IOTA 10 CORE

USER MANUAL

IOTA software version: v5.3.0

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

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 C13 AC power cord
- 1 x power adapter (100-240 VAC to 12 VDC, 12.5 A, 150 W)
- 1 x rack mounting kit (including power adapter bracket)
- 4 x rubber feet

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

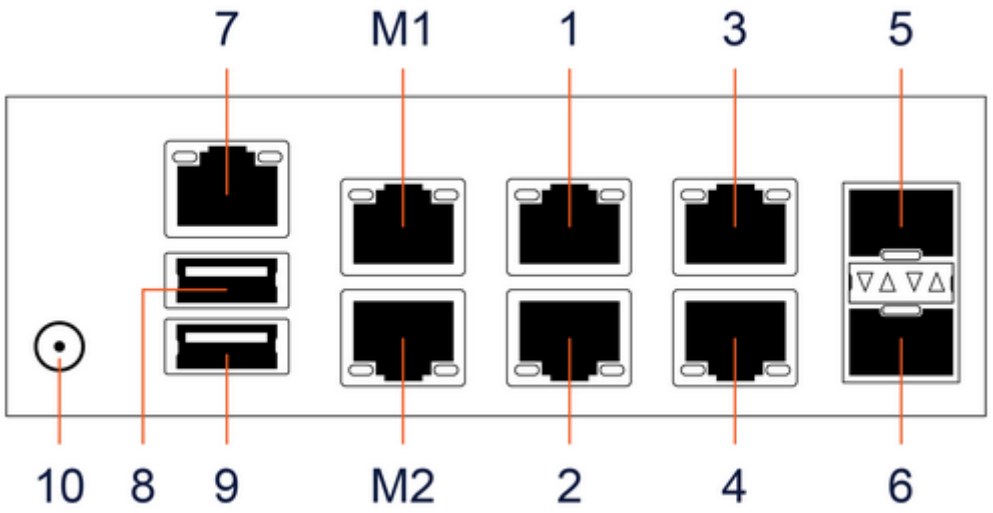
1.3. Specifications

	IOTA 10 CORE
Capture Interfaces	2 x 100M/1G RJ45 2 x 1/10G RJ45 2 x 10G SFP+
Capture Mode	Out-of-band
Supported Capture Speed*	100M / 1G / 10G
Capture Performance*	20 Gbps / 10 Mpps
Internal Storage	4, 8, or 16 TB SSD
Power Input	12 VDC
Power Adapter	100-240 VAC to 12 VDC, 12.5 A, 150 W
Management Interfaces	2 x RJ45 Ethernet 10/100/1000M
Management Service	HTTPS (server)
Additional Functions Interfaces	1 x RJ45 (IPMI) 2 x USB 3.0
Dimensions (WxDxH)	265 x 226 x 43 mm 10.43 x 8.9 x 1.69 in
Weight	2100 g 4.63 lb
Compliance	RoHS, CE, FCC, UKCA, EAC

* Maximum performance in ideal conditions. Packet size may affect these values.

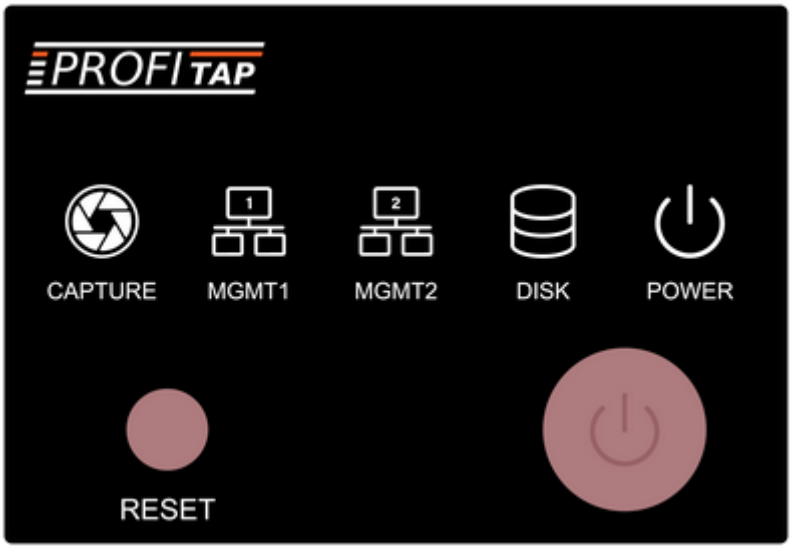
1.4. Interfaces & LED Behavior

1.4.1. Interfaces



M1, M2	Management ports 1 and 2 (RJ45 Ethernet)
1, 2	100M/1G RJ45 capture ports
3, 4	1/10G RJ45 capture ports
5, 6	10G SFP+ capture ports
7	IPMI port (RJ45 Ethernet)
8, 9	USB 3.0 ports
10	12 VDC power input

1.4.2. LED and Button Behavior



LEDs and Buttons	Description
Capture LED blinking	Device is capturing from one or more interfaces.
Capture LED blinking three times	Factory reset has been triggered.
Capture LED off	No capture is currently taking place.
Mgmt1 LED blinking	Activity on management port M1.
Mgmt2 LED blinking	Activity on management port M2.
Disk LED blinking	Disk activity.
Power LED on	Device is powered on.
Reset button	Reboots the unit.
Power button	Turns the unit on or off.

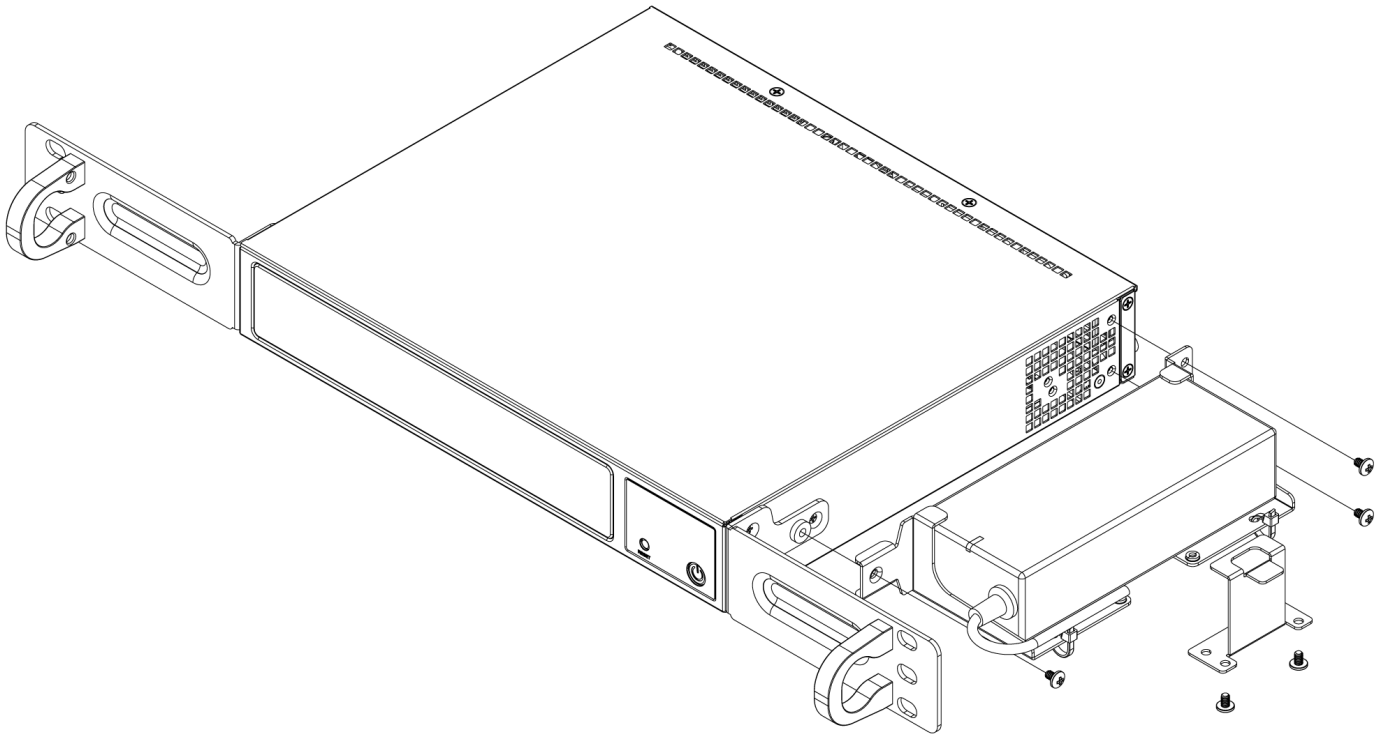
2. Getting Started

2.1. Deploying IOTA

2.1.1. Rack Mounting

IOTA 10 CORE can be mounted in a standard 19" rack, using the provided rack mounting kit.

1. Attach the rack brackets to either the front or back of the unit using the provided screws.
2. If you wish to use the power adapter bracket, place the power adapter in the bracket, then add and secure the retention bracket using the provided screws. Attach the power adapter bracket assembly to the unit using the provided screws.
3. Secure the chassis to the rack.
4. Make sure the rack is grounded properly.



2.1.2. Standalone

A set of rubber feet are included in the package if you wish to use IOTA 10 CORE outside of a rack.

2.1.3. Power and Connectivity

Power

Connect the provided power adapter to the unit's 12 VDC power input. Press the unit's power button to turn it on. The power LED will turn on.

Management interfaces

Connect management port M1 (see Interfaces) to the network used to access the unit. The management interface will attempt to get an IP address from a DHCP server. If it is unable to get an IP address over DHCP, the default fallback IP is 169.254.1.1 with netmask 255.255.0.0.

Network settings can be modified via the IOTA GUI (see Network Configuration) or by using the unit's USB ports.

To modify network settings via USB, create a file called **`iota_networking.json`**, place this file at the root of a USB drive, connect the USB drive to one of the unit's USB ports, and power on or restart the unit.

The **`iota_networking.json`** file should contain the desired network configuration. For instance, to set a static IP, use the following JSON content:

```
{
"dhcp_enabled": false,
"ip": "192.168.1.9",
"netmask": "255.255.255.0",
"gateway": "192.168.1.1",
"nameserver": "192.168.1.1"
}
```

Replace the information above with the desired network settings.

The possible network settings are as follows:

```
"dhcp_enabled": [true/false]
```

If set to "true", the device will attempt to get network settings from a DHCP server. Values for "ip", "netmask", "gateway" and "nameserver" are ignored in this case.

If set to "false", the device will not attempt to get network settings from a DHCP server. Values for "ip", "netmask", "gateway" and "nameserver" must be specified in this case.

```
"ip": "[IPv4 address]"
```

Sets a static IPv4 address if "dhcp_enabled" is set to "false".

```
"netmask": "[IPv4 netmask]"
```

Sets a static IPv4 subnet mask if "dhcp_enabled" is set to "false".

```
"gateway": "[IPv4 gateway]"
```

Sets a static IPv4 gateway if "dhcp_enabled" is set to "false".

```
"nameserver": "[IPv4 DNS]"
```

Sets a static IPv4 DNS if "dhcp_enabled" is set to "false".

```
"hostname": "[string]"
```

Changes the device's hostname.

```
"allow_internal_access": [true/false]
```

If set to "true", connections to the IOTA user interface from the subnetwork IOTA is located on are accepted. If set to "false", they are rejected.

```
"allow_external_access": [true/false]
```

If set to "true", connections to the IOTA user interface from subnetworks other than the one IOTA is located on are accepted. If set to "false", they are rejected.

```
"network_authentication_enabled": [true/false]
```

Enables or disables 802.1x authentication. If enabled, one and only one of the authentication methods' (MD5 or TLS) settings must be specified, as shown below.

802.1x EAP-MD5:

```
"network_authentication_md5":
{
"identity": "foobar",
"password": "barfoo"
}
```

802.1x EAP-TLS:

```
"network_authentication_tls":
{
"identity": "foobar",
"ca_cert": "foobar",
"client_cert": "foobar",
"private_key": "foobar",
"private_key_pw": "foobar"
}
```

Example of a complete **`iota_networking.json`** file:

```
{
"dhcp_enabled": false,
"ip": "192.168.1.9",
"netmask": "255.255.255.0",
"gateway": "192.168.1.1",
"nameserver": "192.168.1.1",
"hostname": "profitap-iota",
"allow_internal_access": true,
"allow_external_access": true,
"network_authentication_enabled": true,
"network_authentication_tls":
{
"identity": "foobar",
"ca_cert": "foobar",
"client_cert": "foobar",
"private_key": "foobar",
"private_key_pw": "foobar"
}
}
```

Capture interfaces

Connect RJ45 Ethernet cables from the line(s) from which to capture traffic to the RJ45 capture ports (ports 1, 2, 3, 4, see Interfaces).

Connect cables and SFP modules from the line(s) from which to capture traffic to the SFP cages (ports 5, 6, see Interfaces).

2.1.4. Accessing IOTA Over the Network

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>`**

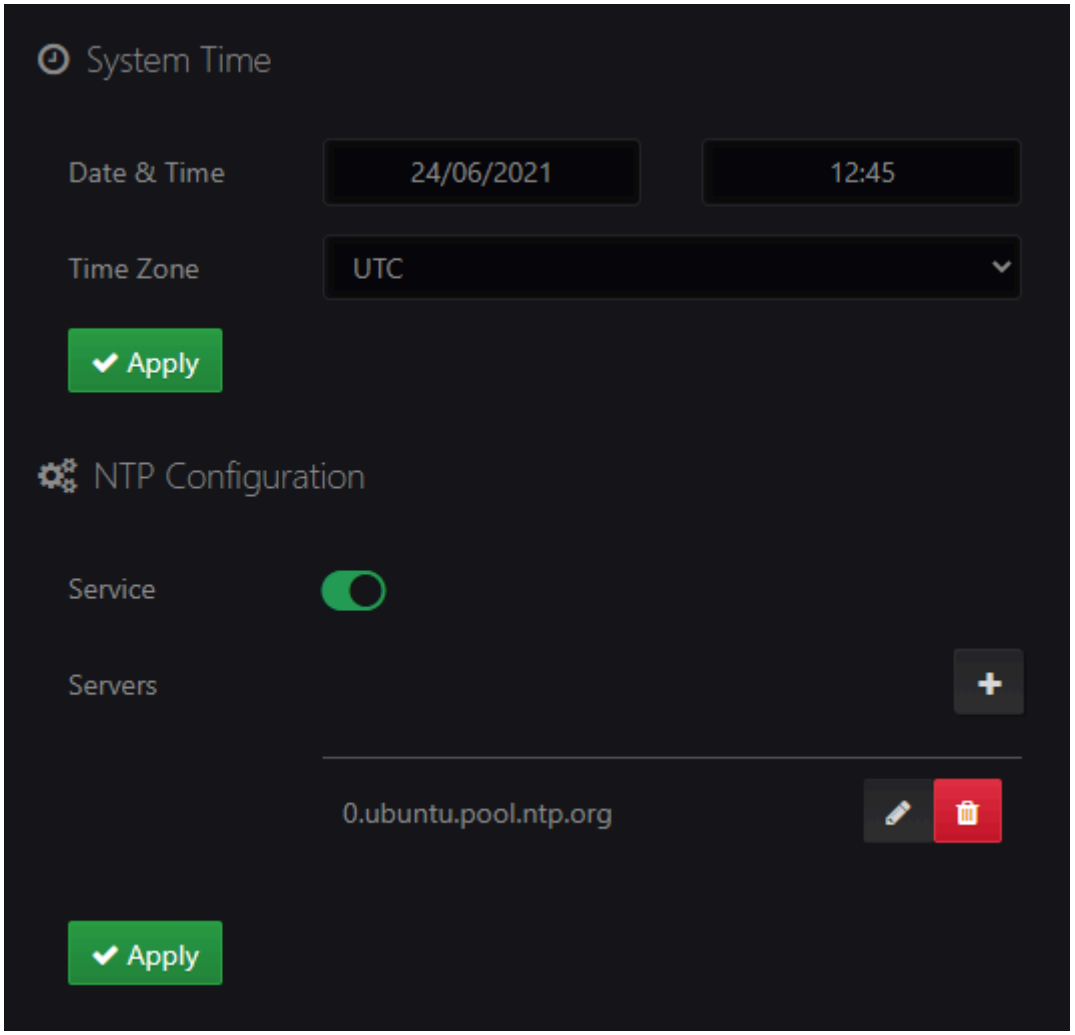
To login, use the following initial credentials:

Default username: **admin**
Default password: **admin**

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

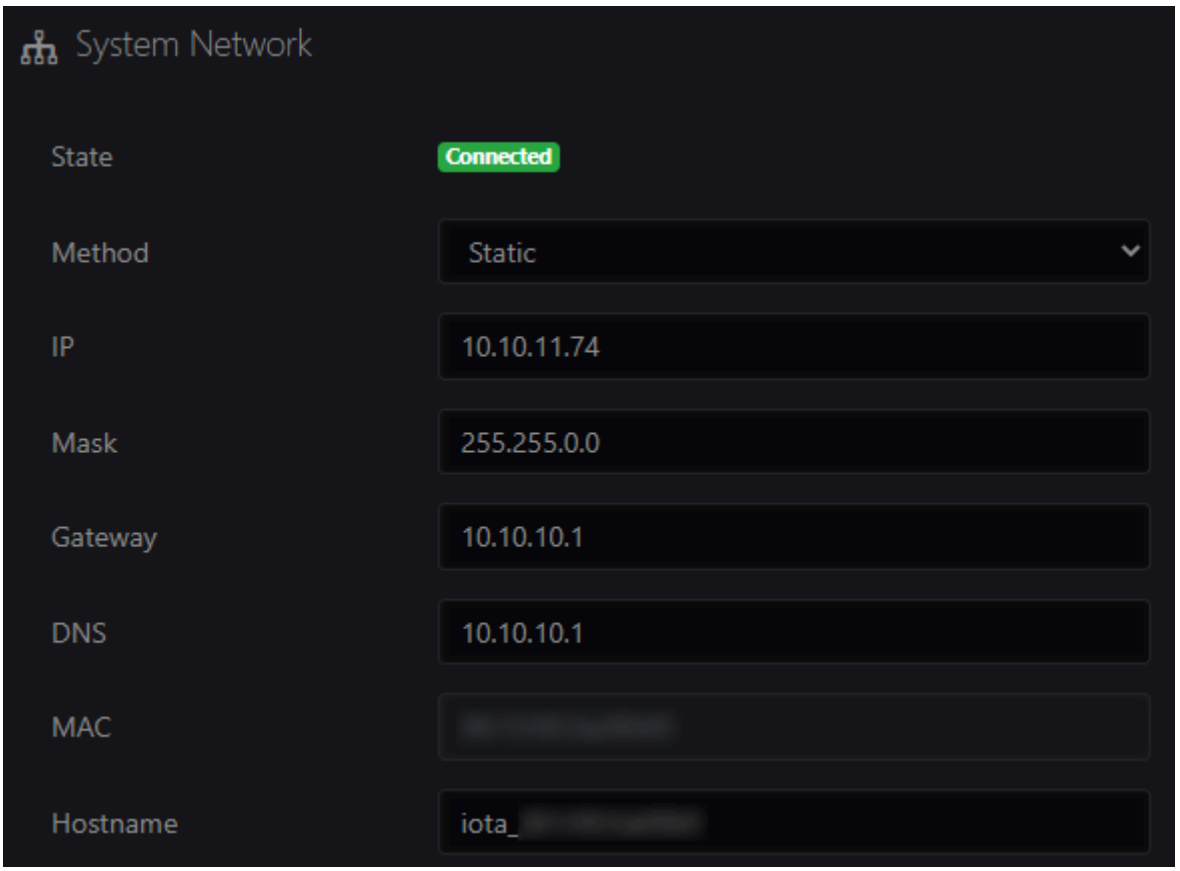
3. IOTA Configuration

3.1. Time Settings



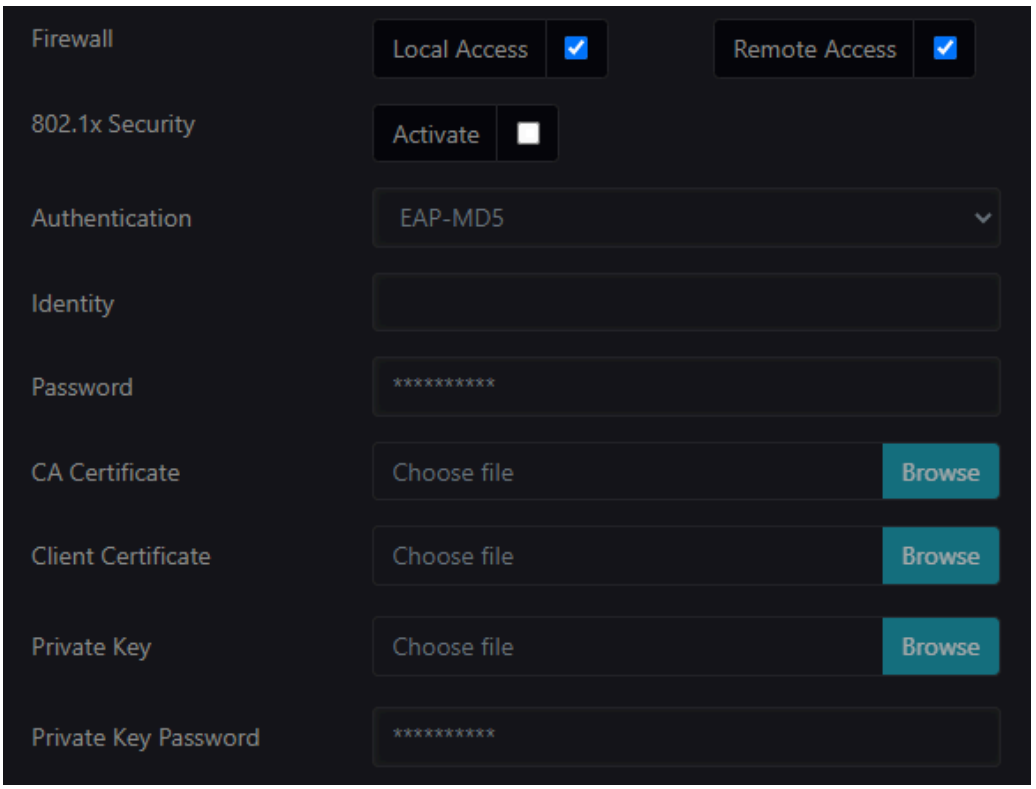
The ***IOTA Settings > Time Settings*** page allows the configuration of the system date, time, time zone, and NTP service. The NTP service is enabled by default, and can be disabled or enabled on this page. NTP servers can be added, modified, or removed. The appropriate time zone should be set manually,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

3.2. Network Configuration



Navigate to ***IOTA Settings > Network Configuration*** to modify the IOTA network settings. The IP address, network mask, gateway and DNS server can be set manually if *Method* is set to *Static*. If *Method* is set to *DHCP Dynamic*, IOTA will attempt to receive network settings from a DHCP server.

3.3. Access / Internal Firewall



3.3.1. Firewall

Local Access
When enabled, connections to the IOTA user interface from the subnetwork IOTA is located on are accepted. When disabled, they are rejected.

Remote Access
When enabled, connections to the IOTA user interface from subnetworks other than the one IOTA is located on are accepted. When disabled, they are rejected.

3.3.2. 802.1x Security

Activate
Enable or disable 802.1x authentication.

Authentication
Defines the authentication method:

- 'EAP-MD5': The EAP-MD5 (message-digest algorithm v5) method checks against the MD5 hash of the user password for authentication. The EAP-MD5 is defined in RFC 2284.
- 'EAP-TLS': The EAP-TLS (Transport Layer Security) uses Public key Infrastructure (PKI) to set up authentication using a RADIUS or other authentication server. This protocol requires client-side certificates for communicating with the authentication server. The EAP-TLS is defined in RFC 5216.

Identity
Specifies the username for the 802.1x EAP-MD5 or EAP-TLS server.

Password
Specifies the password for the 802.1x EAP-MD5 server.

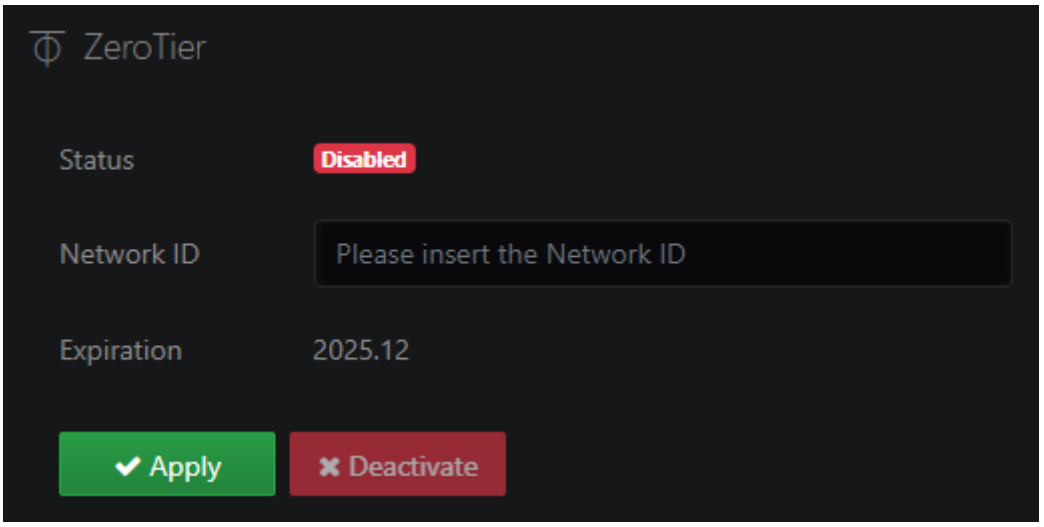
CA Certificate
The CA certificate file (Certificate Authority) in PEM format for the 802.1x EAP-TLS server (optional).

Client Certificate
The client certificate file in PEM format for the 802.1x EAP-TLS server.

Private Key
The private key certificate file in PEM format for the 802.1x EAP-TLS server.

Private Key Password
Specifies the password for the private key file for the 802.1x EAP-TLS server (optional).

3.4. ZeroTier



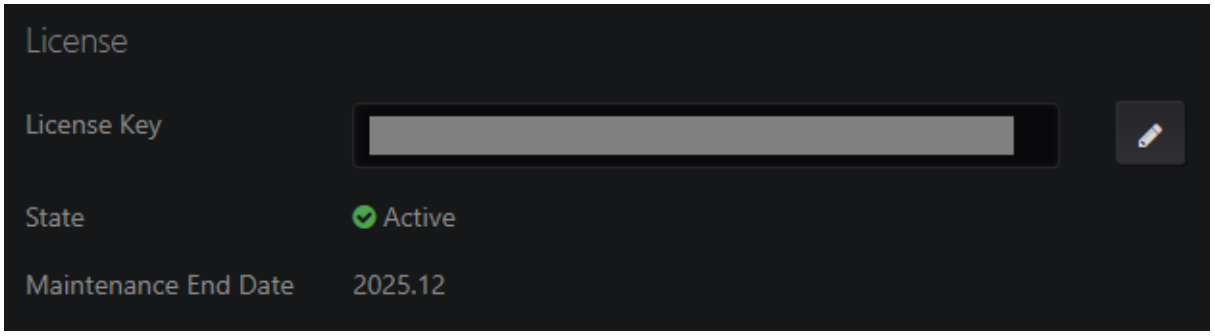
ZeroTier provides an easy way to remotely access the device via a P2P VPN and manage virtual networks on a cloud application. Visit www.zerotier.com for more information.

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

3.5. Firmware & License

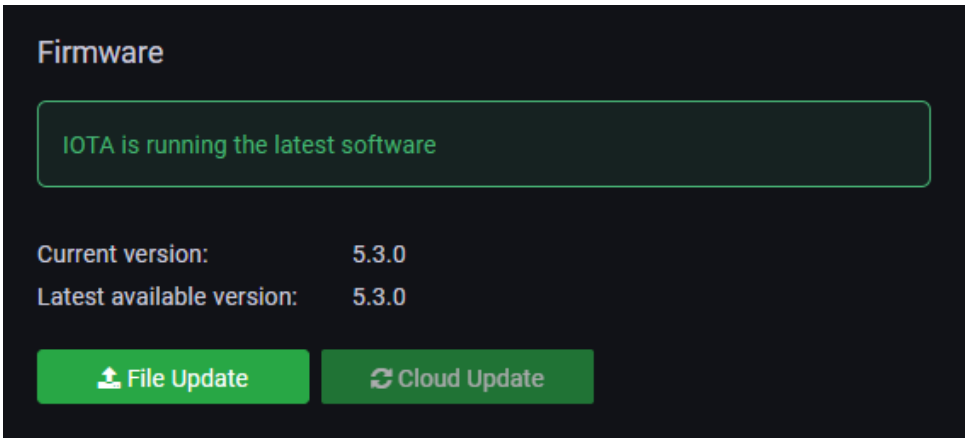
The ***IOTA Settings > Firmware & License*** page provides information about the currently-installed license and firmware, and the ability to update them.

3.5.1. License



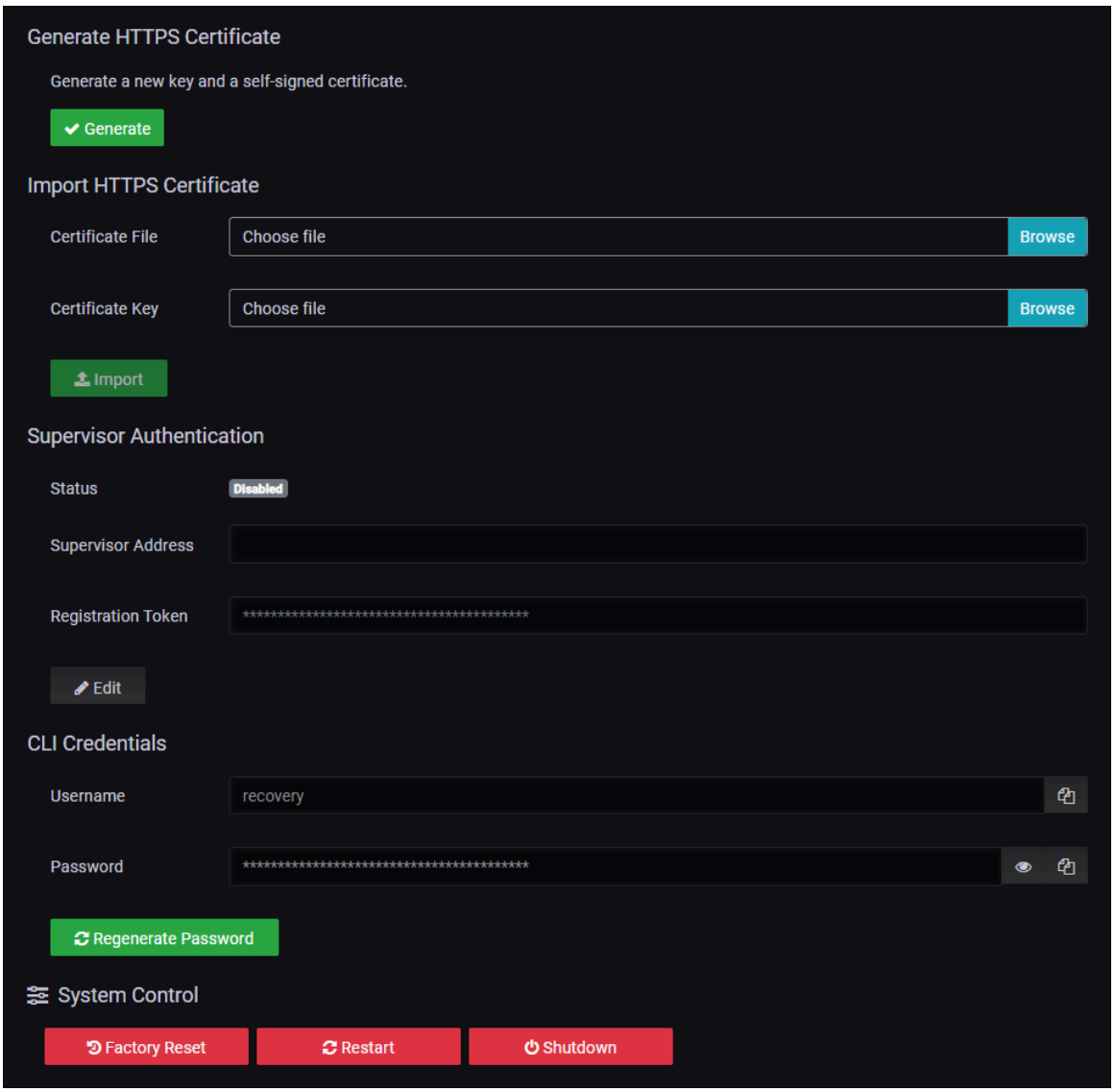
The license concerns the ability of the device to install firmware updates. *Maintenance End Date* displays the expiration date of the license. A device with an expired license can be used indefinitely with the currently-installed firmware version.

3.5.2. Firmware



The *Firmware* section displays the currently-installed firmware version and the *Release Notes* (changelog), and provides the ability to update the firmware.

3.6. Administration



3.6.1. HTTPS Certificate

Click the *Generate* button to generate a new self-signed HTTPS certificate and key for connection to the IOTA management interface. Alternatively, a certificate and certificate key can be imported by clicking the *Browse* buttons, selecting the appropriate files, and clicking the *Import* button. Note that the imported HTTPS certificate must include the EKU and SAN fields.

3.6.2. Supervisor Authentication

Profitap Supervisor can be used as a centralized authentication facility for IOTA devices.

This feature can be enabled in the Supervisor when registering the device. The centralized manager will automatically register in the device as an authentication facility. From this moment on, the IOTA device will query the Supervisor to verify, using its authentication configuration, if the credentials used for login are valid. This feature allows the user to define the whole authentication configuration for all Profitap IOTA EDGE, IOTA 10 CORE, and NPBs in a single point and have it being used across the whole fleet of

devices. Thanks to this feature, it is possible to use TACACS+, RADIUS, and LDAP authentication in IOTA devices (in addition to Local Users).

In the **Supervisor Authentication** section of the **Administration** page, it is possible to visualize if any Supervisor has been registered with the device and eventually modify the address and registration token. Note that the Supervisor is already performing the registration process automatically and these settings shouldn't require any manual change.

When disabling the Profitap Supervisor from this GUI, the IOTA device will stop reaching to the Supervisor for authentication.

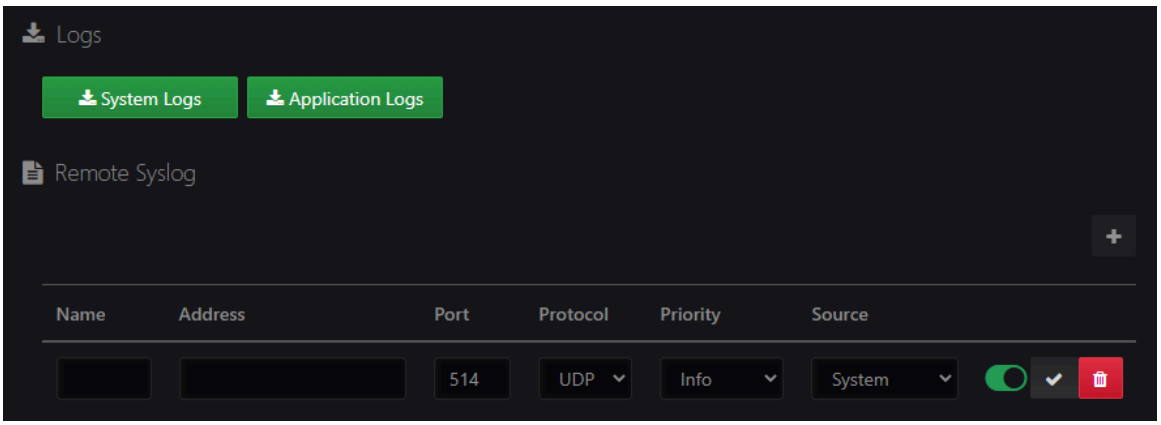
3.6.3. CLI Credentials

The recovery CLI credentials can be found here, and can be regenerated using the *Regenerate Password* button. Either field can be copied to the clipboard by using the buttons to the right of each field. For more information on the recovery CLI, see Device Recovery CLI.

3.6.4. 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 Control* page).

3.7. Logs



3.7.1. Logs

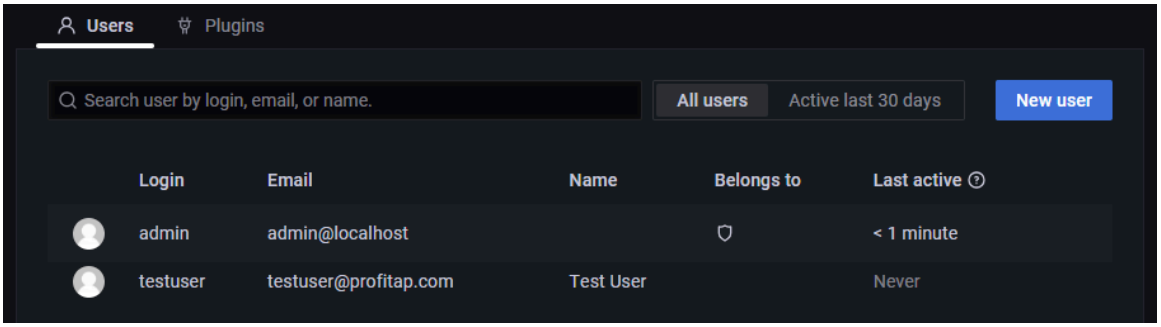
Click the *System Logs* button to download the system logs, which contains all of the embedded OS activity. Click the *Application Logs* button to download the application logs, which contains the activity of the IOTA-specific software.

3.7.2. Remote Syslog

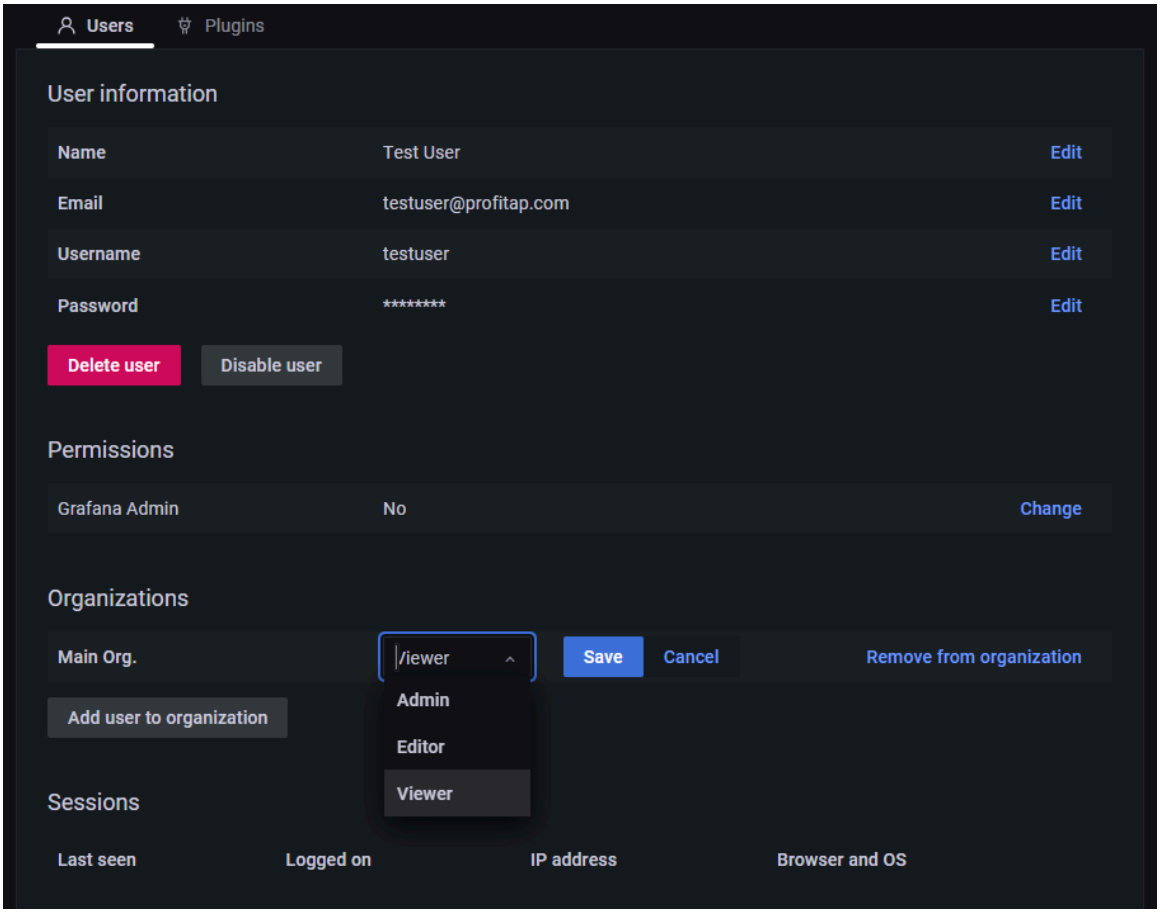
This facility allows the IOTA to send its system and application logs to remote collection servers. For each destination, it is possible to specify the type of logs priority and source to send.

3.8. Users

The **Users** page can be accessed via the *Server Admin* > *Users* menu item by users with **Admin** role. This page allows administrators to add, edit, and delete user accounts.



To add a user account, click the *New user* button, fill in the fields, and click the *Create user* button.



To view a user account, click the account in the list. In this view, it is possible to edit, delete, or disable/enable the selected user account. Click *Change role* to change the account's privileges. Depending on the selected role, the user has the following rights:

- **Admin**: full access;
- **Editor/Viewer**: view the IOTA dashboards only.

3.9. Device Reset

3.9.1. Network Configuration

The Management 1 port's network configuration can be modified via the IOTA GUI (see Network Configuration) or by using the unit's USB ports (see Management interfaces).

3.9.2. Factory Reset

To reset the device to factory settings, create a file called `iota_factory_reset_unit_<pretty_mac>` where `<pretty_mac>` is the Management 1 MAC address in lowercase, without colon separators (:), e.g. `ffffffffffff` for MAC address `FF:FF:FF:FF:FF:FF`. Place this file at the root of a USB drive, connect the USB drive to one of the unit's USB ports, and power on or restart the unit. When this file is detected at startup of the device, the factory reset will be triggered. The Capture LED will blink 3 times to confirm that the factory reset process was triggered successfully.

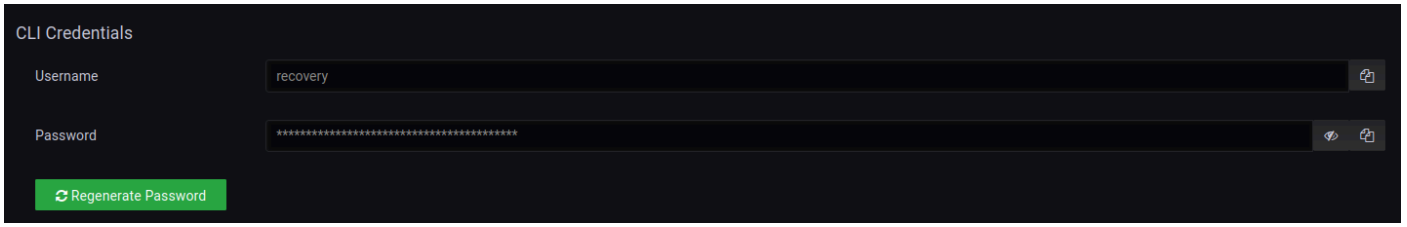
Factory reset can also be initiated via the *Factory Reset* button on the IOTA Settings > Administration page.

Note: Resetting the IOTA to factory settings will remove all data stored on the device.

3.10. 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.

3.10.1. Recovery CLI Credentials



The recovery CLI credentials can be found in the *CLI Credentials* section of the *IOTA Settings* > *Administration* page of the GUI. The username is static and cannot be changed. The password cannot be edited directly, but it can be regenerated using the *Regenerate Password* button. Either field can be copied to the clipboard by using the buttons to the right of each field.

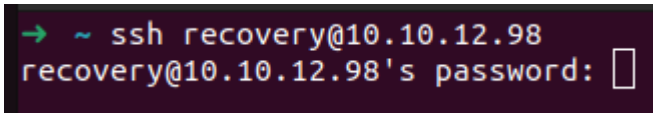
3.10.2. Accessing the CLI

The CLI can be accessed 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 recovery username and **`IOTA_IP`** is the IP address of the device), and submit the recovery 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 recovery credentials 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.

3.10.3. 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]
```

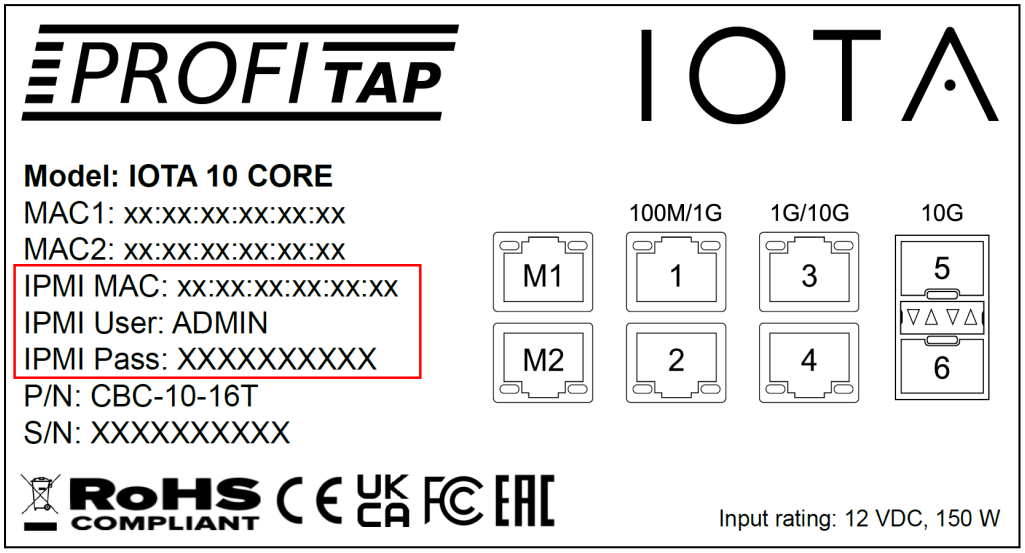
The **`reboot`** command (or **`.reboot`**) reboots the device immediately after confirmation:

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

3.11. BMC IPMI Access

Connect the device's IPMI port (see Interfaces) 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 label on the top of the device.



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 login, use the credentials mentioned above.

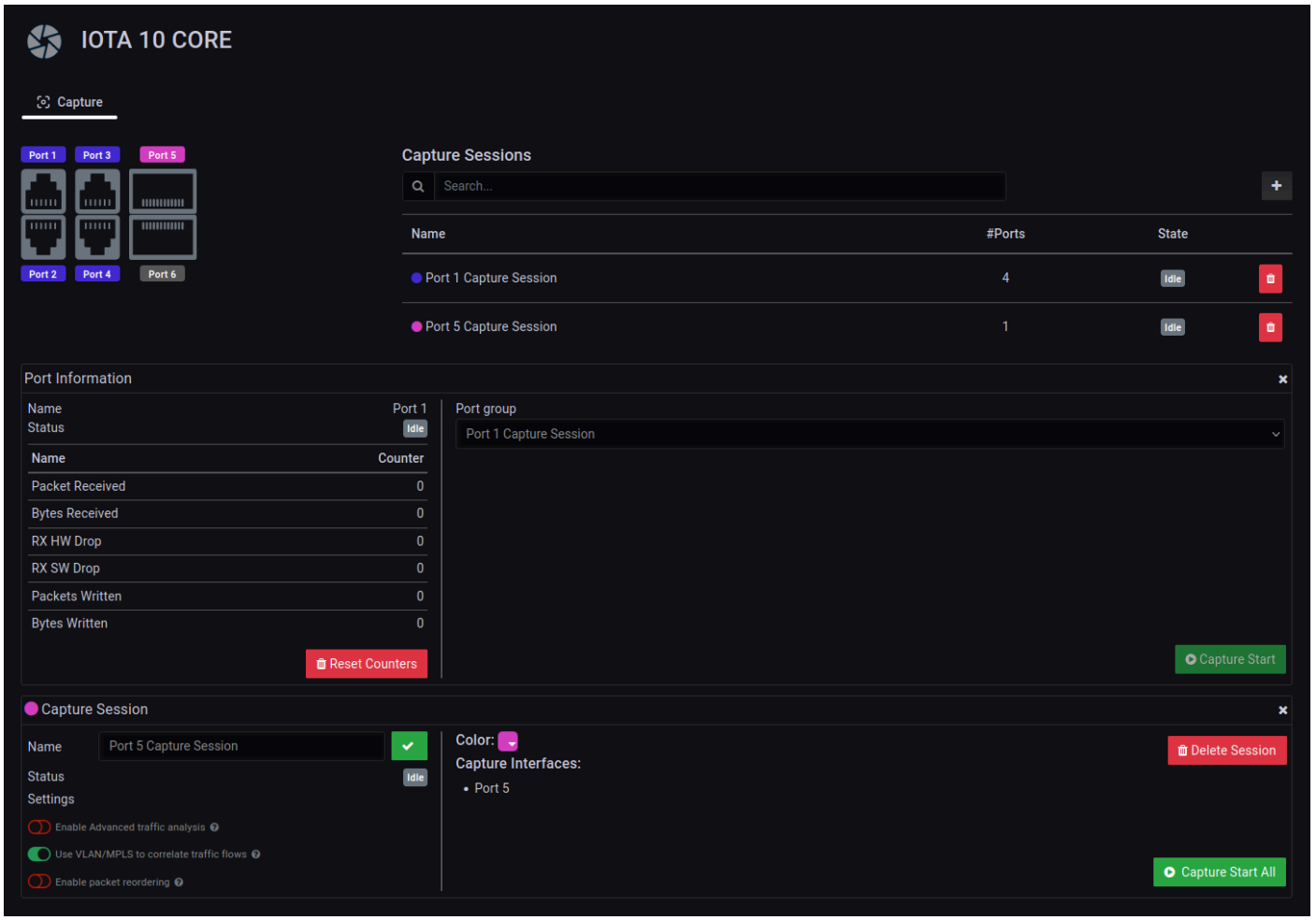
4. Capture Guide

4.1. Capture Control

IOTA 10 CORE can capture out-of-band traffic incoming from TAPs, Network Packet Brokers, and switch SPAN ports. The unit has six interfaces:

- 2 x RJ45 100M/1G
- 2 x RJ45 1G/10G
- 2 x SFP+ 10G

The unit can capture traffic from any four of these interfaces at the same time.



The ***Capture*** page displays the state of the six capture interfaces and the list of capture sessions.

Capture sessions are used to control the capture state and analysis of one or multiple ports at the same time. This facility makes possible to define correlation between traffic incoming on different ports.

You can create a new capture session by clicking the [+] button in the top right-hand corner of the screen. You will be prompted to give it a name. Ports can then be added to this capture session.

Clicking a port opens a card which displays information about this port, and allows you to assign it to an existing capture session. It also allows you to start a capture on this port if it isn't already associated to a capture session, which will create a new capture session containing this interface.

Clicking a capture session opens a card which displays the ports it contains, the capture status, and provides controls for starting and stopping the capture, changing the capture session's color, changing its name, deleting it, as well as controlling the following traffic analysis options:

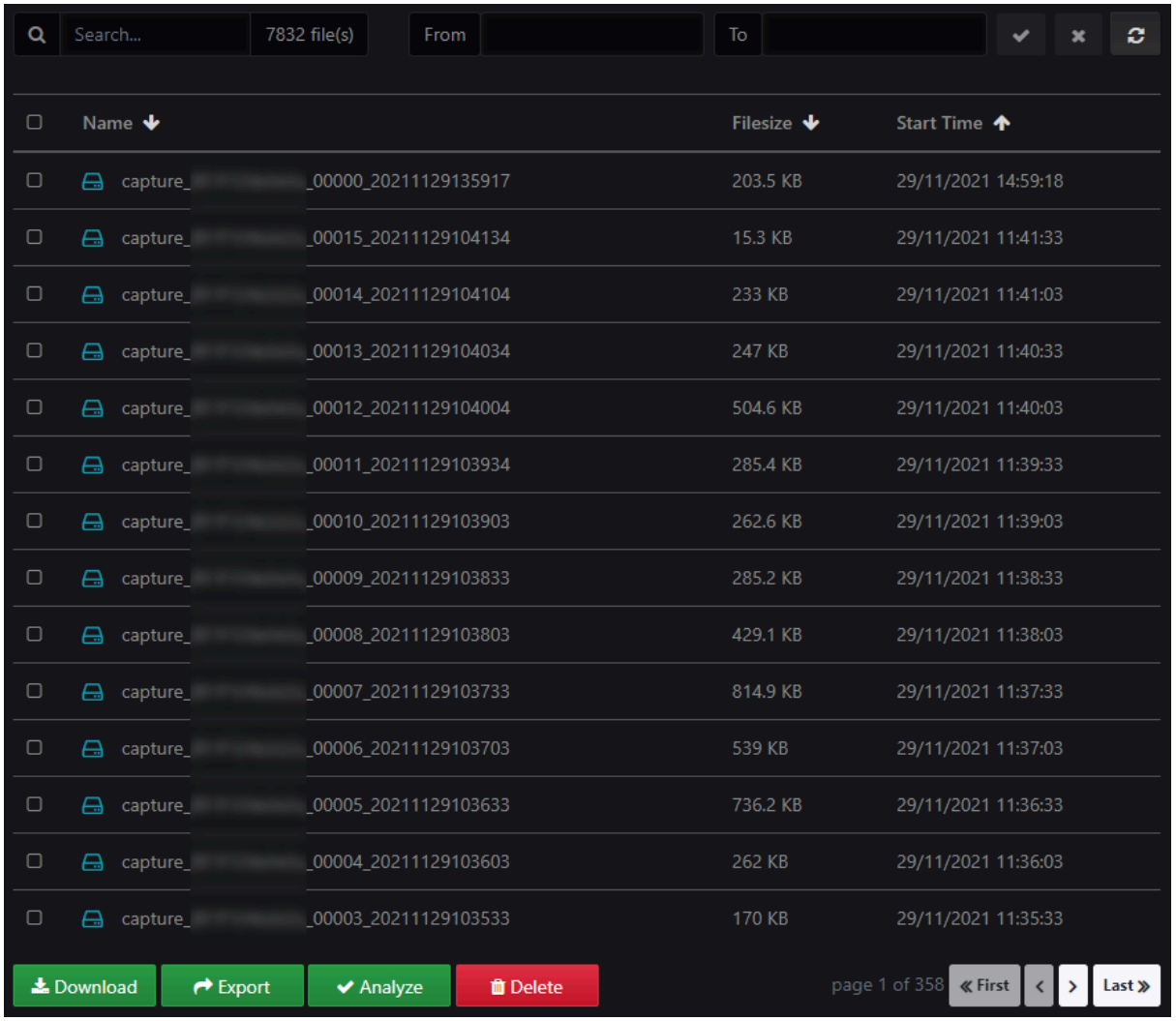
- **Enable Advanced traffic analysis**: This option enables advanced traffic analysis for VoIP, TLS and other dashboards. If this advanced analysis is not necessary, it can be disabled, which will increase overall traffic analysis performance.
- **Use VLAN/MPLS to correlate traffic flows**: If enabled, VLAN tags and MPLS labels will be used to identify traffic flows. If disabled, they will be ignored.
- **Enable packet reordering**: Force TCP packet reordering. This will improve application detection, but it may degrade accuracy of flow performance evaluation.

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.

A typical example use case for capture sessions is when IOTA 10 CORE is connected directly to a TAP receiving two traffic links. These can be joined in a single capture session to make sure that bidirectional traffic is processed correctly.

4.2. Data Vault

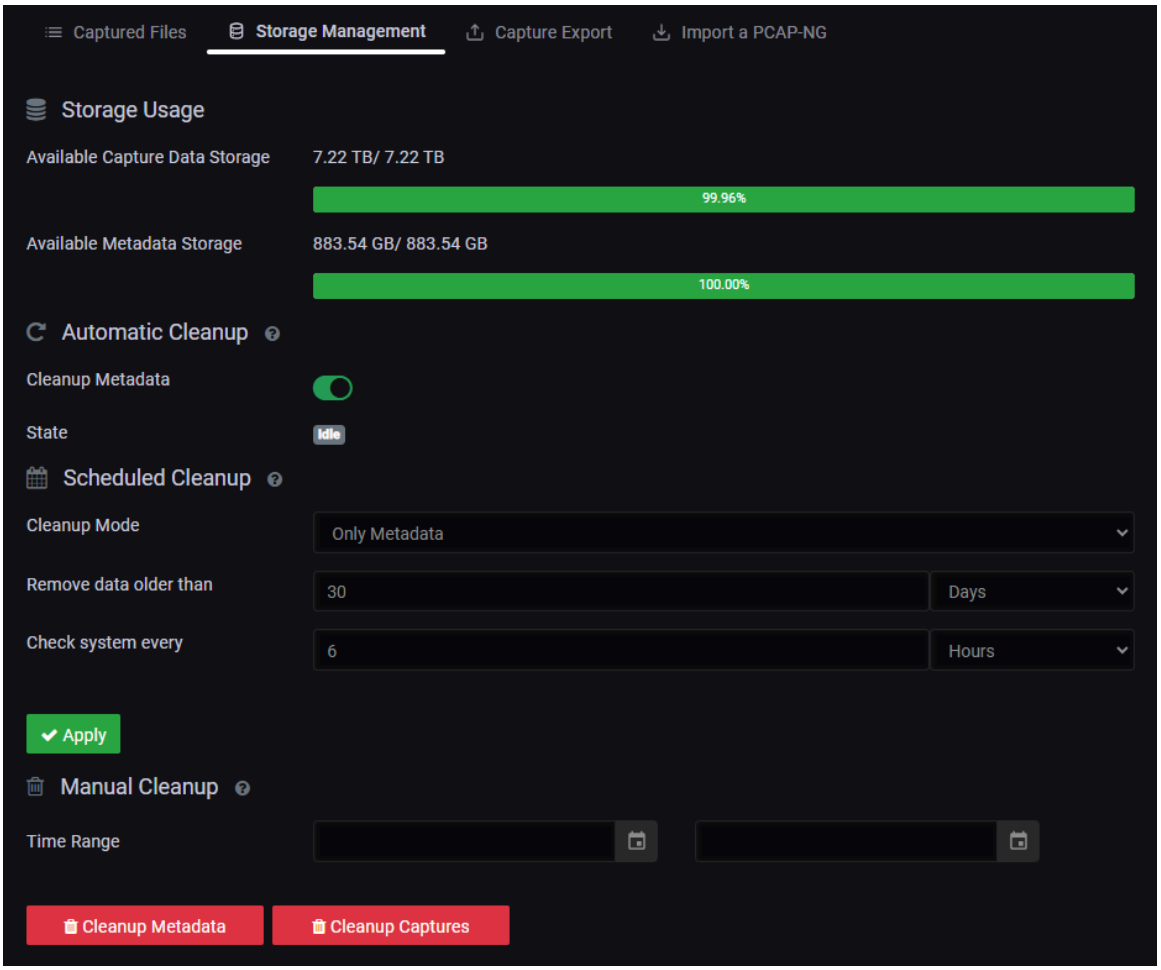
4.2.1. Captured Files



Navigate to ***Data Vault > Captured Files*** to download or delete raw PCAPNG files, or to add them to the analyzer queue. Select one or more files and click the *Download* button to download the selected files (concatenated in a single PCAPNG file), the *Export* button to add them to the capture export queue, the *Analyze* button to add them to the analyzer queue, or the *Delete* button to delete them.

The file list can be filtered via the *Search* field, and by applying a time range via the *From* and *To* fields.

4.2.2. Storage Management



Navigate to ***Data Vault > Storage Management*** to get an overview of the storage usage, including total storage size and available storage space.

Automatic Cleanup
Capture data rotates once storage usage reaches 80%. If the *Cleanup Metadata* option is enabled, older capture files and their metadata are deleted. If the *Cleanup Metadata* option is disabled, only capture files are deleted.

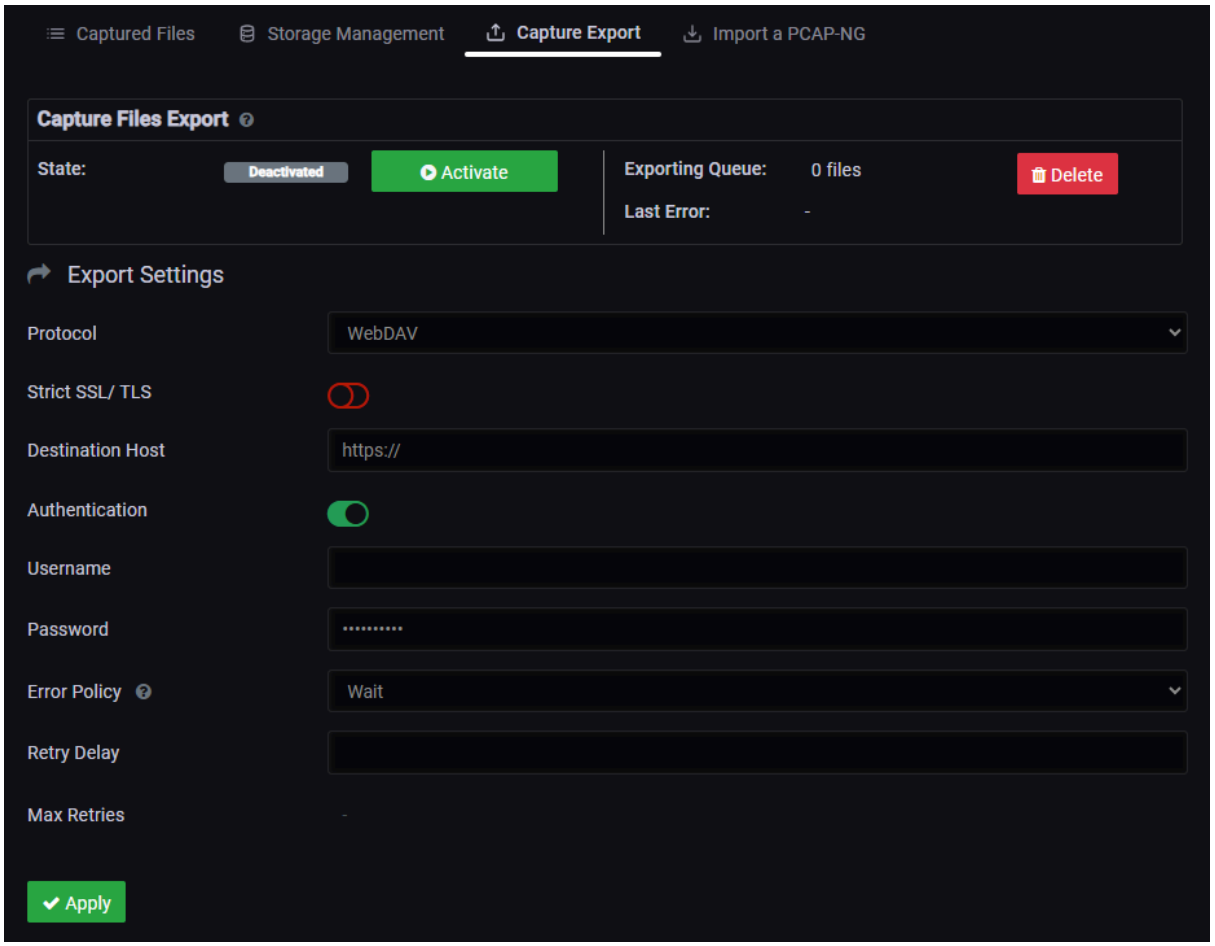
Note: Disabling the automatic cleanup of metadata will reduce the space for new capture files, and may slow down the dashboards visualization.

Scheduled Cleanup
Schedule a cleanup to remove metadata, capture files, or both, that are older than a certain number of hours, days, or weeks.

Manual Cleanup
Traffic metadata and capture files can be deleted via the *Cleanup Metadata* and *Cleanup Captures* buttons respectively. Selecting a time range will only delete data within this time range. If no time range is selected, all data will be deleted.

Note: Deletion of the indexed metadata in a time range will require more system resources and time. This may impact GUI performance, especially if a new capture is started while cleanup is in progress.

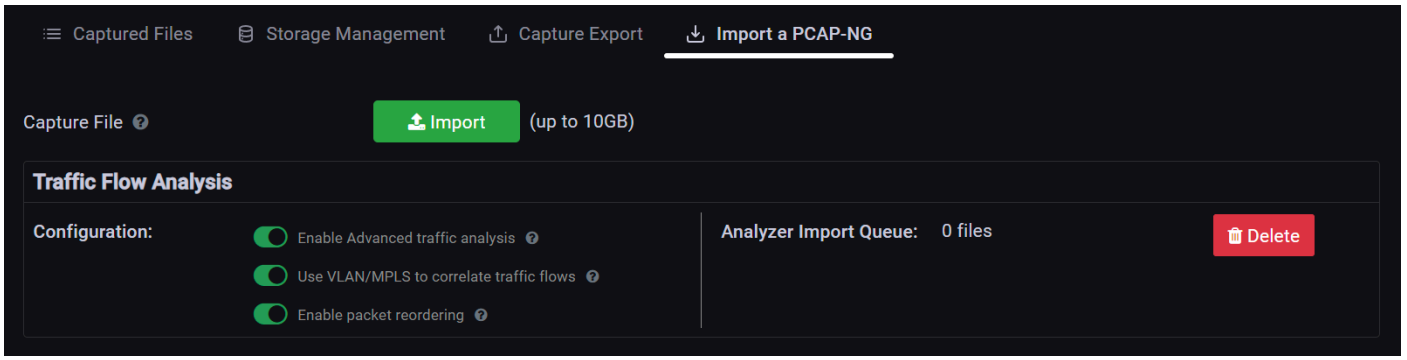
4.2.3. Capture Export



Navigate to ***Data Vault > Capture Export*** to configure the export settings of the capture file export engine.

The engine can be started or stopped via the *Activate/Deactivate* button. When active, new capture files are automatically added to the exporting queue, to be exported to the external host configured on this page. Previously captured files can also be added to the exporting queue on the *Data Vault > Captured Files* page. The exporting queue can be emptied via the *Delete* button.

4.2.4. Importing a PCAP-NG File



PCAPNG and PCAP capture files can be imported via the *Import* button. Imported files are stored on the device and automatically added to the traffic analyzer queue.

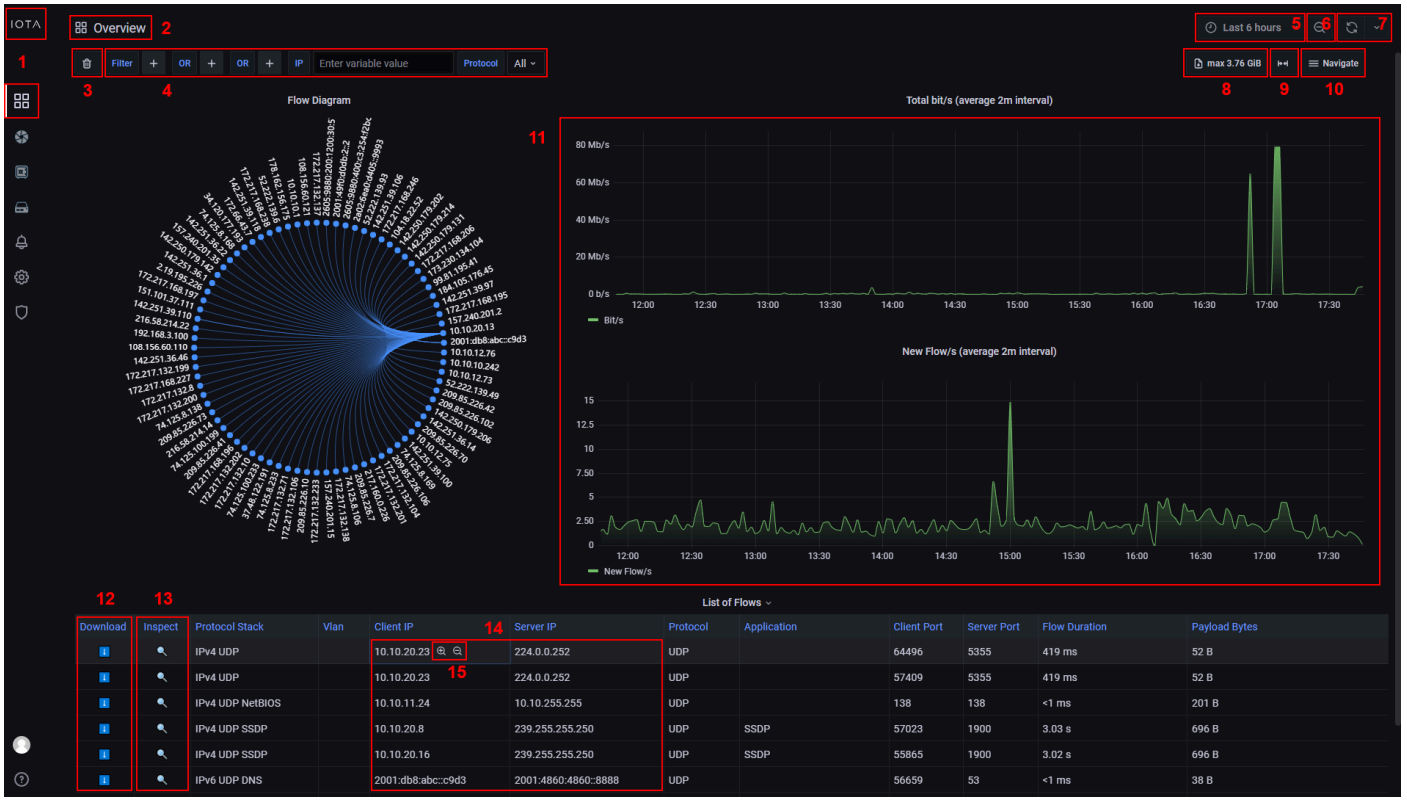
The following traffic analysis options are available:

- **Enable Advanced traffic analysis**: This option enables advanced traffic analysis for VoIP, TLS and other dashboards. If this advanced analysis is not necessary, it can be disabled, which will increase overall traffic analysis performance.
- **Use VLAN/MPLS to correlate traffic flows**: If enabled, VLAN tags and MPLS labels will be used to identify traffic flows. If disabled, they will be ignored.
- **Enable packet reordering**: Force TCP packet reordering. This will improve application detection, but it may degrade accuracy of flow performance evaluation.

The capture analysis and the PCAP import analysis are running in parallel without impacting each other. The analyzer queue can be deleted via the *Delete* button. Deleting the analyzer queue does not delete the capture files from internal storage. Capture files can be (re)added to the analyzer queues from the *Data Vault > Captured Files* page.

5. Analysis Guide

5.1. Dashboard Overview



[1] Click the IOTA logo or Dashboards menu item to navigate to the home dashboard with filters and time range reset to default.

[2] The name of the current dashboard.

[3] Click the trash can button to clear all filters.

[4] Set filters here. Filters apply to both the dashboard display and PCAP download.

[5] Set the time range here. Default is "last 6 hours".

[6] Zoom out from the current time range.

[7] Refresh the dashboard display to take into account newly analyzed data. Can bet set to auto-refresh every 30 seconds, 1 minute, 5 minutes, or 15 minutes.

[8] Download the PCAP file for the selected time range and filters.

[9] Zoom in on available data.

[10] Use this menu to navigate between dashboards while keeping the selected time range and filters.

[11] Click and drag on any graph to zoom in on a time range.

[12] Click the download button next to a flow to download the flow as a PCAP file.

[13] Click the inspect button next to a flow to navigate to the Flow Details dashboard for this flow.

[14] Click any IP address to navigate to the Host Details dashboard for this IP address.

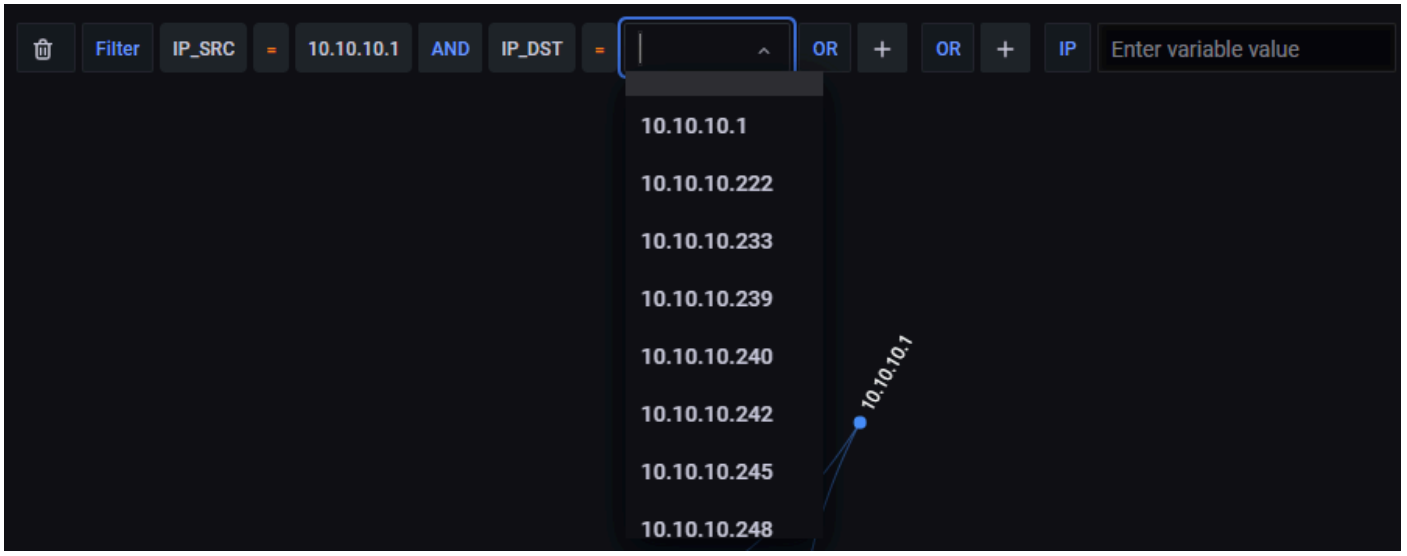
[15] When hovering a value, + and - magnifying glass icons appear. Click + to filter for this value, or - to filter out this value.

For examples on using the dashboards for analysis and troubleshooting, take a look at the *Workflow* section of our IOTA Knowledge Base: kb.profitap.com/iota/.

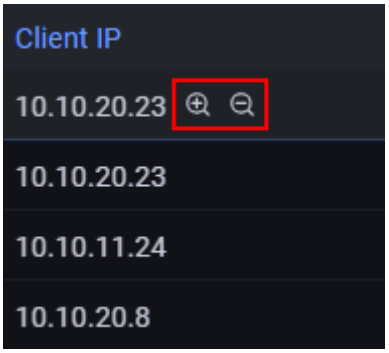
5.2. Traffic Filtering

Filters can be defined manually by clicking the + icon next to the *Filters* box, then selecting the filter type and value it needs to filter on. Clicking the + icon next to an existing filter will add an *AND* filter. Clicking the + icon next to an *OR* box will add an *OR* filter.

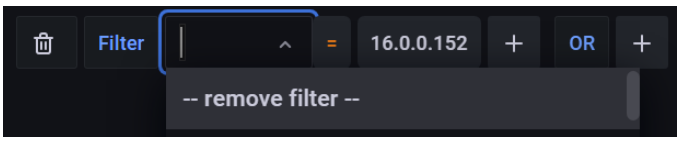
These filters are applied both to the dashboard display and to the *Download PCAP* feature.



Filters can also be applied quickly in the dashboards by using the + magnifier icon (*include* filter), or the - magnifier icon (*exclude* filter).



Filters can be removed by clicking the filter type again and selecting *--remove filter--*.



The *Custom Search* field accepts various filter statements, such as filters from the *Filters* section using both the variable name and value (e.g. *IP_SRC:10.10.10.10*), only the value (e.g. *10.10.10.10*), and modifiers such as *NOT* (e.g. *!IP_SRC:10.10.10.10*), *AND* (e.g. *IP_SRC:10.10.10.10 AND IP_DST:20.20.20.20*), and

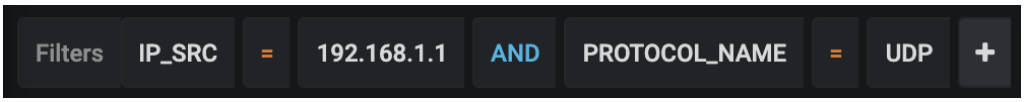
OR (e.g. *IP_SRC:10.10.10.10 OR IP_DST:20.20.20.20*). **These filters are only applied to the dashboard display, and not the *Download PCAP* feature.**

5.3. PCAP File Download

PCAPNG files can be downloaded using the following methods:

● "Download PCAP" button in the top right corner of any dashboard

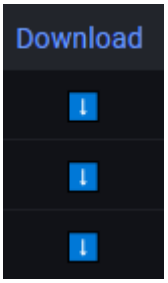
Use the "Download PCAP" button to download the PCAPNG file of the traffic for the selected time range. The following filters also apply to the downloaded PCAPNG files: IP address, MAC address, VLAN ID, Protocol, Port.



If a MAC address, IP address, or port is selected, the filter affects both source and destination.

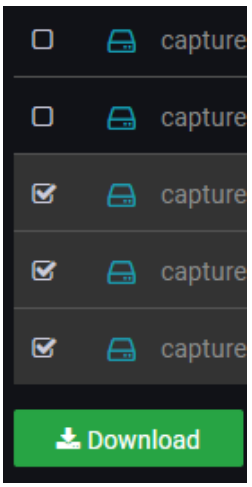
● Flow download buttons

Clicking the download icon in the *Download* column for any flow starts the PCAPNG file transfer for that flow. Filters are ignored with this method.



● Download the raw PCAPNG file(s) from the list of all captured files (*Data Vault > Captured Files*)

Select one or more files and click the *Download* button to download the selected files, concatenated into a single file.



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