

IOTA 1G

USER MANUAL

Top Client			Server IP		
Data	Average bps	Max bps	Data	Average bps	Max bps
2.98 GB	107.53 kbps	2.42 Mbps	172.28.190.238	2.01 GB	413.78 kbps
489.02 MB	243.02 kbps	2.31 Mbps	10.0.0.10	974.08 MB	101.46 kbps
11.38 MB	113.95 kbps	529.08 kbps	192.168.1.1	506.54 MB	121.78 kbps
3.57 MB	12.60 kbps	670.73 kbps	192.168.1.230	615.83 kB	71.40 kbps
1.27 MB	49.24 kbps	57.07 kbps	10.13.41.195	51.51 kB	17.41 kbps
1.25 MB	49.64 kbps	57.08 kbps	192.168.1.255	21.54 kB	340.32 bps
18.72 kB	222.50 bps	288.00 bps	192.168.195.1	1.84 kbps	1.84 kbps
18.36 kB	216.50 bps	288.00 bps			
4.05 kB	658.67 bps	1.02 kbps			
3.57 kB	988.00 bps				



www.profitap.com

*BRINGING CLARITY INTO NETWORKS.
ANYTIME. ANYWHERE.*

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

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

or by email:

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

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

[*https://www.profitap.com/resource-center/*](https://www.profitap.com/resource-center/)

TABLE OF CONTENTS

1. Product Overview **1**

- 1.1 Hardware Overview 1
- 1.2 Specifications 2
- 1.3 Interfaces & LED Behavior 3

2. Getting Started **5**

- 2.1 Deploying the IOTA 5
- 2.2 Powering the device 7
- 2.3 Access IOTA over network 7
- 2.4 IOTA Configuration 9
 - System Time 9
 - System Network 10
 - Access / Internal Firewall 10
 - ZeroTier 11
 - System Control 11
 - System Updates 12

3. Capture Guide **13**

- 3.1 Capture Control 13
- 3.2 Interface Configuration 15
 - Port Control 15
 - Port Status 15
 - Capture Features 16
 - Firmware 17
- 3.3 Autonomous Capture 17

3.4 Data Vault	18
Captured Files	18
Import a PCAP-NG	18
3.5 Data Management	19
Disk Usage	19
Schedule a Cleanup	19
Manual Disk cleanup	20

4. Analysis Guide **21**

4.1 Dashboard overview	21
4.2 Basic Navigation	22
Main dashboard selection menu	22
Time range selection	23
Filtering traffic	24
Graphs	25
4.3 PCAP file download	26

5. Legal **28**

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 engineers 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, eliminating the need of an on-site network expert.

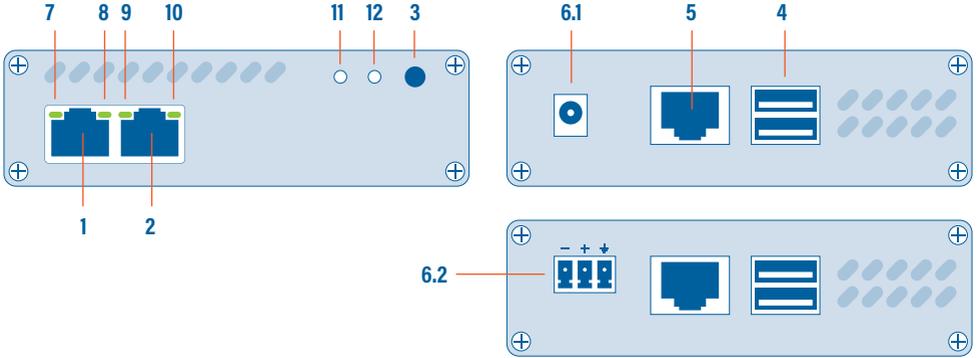


1.2 SPECIFICATIONS

IN-LINE MODE		Yes
IN-LINE LATENCY		1G: 380 ± 8 ns 100M: 720 ± 24 ns 10M: 7600 ± 25 ns
IN-LINE JITTER		20 ns
DUAL SPAN INPUTS MODE		Yes
FAIL-SAFE		Yes
CAPTURE PERFORMANCE		3.2 Gbps / 3.2 Mpps
PACKET PROCESSOR		Yes, 2 Gbps / 3.2 Mpps
HARDWARE TIMESTAMPING		Yes: 8 ns, NTP synchronized
INTERNAL STORAGE		1 TB
POWER INPUTS	12V MODEL	12 VDC
		PoE (management RJ45)
	24V MODEL	24–48 VDC
		PoE (management RJ45)
POWER CONSUMPTION		12 W
MANAGEMENT	Interfaces	10/100/1000 Ethernet
		2 x USB 3.0
	Services	HTTPS (server), UPnP/VPN

1.3 INTERFACES & LED BEHAVIOR

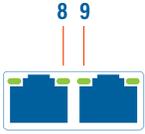
IOTA 1G Interface



- | | |
|---------------------------|-----------------------------------|
| 1, 2 Ethernet port A, B | 5 RJ45 Management port (PoE) |
| 3 START/STOP/RESET button | 6.1 12 VDC power input |
| 4 2 x USB 3.0 port type A | 6.2 24-48 VDC power input |
| | 7, 8, 9, 10, 11, 12 Activity LEDs |

IOTA 1G LED Behavior

LEDs	STATE	MEANING
	7 and/or 10 steady green	The port is linked.
	7 and/or 10 blinking green	The port is linked and has RX/TX activity (traffic is passing through).
	8 steady green 9 off	Capture interface operating at 10 Mbps speed.
	8 blinking green 9 off	Capture interface is initializing.
	8 off 9 steady green	Capture interface operating at 100 Mbps speed.
	8 off 9 blinking green	Capture interface firmware is corrupted.

<i>LEDs</i>	<i>STATE</i>	<i>MEANING</i>
	8+9 steady green	Capture interface operating at 1 Gbps speed.
	8+9 blinking green	The port is linked and has RX/TX activity (traffic is passing through).
	8+9 alternating blinking	Capture interface cannot find a common speed between the connected devices.

<i>LEDs</i>	<i>LED 11 STATE</i>	<i>LED 12 STATE</i>	<i>MEANING</i>
	Orange Blink	OFF	Booting
	Green	Green	Running
	Green	Green Blink	Capturing
	Green	Orange Blink	Capturing warning
	Green	Red	Disk Full
	Orange Green Blink	Orange Green Blink	Updating
	Red Blink	Red Blink	Hardware Failure
	Orange Blink	Orange Blink	Factory Reset
	Green Blink	OFF	Shutting down
	OFF	OFF	Shutdown completed

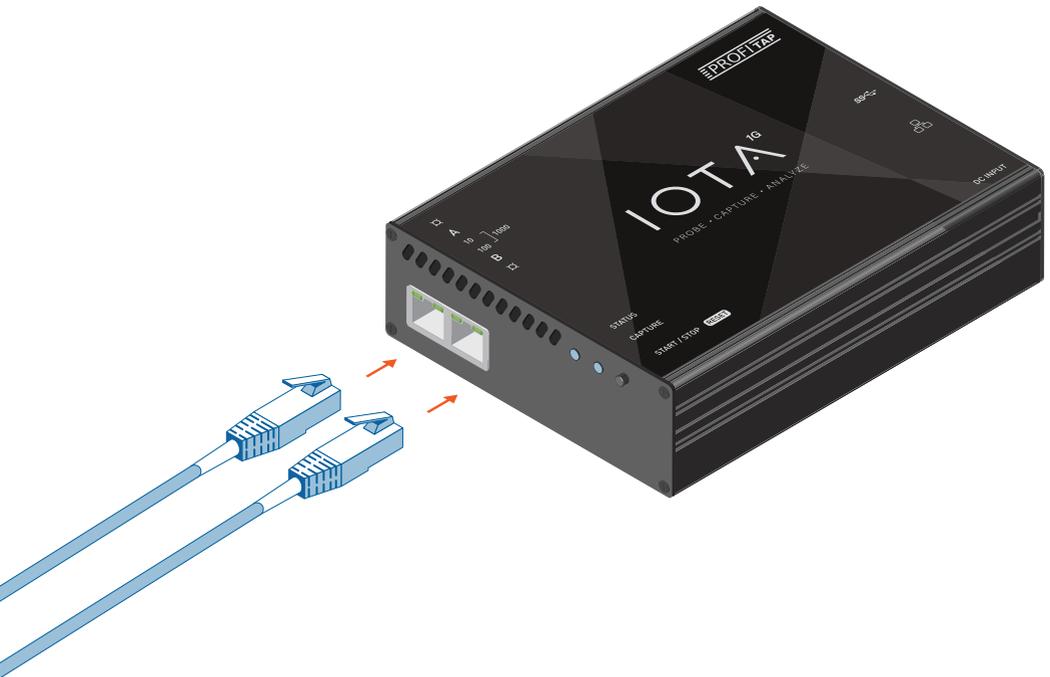
GETTING STARTED

2.1 DEPLOYING THE IOTA

IOTA 1G

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

- ▶ **Note:** When deploying IOTA 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.



IOTA 1G RACKMOUNT MODEL

The rackmount model 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 THE DEVICE

Connect the 12V/2.5A DC power supply, or the 24–48VDC terminal block, depending on the IOTA model. Alternatively, the device can be powered via PoE, over the management port. 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.

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

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

2.3 ACCESS IOTA OVER NETWORK

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

The full URL should be: `https://x.x.x.x:3000`

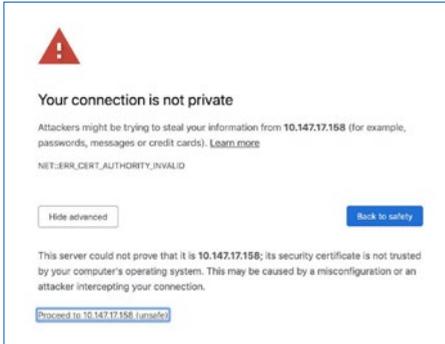
DHCP mode is enabled by default. If no IP is assigned to the IOTA, the default fallback IP is **169.254.1.1**.

For the initial login, use the following credentials:

Default username: **admin**

Default password: **admin**

- ▶ **Note:** In case your browser displays a 'Your connection is not private' warning, click on **advanced > proceed to...** URL at the bottom to proceed to the IOTA login page.



2.4 IOTA CONFIGURATION

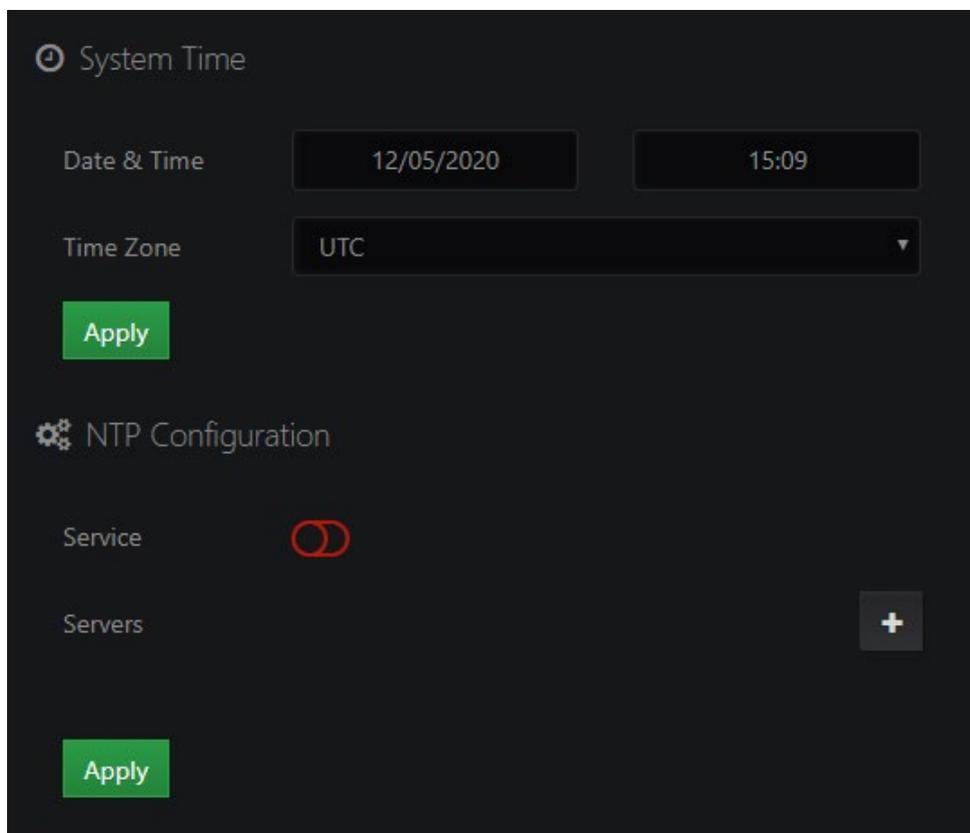
System Time

NTP service is enabled by default: if Internet access is provided to IOTA, no extra configuration is required. System time can also be adjusted manually.

The system time is used by:

- the embedded OS,
- the capture interface to constantly discipline the hardware timestamp counter.

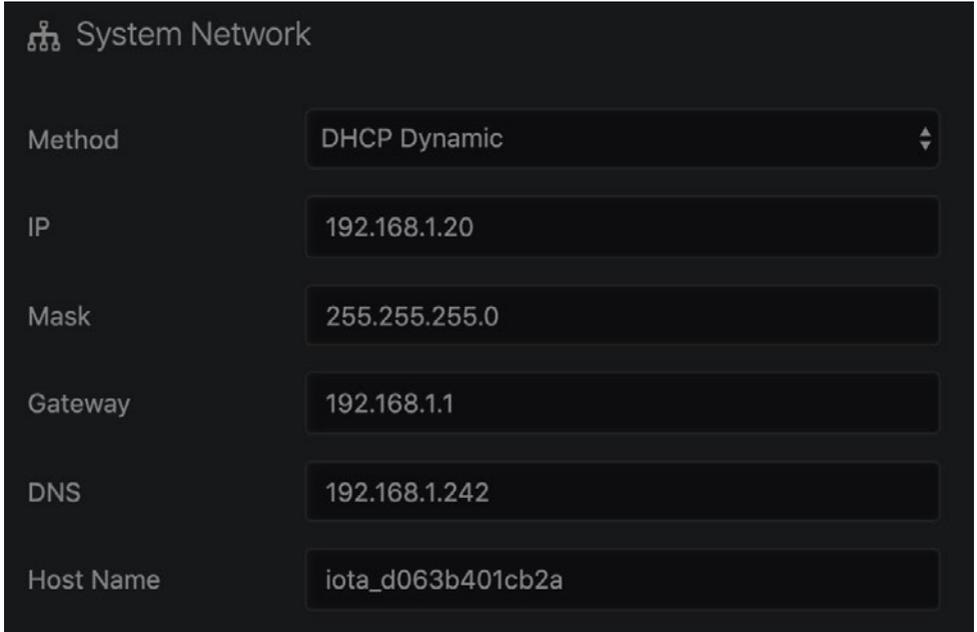
Changing time may require a restart of the capture interface to take effect.



The screenshot shows a dark-themed configuration window. At the top, there is a clock icon and the text "System Time". Below this, there are two input fields for "Date & Time": the first contains "12/05/2020" and the second contains "15:09". Underneath is a "Time Zone" dropdown menu currently set to "UTC". A green "Apply" button is positioned below the time zone selection. The second section is titled "NTP Configuration" with a gear icon. It features a "Service" toggle switch that is currently turned on, indicated by a red circle. Below the toggle is a "Servers" label and a grey button with a white plus sign. A second green "Apply" button is located at the bottom left of the NTP Configuration section.

System Network

Navigate to IOTA Settings / Configuration to change default network settings like IP, Mask, Gateway, DNS and Host Name.

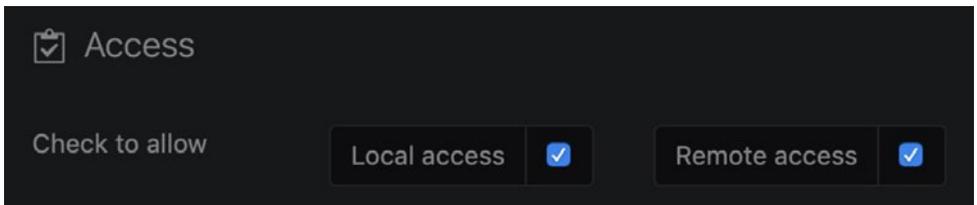


The screenshot shows a dark-themed configuration window titled "System Network" with a network icon. It contains several input fields for network settings:

Field	Value
Method	DHCP Dynamic
IP	192.168.1.20
Mask	255.255.255.0
Gateway	192.168.1.1
DNS	192.168.1.242
Host Name	iota_d063b401cb2a

Access / Internal Firewall

Used to limit access from local clients (LAN subnetwork) and/or remote clients (WAN, ZeroTier).



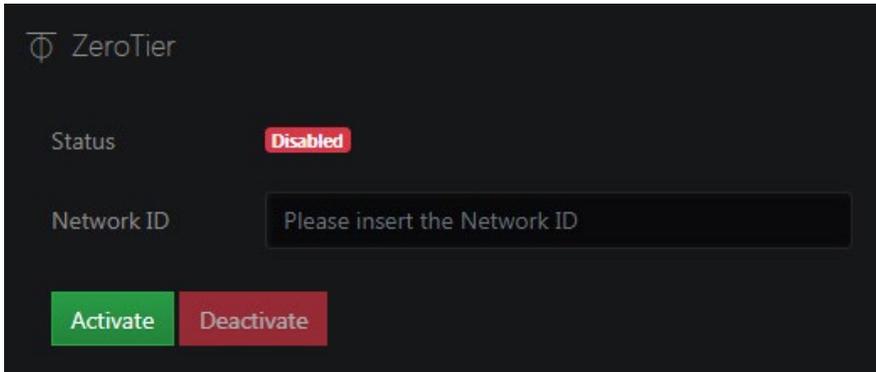
The screenshot shows a dark-themed configuration window titled "Access" with a checkmark icon. It contains two toggle switches for access control:

Check to allow	Local access	Remote access
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

ZeroTier

ZeroTier provides an easy way to remotely access the device via a P2P VPN and manage virtual networks on a cloud application.

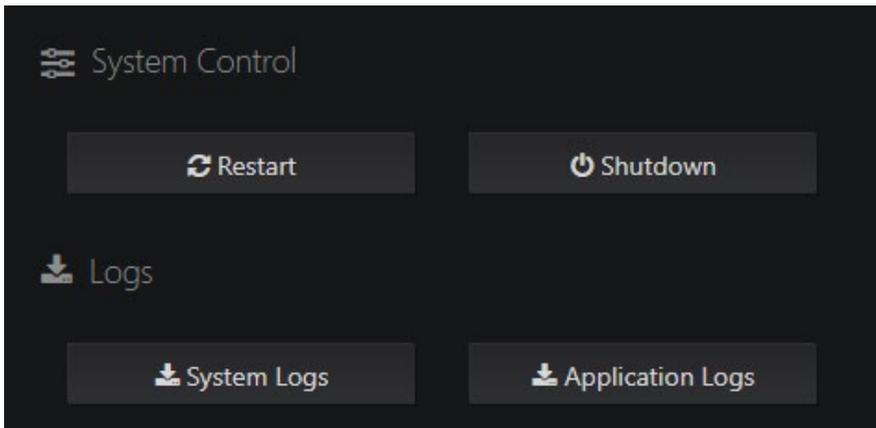
(more information: www.zerotier.com)



System Control & Logs

Remotely restart or turn off your IOTA by pressing the 'Restart' or 'Shutdown' button.

Download system logs and application logs by pressing the 'System Logs' or 'Application Logs' button.



System Updates

The ***IOTA Settings > System Updates*** page provides information about the current IOTA software version, latest available version, and changelog. If the IOTA can access the internet, the latest version number and changelog are fetched automatically, and the IOTA software can be updated via the '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 'Select a file' button.

CAPTURE GUIDE

3.1 CAPTURE CONTROL

The interface in **Capture > Capture Control** contains options for the capture of traffic and indexing of captured traffic.

When a capture is in progress, the traffic is automatically indexed in the specified datasource. If the 'Keep Files' option is enabled in the capture interface's settings, the captured traffic is saved on the disk, with new files being automatically created either every 30 seconds, or when the current file's size reaches 4 GB.

- ▶ **Note:** Capture files are automatically analyzed and indexed. The 'keep file' option determines whether or not the trace files are conserved in the data vault after having been analyzed.

If the 'keep file' option is enabled, it will be possible to retrieve the complete trace file, part of it, or a filtered copy, from the dashboards.

If the 'keep file' option is disabled, the dashboards will only display the indexed data, and it will not be possible to retrieve the original trace file.

The *Indexing* section defines the database and the index in which the captured data will be indexed.

The default datasource is the database already present on the IOTA device. Other datasources can be selected if they have been set up in **Configuration > Data Sources**.

The *Index* subsection defines which index the captured data will be saved to. Either select an index already present on the selected database, or create a new one by selecting the second option and typing a name (must start with 'profisight').

Edit ProfShark ✕

Nickname: profishark_80_0b

Interface Name: profishark_80_0b

Device Model: IOTA 10G

Device MAC: 80:1f12:3a:02:0b

Keep Files

Close Apply

Packet Analyzer Settings

DNS Resolution

Indexing

Select a valid Datasource: Elasticsearch - localhost - Default

Index Select a index

profisight-23.6.2020

Session Keyword profisight

Files will be available only after the first 30 seconds of capture.

▶ Start Capturing Session ▶ Stop Capturing Session

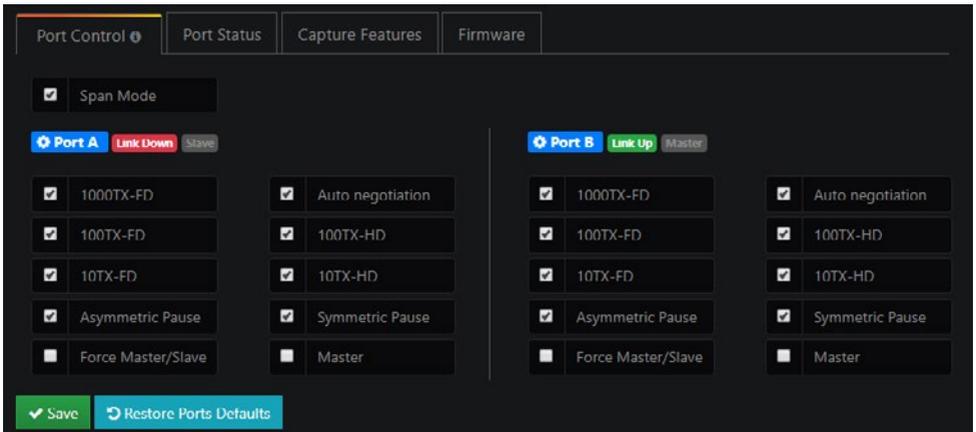
3.2 INTERFACE CONFIGURATION

The **Capture > Interface Configuration** screen gives an overview of connected devices, Capture Statistics and Device information. To change interface settings, several tabs are available:

Port Control

If IOTA is intended to be used in-line, the appropriate configuration must be set. 'In-Line mode' is the default mode ('Span Mode' checkbox unticked). IOTA can be set to SPAN Mode by ticking the 'Span Mode' checkbox.

Port speed and behavior can be set on this screen, for both port A and port B.



Port Status

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

Port Control			Port Status			Capture Features			Firmware		
Link Partner Status						Fault Status					
		A	B				A	B			
Link Partner Auto-Neg Capable	Yes	Yes				Parallel Decetion Fault	No	No			
Next Page Request	Yes	Yes				Remote Fault	No	No			
Link Partner Next Page Capable	Yes	Yes				Master/Slave Fault	No	No			
Link Partner Acknowledge Capable	Yes	Yes				Local Receiver Fault	Yes	Yes			
Link Partner Advertise 1000BASET_FDX	Yes	Yes				Remote Receiver Fault	Yes	Yes			
Link Partner Advertise 1000BASET_HDX	No	No				Idle Entry Count	0	0			
Link Partner Advertise 100BASETX_FDX	Yes	Yes				100BASEIX Lock Error	No	No			
Link Partner Advertise 100BASETX_HDX	Yes	Yes				100BASETX Receive Error	No	No			
Link Partner Advertise 10BASEI_FDX	Yes	Yes				100BASEIX Transmit Error	No	No			
Link Partner Advertise 10BASET_FDX	Yes	Yes				100BASETX SSD Error	No	No			
Link Partner Advertise Asymmetric Pause	No	No				100BASEIX ESD Error	No	No			
Link Partner Advertise Symmetric Pause	No	Yes				1000BASET Lock Error	No	No			
						1000BASEI Receive Error	No	No			
						1000BASETX Transmit Error	No	No			
						1000BASEIX SSD Error	No	No			
						1000BASETX FSD Error	No	No			
						1000BASETX Carrier Extension Error	No	No			

Capture Features

Port Control		Port Status		Capture Features		Firmware	
<input type="checkbox"/>	Keep CRC32	<input type="checkbox"/>	Disable Port A	<input type="checkbox"/>	Disable Port B	<input checked="" type="checkbox"/>	Packet Slicing (128 bytes)
<input type="checkbox"/>	Transmit CRC Errors						
Save							

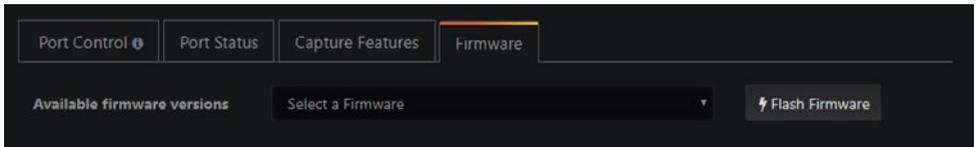
This tab allows the configuration of the following capture settings:

- Transmit CRC Errors
- Keep CRC32
- Packet Slicing (128 bytes)
- Disable Port A
- Disable Port B

Features can be enabled and disabled by ticking or unticking the related checkbox.

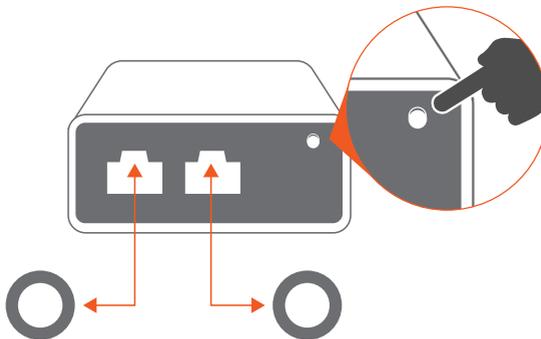
Firmware

The firmware can be flashed by selecting a firmware version from the drop-down menu and clicking the 'Flash Firmware' button.



3.3 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 physical START/STOP button.



START: Starts capture. IOTA will use latest settings in Capture Control

STOP: Stop Capture

FACTORY RESET: Disconnect power from IOTA. Long-press the START/STOP button and while holding, reconnect power and hold for 20 seconds. FACTORY RESET is complete when LEDs are green.

RESET: Long-press the START/STOP button and hold for 20 seconds. RESET is complete when LEDs are green. This will reset password and network parameters.

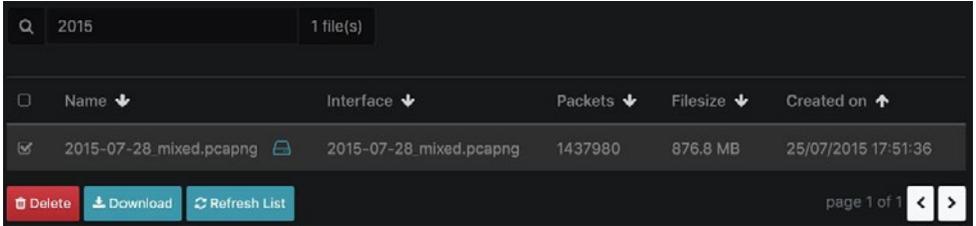
SHUTDOWN: Press and hold for 10 seconds for safe device shutdown. This will stop capture and unmount the internal disk in order to end capture session.

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

3.4 DATA VAULT

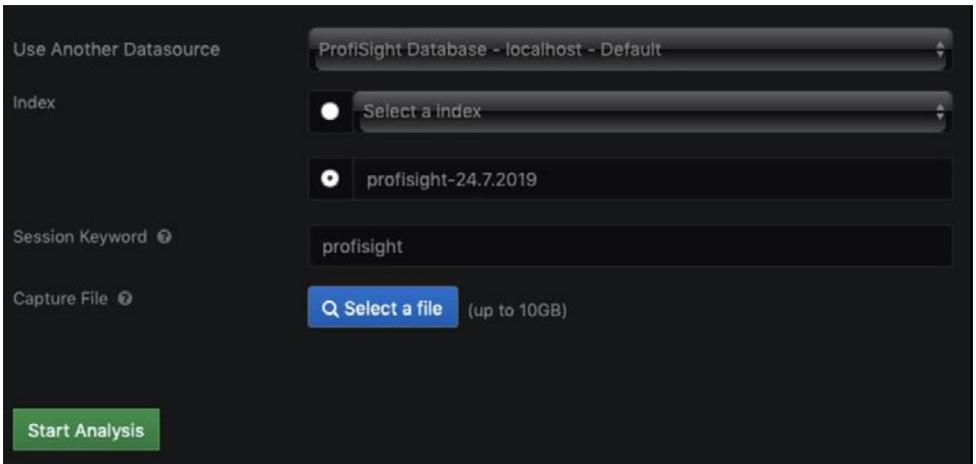
Captured Files

Navigate to **Data Vault > Captured Files** to download or delete raw PCAP-NG files. Select one or more files and click the 'Download' button to download a .zip archive of the selected files, or the 'Delete' button to delete them.



Import a PCAP-NG

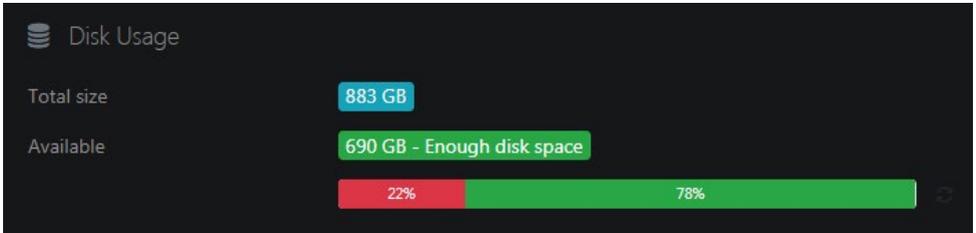
Importing a PCAP-NG or PCAP file to the IOTA can be done by clicking the 'Select a file' button, selecting the file, and clicking the 'Start Analysis' button. Once uploaded, set the time range of the dashboards to that of the file to ensure the graphs display the correct data.



3.5 DATA MANAGEMENT

Disk Usage

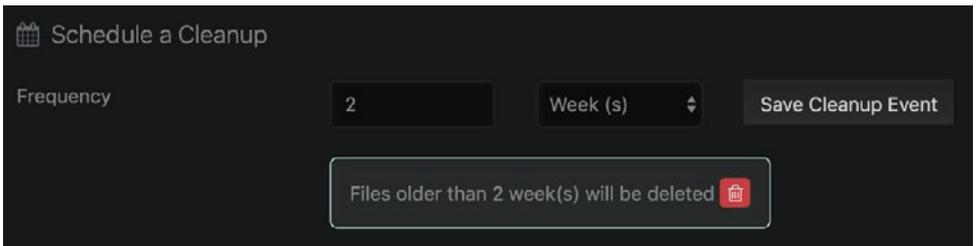
Navigate to **Data Management > Capture Machine** to get an overview of the disk usage, including total disk size and available disk space.



► **Note:** Capture data rotates once disk usage reaches 80%.

Schedule a Cleanup

Data retention management is available at **Data Management > Capture Machine > Schedule a Cleanup**. Capture files and index older than the specified time range will be deleted regularly.



The screenshot shows the 'Schedule a Cleanup' form with a dark background. It includes a 'Frequency' input field with the value '2', a dropdown menu set to 'Week (s)', and a 'Save Cleanup Event' button. Below the input fields is a confirmation box with the text 'Files older than 2 week(s) will be deleted' and a trash can icon.

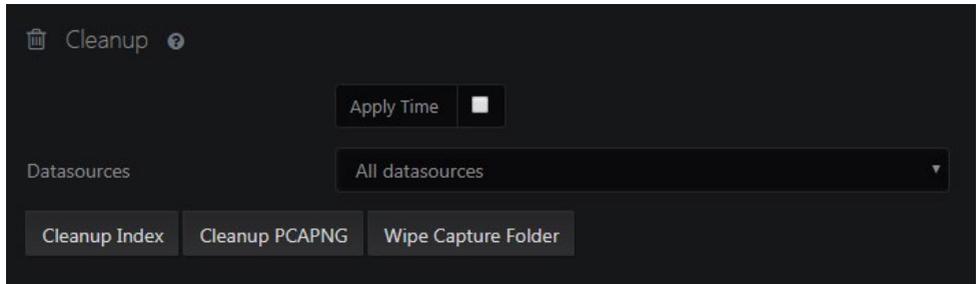
Frequency: 2 Week (s) Save Cleanup Event

Files older than 2 week(s) will be deleted

Manual Disk Cleanup

Manual cleanup of capture files and index is possible with the following options:

- Selective cleanup based on time
- Selective cleanup based on index
- Cleanup index or PCAP files or both



ANALYSIS GUIDE

4.1 DASHBOARD OVERVIEW



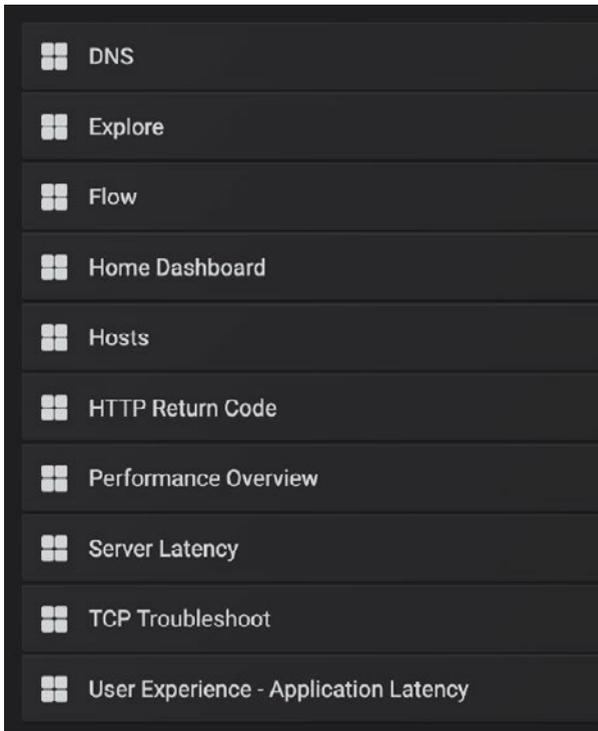
1. Main menu
2. Logout
3. Main dashboard selection
4. Time range selection
5. Dashboard area
6. Display filter
7. PCAP file download
8. Dashboard navigation with filters and time selection
9. Dashboard configuration

4.2 BASIC NAVIGATION

Main dashboard selection menu

This menu displays all the available dashboards. The list of dashboards is non-exhaustive and will change over time to include new features and other improvements.

- ▶ **Note:** Accessing a dashboard from this menu resets the Time pickers time range and the Display filter defined in the current dashboard. To navigate through dashboards while keeping the time range and filters set, use the '**Goto >>**' dashboard navigation.



Time range selection

Time range and automatic refresh rate can be set from this menu.

The screenshot shows a dark-themed interface for selecting time ranges. At the top, there is a toolbar with icons for chart, star, share, save, settings, and a monitor. A dropdown menu is open, showing 'Last 24 hours' selected. Below the toolbar, the menu is divided into two sections: 'Quick ranges' and 'Custom range'.

Quick ranges

Last 2 days	Yesterday	Today	Last 5 minutes
Last 7 days	Day before yesterday	Today so far	Last 15 minutes
Last 30 days	This day last week	This week	Last 30 minutes
Last 90 days	Previous week	This week so far	Last 1 hour
Last 6 months	Previous month	This month	Last 3 hours
Last 1 year	Previous year	This month so far	Last 6 hours
Last 2 years		This year	Last 12 hours
Last 5 years		This year so far	<u>Last 24 hours</u>

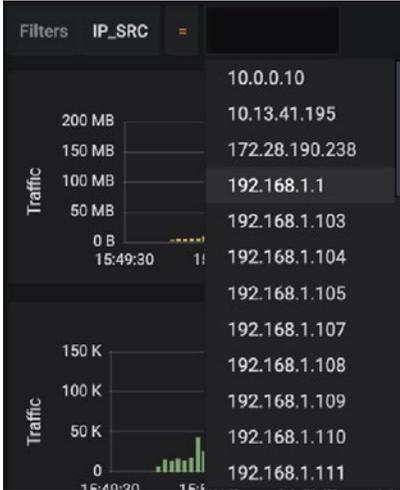
Custom range

From: 

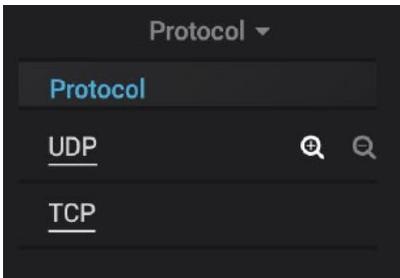
To: 

Filtering traffic

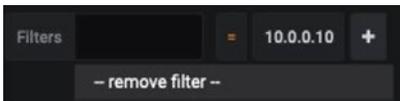
Display filters can be defined manually by clicking the + icon next to the Filter box (top left) and selecting the filter type and value it needs to filter on.



Alternatively, in the dashboards, filters can be applied quickly by using the + magnifier icon (include filter), or the - magnifier icon (exclude filter)

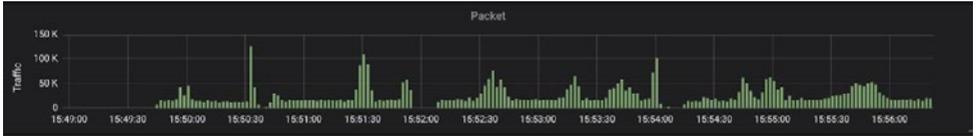


Filters can be removed by clicking the filter type again and selecting '--remove filter--'

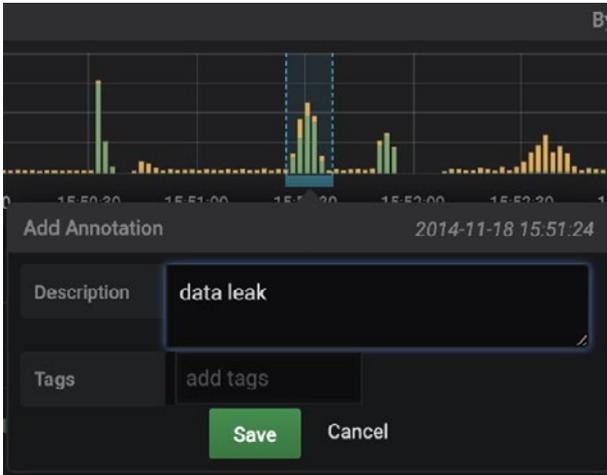


Graphs

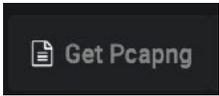
Click and drag to zoom in on a specific time range.



Use CTRL/CMD + mouse drag to add annotations to the graph.



4.3 PCAP FILE DOWNLOAD



Use the 'Get Pcapng' button at the top right corner of any dashboard to download the PCAPNG file.

The time range of the downloaded PCAP file corresponds with the time range selected in the Time picker menu.

The following filters will 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.

Additional methods to download PCAP files:

1 - Use the direct download link

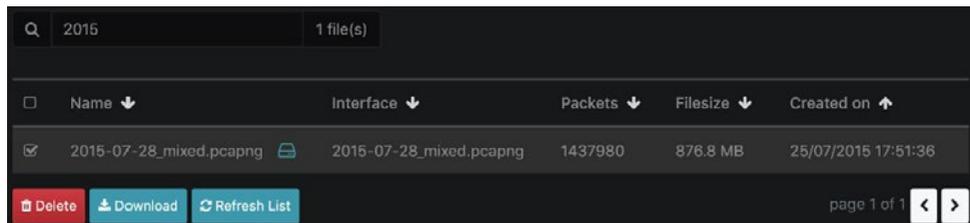
Clicking on any link starts the PCAP file transfer, filtered with value only. Filters are ignored with this method.

Top Client ▾				
Client IP		Data ▾	Average bps	Max bps
192.168.1.1	Download PCAP	223.36 MB	89.62 kbps	510.06 kbps
172.28.190.238		15.37 MB	361.52 kbps	2.31 Mbps
192.168.1.241		97.55 kB	44.54 kbps	54.72 kbps
192.168.1.242		82.67 kB	46.54 kbps	54.72 kbps

2 - Download the raw PCAP-NG file(s) from a list

(Data Vault > Captured Files)

The file or group of files are downloaded in a .zip archive.



The screenshot shows a file management interface with a search bar containing '2015' and a result count of '1 file(s)'. Below is a table with columns for Name, Interface, Packets, Filesize, and Created on. A single file is listed: '2015-07-28_mixed.pcapng' with an interface of '2015-07-28_mixed.pcapng', 1437980 packets, and a filesize of 876.8 MB. At the bottom, there are buttons for 'Delete', 'Download', and 'Refresh List', along with pagination information 'page 1 of 1' and navigation arrows.

<input type="checkbox"/>	Name ↓	Interface ↓	Packets ↓	Filesize ↓	Created on ↑
<input checked="" type="checkbox"/>	2015-07-28_mixed.pcapng 	2015-07-28_mixed.pcapng	1437980	876.8 MB	25/07/2015 17:51:36

page 1 of 1

Legal

DISCLAIMER

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

COPYRIGHT

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

TRADEMARKS

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

*BRINGING CLARITY
INTO NETWORKS,
ANYTIME,
ANYWHERE.*

PROFITAP HQ B.V. — High Tech Campus 9
5656 AE Eindhoven — The Netherlands

sales@profitap.com
www.profitap.com

© 2021 Profitap — v2.6-03

