IOTA 1G
IOTA 1G+
IOTA 10G
IOTA 10G+

USER MANUAL

IOTA software version: v3.0.0

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 is a multifunctional passive network probe with integrated traffic capture and analysis capabilities. Designed as a secure and flexible analysis solution, IOTA is a great asset to get access and visibility into industrial or enterprise level networks.

Profitap IOTA is used by network administrators and IT analysts to get a fast and clear overview of the network traffic. This means a comprehensive analysis can be performed quickly, helping engineers get to the root cause in a matter of clicks.

The device can be deployed as a dedicated probe, or programmed for autonomous analysis, thus reducing the need of an on-site network expert.

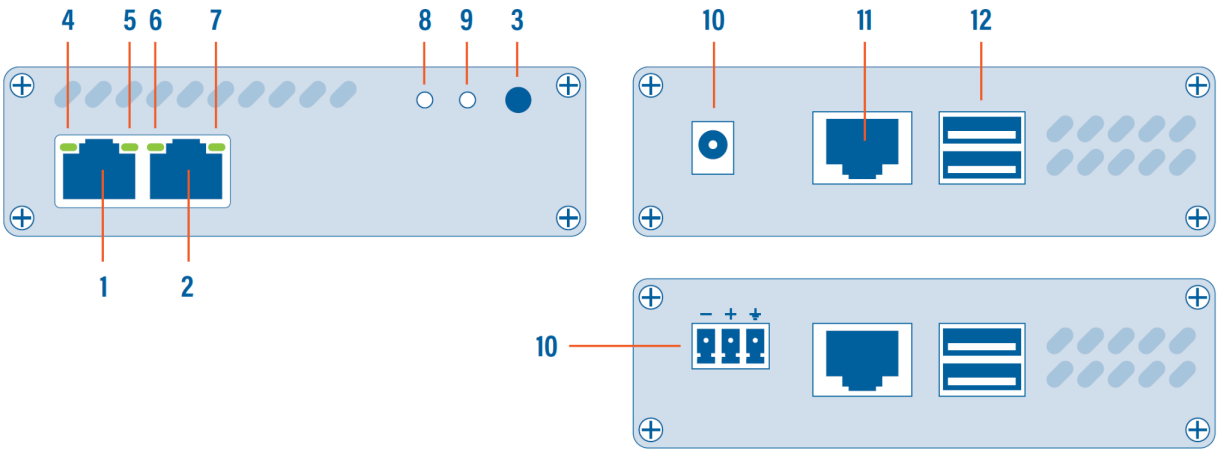
1.2. Specifications

	IOTA 1G	IOTA 1G+	IOTA 10G	IOTA 10G+
Capture Interface	2 x RJ45 Ethernet 10/100/1000M	2 x RJ45 Ethernet 10/100/1000M	2 x SFP+ Ethernet 1/10G	2 x SFP+ Ethernet 1/10G
In-Line Mode	Yes	Yes	Yes	Yes
Dual SPAN Inputs Mode	Yes	Yes	Yes	Yes
In-Line Latency	1G: 380 ± 8 ns 100M: 720 ± 24 ns 10M: 7600 ± 25 ns	1G: 380 ± 8 ns 100M: 720 ± 24 ns 10M: 7600 ± 25 ns	500 ns	500 ns
In-Line Jitter	20 ns	20 ns	20 ns	20 ns
Fail-Safe	Yes	Yes	No	No
Supported Capture Speed*	10M / 100M / 1G	10M / 100M / 1G	1G / 10G	1G / 10G
Capture Performance*	3.2 Gbps / 3.2 Mpps	3.2 Gbps / 3.2 Mpps	3.2 Gbps / 5 Mpps	3.2 Gbps / 5 Mpps
Packet Processor (slicing, filtering, timestamping)*	Yes: 2 Gbps / 3.2 Mpps	Yes: 2 Gbps / 3.2 Mpps	Yes: 20 Gbps / 32 Mpps	Yes: 20 Gbps / 32 Mpps
Hardware Timestamping	Yes: 8 ns, NTP synchronized	Yes: 8 ns, NTP synchronized	1G: 8 ns, NTP synchronized 10G: 6.4 ns, NTP synchronized	1G: 8 ns, NTP synchronized 10G: 6.4 ns, NTP synchronized
Internal Storage	1 TB SSD	1 TB or 2 TB swappable SSD (NVMe)	1 TB SSD	1 TB or 2 TB swappable SSD (NVMe)
Power Inputs (12V Model)	12 VDC	12 VDC, PoE+ (management RJ45)	12 VDC	12 VDC, PoE+ (management RJ45)
Power Inputs (24V Model)	24–48 VDC	24–48 VDC, PoE+ (management RJ45)	24–48 VDC	24–48 VDC, PoE+ (management RJ45)
Power Consumption	12 W	14 W	15 W	25 W
Management Interface	RJ45 Ethernet 10/100/1000M	RJ45 Ethernet 10/100/1000M	RJ45 Ethernet 10/100/1000M	RJ45 Ethernet 10/100/1000M
Management Service	HTTPS (server)	HTTPS (server)	HTTPS (server)	HTTPS (server)

*These relate to the capture interface. Captured traffic analysis performance will depend on the type of traffic, and the type of analysis performed (see 4.1).

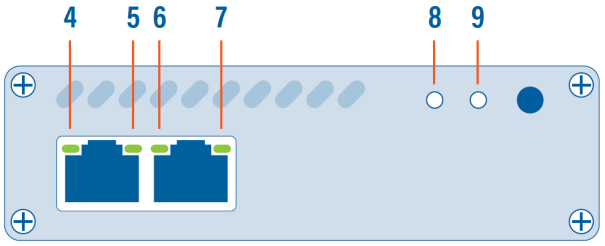
1.3. Interfaces & LED Behavior

1.3.1. IOTA 1G Interface



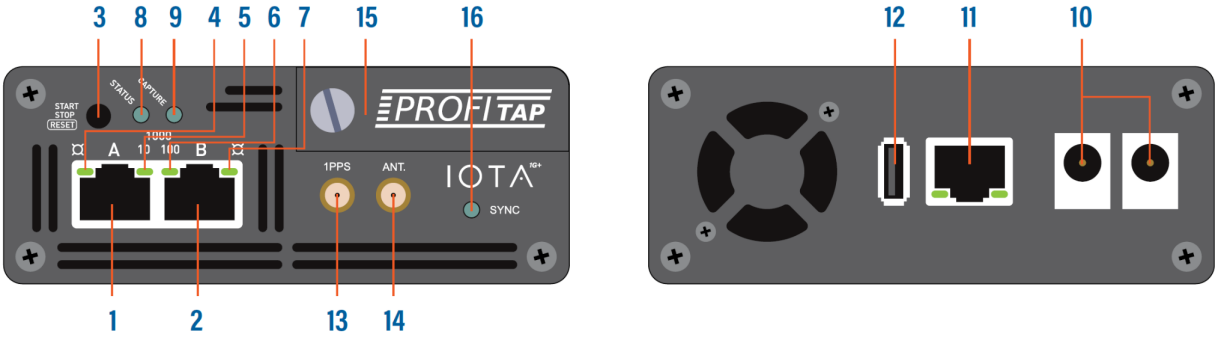
1, 2	RJ45 Ethernet port A and B
3	START/STOP/RESET button
4, 5, 6, 7	Network status and activity LEDs
8	Status LED
9	Capture LED
10	12 VDC power input (12V model)
10	24-48 VDC power input (24V model)
11	RJ45 Management port (PoE+)
12	2 x USB 3.0 port type A

1.3.2. IOTA 1G LED Behavior



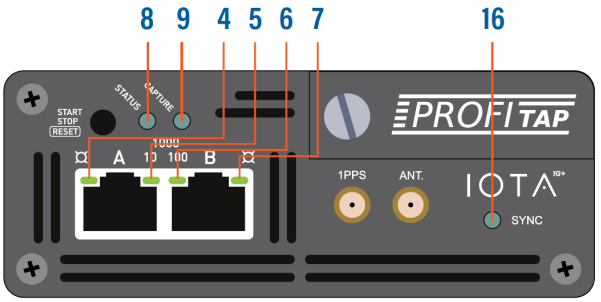
LED state	Meaning
4 and/or **7** steady green	The port is linked.
4 and/or **7** blinking green	The port is linked and has RX/TX activity (traffic is passing through).
5 steady green **6** off	Capture interface operating at 10 Mbps speed.
5 blinking green **6** off	Capture interface is initializing.
5 off **6** steady green	Capture interface operating at 100 Mbps speed.
5 off **6** blinking green	Capture interface firmware is corrupted.
5+6 steady green	Capture interface operating at 1 Gbps speed.
5+6 blinking green	The port is linked and has RX/TX activity (traffic is passing through).
5+6 alternating blinking	Capture interface cannot find a common speed between the connected devices.
8 blinking orange **9** off	Booting
8 green **9** green	Running
8 green **9** blinking green	Capturing
8 blinking orange and green **9** blinking orange and green	Updating
8 blinking red **9** blinking red	Hardware failure
8 blinking orange **9** blinking orange	Factory reset
8 blinking green **9** off	Shutting down
8 off **9** off	Shutdown completed

1.3.3. IOTA 1G+ Interface



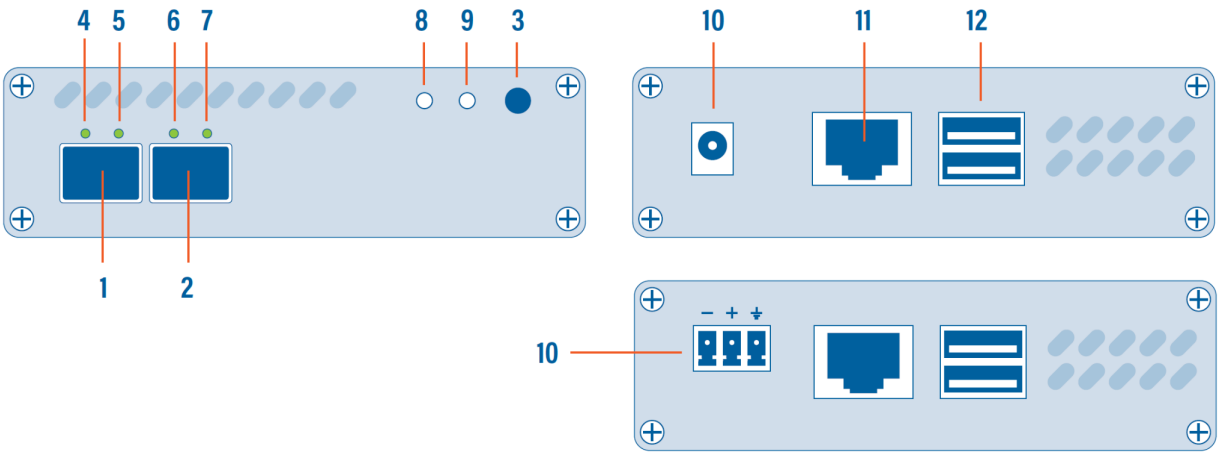
1, 2	RJ45 Ethernet port A and B
3	START/STOP/RESET button
4, 5, 6, 7	Network status and activity LEDs
8	Status LED
9	Capture LED
10	12 VDC redundant power inputs (12V model)
11	RJ45 Management port (PoE+)
12	USB 3.0 port type A
13	SMA female connector (PPS in/out)
14	SMA female connector (GPS/GLONASS antenna)
15	Removable SSD
16	Sync LED

1.3.4. IOTA 1G+ LED Behavior



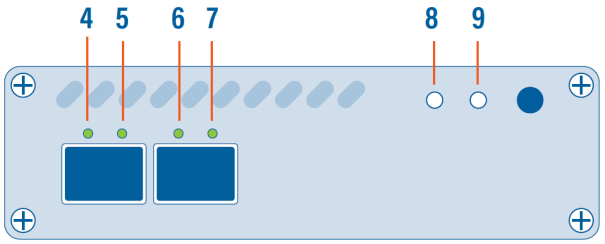
LED state	Meaning
4 and/or **7** steady green	The port is linked.
4 and/or **7** blinking green	The port is linked and has RX/TX activity (traffic is passing through).
5 steady green **6** off	Capture interface operating at 10 Mbps speed.
5 blinking green **6** off	Capture interface is initializing.
5 off **6** steady green	Capture interface operating at 100 Mbps speed.
5 off **6** blinking green	Capture interface firmware is corrupted.
5+6 steady green	Capture interface operating at 1 Gbps speed.
5+6 blinking green	The port is linked and has RX/TX activity (traffic is passing through).
5+6 alternating blinking	Capture interface cannot find a common speed between the connected devices.
8 blinking orange **9** off	Booting
8 green **9** green	Running
8 green **9** blinking green	Capturing
8 blinking orange and green **9** blinking orange and green	Updating
8 blinking red **9** blinking red	Hardware failure
8 blinking orange **9** blinking orange	Factory reset
8 blinking green **9** off	Shutting down
8 off **9** off	Shutdown completed
16 on	Internal timestamp synchronized with the configured time system (GPS, NTP, etc.) with an accuracy of ± 16 ns.

1.3.5. IOTA 10G Interface



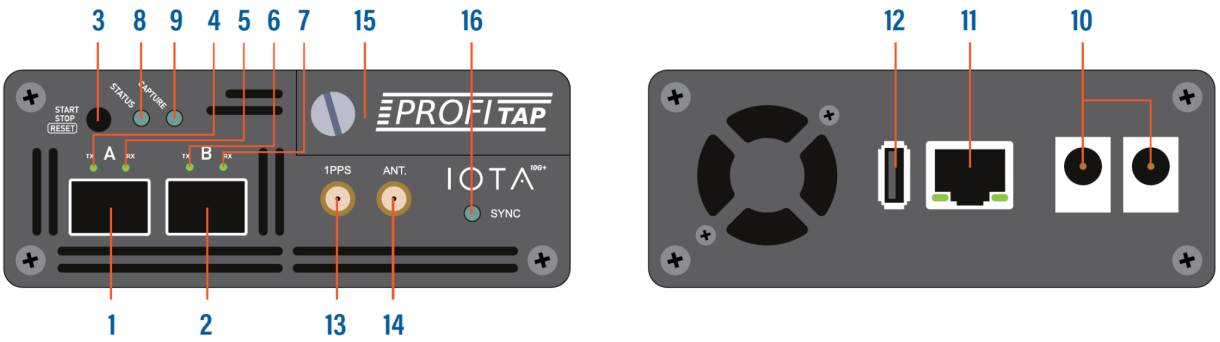
1, 2	SFP+ port A and B
3	START/STOP/RESET button
4, 5, 6, 7	SFP and network status and activity LEDs
8	Status LED
9	Capture LED
10	12 VDC power input (12V model)
10	24-48 VDC power input (24V model)
11	RJ45 Management port (PoE+)
12	2 x USB 3.0 port type A

1.3.6. IOTA 10G LED Behavior



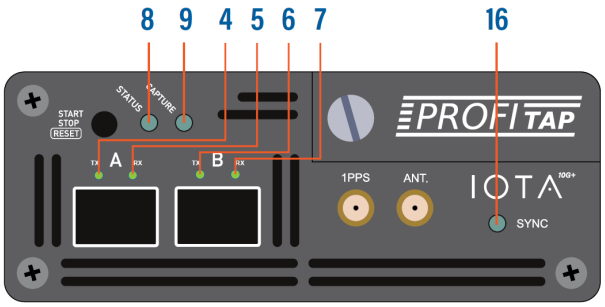
LED state	Meaning
4+**5** and/or **6**+**7** orange	No SFP module present or detected.
4+**5** and/or **6**+**7** green slow blink	No link.
4+**5** and/or **6**+**7** red	Connect additional power.
5 and/or **7** green	SPAN mode, link up.
5 and/or **7** green fast blink	SPAN mode, traffic activity.
4+**5**+**6**+**7** green	In-Line mode, link up.
4+**5**+**6**+**7** green fast blink	In-Line mode, traffic activity.
8 blinking orange **9** off	Booting
8 green **9** green	Running
8 green **9** blinking green	Capturing
8 blinking orange and green **9** blinking orange and green	Updating
8 blinking red **9** blinking red	Hardware failure
8 blinking orange **9** blinking orange	Factory reset
8 blinking green **9** off	Shutting down
8 off **9** off	Shutdown completed

1.3.7. IOTA 10G+ Interface



1, 2	SFP+ port A and B
3	START/STOP/RESET button
4, 5, 6, 7	SFP and network status and activity LEDs
8	Status LED
9	Capture LED
10	12 VDC redundant power inputs (12V model)
11	RJ45 Management port (PoE+)
12	USB 3.0 port type A
13	SMA female connector (PPS in/out)
14	SMA female connector (GPS/GLONASS antenna)
15	Removable SSD
16	Sync LED

1.3.8. IOTA 10G+ LED Behavior



LED state	Meaning
4+**5** and/or **6**+**7** orange	No SFP module present or detected.
4+**5** and/or **6**+**7** green slow blink	No link.
4+**5** and/or **6**+**7** red	Connect additional power.
5 and/or **7** green	SPAN mode, link up.
5 and/or **7** green fast blink	SPAN mode, traffic activity.
4+**5**+**6**+**7** green	In-Line mode, link up.
4+**5**+**6**+**7** green fast blink	In-Line mode, traffic activity.
8 blinking orange **9** off	Booting
8 green **9** green	Running
8 green **9** blinking green	Capturing
8 blinking orange and green **9** blinking orange and green	Updating
8 blinking red **9** blinking red	Hardware failure
8 blinking orange **9** blinking orange	Factory reset
8 blinking green **9** off	Shutting down
8 off **9** off	Shutdown completed
16 on	Internal timestamp synchronized with the configured time system (GPS, NTP, etc.) with an accuracy of ± 16 ns.

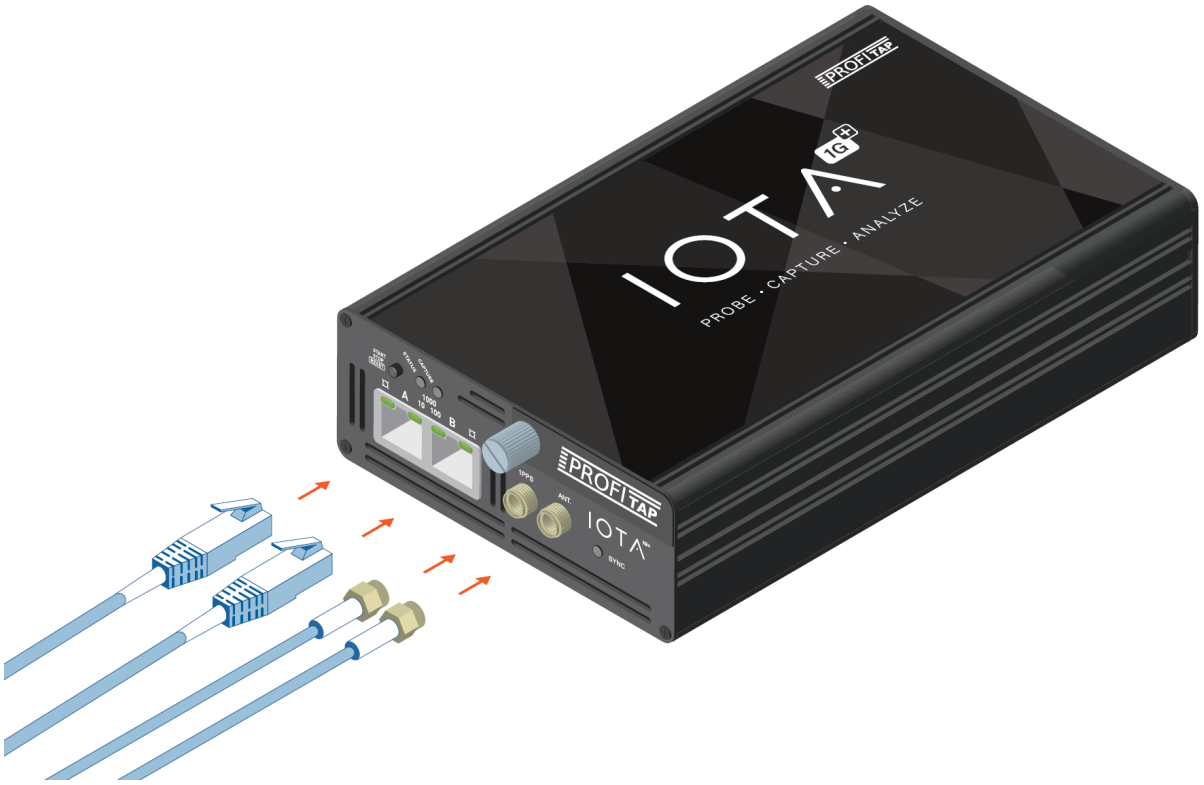
2. Getting Started

2.1. Deploying IOTA

2.1.1. IOTA 1G / 1G+

Insert Ethernet cables of the line you want to monitor into the RJ45 ports A and B of the IOTA, using category 5 UTP cables, rated for Gigabit operations.

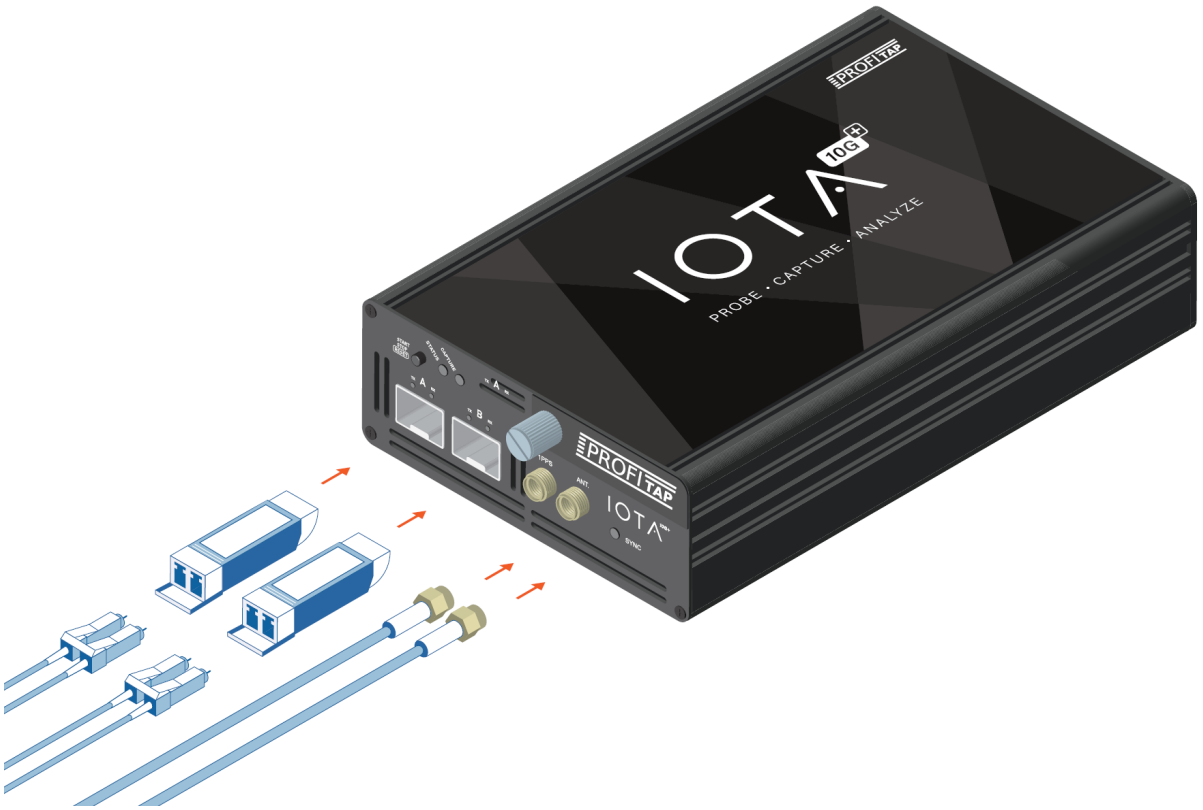
Note: When deploying IOTA 1G/1G+ in-line, connect it to the network prior to powering it in order to make full use of its fail-safe capabilities. This step is critical to verify the availability of the in-line path in case of failover.



2.1.2. IOTA 10G / 10G+

Insert the cables of the line to be monitored in the SFP modules. In the case of LC optical fiber cables, make sure to match the Tx-Rx / Tx-Rx signal direction at the other end.

Note: Due to the nature of SFP modules requiring power for operation, IOTA 10G/10G+ doesn't include a bypass feature for fail-safe monitoring. An external TAP can be employed in order to implement fail-safe monitoring.



2.1.3. IOTA Rackmount Models

The rackmount models can be mounted in a standard 19" rack, using the Profitap Rackmount Chassis Kit (sold separately; reference: ARKB-1U). Secure the chassis to the rack using the provided screws, then insert the IOTA and secure it to the chassis using the thumbscrews on the front panel of the device.

2.2. Powering Up the Device

Connect the 12V/2.5A DC power supply, or the 24–48VDC terminal block, depending on the IOTA model. IOTA can also be powered via PoE+ over the management port by connecting it to a PoE+ switch. Connect both power port and PoE+ management port for redundant powering, ensuring continued operation in case either port were to be disconnected or unable to provide power.

IOTA boots automatically after a power connection is established. Its status can be observed via the activity LEDs.

Once powered, the in-line failover circuit is disabled, effectively placing the device in-line.

Note: Initial boot may take some time to complete. When both the Status and Capture LEDs are green, IOTA has completed the boot sequence.

Note: When using an IOTA 10G+ with two 10GBASE-T SFPs, PoE+ alone may not provide enough power for operation. If that is the case, it is recommended to connect the 12 VDC (12V Model) or 24–48 VDC (24V Model) power inputs.

2.3. 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://x.x.x.x

DHCP mode is enabled by default. If no IP is assigned to the IOTA, the default fallback IP is 169.254.1.1.

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.

2.4. Swapping SSD

IOTA 1G+ / 10G+

The procedure for swapping the SSD is as follows:

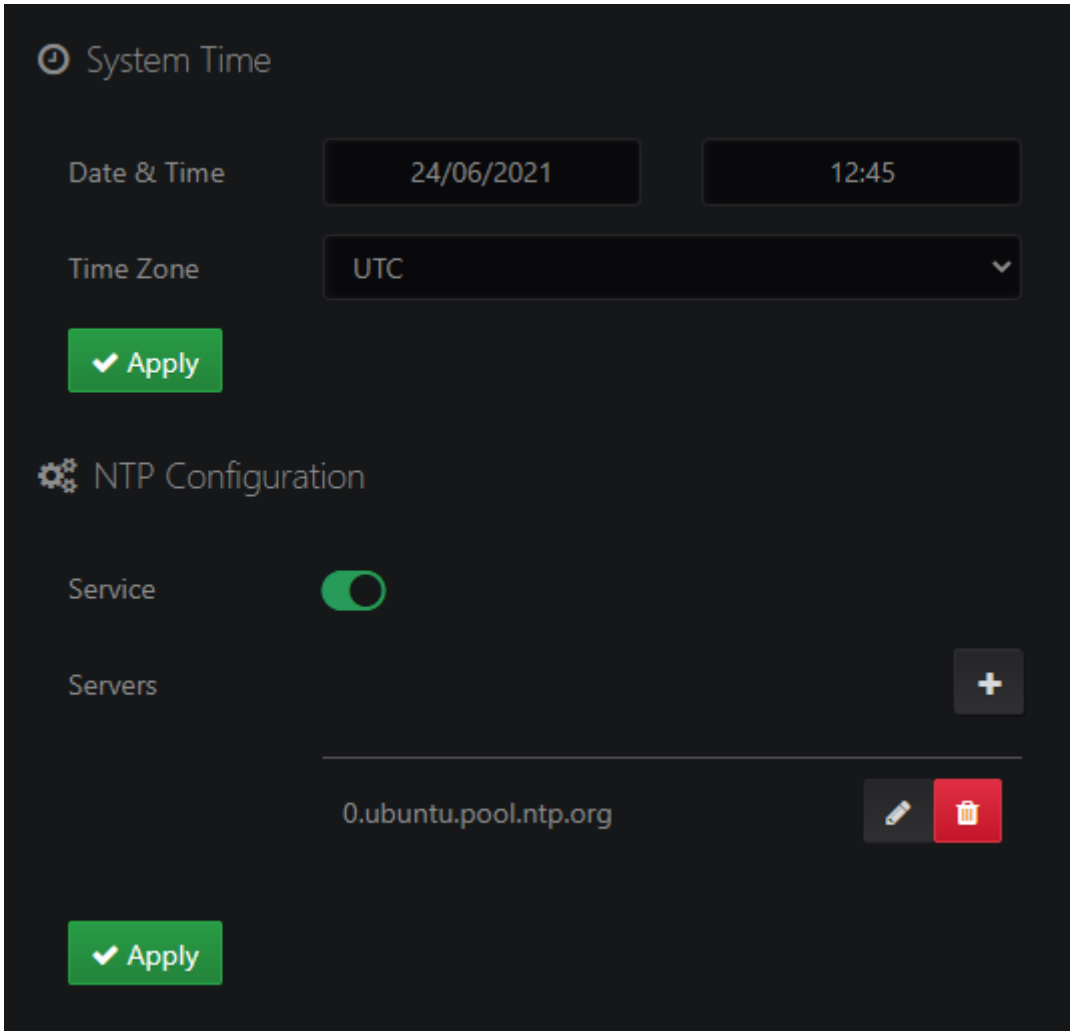
- Power off the device
- Unscrew the front panel drawer
- Remove the drawer
- Remove the SSD
- Install the new SSD in the drawer
- Place the drawer in the device
- Tighten the drawer screw
- Power on the device

Note that it will take several minutes for the system to install on the new SSD (~4–5 minutes depending on the model of SSD).

The recommended SSD types are Samsung EVO 1 TB and 2 TB (NVMe). They can be ordered directly from Profitap (sales@profitap.com).

3. IOTA Configuration

3.1. Time Settings

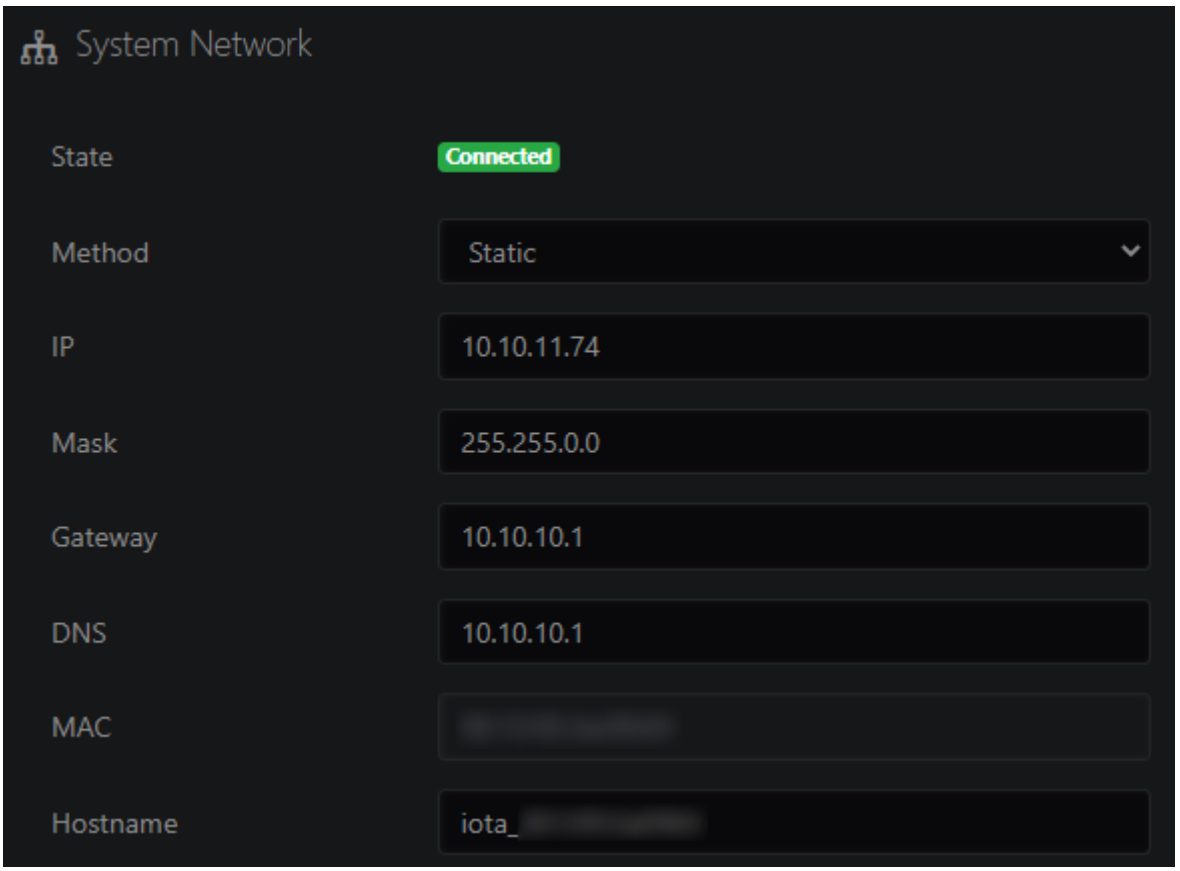


The ***IOTA Settings > Time Settings*** page allows the configuration of the system date, time, time zone, and NTP service. The NTP service is enabled by default, and can be disabled or enabled on this page. NTP servers can be added, modified, or removed. The appropriate time zone should be set manually,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

The system time is used by:

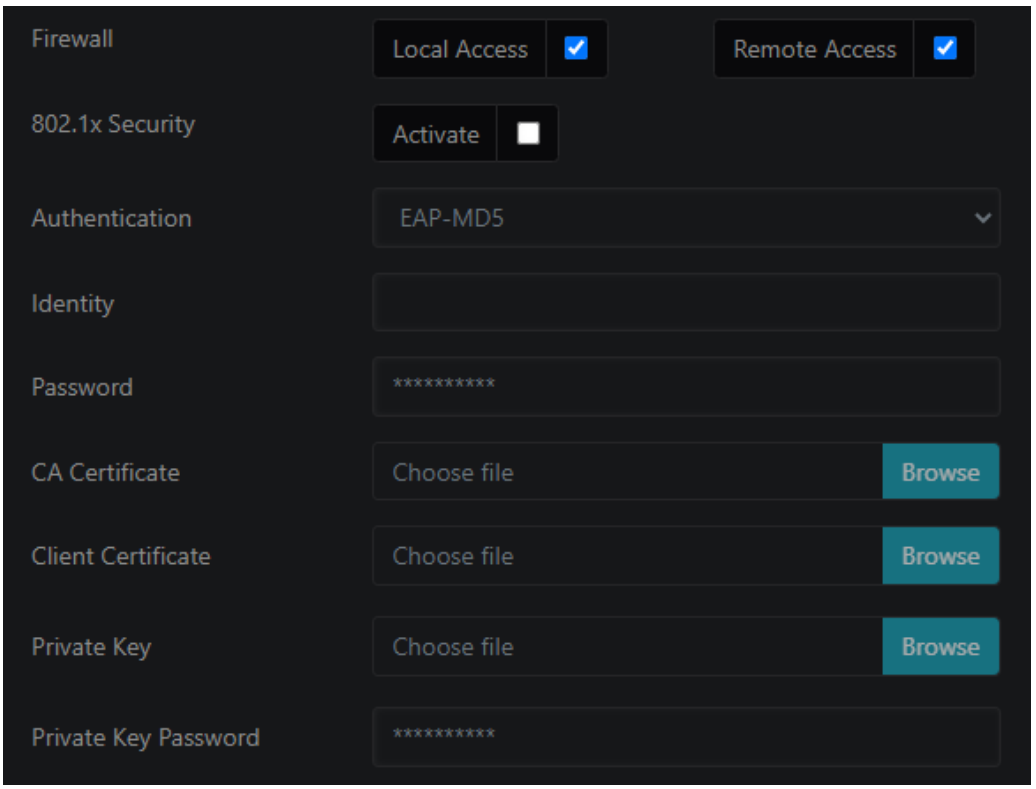
- The embedded OS.
- The capture interface, in order to constantly discipline the hardware timestamp counter. Changing the time may require a restart of the capture interface to take effect.

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.

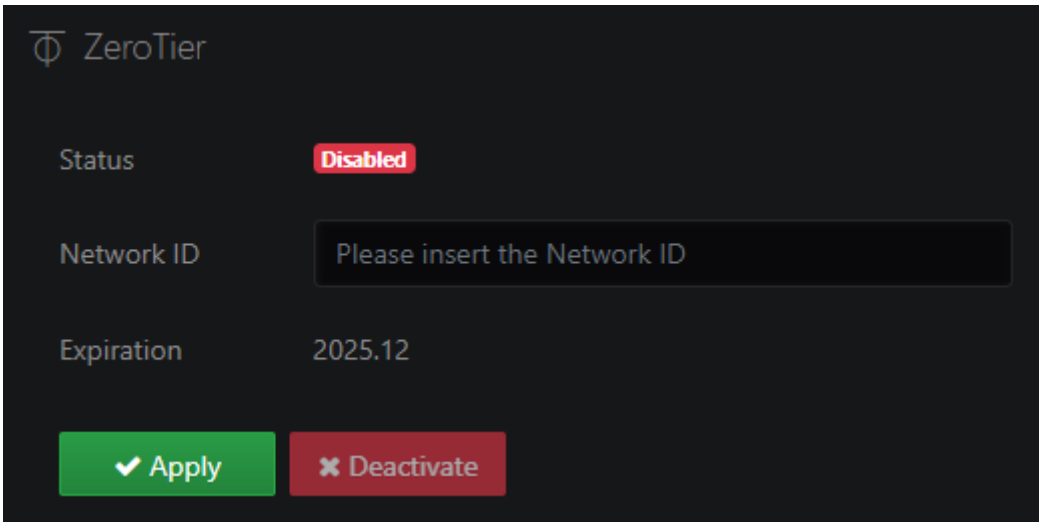
CA Certificate
The CA certificate file (Certificate Authority) in PEM format for the 802.1x EAP-TLS server (optional).

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



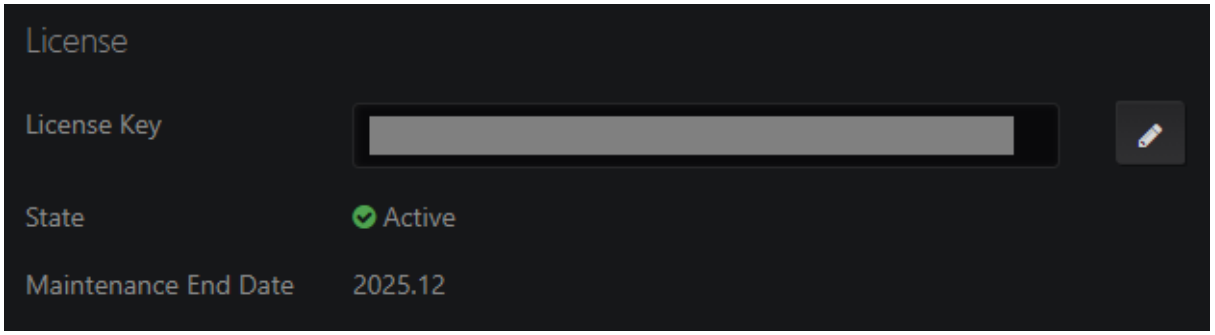
ZeroTier provides an easy way to remotely access the device via a P2P VPN and manage virtual networks on a cloud application. Visit www.zerotier.com for more information.

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

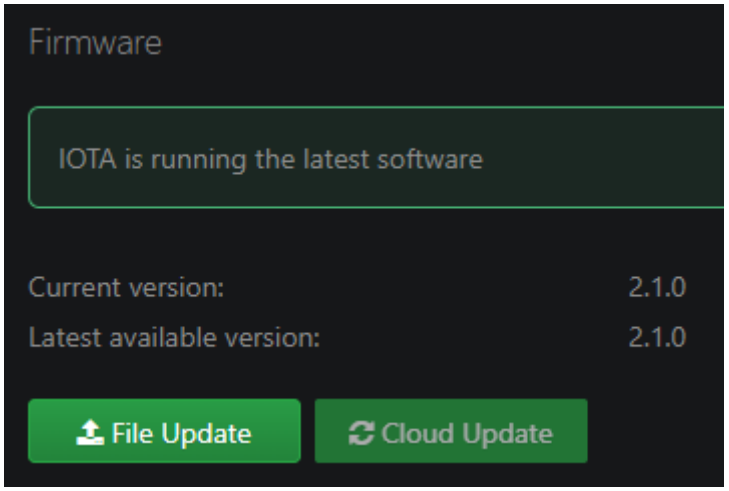
The ***IOTA Settings > Firmware & License*** page provides information about the currently-installed license and firmware, and the ability to update them.

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



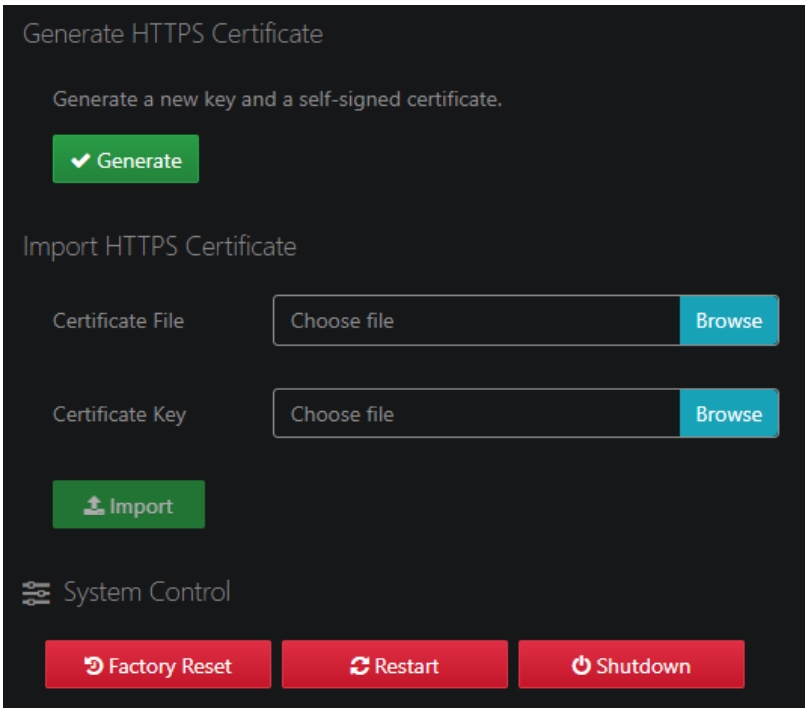
The *Firmware* section displays the currently-installed firmware version, the latest available version, and the *Release Notes* (changelog), and provides the ability to update the firmware.

If IOTA can access the internet, the latest available version number and changelog are fetched automatically and displayed, and the IOTA software can be updated via the *Cloud Update* button. If the device cannot access the internet, the latest IOTA software can be downloaded from ***https://iota.profitap.com/*** and updated via the *File Update* button.

Note: If your IOTA device is running a version older than v2.2.2, you will first need to update it to v2.2.2 or v2.2.3 before updating it to the latest version. The procedure is as follows:

1. Retrieve the v2.2.2 or v2.2.3 release file from https://iota.profitap.com/release/.
2. Update your IOTA device using this file by clicking the *File Update* button and selecting the file.
3. Update your IOTA device to the latest version, either by clicking the *Cloud Update* button, or by repeating the above steps using the latest release from https://iota.profitap.com/release/.

3.6. Administration



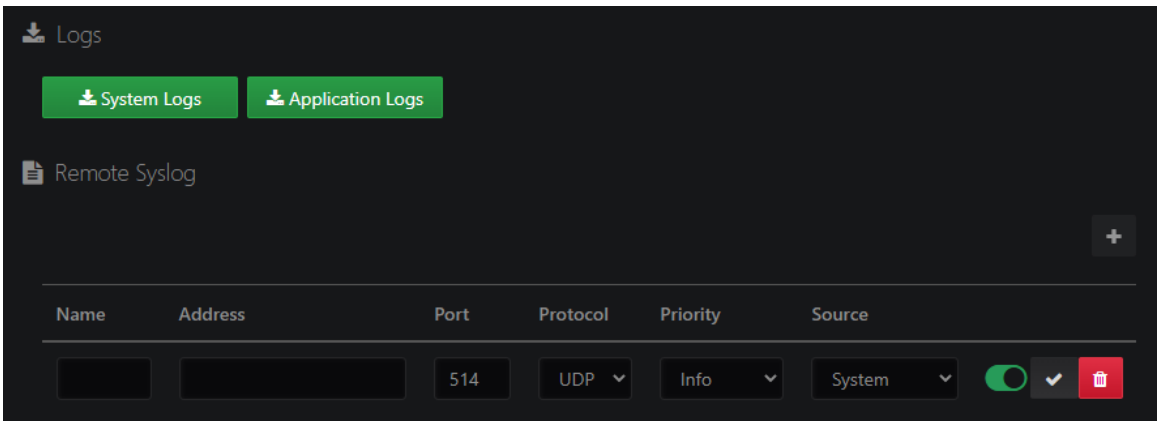
3.6.1. HTTPS Certificate

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. 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 > 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. Device Reset

3.8.1. Soft Reset

To reset the password and network parameters, use the following procedure: while the device is **POWERED**, press and hold the *START/STOP/RESET* button for 20 seconds. The procedure is complete when the LEDs turn green.

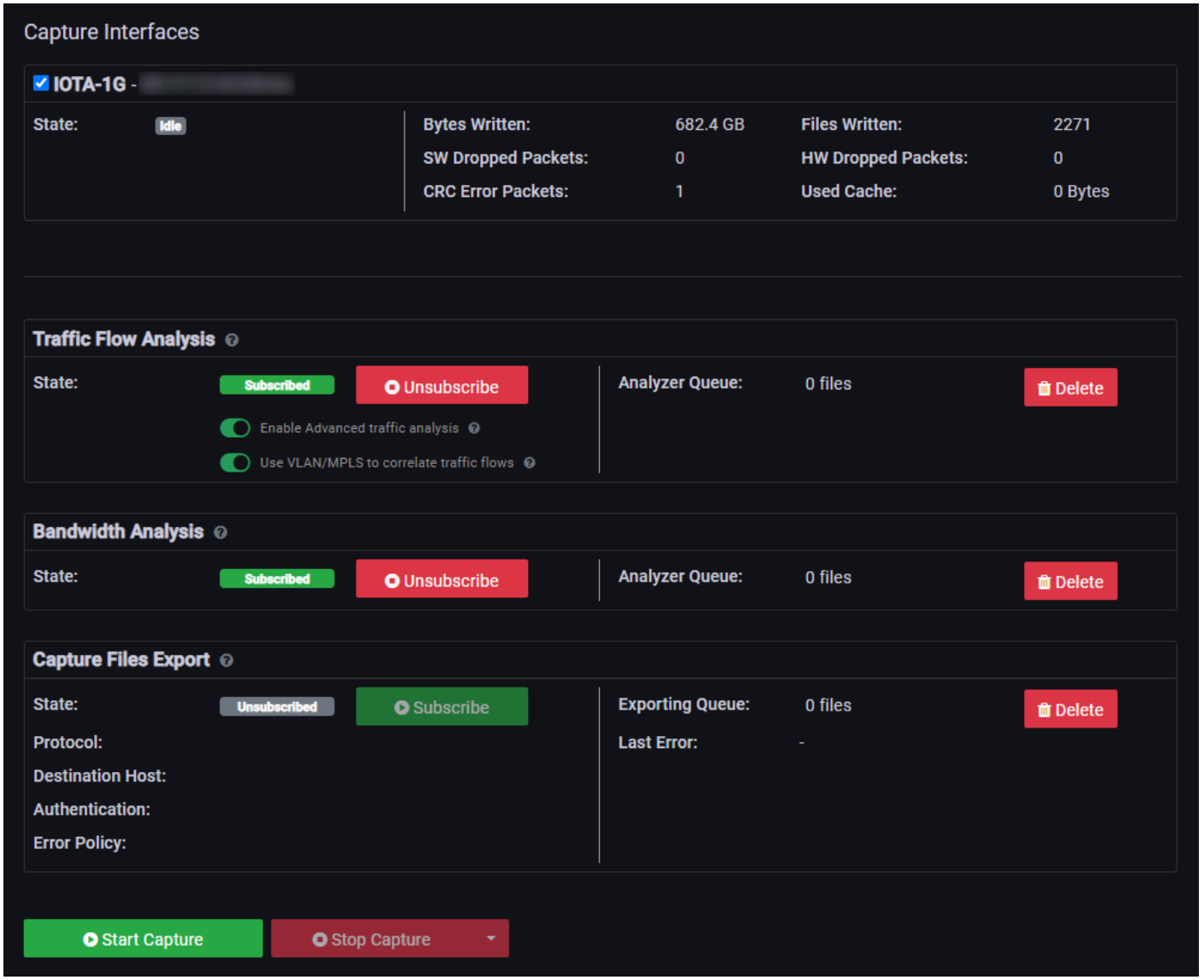
3.8.2. Factory Reset

To reset the IOTA to factory settings, use the following procedure: while the device is **UNPOWERED**, press and hold the *START/STOP/RESET* button, connect the power cable, and keep holding the button until the LEDs turn orange (~20 seconds). Release the button, and wait until the LEDs turn green (~5 minutes).

Note: Resetting the IOTA to factory settings will remove all data stored on the device. The software version will return to the one installed during production, and thus may need to be updated.

4. Capture Guide

4.1. Capture Control



The ***Capture > Capture Control*** page contains information and options regarding the capture of traffic, analysis of captured traffic, and exporting of capture files.

Traffic capture (capture interfaces) and traffic analysis (traffic flow analyzer) can be controlled independently. Traffic capture can be started or stopped via the *Start Capture* and *Stop Capture* buttons respectively. These will act on the selected capture interfaces. Clicking the arrow on the right-hand side of the *Stop Capture* button and selecting *Stop Capture & Analysis* will both stop the capture and unsubscribe the traffic analyzer.

4.1.1. Traffic Flow Analysis

The traffic flow analyzer is by default configured to be subscribed to process the new capture files. This means that any time a new PCAPNG is created, it will be added to the analyzer queue. Using the *Unsubscribe/Subscribe* button of the *Traffic Flow Analysis* section, it is possible to stop the analyzer from processing new files, without impacting the capture. It is also possible to reset the analyzer queue via the *Delete* button, in order to drop all of the pending files that are waiting for analysis. These can be (re)added to the analyzer queue from the *Data Vault > Captured Files* page.

Advanced traffic analysis can be enabled or disabled via the *Enable advanced traffic analysis* toggle. When disabled, the analyzer will stop recording metrics for the VoIP, TLS and Modbus dashboards, which will increase overall traffic analysis performance.

If *Use VLAN/MPLS to correlate traffic flows* is enabled, VLAN tags and MPLS labels will be used to identify traffic flows. Otherwise, they will be ignored.

4.1.2. Bandwidth Analysis

The bandwidth analysis engine can be started or stopped via the *Subscribe/Unsubscribe* button of the *Bandwidth Analysis* section. This engine provides accurate analysis of bandwidth usage, which can be visualized in the dashboards (e.g. *Bandwidth* and *Microbursts* dashboards). It is also possible to reset the analyzer queue via the *Delete* button, in order to drop all of the pending files that are waiting for analysis.

4.1.3. Capture Files Export

The capture file export engine can be started or stopped via the *Subscribe/Unsubscribe* button of the *Capture Files Export* section. This engine exports new capture files to an external host, configured on the *Data Vault > Capture Export* 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.

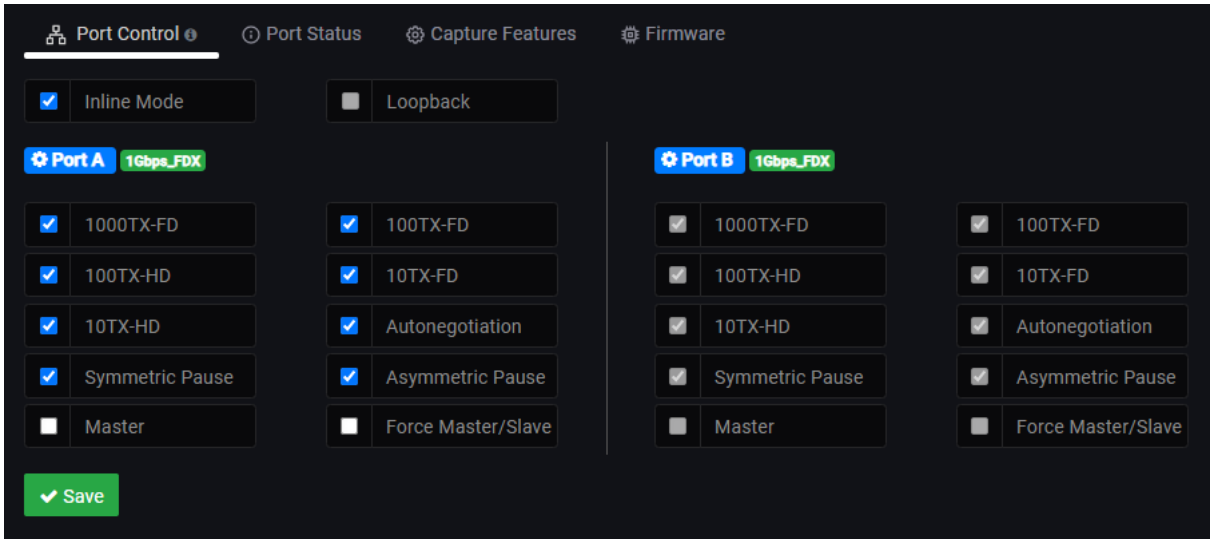
4.2. Interface Configuration

The ***Capture > Interface Configuration*** page contains information and settings for the capture interface. To change the interface settings, several tabs are available.

4.2.1. Port Control

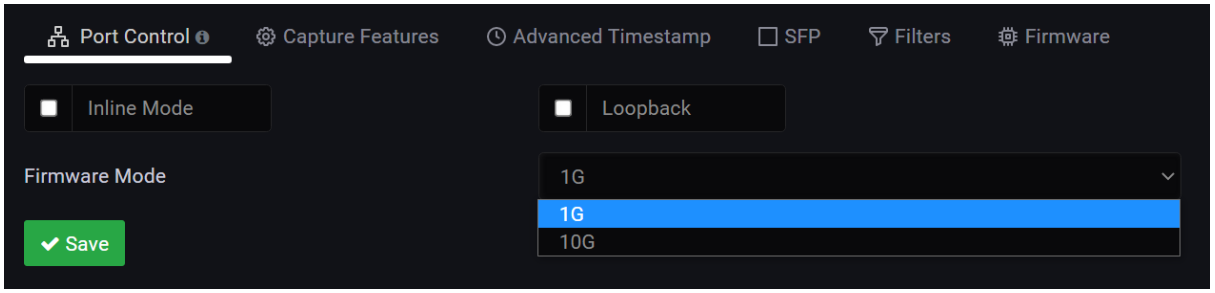
If IOTA is intended to be used in-line, the appropriate configuration must be set. *In-Line mode* is the default mode (*Inline Mode* checkbox ticked). IOTA can be set to *SPAN mode* by unticking the *Inline Mode* checkbox.

IOTA 1G / 1G+



Port speed and behavior can be set on this screen.

IOTA 10G / 10G+

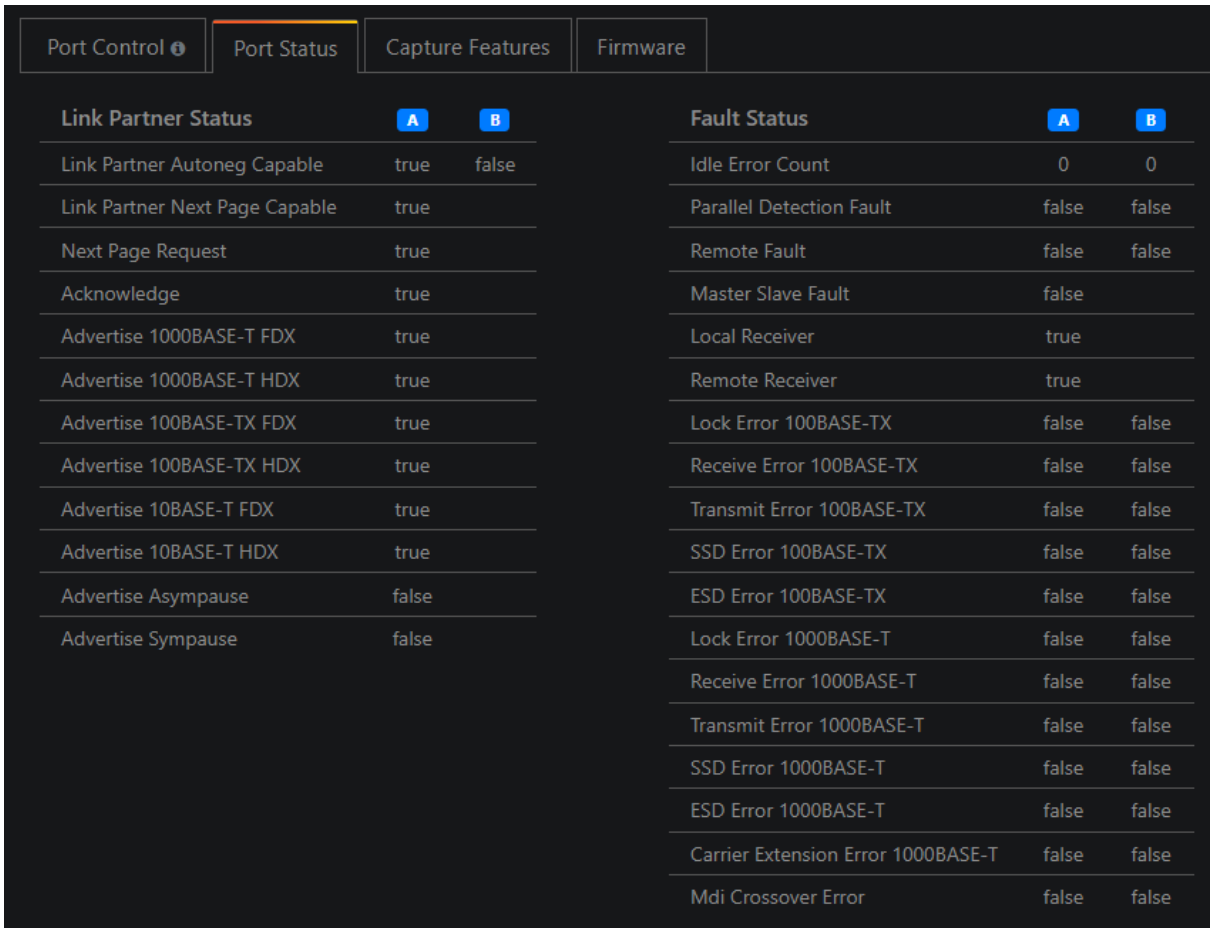


Loopback mode can be enabled when SPAN mode is enabled (*Inline Mode* checkbox unticked) by ticking the *Loopback* checkbox.

The firmware can be set to either 1G or 10G mode via the *Firmware Mode* drop-down menu.

4.2.2. Port Status

IOTA 1G / 1G+

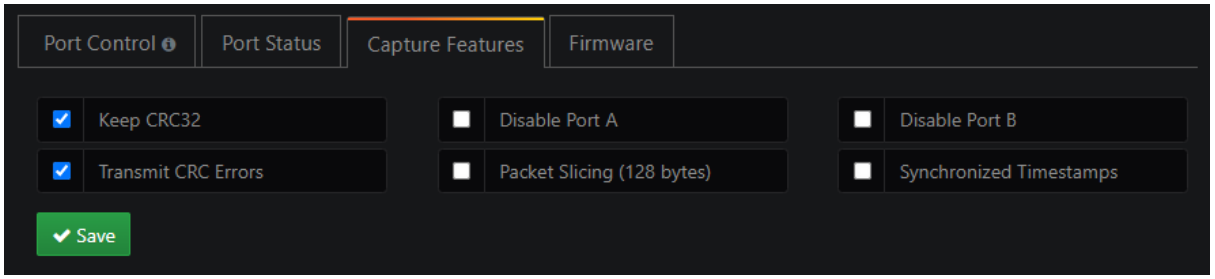


This tab provides an overview of the Link Partner Status and Fault Status for both ports A and B.

4.2.3. Capture Features

This tab allows the configuration hardware capture settings. The available settings depend on the IOTA model. Features can be enabled and disabled by ticking or unticking the related checkboxes.

IOTA 1G / 1G+



Keep CRC32
The CRC32 information (32-bit Frame Check Sequence) located at the end of the packets will be kept in the capture.

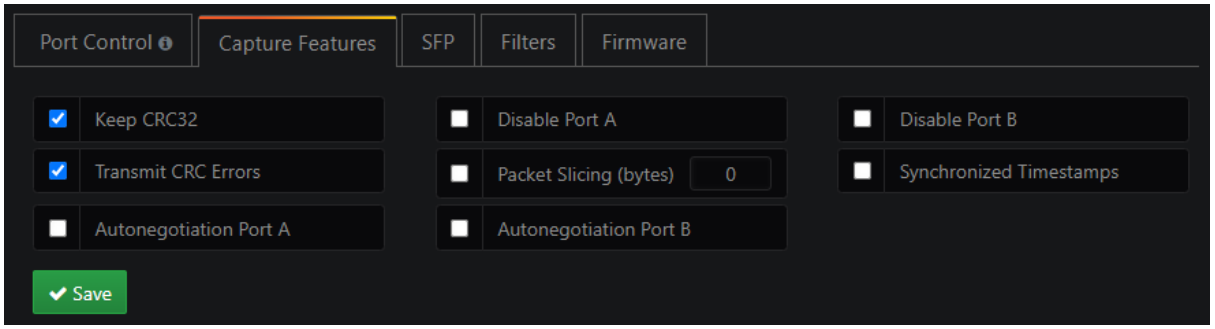
Disable Port A
Frames from port A will not be captured.

Disable Port B
Frames from port B will not be captured.

Transmit CRC Errors
Packets with CRC errors will be included in the capture. These packets are usually filtered out by network interfaces.

Packet Slicing (128 bytes)
The payload of every captured frame will be dropped, keeping only the header information (the first 128 bytes) up to the application layer.

Synchronized Timestamps
Allows the capture interface's clock to be disciplined with the IOTA's embedded OS clock, thereby avoiding drift.



Keep CRC32
The CRC32 information (32-bit Frame Check Sequence) located at the end of the packets will be kept in the capture.

Disable Port A
Frames from port A will not be captured.

Disable Port B
Frames from port B will not be captured.

Transmit CRC Errors
Packets with CRC errors will be included in the capture. These packets are usually filtered out by network interfaces.

Packet Slicing (bytes)
Only the specified amount of data will be captured for each frame, starting from the beginning of the frame, specified in bytes.

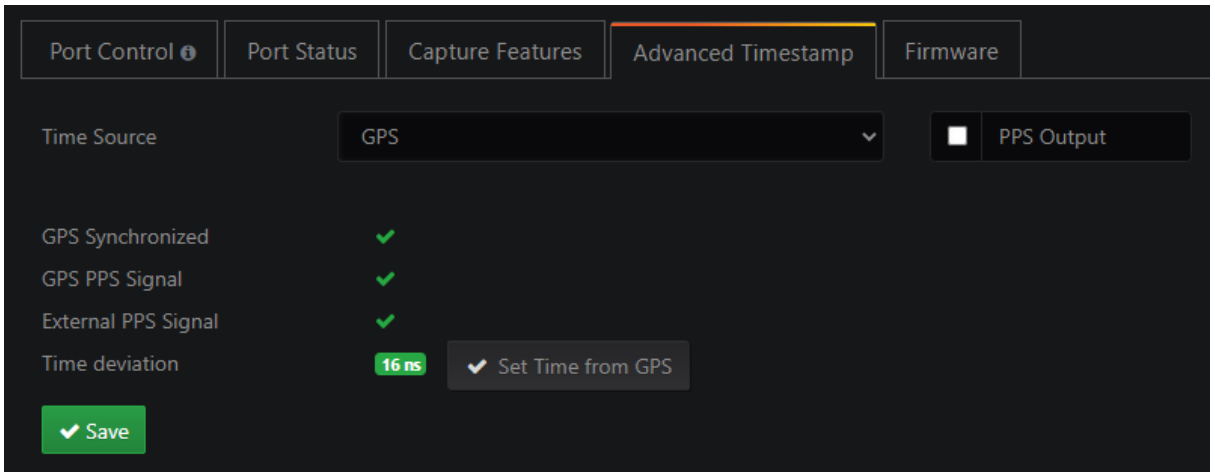
Synchronized Timestamps
Allows the capture interface's clock to be disciplined with the IOTA's embedded OS clock, thereby avoiding drift.

Autonegotiation Port A
Enables Ethernet autonegotiation on port A.

Autonegotiation Port B
Enables Ethernet autonegotiation on port B.

4.2.4. Advanced Timestamp

IOTA 1G+ / 10G+



Time Source
Select the source from which the time will be used for timestamping:

- **System**: Use the system time and ignore any PPS signal coming from the PPS port.
- **System PPS**: Use the system time and synchronize it with the PPS signal coming from the PPS port (if present).
- **GPS**: Use the time received from the GPS antenna connected to the GPS port (if present).

PPS Output
If checked, the PPS port will be set to output mode, sending out a PPS signal if the GPS is synchronized.

GPS Synchronized
Shows whether the GPS port is receiving time information from the GPS antenna.

GPS PPS Signal
Shows whether the GPS signal is stable enough for GPS PPS to be used.

External PPS Signal
Shows whether the PPS port is receiving a PPS signal.

Time deviation
Shows the deviation between the internal clock and the reference (external PPS, GPS PPS, or system PPS).

Set Time from GPS
Forces device to instantly synchronize its timestamp clock with the GPS source (if available).

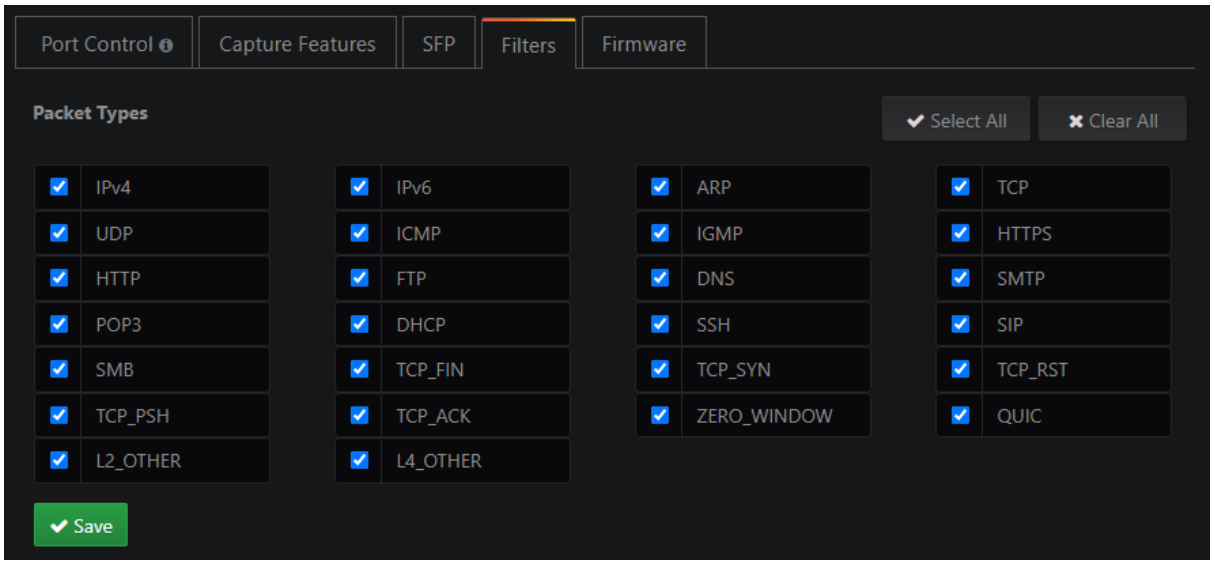
4.2.5. SFP

IOTA 10G / 10G+

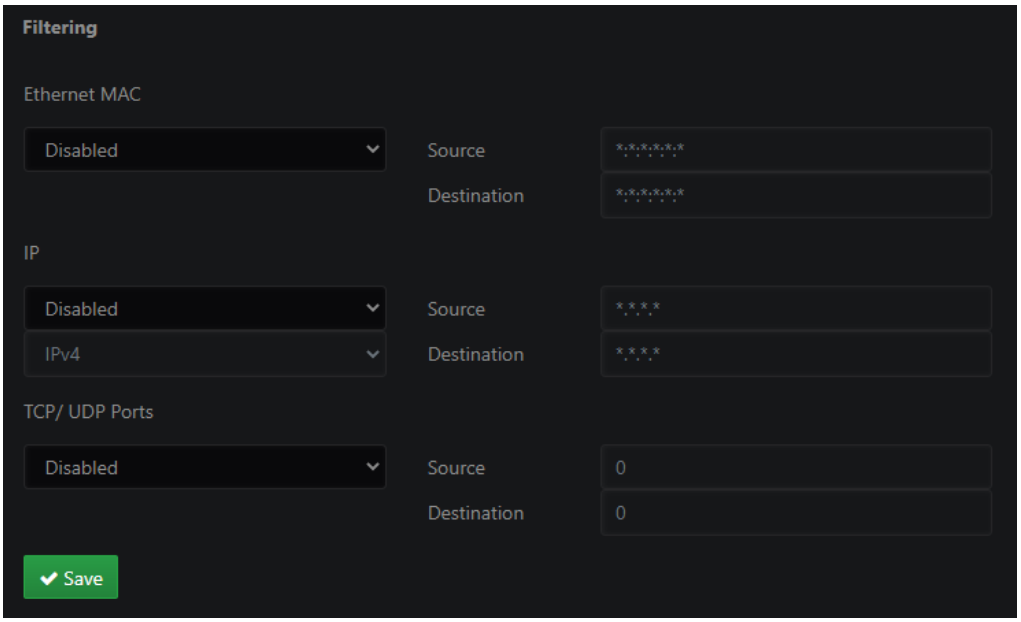
This tab provides SFP information for both port A and B.

4.2.6. Filters

IOTA 10G / 10G+

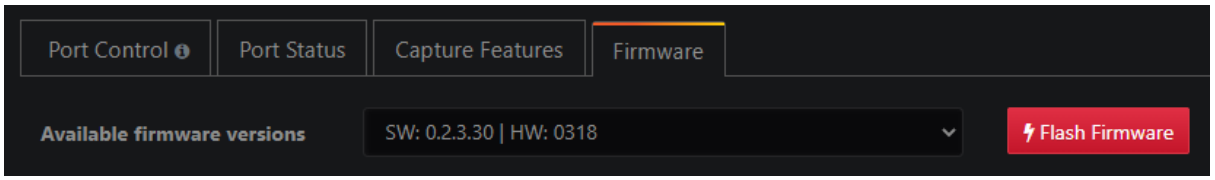


The hardware filters in the Filters tab allow you to include or exclude packets based on their type. Selected packet types will be included in the capture, and unselected packet types will be excluded.



The *Filtering* section allows filtering on Ethernet MAC, IPv4/6 addresses, and TCP/UDP ports, on source, destination, both, or either.

4.2.7. Capture Interface Firmware



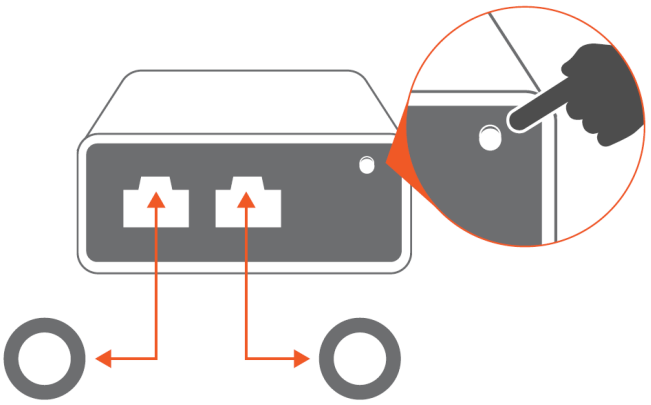
The **Capture > Interface Configuration > Firmware** page contains information about the capture interface's firmware, and provides the ability to update it. The latest capture interface firmware version is always included when updating the IOTA firmware. The update is not performed automatically.

On the *Interface Configuration* dashboard, compare the *HW Firmware Version* with the *Available Firmware Version*. If they are the same, you have the latest firmware version. If the *Available Firmware Version* is higher, you can click *Flash Firmware* to update your unit to the latest capture interface firmware. A progress bar shows the progress of the installation. After a firmware version is successfully updated, a power cycle is recommended. After the power cycle, go back to the *Interface Configuration Dashboard* and verify that you are now on the latest version.

Note: It is not recommended to update the capture interface firmware while your unit is in a production environment, as it may temporarily disconnect the A and B ports during the update.

4.3. Autonomous Capture

To be able to capture traffic in networks where remote access over the network is not allowed or not possible, you can start IOTA's autonomous capture feature by pressing the *START/STOP* button located at the front of the device.



START: Press the *START/STOP* button while no capture is in progress (*CAPTURE* LED not blinking) to start the capture. IOTA will use the settings configured in *Capture > Interface Configuration*.

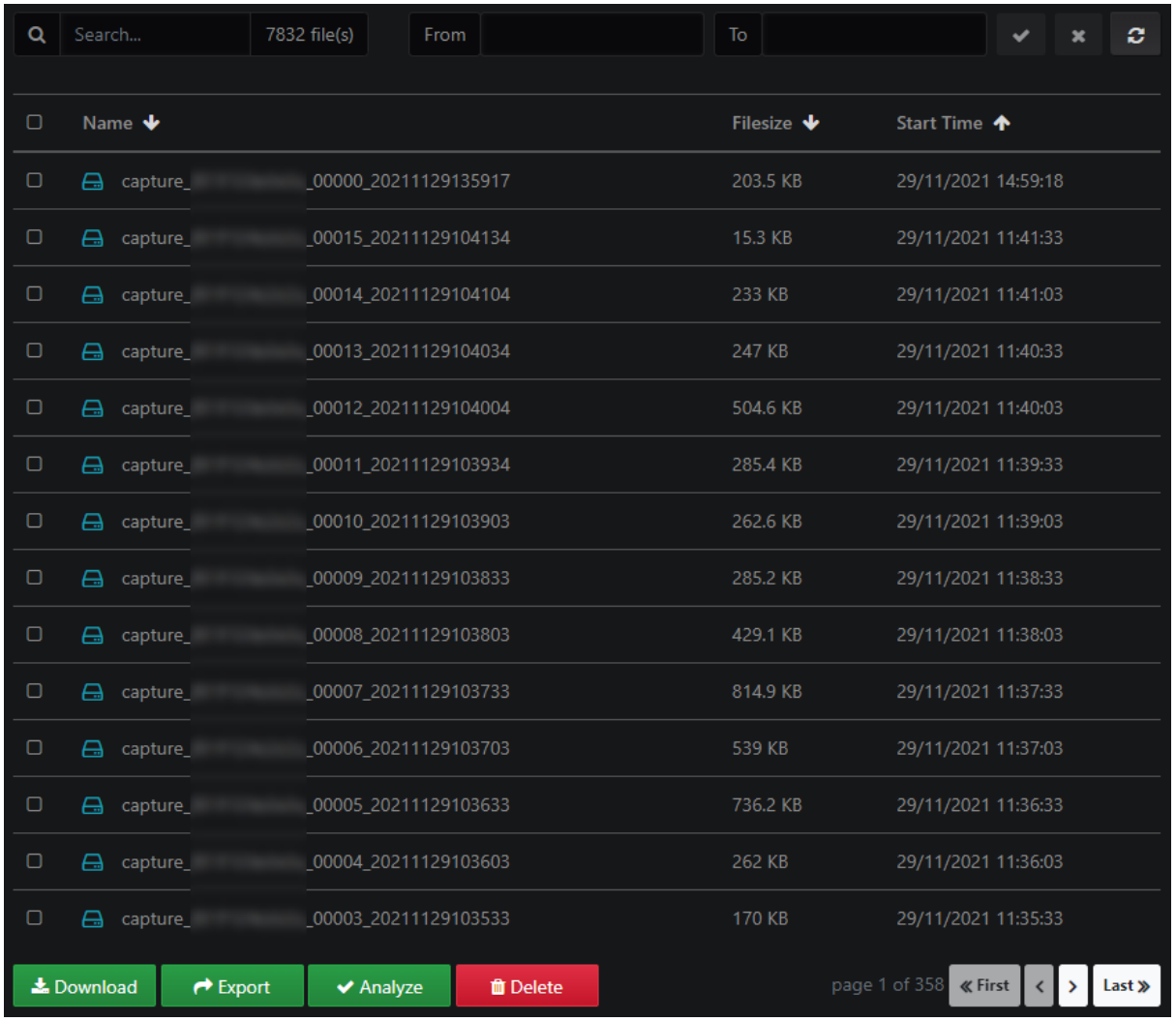
STOP: Press the *START/STOP* button while a capture is in progress (*CAPTURE* LED blinking) to stop the capture.

SHUTDOWN: Press and hold the *START/STOP* button for 10 seconds for safe device shutdown (note that holding the button for 20 seconds will initiate a Soft Reset). This will stop the capture and unmount the internal storage in order to end the capture session.

Note: Make sure the appropriate settings have been applied in *Capture > Interface Configuration* before deploying the IOTA in the network you want to analyze.

4.4. Data Vault

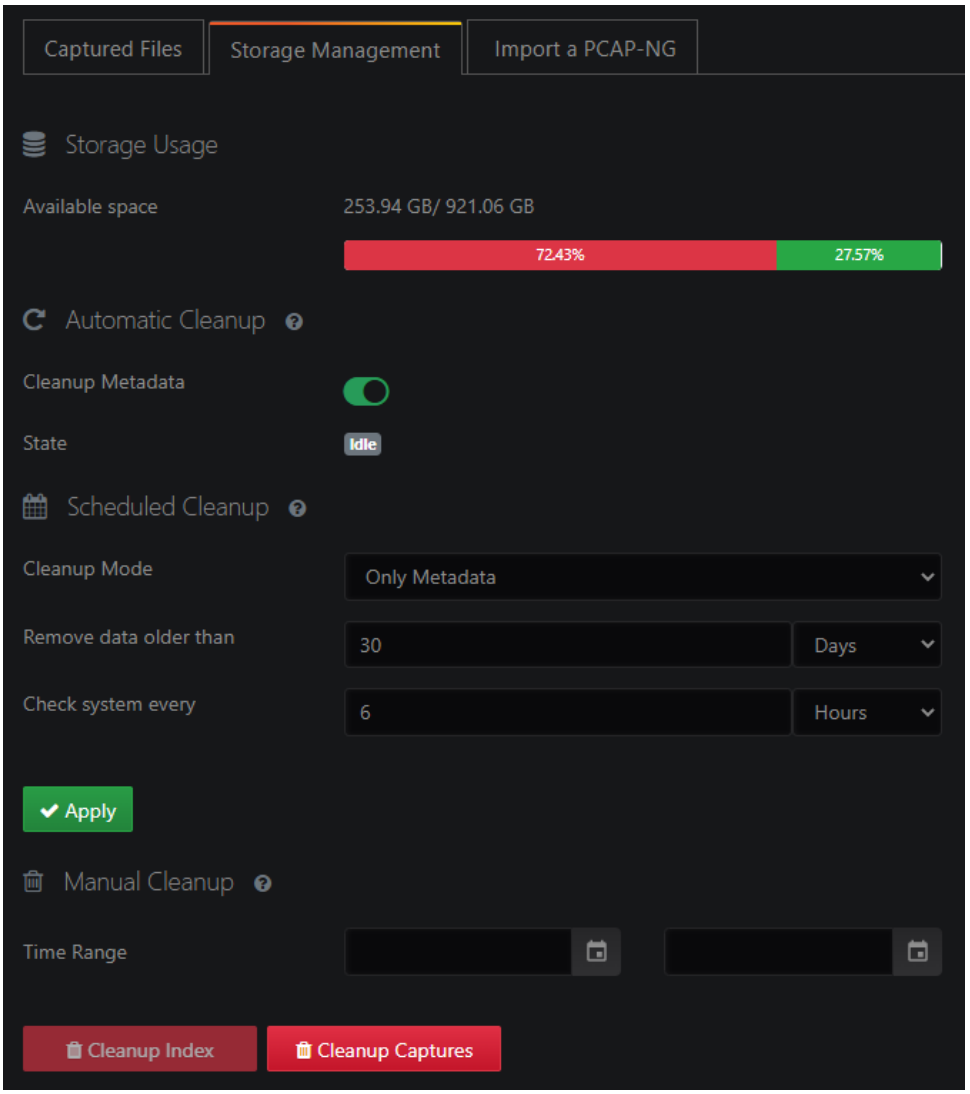
4.4.1. Captured Files



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.

4.4.2. 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.

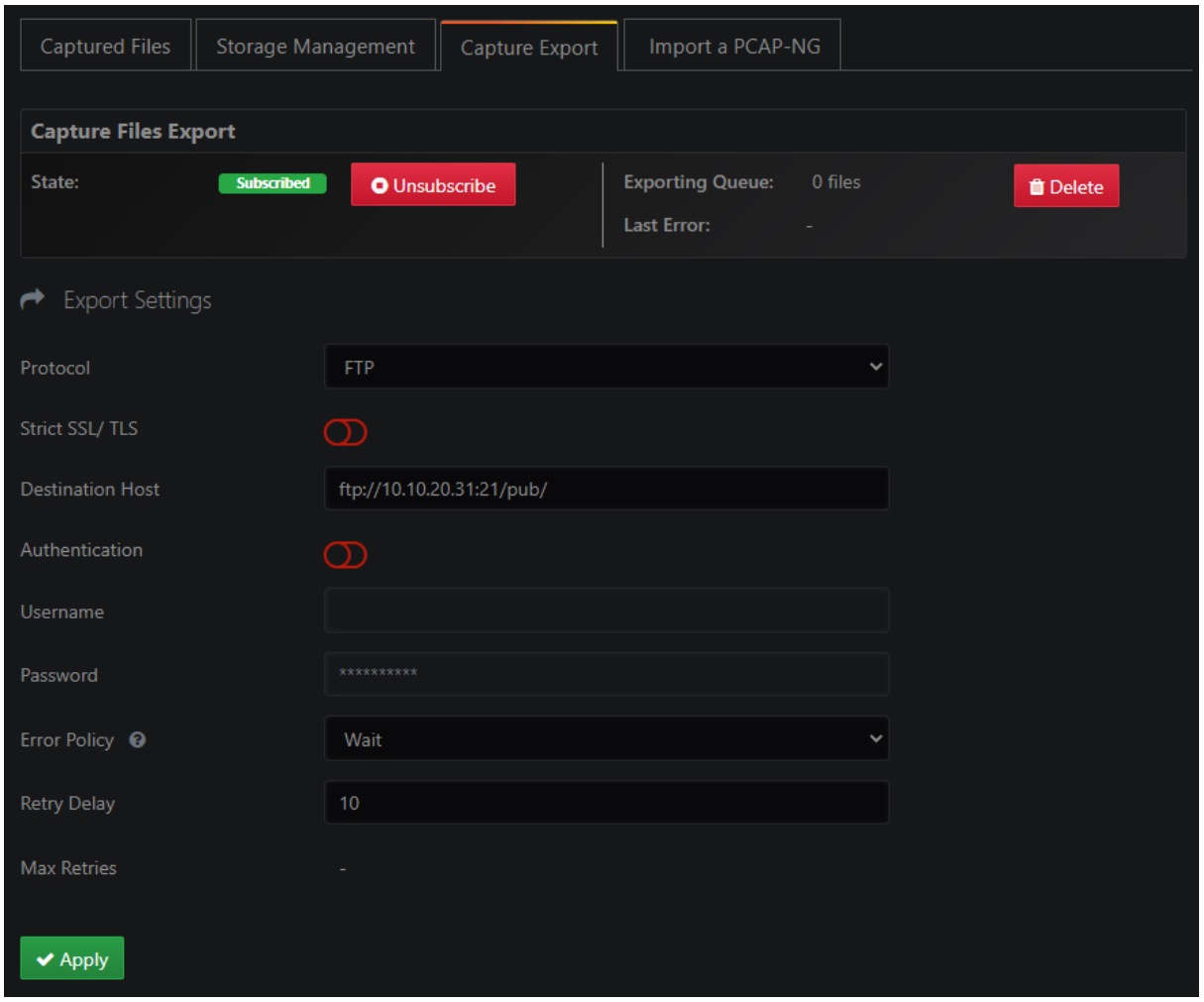
Note: Disabling the automatic cleanup of metadata will reduce the space for new capture files, and may slow down the dashboards visualization.

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
Indexed capture metadata and capture files can be deleted via the *Cleanup Index* 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.

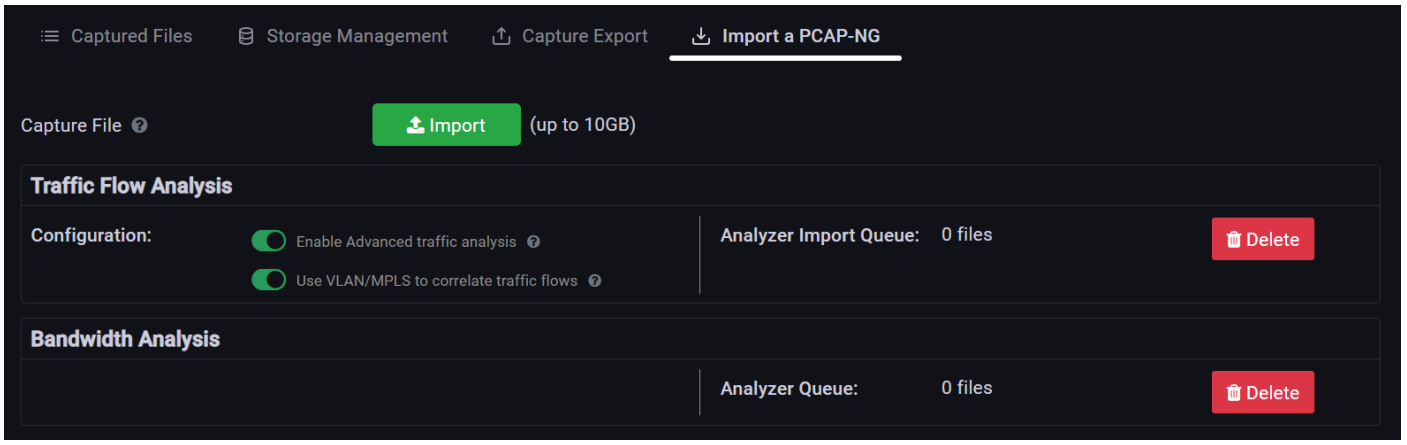
4.4.3. Capture Export



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 *Subscribe/Unsubscribe* button. When subscribed, 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.

4.4.4. Importing a PCAP-NG File

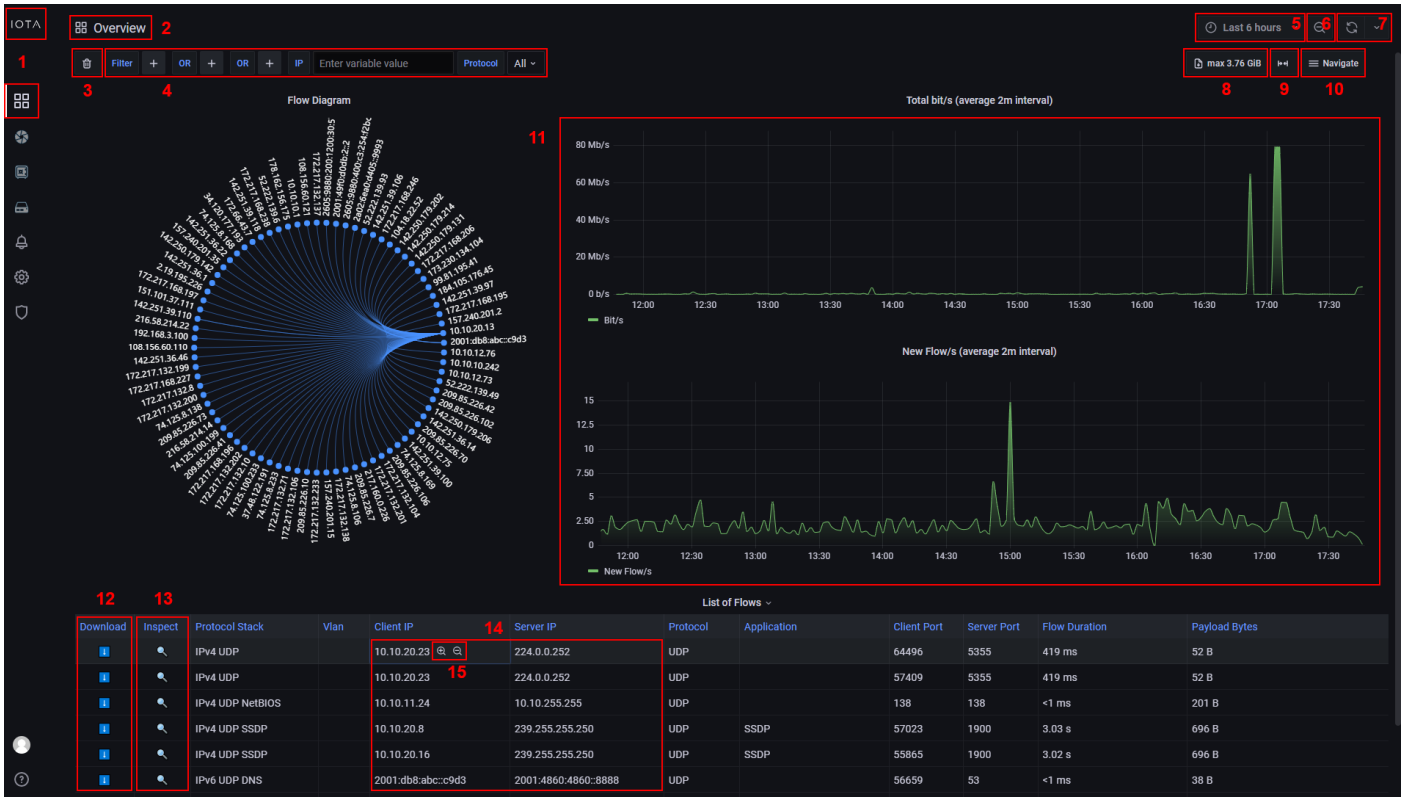


PCAPNG and PCAP capture files can be imported via the *Import* button. Imported files are stored on the device and automatically added to the traffic analyzer and bandwidth analyzer queues.

The capture analysis and the PCAP import analysis are running in parallel without impacting each other. The analyzer queues can be deleted via the *Delete* buttons. Deleting the analyzer queues 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.

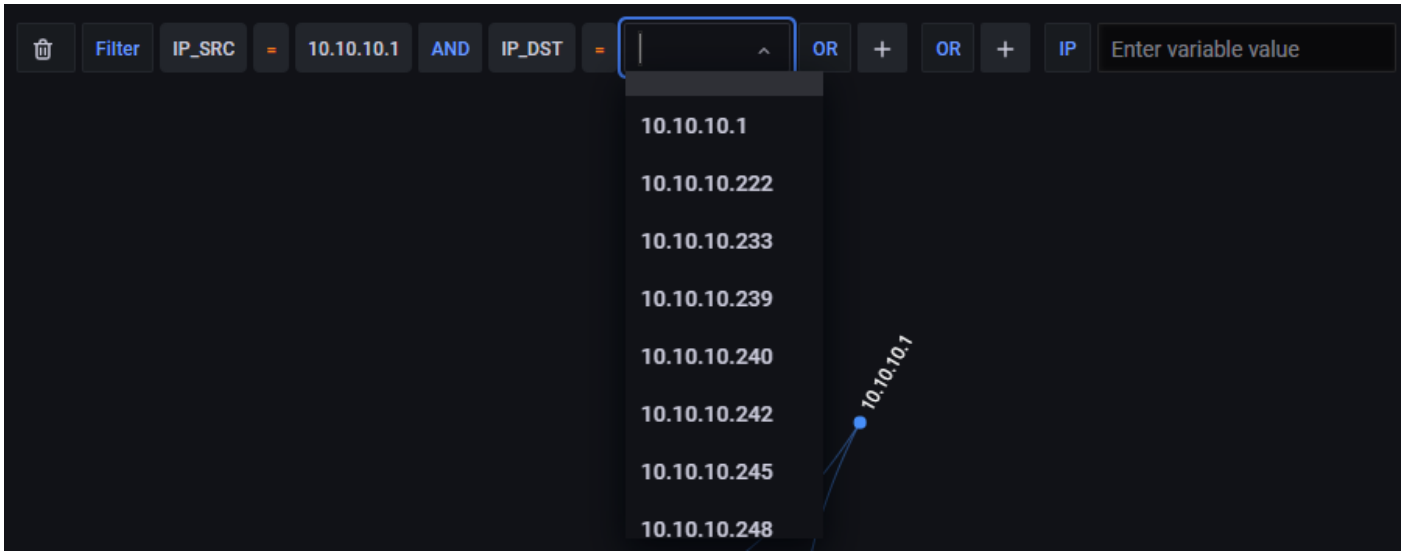
[14] Click any IP address to navigate to the Host Details dashboard for this IP address.

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

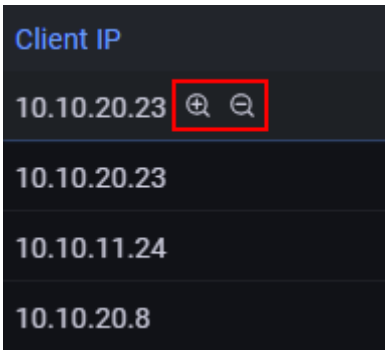
5.2. Traffic Filtering

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.

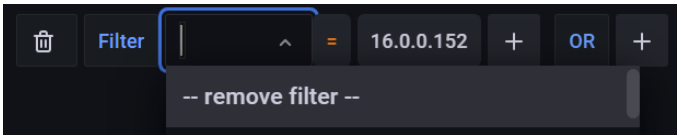
These filters are applied both to the dashboard display and to the *Download PCAP* feature.



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--*.



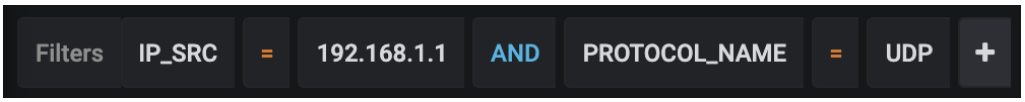
The *Custom Search* field accepts various filter statements, such as filters from the *Filters* section using both the variable name and value (e.g. *IP_SRC:10.10.10.10*), only the value (e.g. *10.10.10.10*), and modifiers such as *NOT* (e.g. *!IP_SRC:10.10.10.10*), *AND* (e.g. *IP_SRC:10.10.10.10 AND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

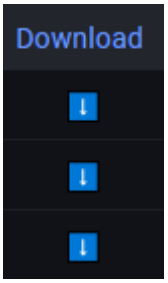
Use the "Download PCAP" button to download the PCAPNG file of the traffic for the selected time range. The following filters also apply to the downloaded PCAPNG files: IP address, MAC address, VLAN ID, Protocol, Port.



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

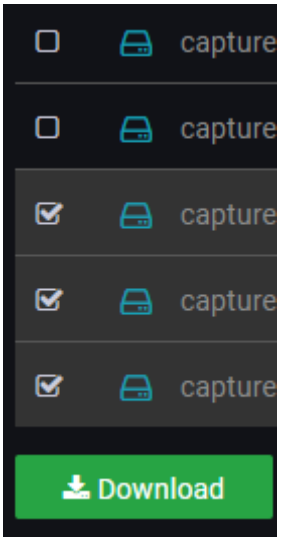
● Flow download buttons

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