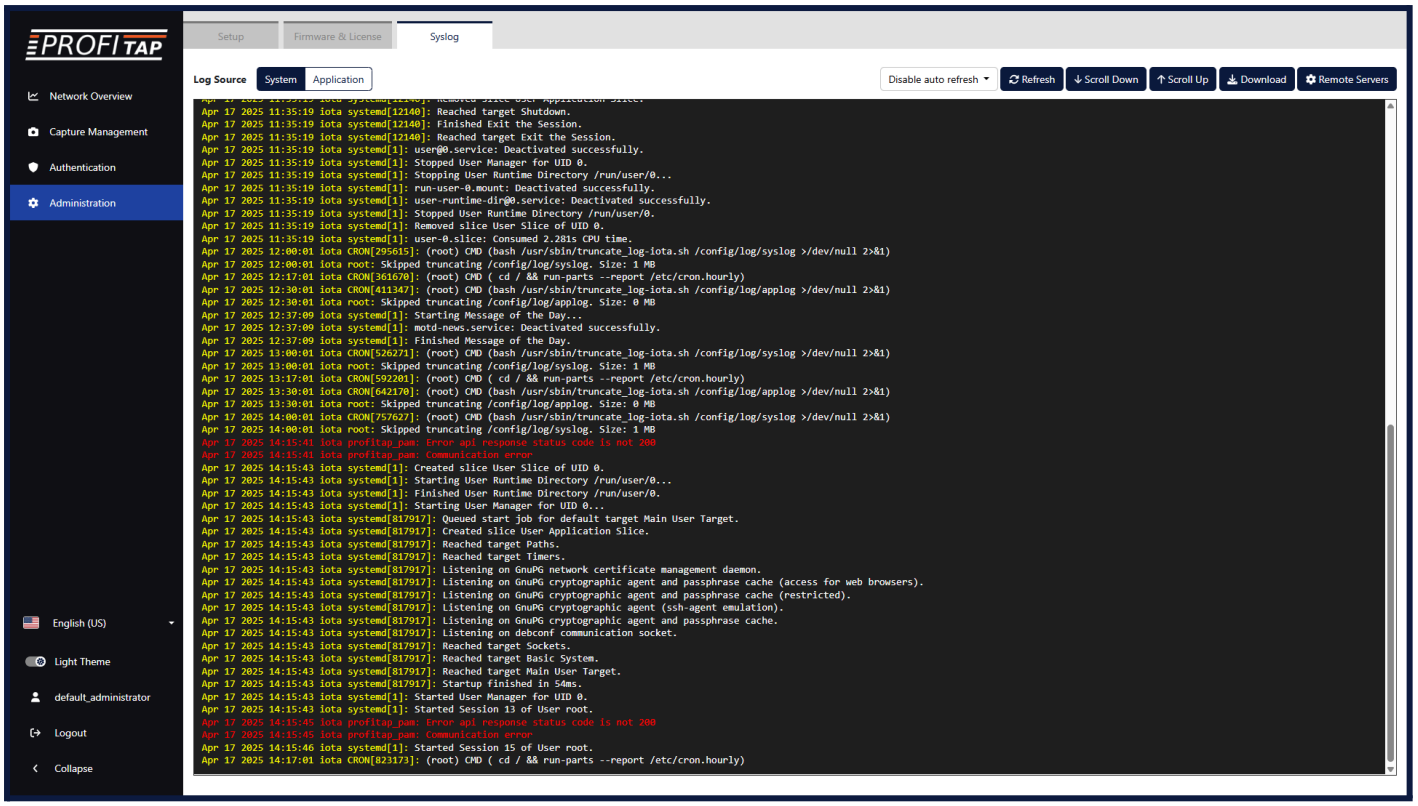
3.1.7. License

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.

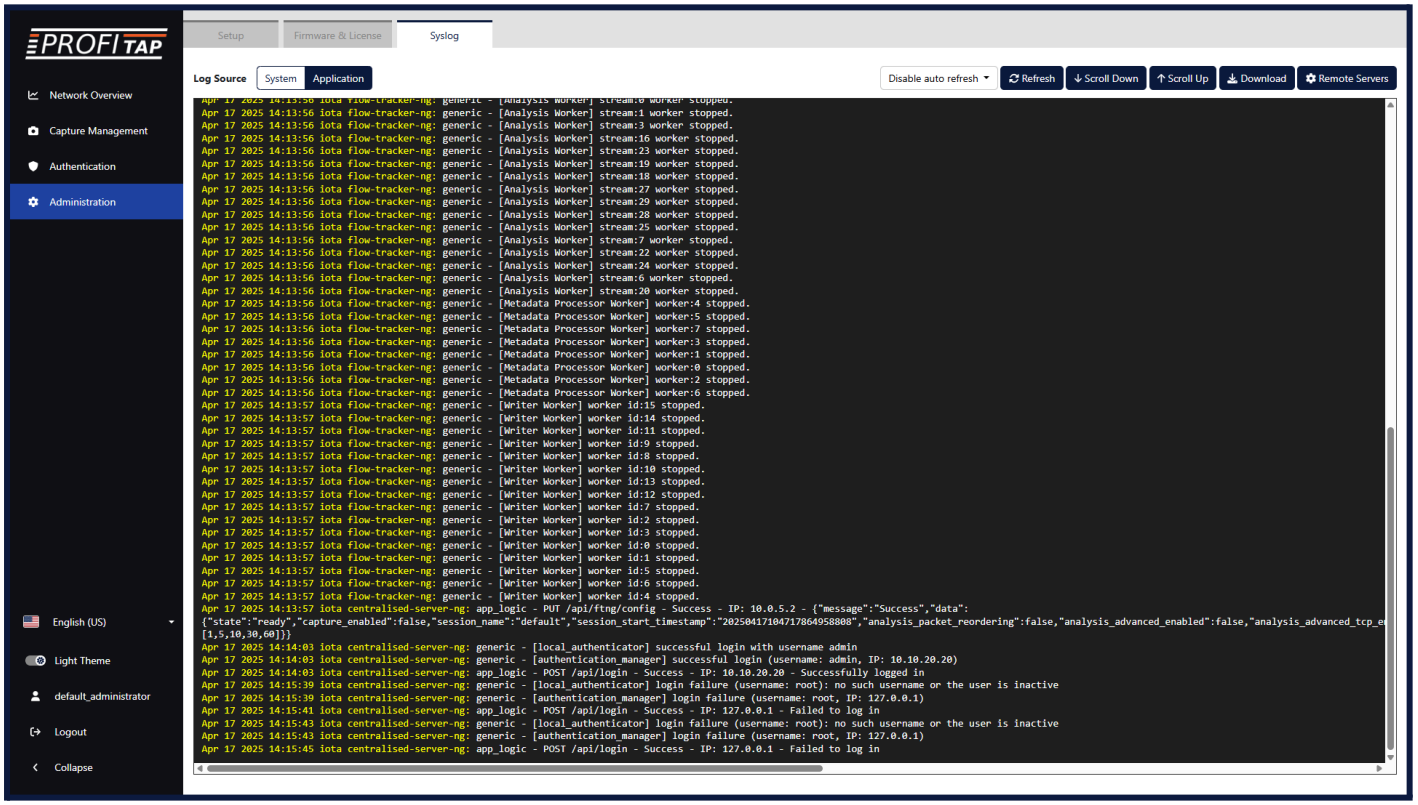


3.1.8. Logs

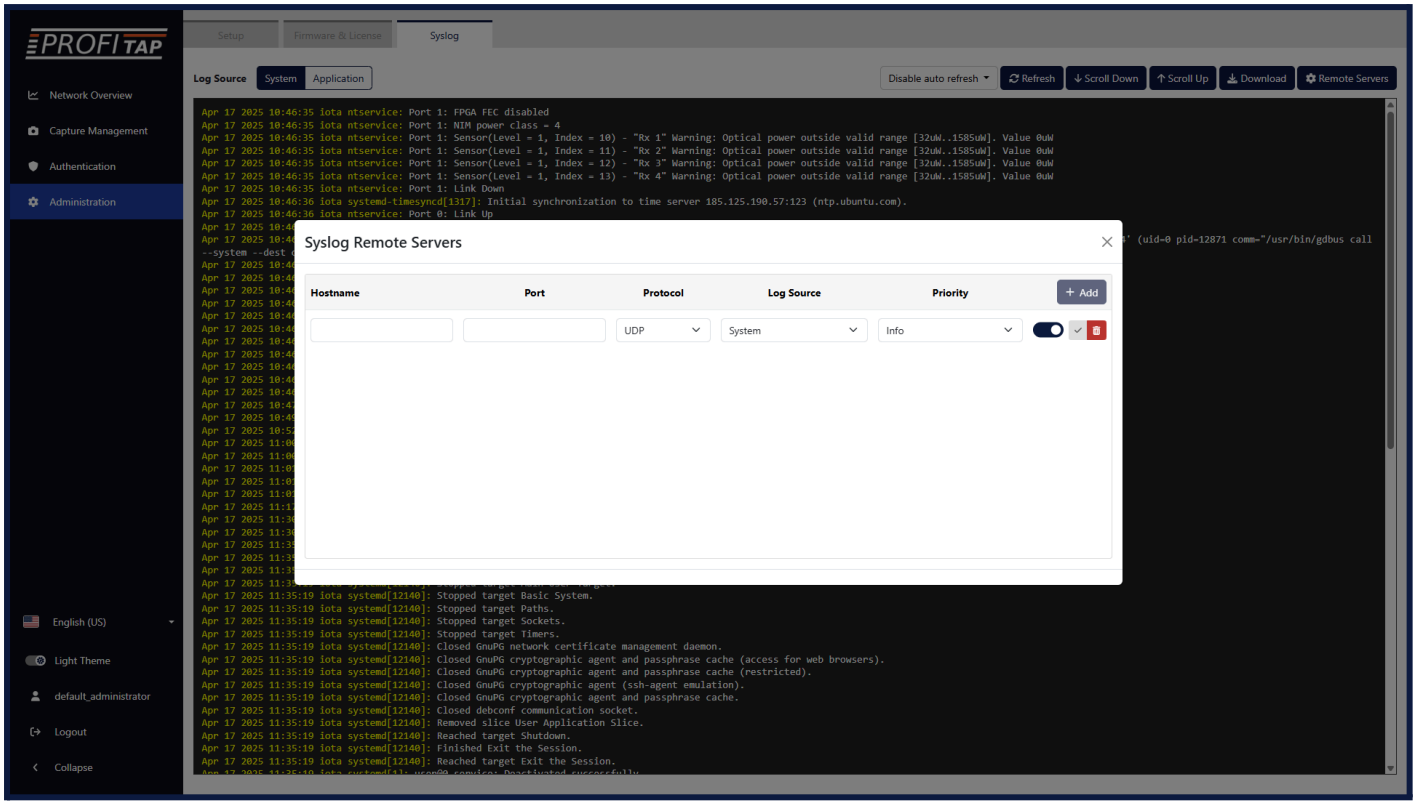
The **Administration > Syslog** page displays the logs of the IOTA system and application.



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.



On this page, the displayed logs can be manually refreshed or set to auto-refresh. They can be downloaded via the *Download* button. It is also possible to configure remote log collectors by clicking the *Remote Servers* button and using the view that appears to configure the remote logging server details. For each destination, it is possible to specify the type of logs priority and source to send.



3.2. Authentication

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

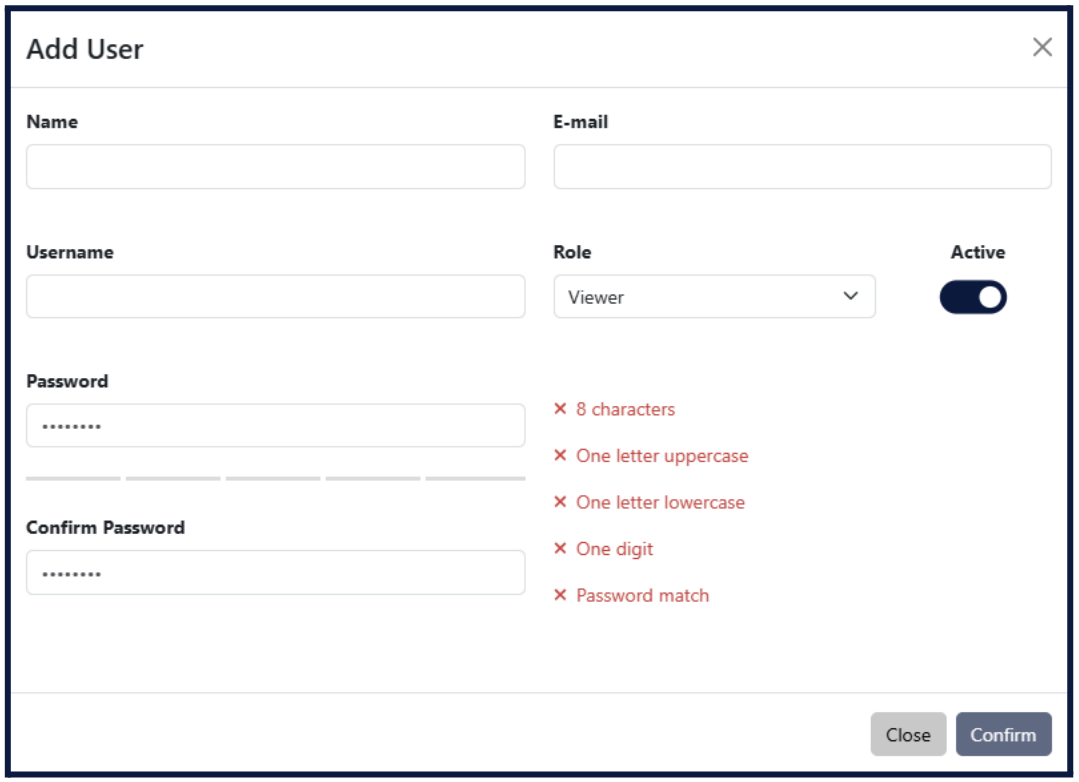
3.2.1. Local Users

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:

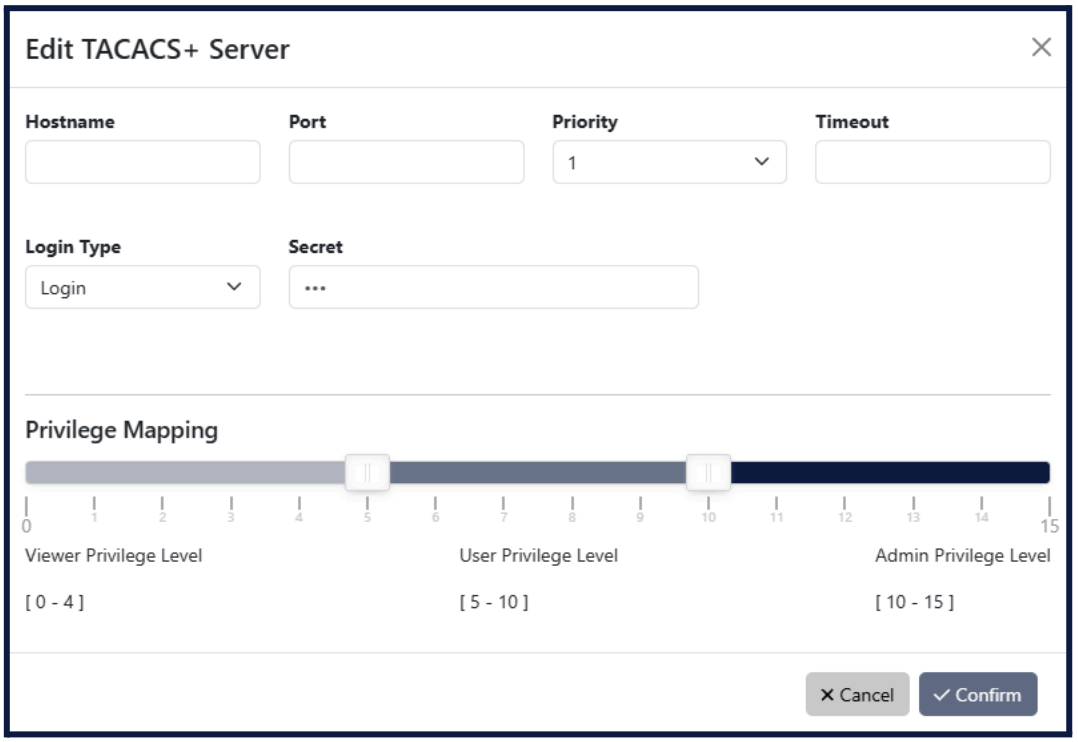
- 8 characters;
- one letter uppercase;
- one letter lowercase;
- one digit.



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).

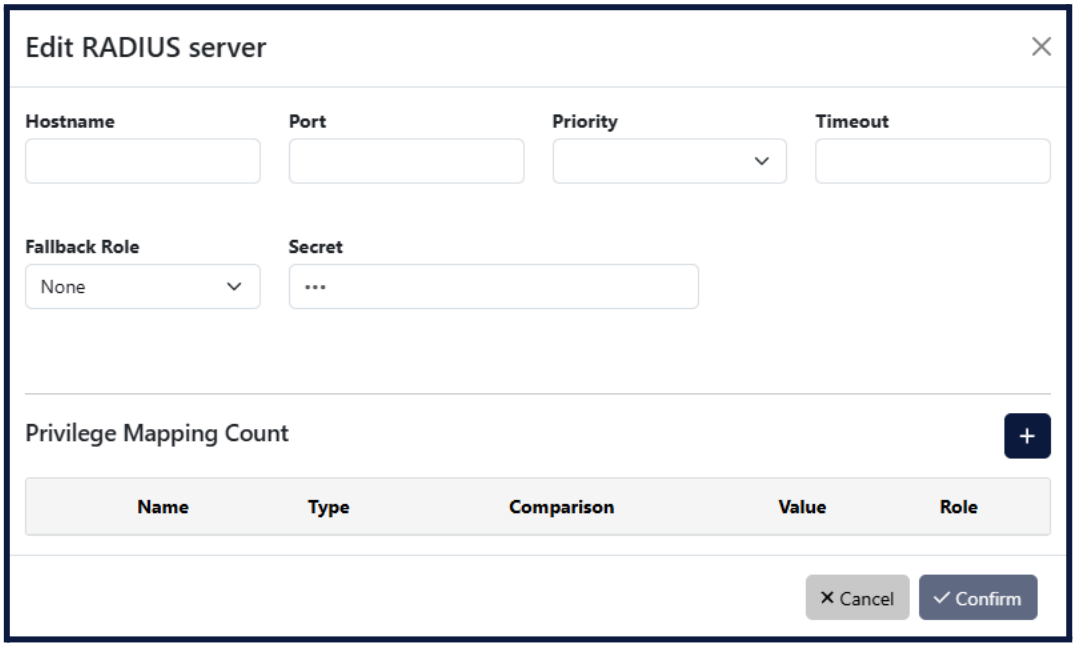


3.2.3. RADIUS

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).

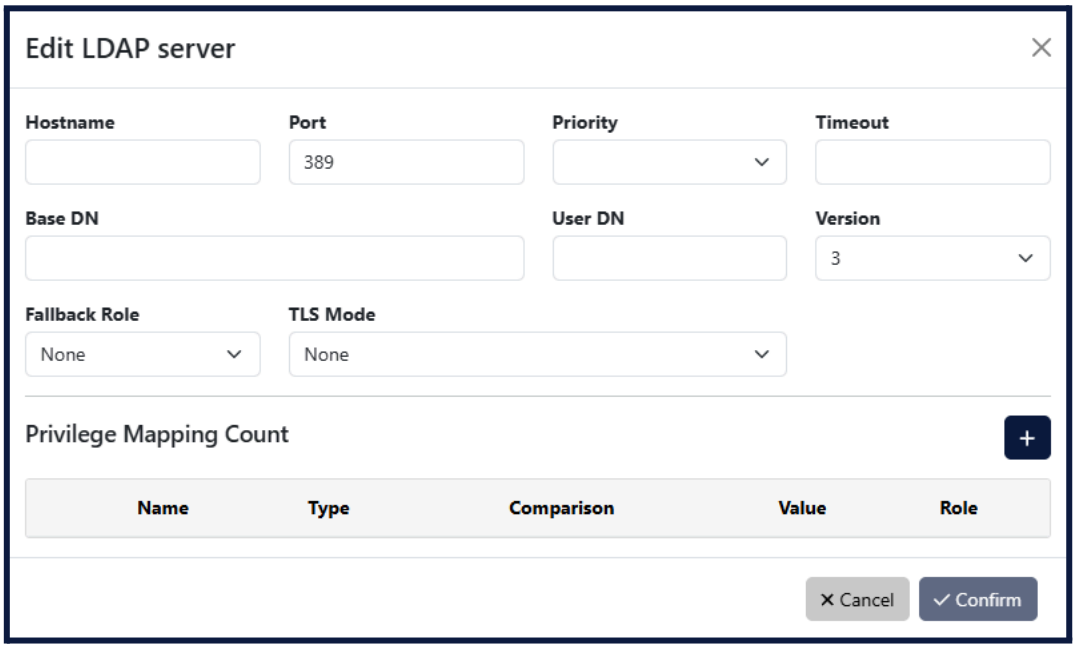


3.2.4. LDAP and LDAPS

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).



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.

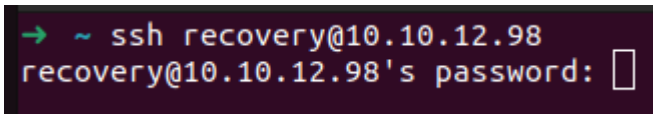
3.4.1. Accessing the CLI

The recovery CLI can be accessed by users with **administrator** privileges (both local users and AAA, see Authentication) either via SSH, or by connecting a monitor and a keyboard to the device.

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:



The other way of accessing the CLI is to connect a monitor to the IOTA device's VGA port and a keyboard to one of its USB ports, and then logging in using the credentials of a user account with administrator privileges in the appearing shell.

For example:

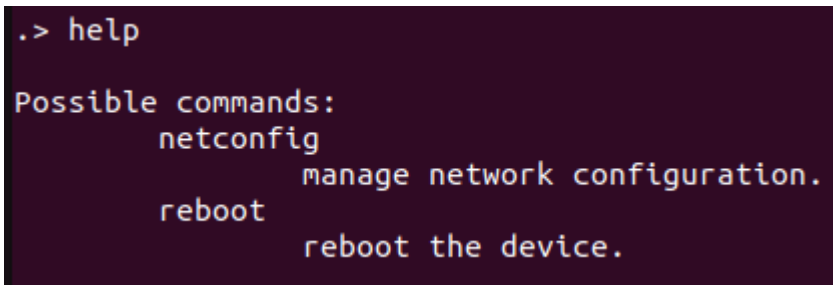
The first method will work if the IOTA device has correctly configured network settings. The second method will always work.

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



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]
```

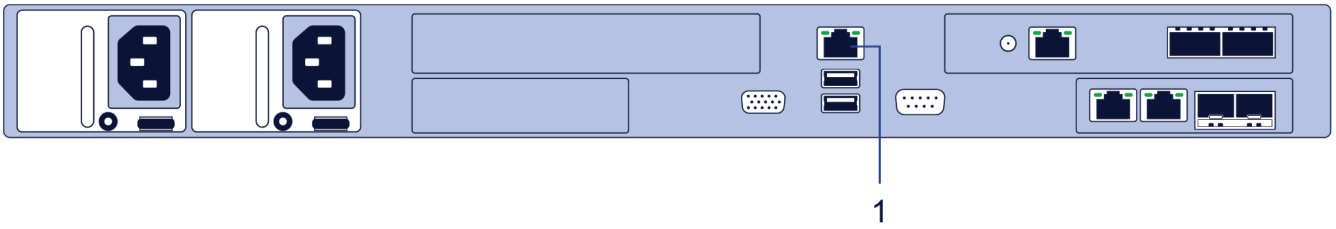
The following interfaces can be configured:

- **Management 1:** RJ45 1/10G
- **Management 2:** RJ45 1/10G
- **Management 3:** SFP+ 1/10G
- **Management 4:** SFP+ 1/10G

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

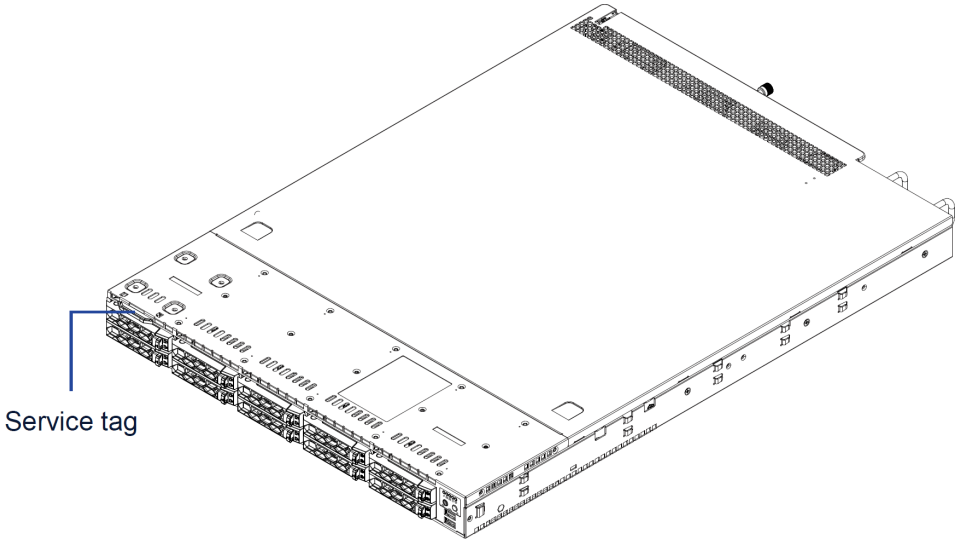
```
.> reboot
Are you sure you want to reboot the device? (yes/no)
```

3.5. BMC IPMI Access



Connect the device's IPMI port (**1** in the image above) to the network used to access the unit. The IPMI will attempt to get an IP address from a DHCP server. A static IP address can also be set in the device's BIOS.

The **IPMI MAC**, **username** and **password** can be found on the service tag accessible at the front of the unit.



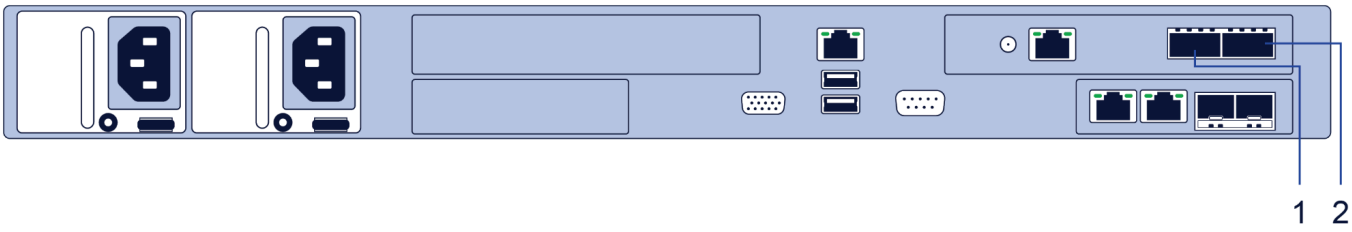
To access the BMC IPMI over the network, connect to the HTTPS interface by browsing to the IP address of the IPMI.

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

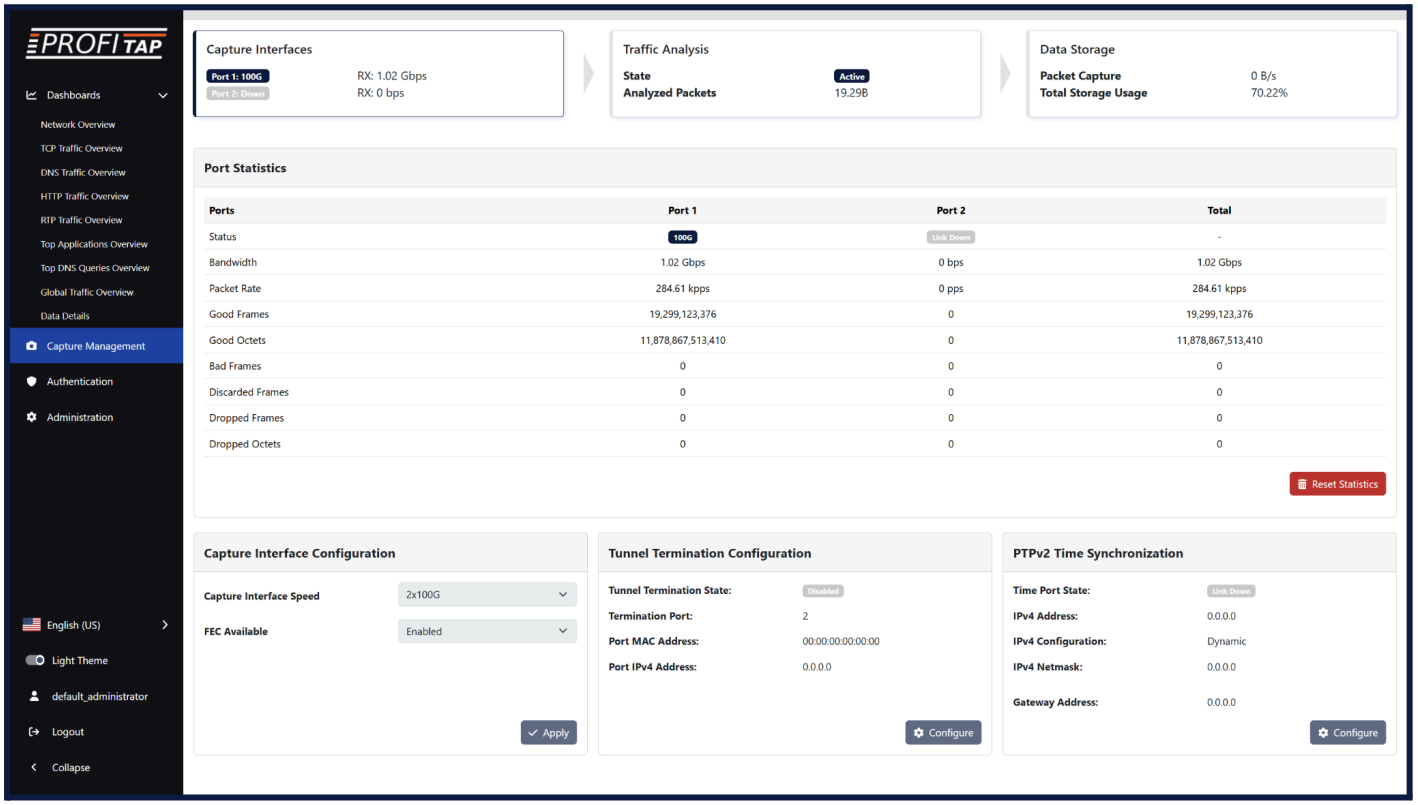
To log in, use the credentials mentioned above.

4. Capture Management

4.1. Capture Interfaces



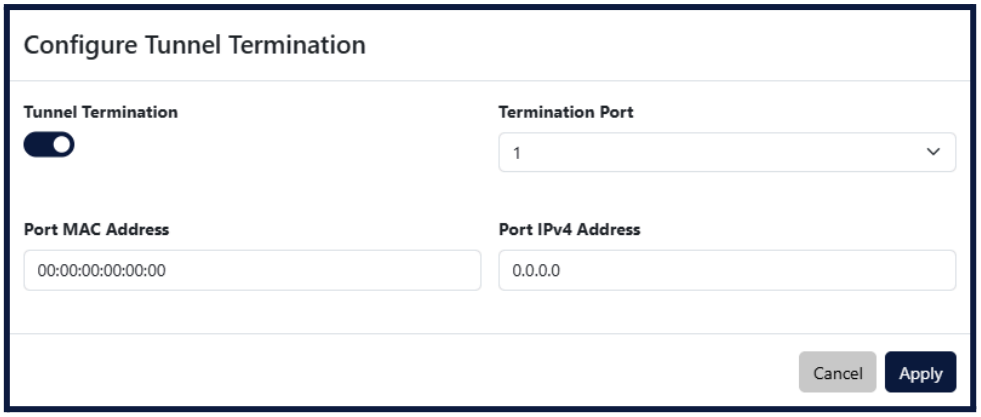
IOTA 100 CORE can capture out-of-band traffic incoming from TAPs, Network Packet Brokers, and switch SPAN ports. The unit features two 40/100G QSFP28 capture interfaces (**1** and **2** in the image above), and can capture 40/100G traffic from both of these interfaces at the same time, or from one interface when using breakout cables for 8 x 10G or 4 x 25G.



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

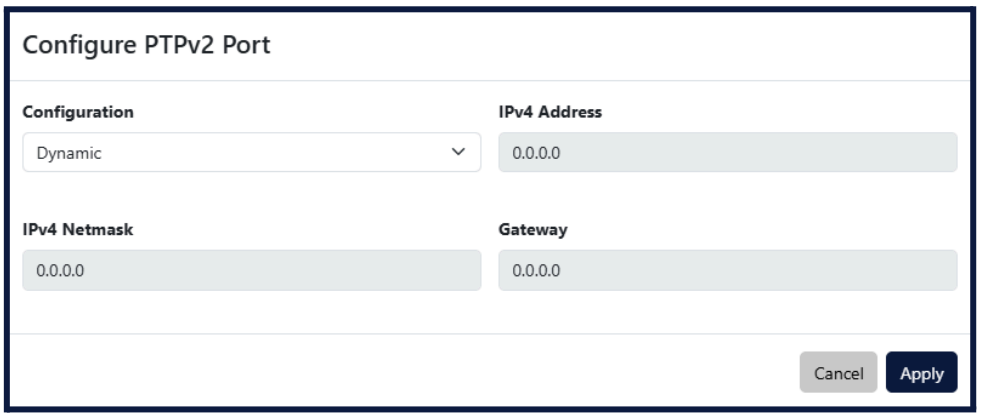
The **Capture Interface Configuration** section allows you to set the speed of the capture interfaces, and to enable or disable Forward Error Correction (FEC). Selecting 2x100G or 2x40G will set the speed of both capture ports 1 and 2 to 100G or 40G, and selecting 4x25G or 8x10G will set this speed on capture port 1 and disable capture port 2 (see Interfaces).

The **Tunnel Termination Configuration** section displays the state of the tunnel termination feature and provides the ability to configure it by clicking the *Configure* button. This feature allows the device to terminate GRE-TAP (L2GRE), ERSPAN type 2/3 and VXLAN tunnels.



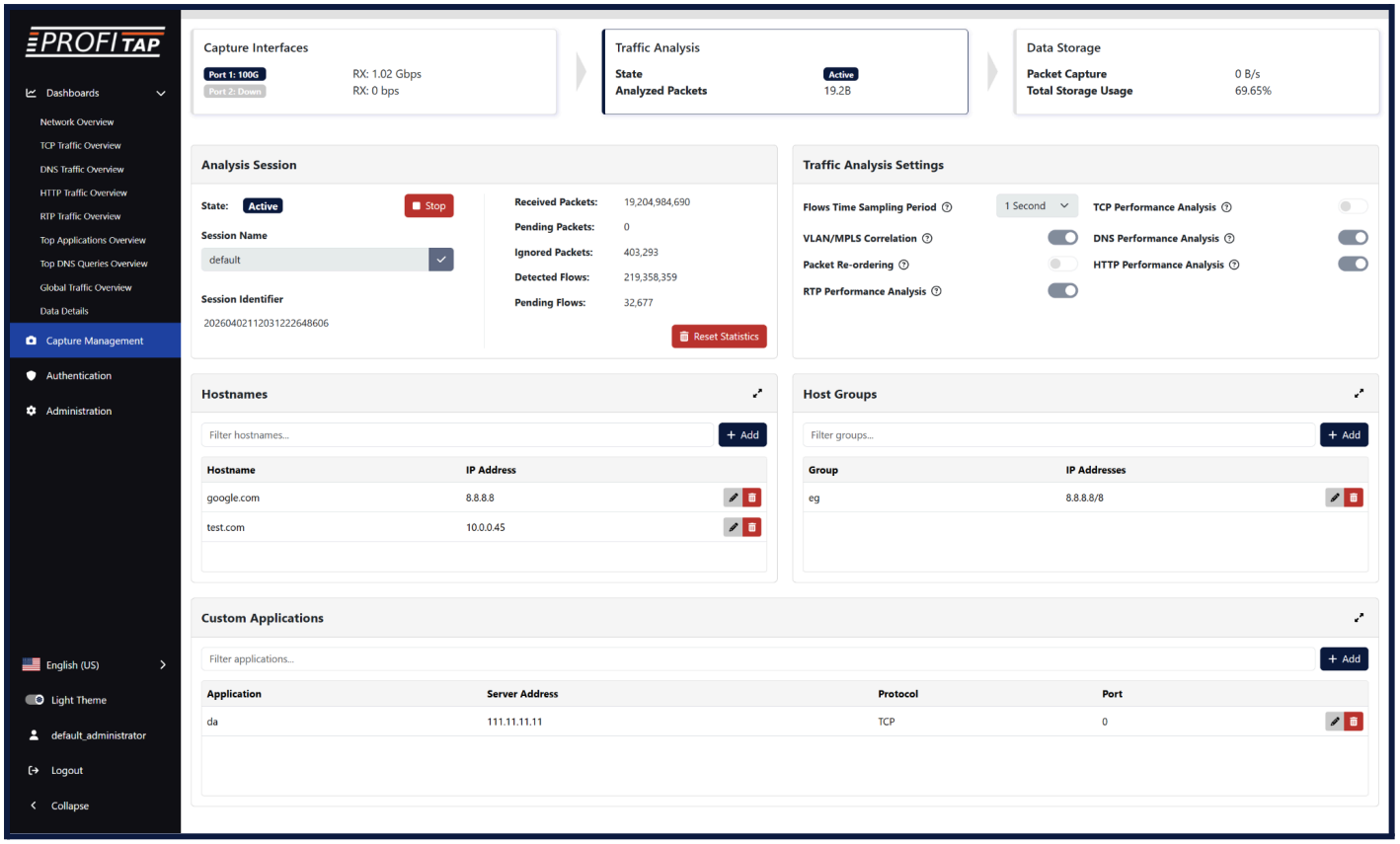
- **Tunnel Termination:** Enable or disable the tunnel termination feature.
- **Termination Port:** Select the capture interface on which to enable tunnel termination.
- **Port MAC Address:** MAC address of the capture interface.
- **Port IPv4 Address:** IPv4 address of the capture interface.

The **PTPv2 Time Synchronization** section displays the state of the PTPv2 time synchronization feature and provides the ability to configure the network settings of the interface by clicking the *Configure* button.



If *Configuration* is set to *Static*, the IP address, network mask and gateway can be set manually. If *Configuration* is set to *Dynamic*, the PTPv2 interface will attempt to receive network settings from a DHCP server.

4.2. Traffic Analysis



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.

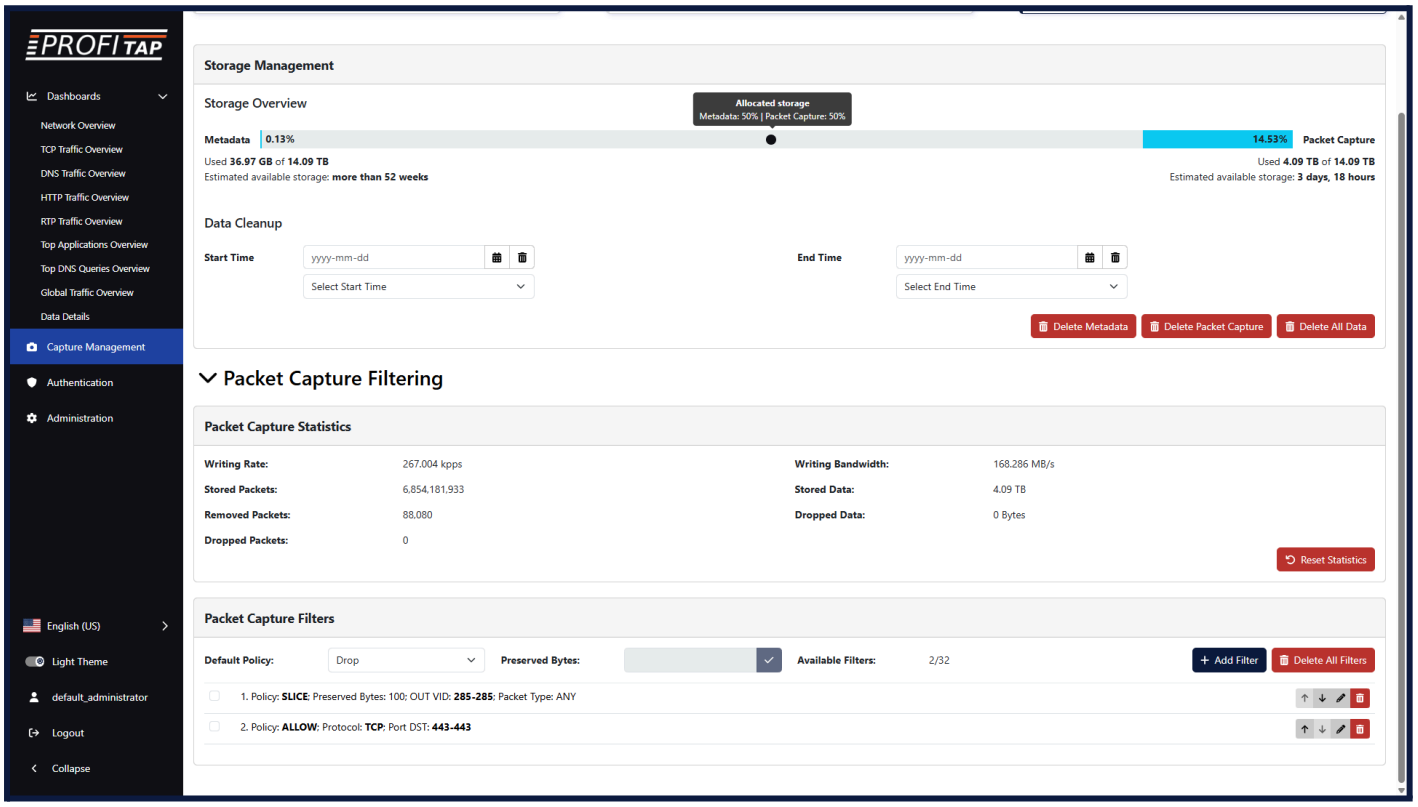
- **HTTP Performance Analysis:** When enabled, the analysis engine will generate HTTP performance metrics. This may impact analysis performance.
- **RTP Performance Analysis:** When enabled, the analysis engine will generate RTP performance metrics. This may impact analysis performance.

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 **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.

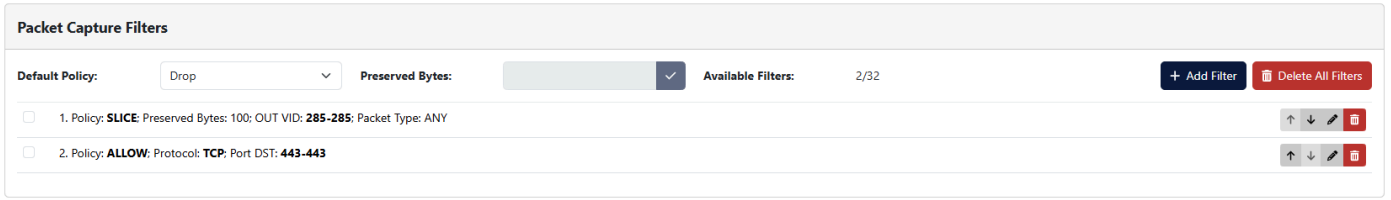
The cleanup of previously captured data is done by defining a start time and end time for the data to delete, then clicking the *Delete Metadata* button to remove metadata extracted from captured traffic, the *Delete Packet Capture* button to remove raw captured data, or the *Delete All Data* button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

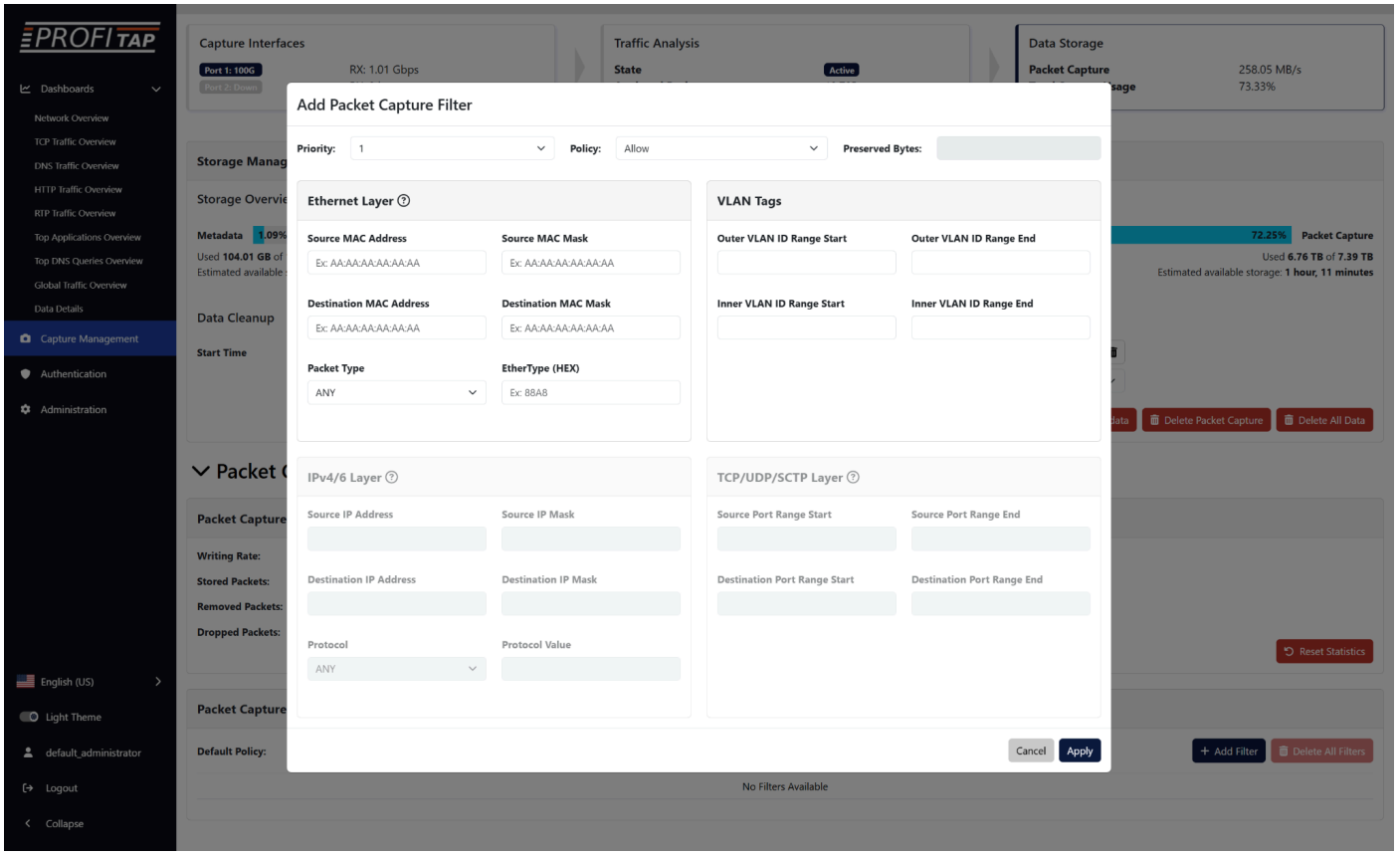


The *Default Policy* can be set to **Allow**, **Drop**, or **Slice**:

- **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:

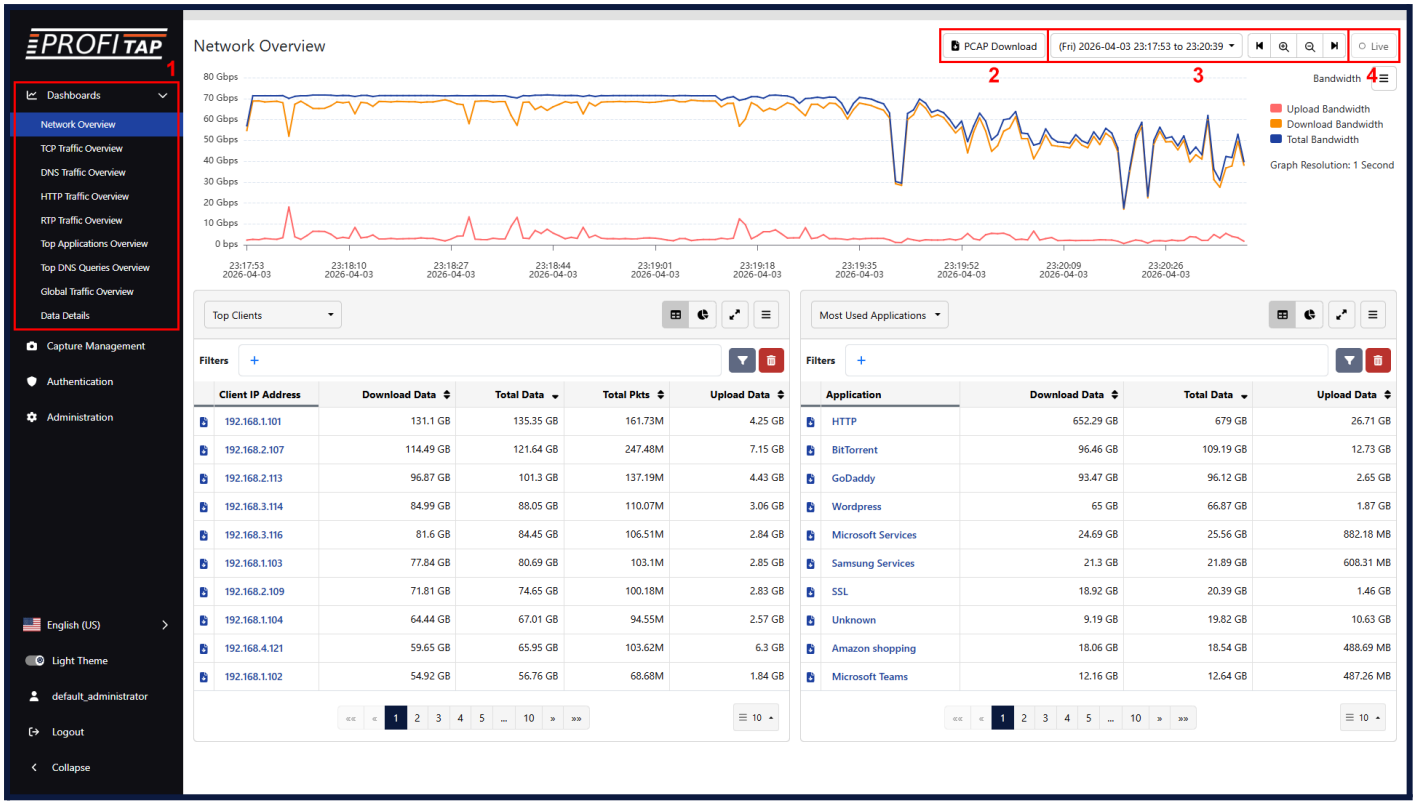
- **Ethernet Layer**
  Only frames matching MAC details configured in this section will be targeted (Source/Destination MAC Address, Source/Destination MAC Mask), with the possibility to select the **Packet Type** (ARP, IPv4, IPv6, TCP (IPv4/6), UDP (IPv4/6), SCTP (IPv4/6), Custom Protocol (IPv4/6),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

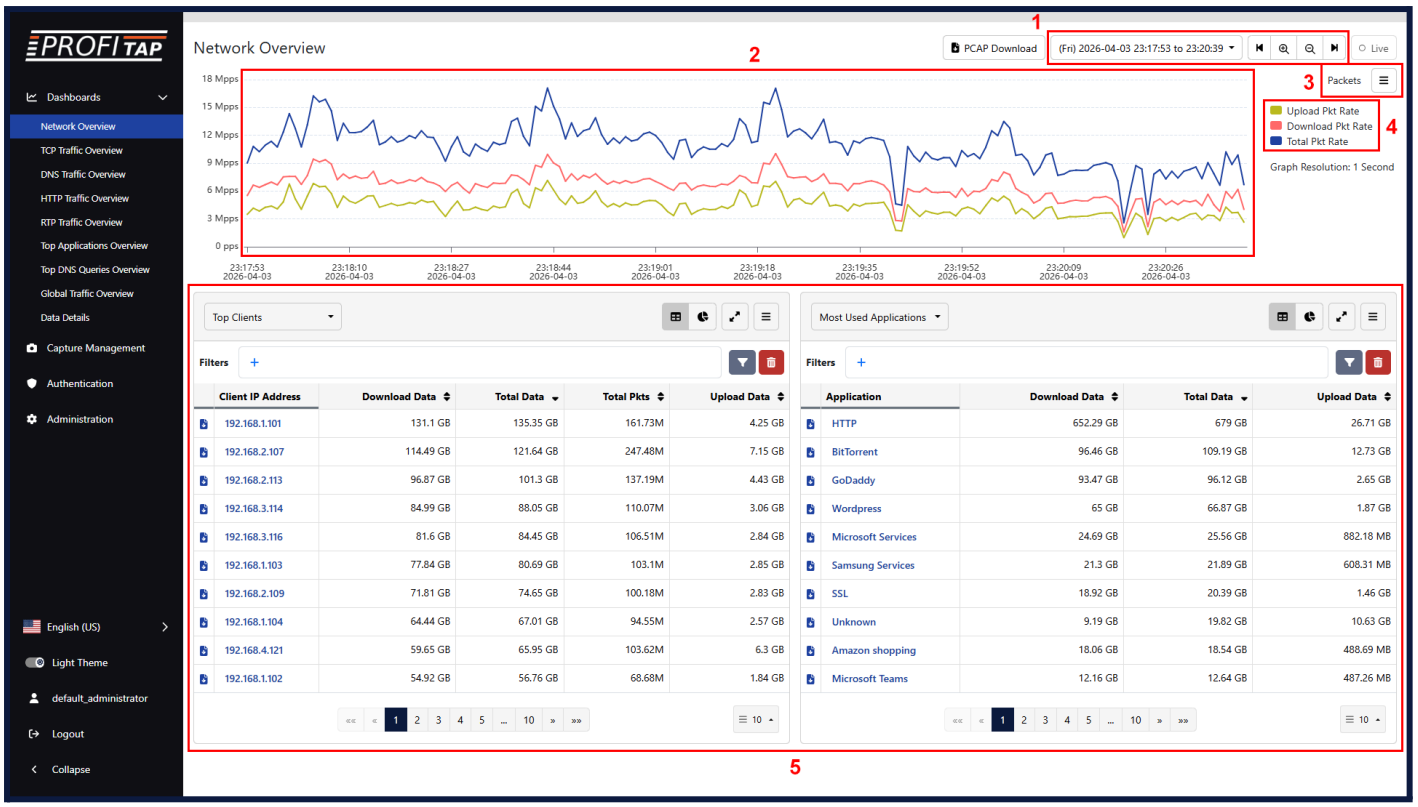


Network Overview dashboard - Bandwidth view

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.

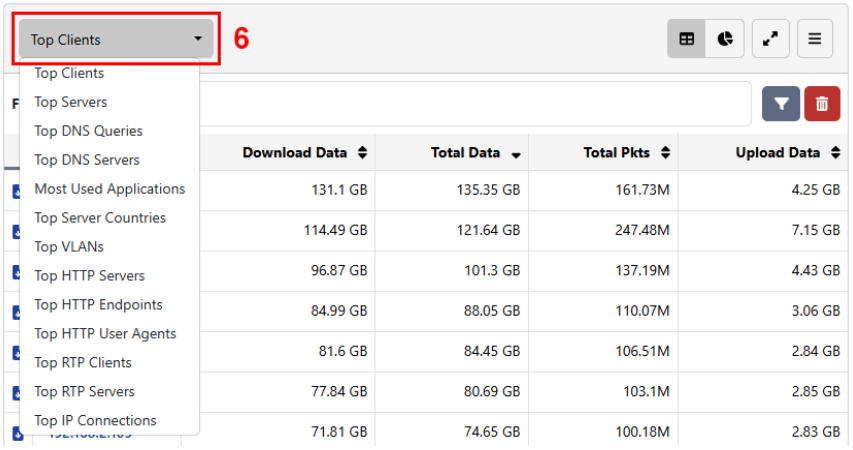
5.1. Network Overview



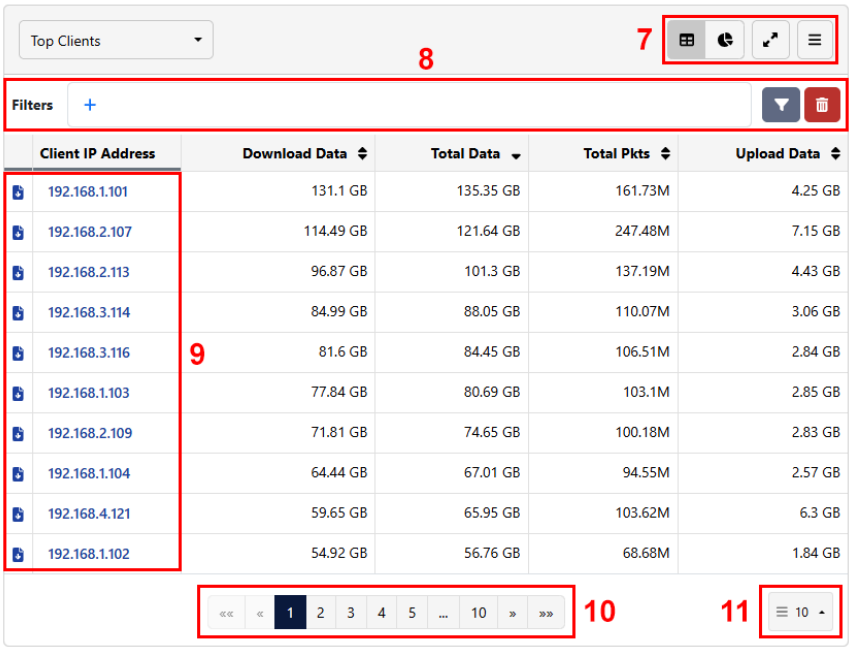
Network Overview dashboard - Packets view

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.

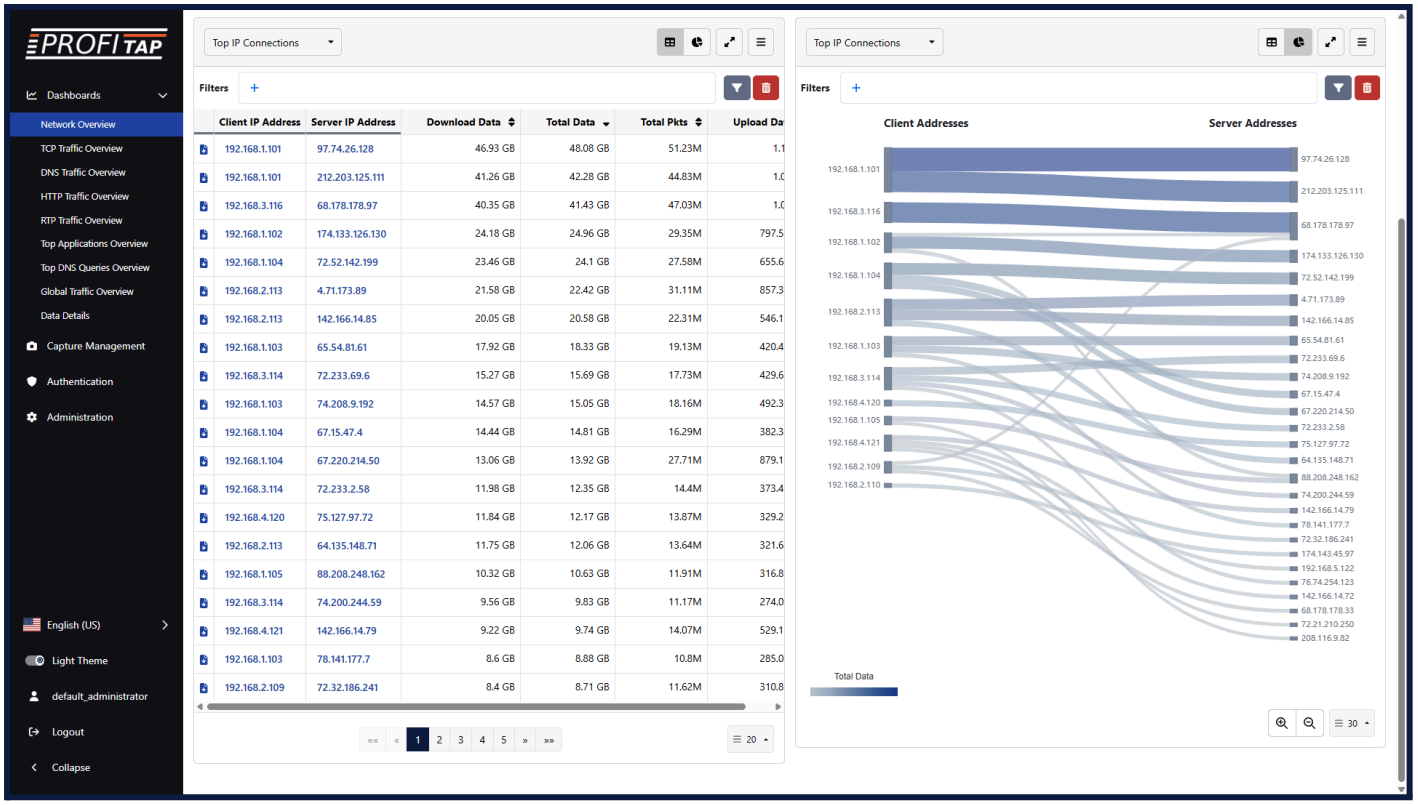
[1] You can select the time range in the top-right corner of the screen.
[2] You can also click and drag on the time graph itself to create a selection for a specific time range. You can click and drag this selection to move it along the time graph, and click and drag the edges of this selection to adjust 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 *Bandwidth* and *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.



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



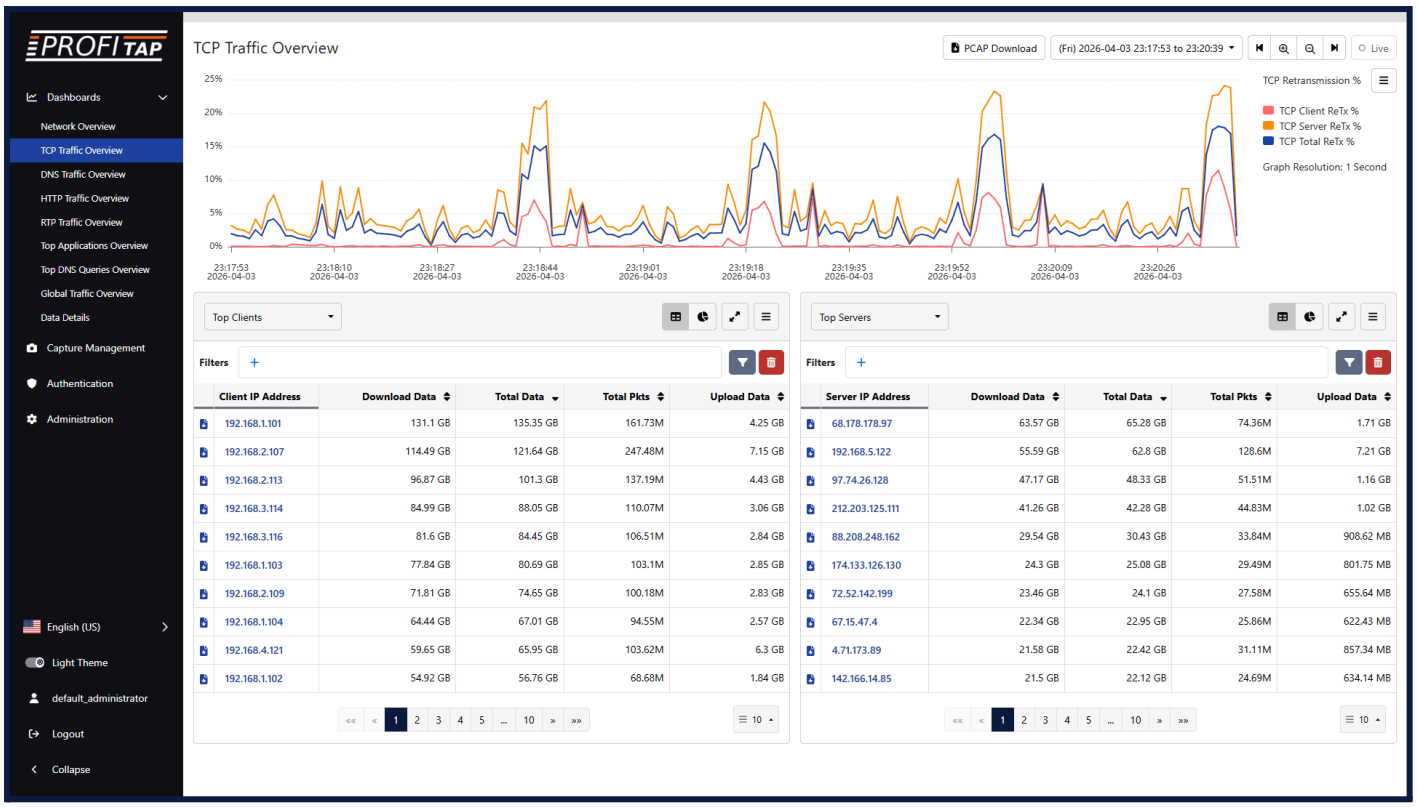
[7] In the top-right corner of each section, the view can be changed between table view and diagram view using the two leftmost buttons. The *Expand/Collapse* button toggles the width of the section between half-width and full-width. The rightmost button open a menu for selecting the metrics to display. 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



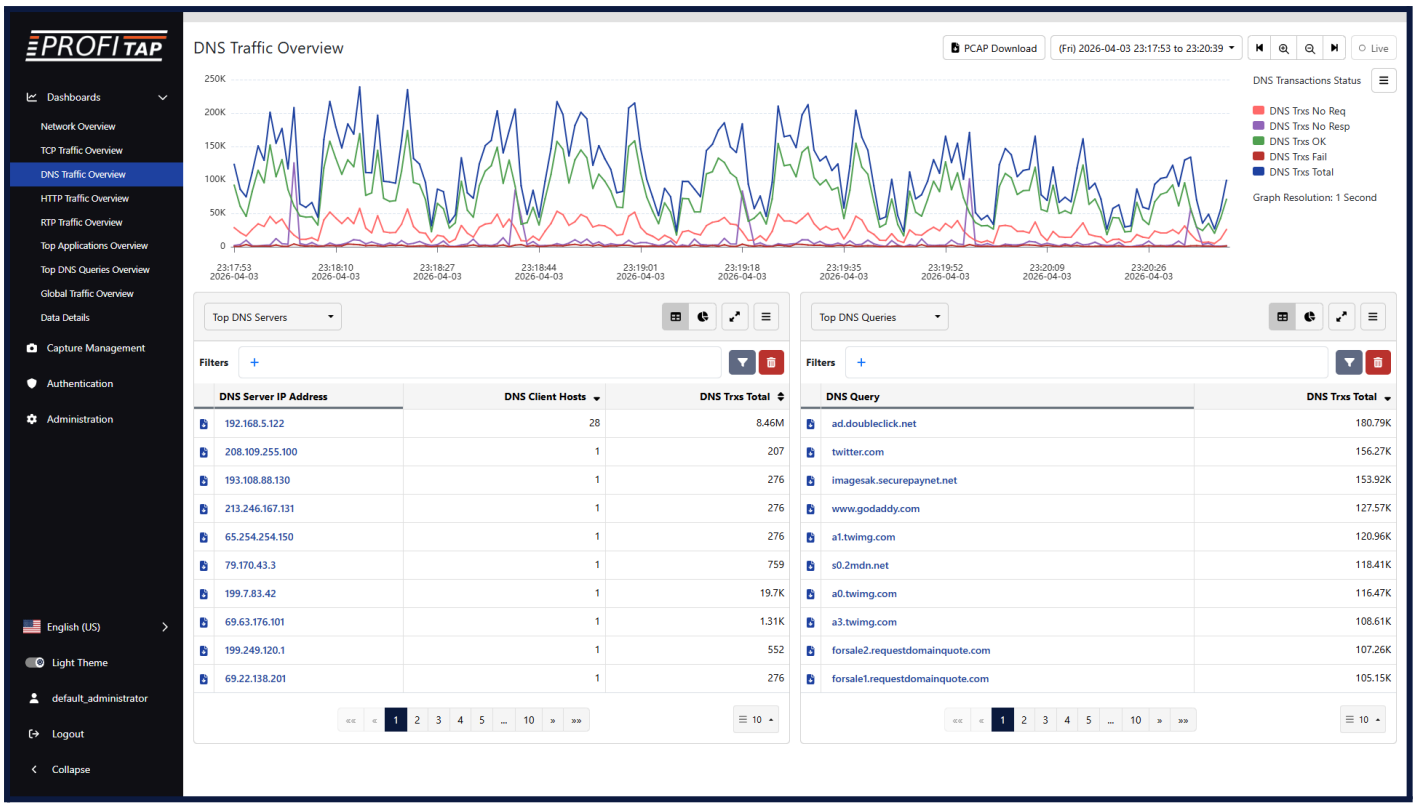
TCP Traffic Overview dashboard

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

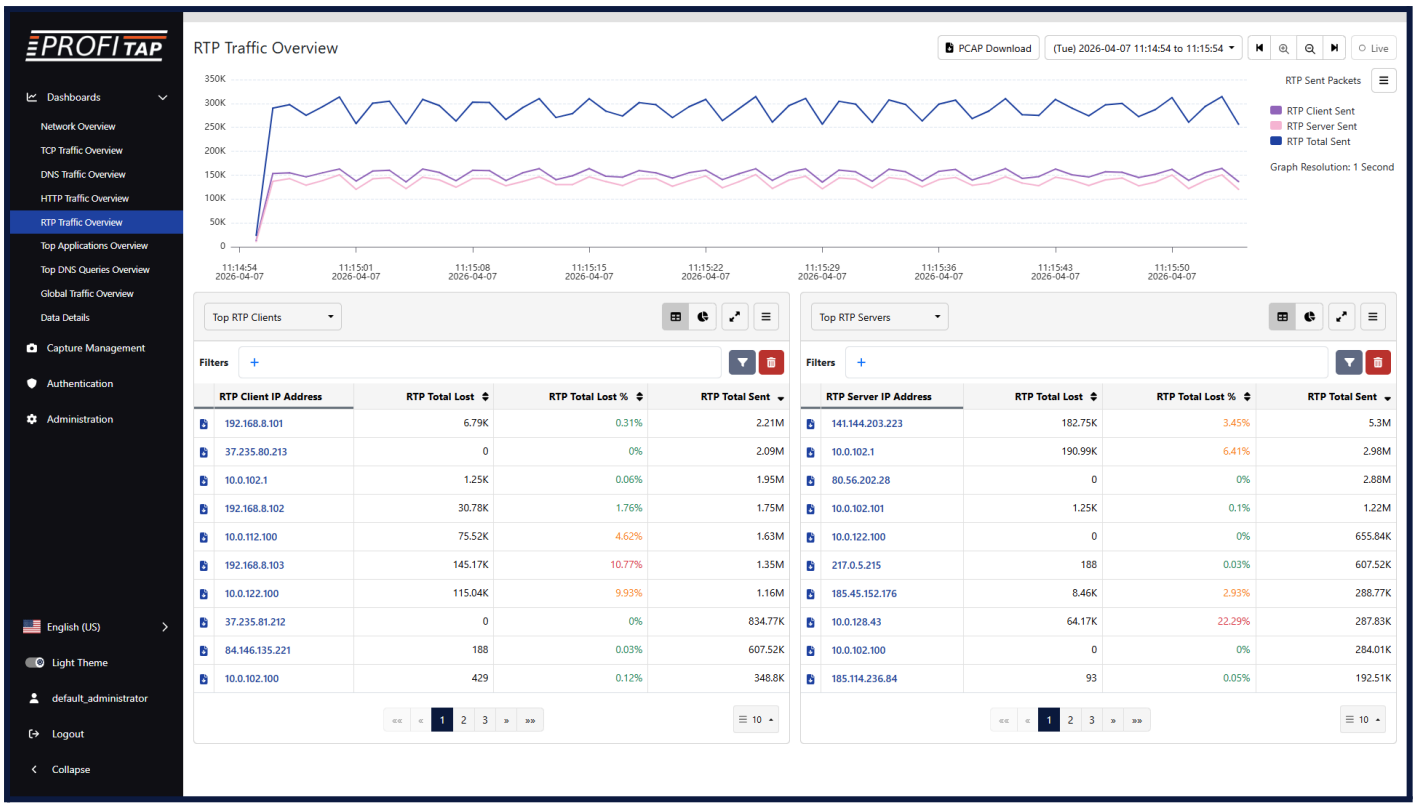
HTTP Traffic Overview dashboard

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



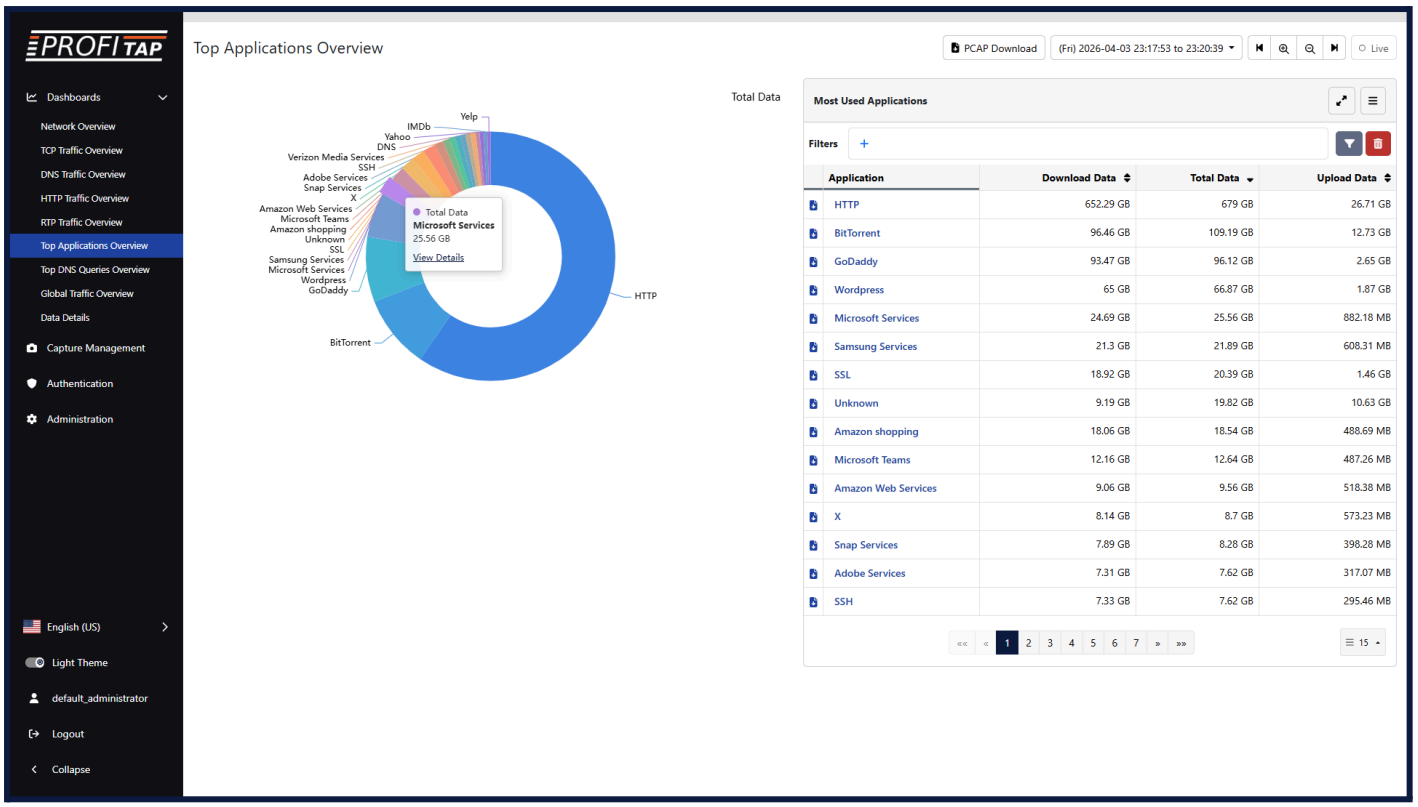
RTP Traffic Overview dashboard

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



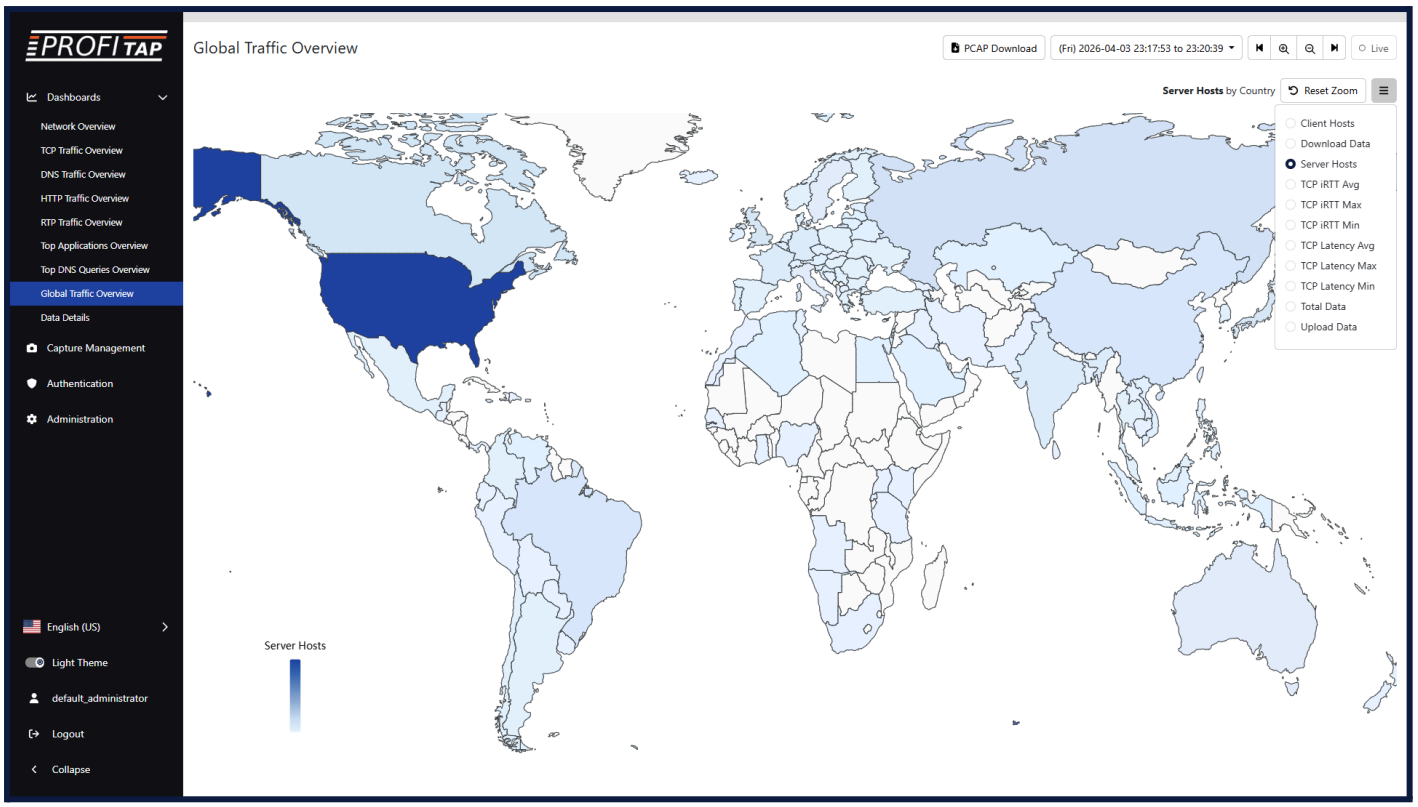
Top Applications Overview dashboard

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.

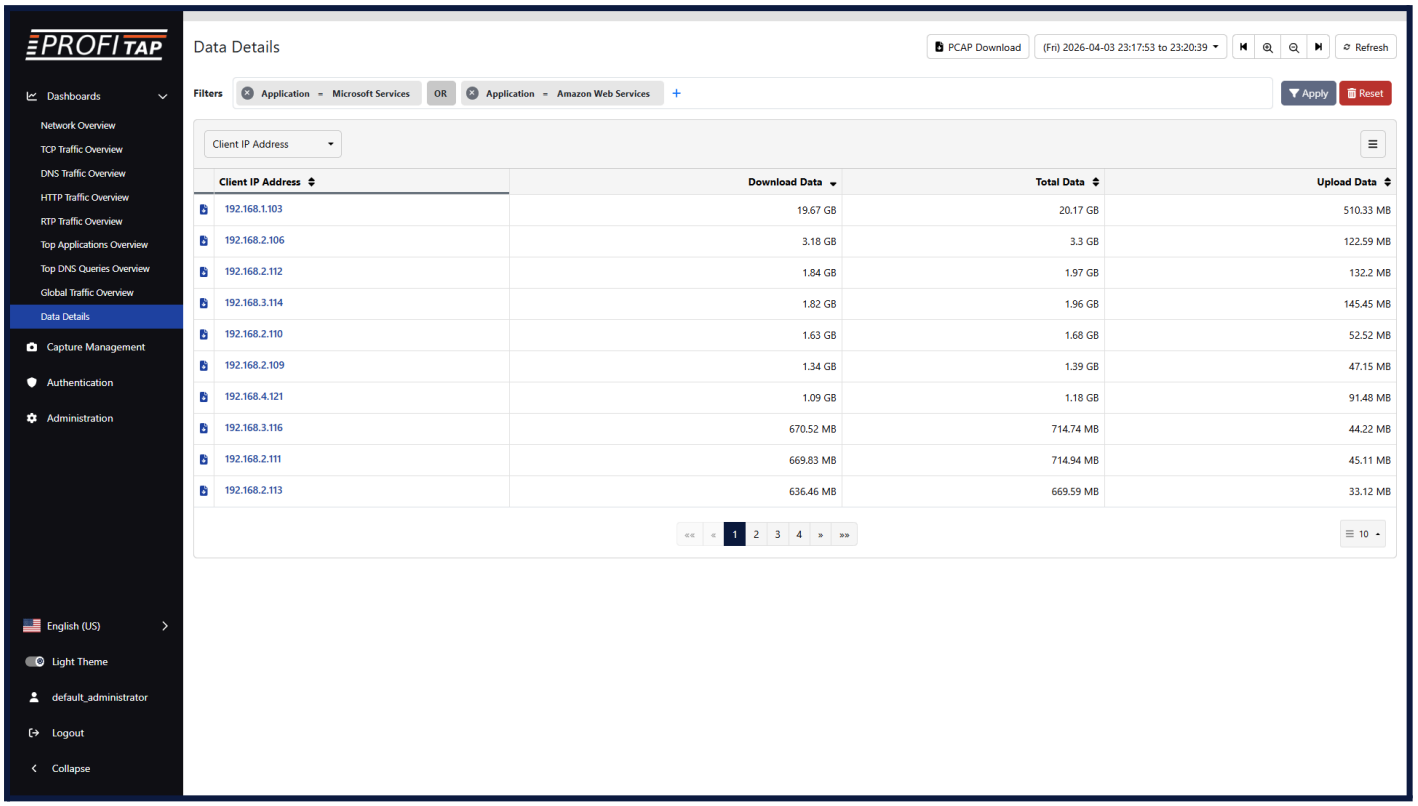
The metric to target can be changed using the menu in the top-right corner of the map.

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.



Data Details dashboard

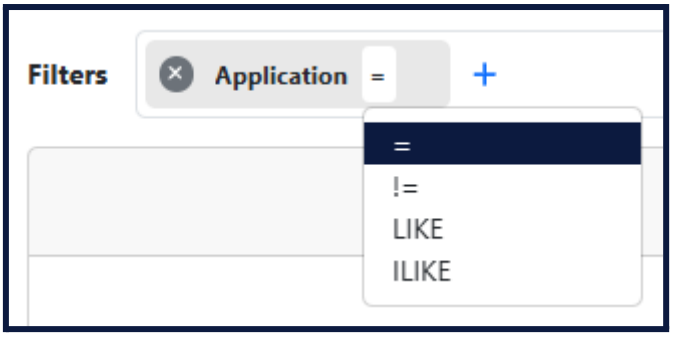
5.8.1. Filters

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

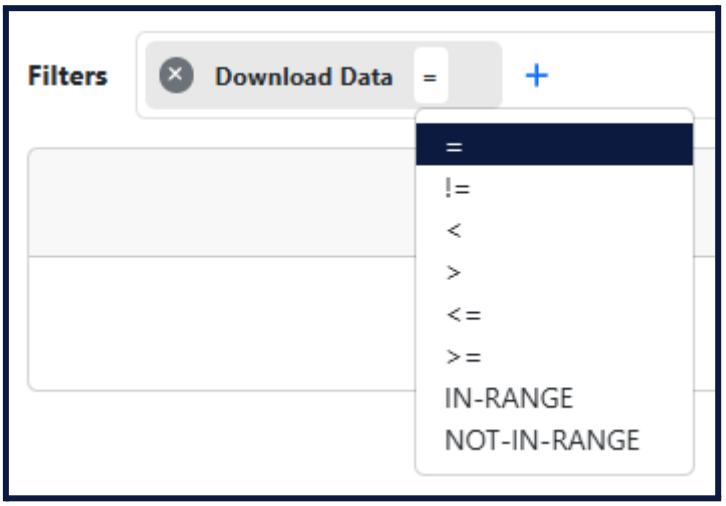
To add a filter, click the + button and select a filter parameter from the list, after which a list of possible values to choose from will be displayed (this can take a few seconds to appear depending on the amount of data). Select a value from the list or type one in.

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.

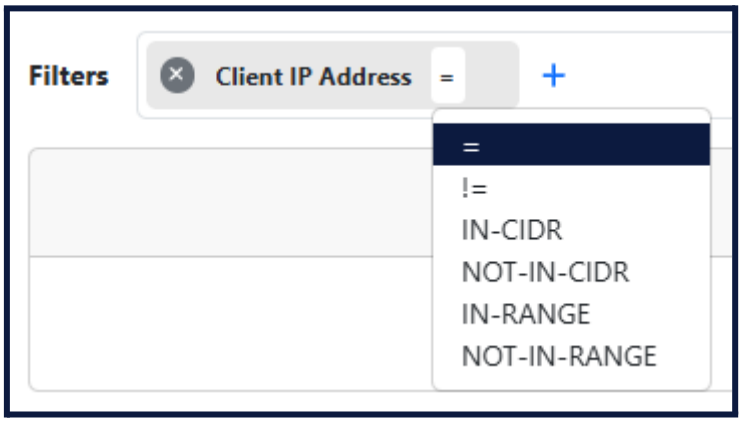
Alphanumeric filter parameters provide the *LIKE* operator for case-sensitive matching and *ILIKE* for case-insensitive matching.



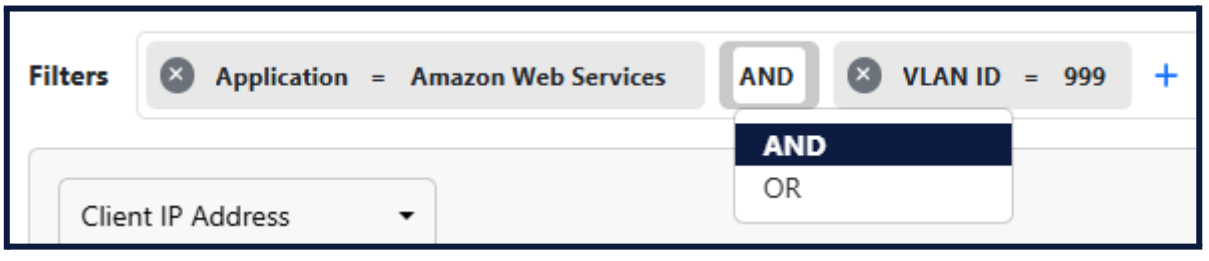
Numeric filter parameters provide the *less-than*, *greater-than*, *less-than-or-equal-to*, *greater-than-or-equal-to*, *IN-RANGE*, and *NOT-IN-RANGE* operators.



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



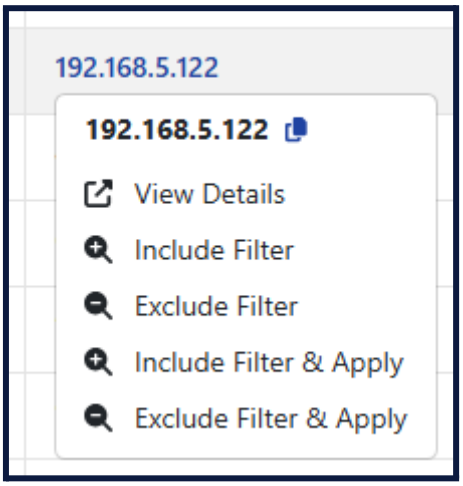
When adding more than one filter, the operator between filters can be changed between *AND* and *OR*.



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

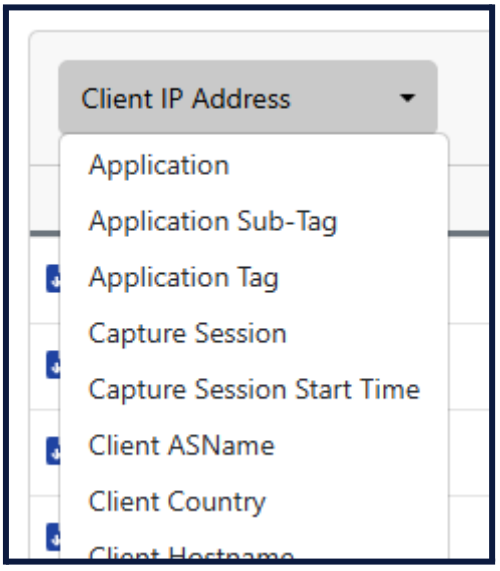
Click the *Apply* button to query the database and display data matching the selected filters and time range. Click the *Reset* button to clear the filters.

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.

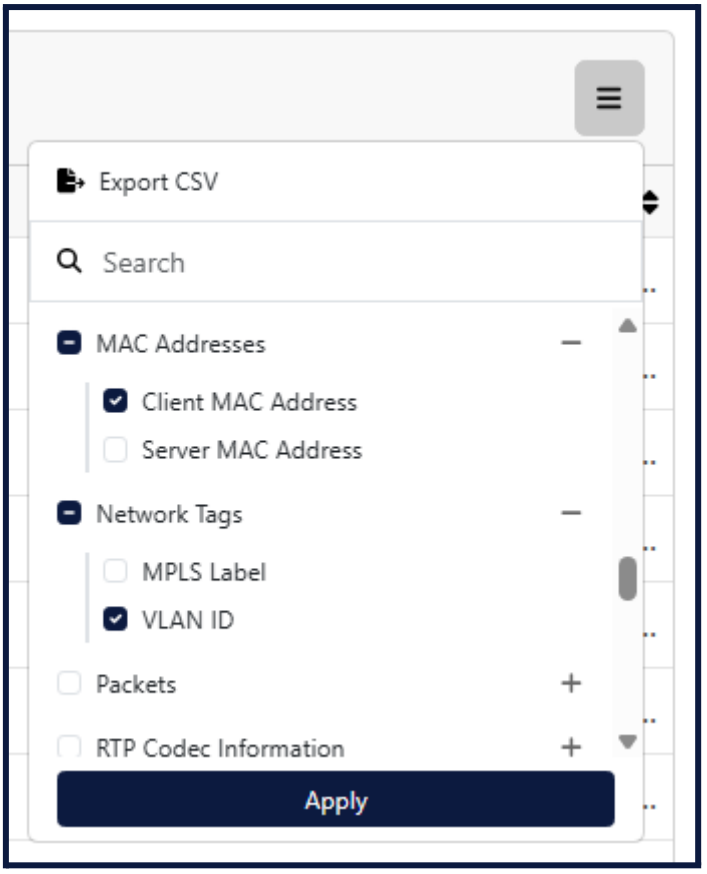


5.8.2. Table

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 navigate between pages.

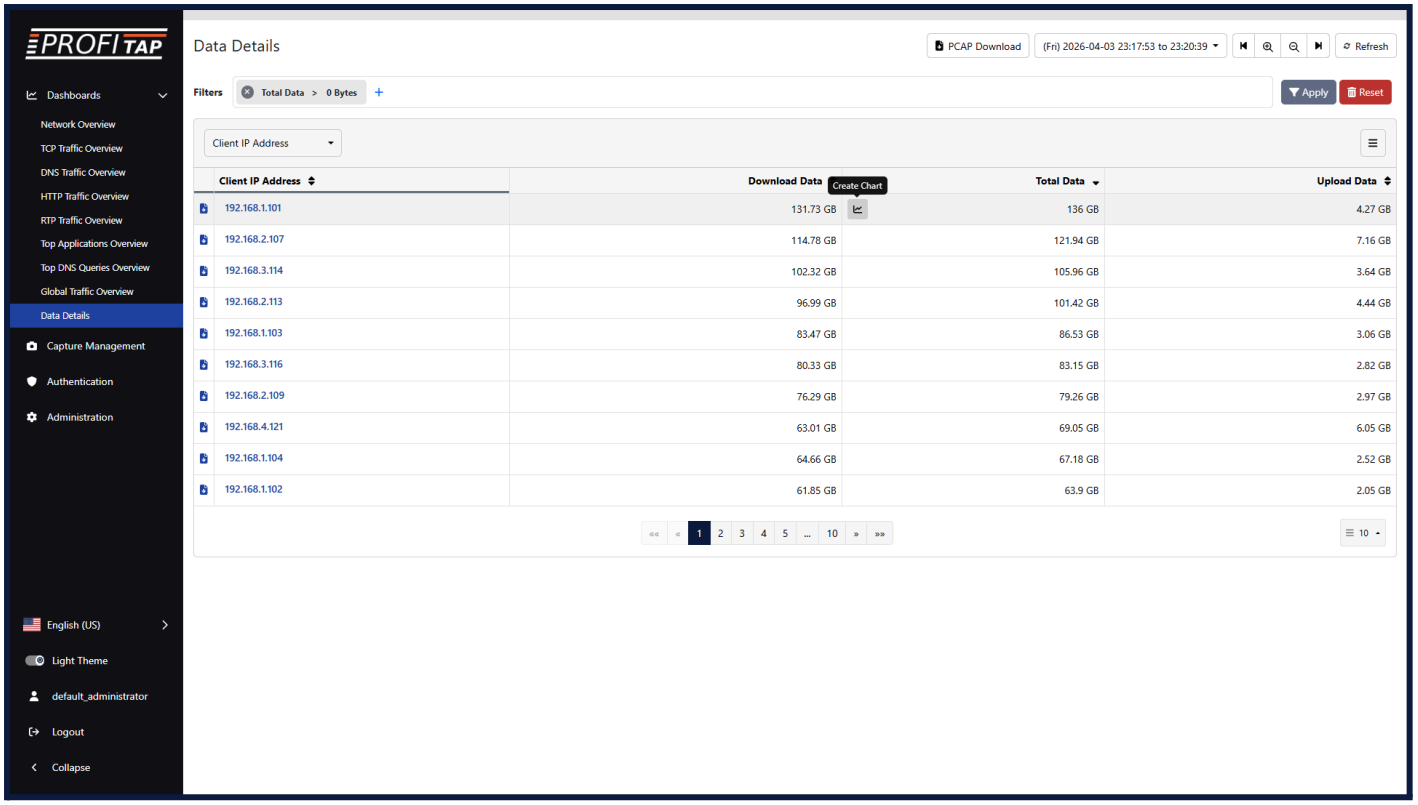
The number of entries displayed on each page of the table can be selected in the bottom-right corner.

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

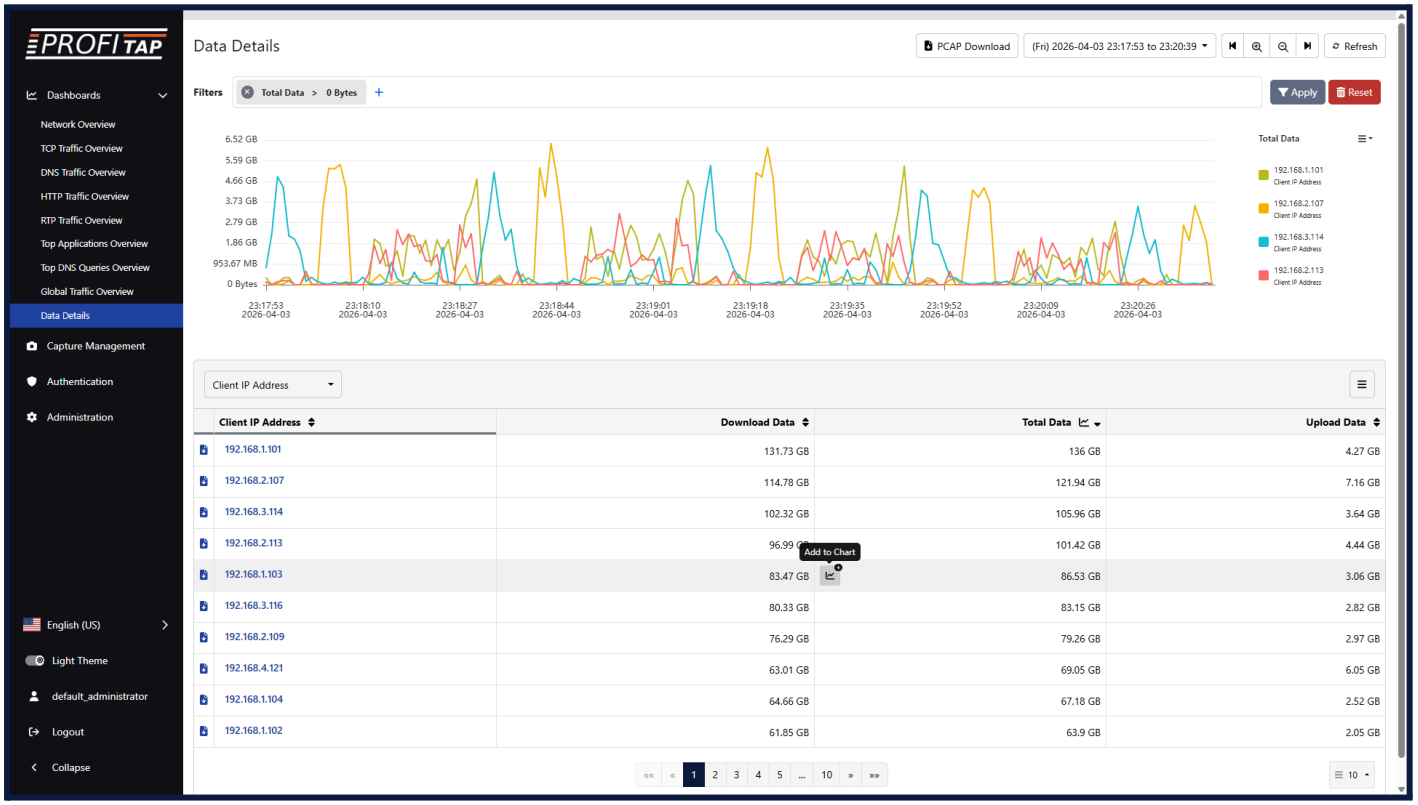
The *PCAP Download* button in the top-right corner of the page allows you to download the accumulated traffic for all displayed entries in the selected time range.

5.8.3. Time graphs

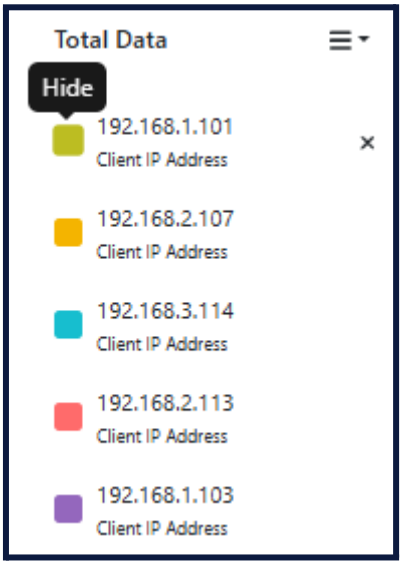
Hovering certain values in the table gives the option to create a time graph for tracking the selected metric over time for the selected primary parameter entry. Up to 3 time graphs can be created, for 3 different metrics.



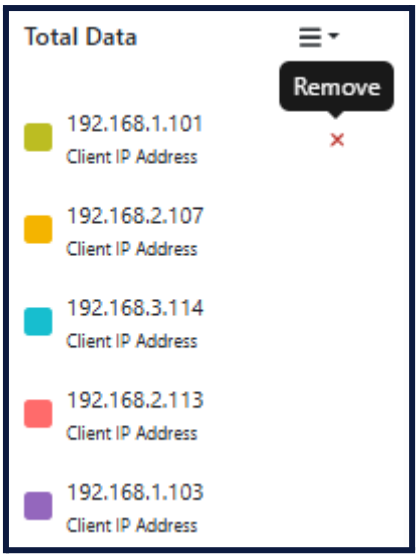
With a time graph created for a metric, hovering the value of a different entry for that same metric allows you to add a line in the time graph for tracking that metric for that entry. Up to 5 lines can be created.



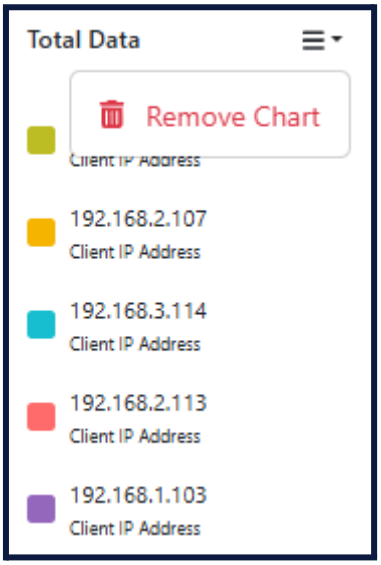
Click the square next to each parameter to show or hide the corresponding line on the time graph.



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

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