TNA-30x Web UI Manual

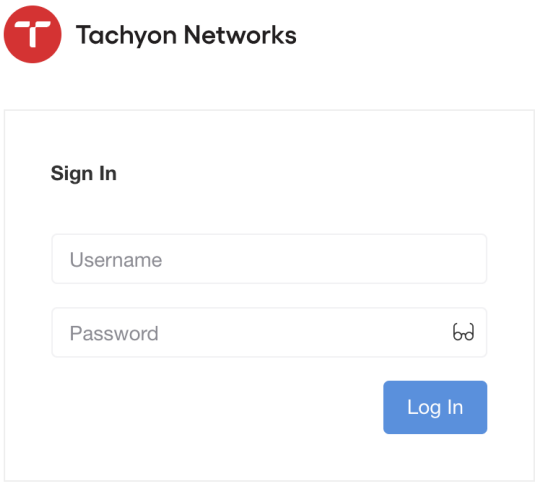
Modified on: Fri, 25 Aug, 2023 at 11:53 AM

This version of the TNA-30x Web UI manual applies to firmware versions v1.11.2 and later. You can find the current firmware version of your device on the Dashboard page, within the System information widget.

Please refer to the **TNA-30x Operating Manual** (https://tachyon-networks.freshdesk.com/support/solutions/articles/67000670226-tna-30x-operating-guide/) for information about how to power your device, what the device LEDs mean, aiming tips, and other useful information.

Table of contents

Login & access



ⓘ **Note**: The device's default fallback IP is **192.168.1.1,** and the default username and password are **root/admin.**

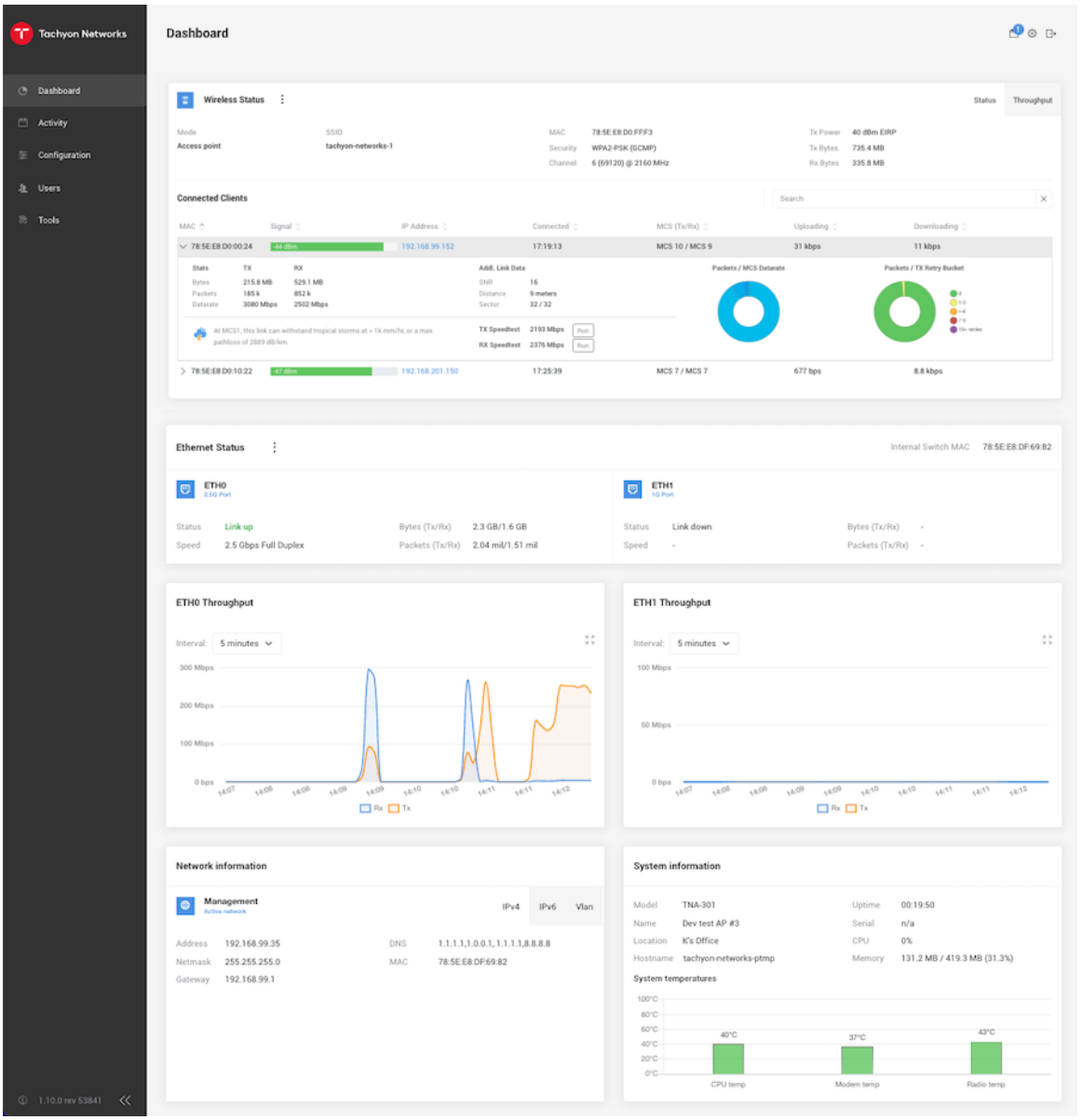
1. Insert an ethernet cable into either the ETH0 (2.5G) or the ETH1 (1G) port in order to give your device connectivity.
2. By default, DHCP client is enabled on the main local network bridge. If your device cannot get an IP from an upstream DHCP server, it will fallback to 192.168.1.1.
3. Access your device's local web UI in your web browser at the DHCP-assigned IP or the fallback IP mentioned in the previous step.
4. Login using the default login credentials of username: `root` & password: `admin`. You will automatically be logged out of your session if you're inactive for more than 30 minutes.

! Change the device's default user credentials after you log in for the first time.

Dashboard

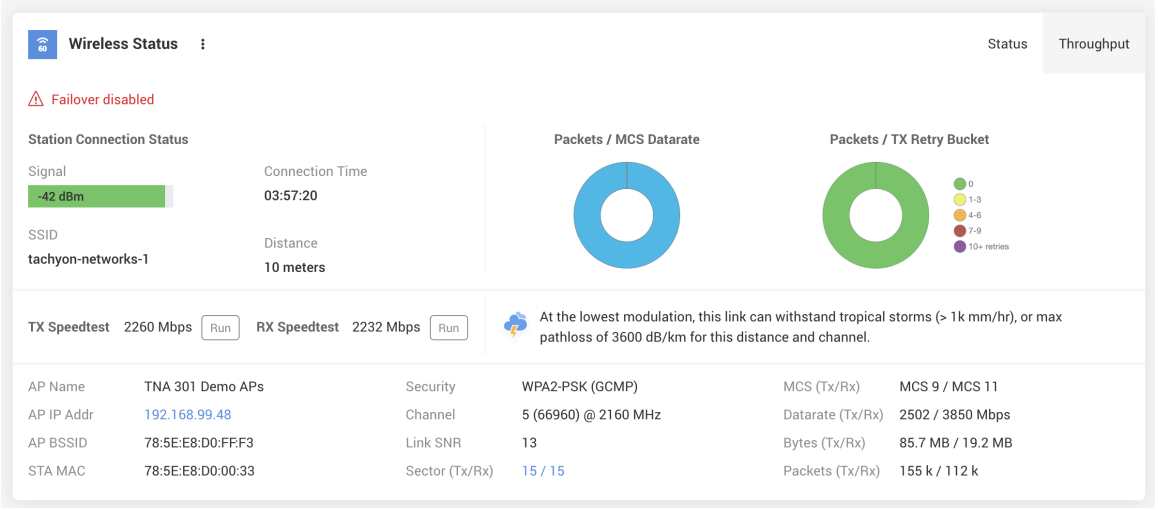
The device dashboard shows the overall status of your device, including:

- Wireless status information
- Ethernet port PoE and link status
- Failover status
- Networking details (including management and/or data VLAN) for the local bridge interface(s)
- Traffic graphs for the wireless and ethernet interfaces
- System information, including device name, system resources and temperatures, and firmware versions running on each device bootbank (active and alternate/backup).

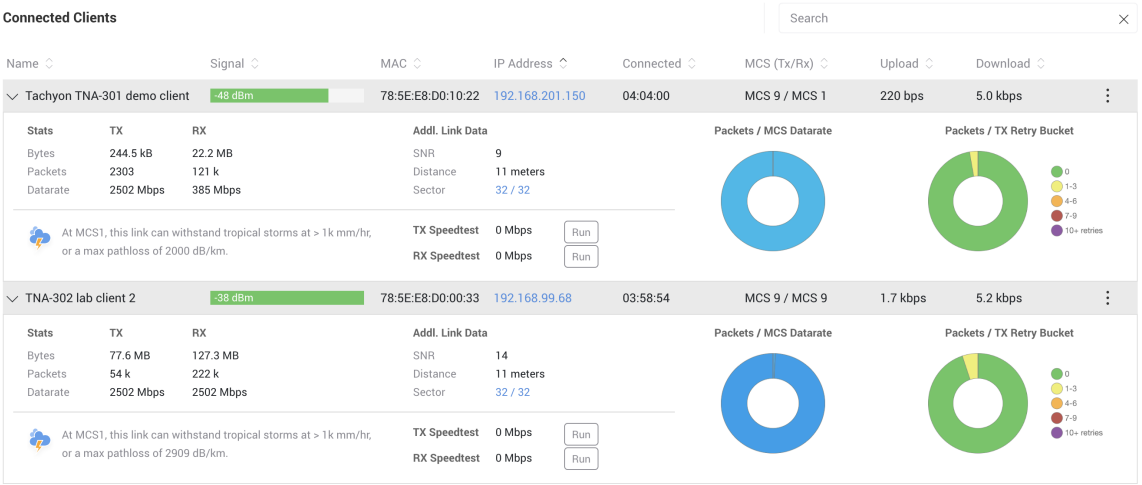


Wireless Status

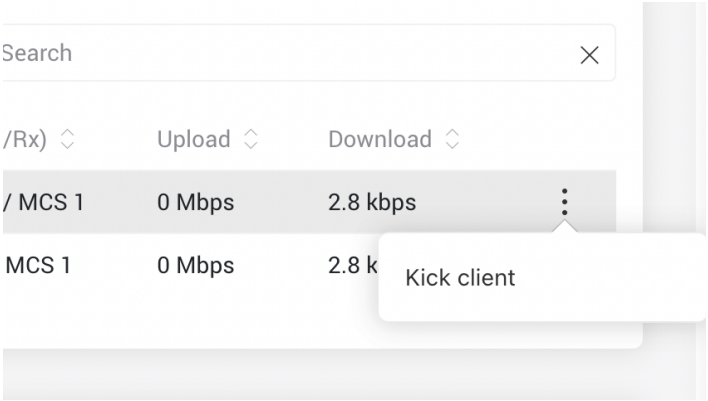
Here's what the wireless status will look like in **station/client mode** *(click to make the image larger)*:



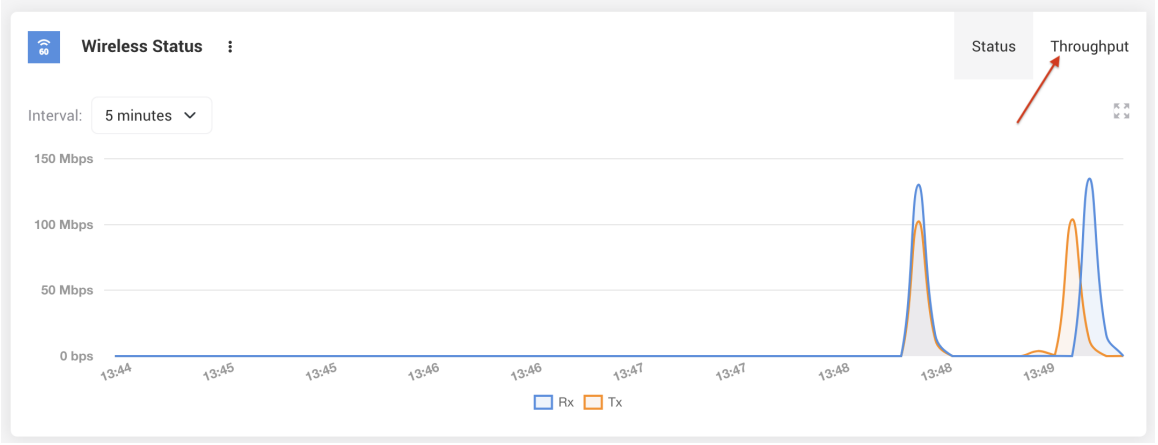
And here's the wireless status section of the dashboard when the device is operating in **AP mode:**



You can kick an associated client off of a device operating in AP mode by clicking the "three dot" menu at the right end of the row, and selecting "Kick client". This can be useful when using station connection profiles to force your station to connect to a different AP.



To view the wireless throughput graph, click on the upper right corner of the wireless widget on the dashboard:



Connected Peer Stats

- **IP Address and peer name:** A connected device's management IP is available once discovery/LLDP data is available for the peer, which may take a few minutes after association. If the discovery tool or LLDP server are disabled on either the AP or station, then discovery data (including IP and device name) will be not be available.
- **Packets/MCS Datarate chart:** The system observes a client's traffic during the 5 minute interval, and determines how many packets were sent for each MCS rate. Lower MCS rates have a lighter yellow color, and gradually turn a darker blue the higher the rate. When clients first connect, you'll see that lower MCS rates are being used, and then when traffic increases over the link, the number of packets in the upper MCS rates will grow.
- **Packets/ TX Retry bucket chart:** The system also checks to see how many packets were retried across the wireless link during the observational period, and categorizes them into buckets based on the number of retries. If you have many packets outside of the "green" bucket, check your link for obstructions. If there are none, you might have an environmental issue with reflections.
- **Link Availability**: This section shows how much rain the link can withstand at MCS1 before it will go down.
- **Sector IDs:** You can read more about **TNA-30x sector IDs here** (https://tachyon-networks.freshdesk.com/support/solutions/articles/67000717208-what-do-the-tna-30x-tx-rx-sector-numbers-mean-). A connected peer's sector ID can now be visualized on the **Sector Info Tool**.

Note: The connected client charts "Packets/MCS Datarate" and "Packets/TX Retry Bucket" will show up only after the client has been connected at least 5 minutes. Data for these charts are collected for a 5 minute interval, and then pushed to the UI. The data is not cumulative across the lifespan of the link, only for the previous 5 minute duration.

Wireless Peer Speedtest

You can also perform a speed test by pressing the "Run" button near the TX or RX Speedtest labels next to a connected client in AP mode, or from the wireless status widget in Station mode. This can be used to test throughput between the AP and clients, or visa versa. It's useful to also rule out ethernet or other network issues when troubleshooting link performance.

Note: the speedtest tool pushes small burst of packets across a link, so running it will not have any noticeable effect on customer traffic, nor on the wireless throughput graph.

Configuration

ⓘ Only admin-level users have rights to access and change settings on the configuration pages of the web UI.

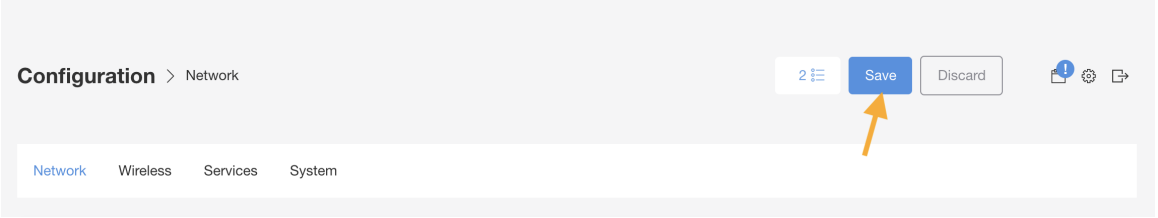
Applying configuration changes

While you're configuring your device, feel free to make changes to one or more settings located on any of the configuration pages mentioned in the sections below.

Once you're done, click the *Save* button at the top of the page in order to write and apply the changes. Please note that your device will become temporarily unreachable while networking and other system services are restarted.

If you wish to discard your changes, refresh the page, or click the *Discard* button.

You can also view which changes are pending by clicking the list button to the left of the *Save* button.

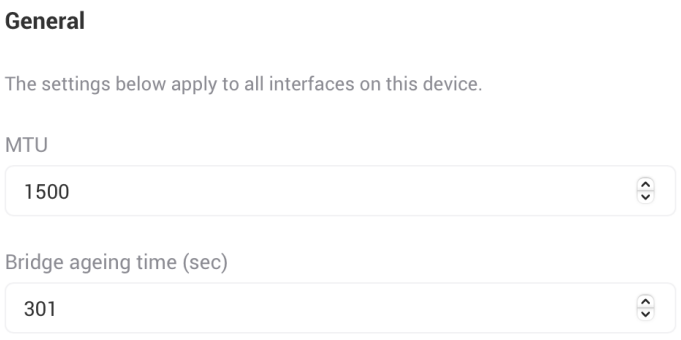


Network Settings

/General

MTU: Maximum transmission unit. This setting will apply to the wireless interfaces, ethernet ports, and management/local bridge. The minimum allowed value is 1280, and the max is 7900.

Bridge ageing time: Ageing determines the number of seconds a MAC address is kept in the FDB after a packet has been received from that address. Set to this 0 to disable ageing.

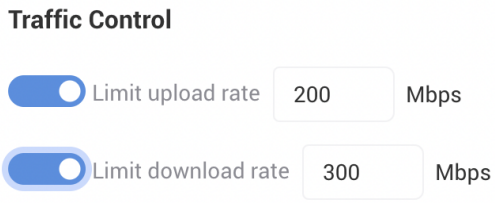


/Traffic Control

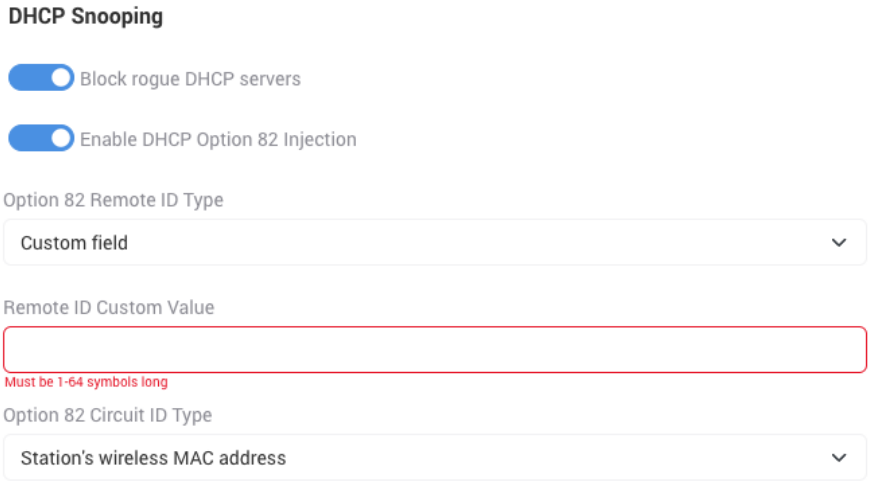
***Note**: Traffic Control settings are only visible when operating in Station mode. These settings are available in firmwares v1.11.1 and later.*

Limit upload rate: Enable or disable traffic shaping on the upload (wireless) path, and set upload or download limit in Mbps.

Limit download rate: Enable or disable traffic shaping on the download (ethX) path, and set upload or download limit in Mbps.



/DHCP Snooping



Note: *DHCP Snooping settings are only visible when operating in Station mode. These settings are available in firmwares v1.11.1 and later.*

Block rogue DHCP servers: When this setting is enabled, DHCP discovery packets are dropped at the Station before being passed downstream*, and DHCP offer packets are dropped at the Station before being passed upstream.

Rogue DHCP servers can occur when a user plugs their router in backwards, exposing the DHCP server to the upstream WAN network, instead of to their local network.

Enable DHCP Option 82 Injection: Enable this setting to inject DHCP Option 82 fields into upstream* DHCP request packets. You can choose to populate the Remote ID field, the Circuit ID field, or both. These fields can be set to one of the following options:

1. **Station's wireless MAC**: Insert the stations's wireless MAC address into the specified DHCP option 82 field. When the MAC address is inserted, it will be ASCII encoded, and will include the colons. (example: 78:5e:e8:d0:00:02).

2. **Custom**: Insert an ASCII string of your choice (such as a customer's ID number or phone number) into the specified option 82 field. The string must be between 1 and 64 characters.

3. **None**: don't insert anything into the specified option 82 field

Any DHCP requests that come from devices connected to the TNA-30x over the wired ports, as well as from the station device itself, will be injected with the DHCP option 82 fields.
Terminology

- *Upstream* indicates traffic over the uplink, from the Station to the Access point.
- *Downstream* indicates traffic originating at the station, moving down stream to any devices connected to the wired ports.

Limitations:

- DHCP option 82 injection is not currently supported when data VLANs are enabled. Please contact support@tachyon-networks.com if you'd like to make a request for this feature.

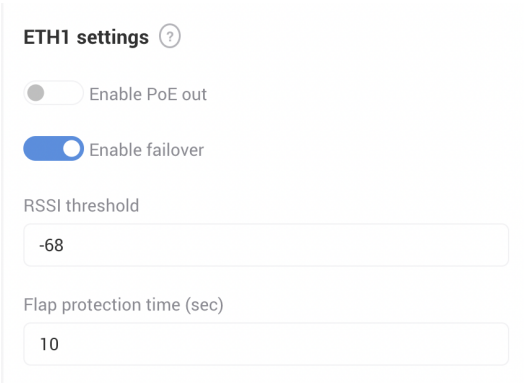
/ETH1 settings

Enable PoE Out: Enable or disable PoE out on the ETH1 1G interface. Please refer to the **Operating Manual** (https://tachyon-networks.freshdesk.com/support/solutions/articles/67000670226-tna-30x-operating-manual)for more information about input and output power.

Enable Failover: (only available in station mode, and when data VLAN is disabled). Enable failover/backup over a device connected to the ETH1 port. Please refer to the **TNA-30x failover FAQs article** (https://tachyon-networks.freshdesk.com/support/solutions/articles/67000721350-tna-30x-failover-faqs) for more information about the TNA-30x failover/backup mechanism.

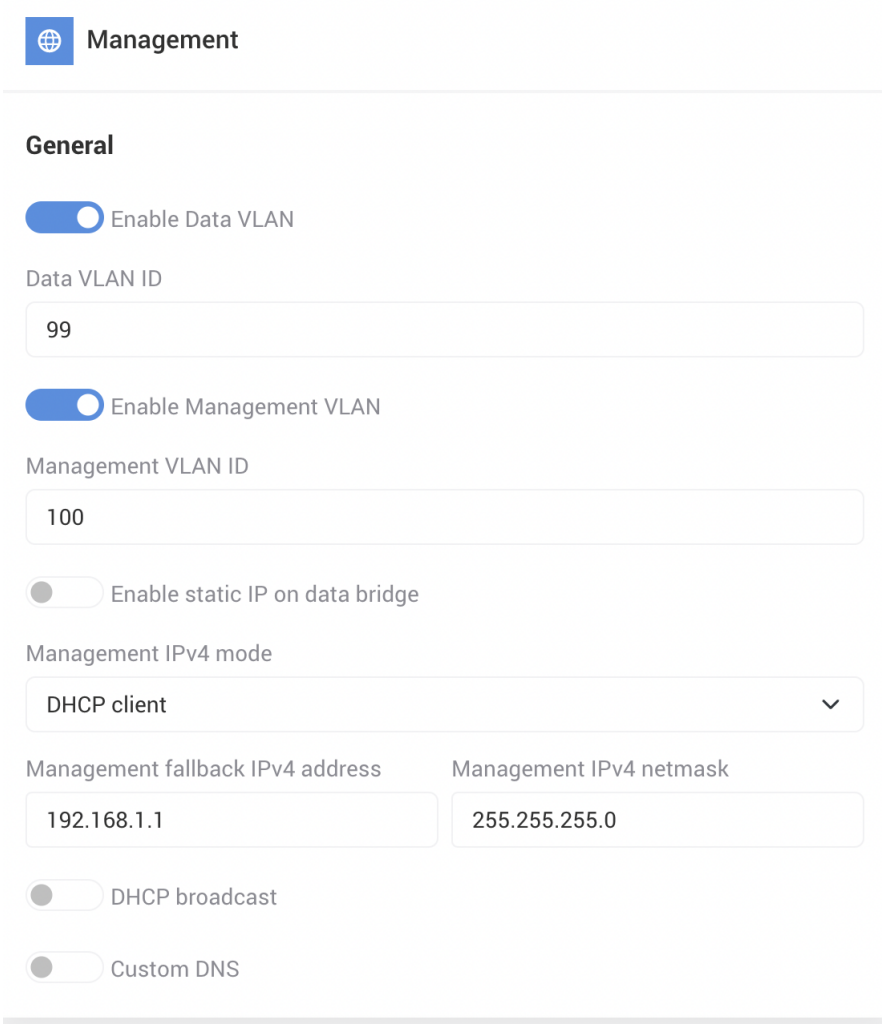
RSSI Threshold: The wireless signal threshold at or below which the device will switch into failover mode.

Flap Protection Time: The amount of time in seconds to wait before switching back to normal operation once the wireless link RSSI has moved back into the normal range. Once this happens and the flap timer countdown has begun, the flap timer will be reset if at any time the RSSI drops back below the threshold during the countdown.



/Management network general settings

These settings apply to the device's local/management network.



Enable Management VLAN: enable or disable management VLAN on the device.

[!] **Warning**: once this setting is enabled, you must have your management VLAN settings correctly configured or you will not be able to reach your device again without resetting to defaults, unless you have a data bridge static IP set (continue reading below about this).

When management VLAN is enabled, you will see the following settings:

- **VLAN ID**: ID in the range of 2 to 4094
- **Enable static IP on data bridge**: When this setting is enabled, you will be able to set an IPv4 static IP and netmask on the data bridge, giving one access to the local UI over the data network instead of the management VLAN network. This can be helpful in the case where a tech needs to have access to the device during installation over the non-management VLAN network. Once aiming and installation is complete, this setting can be turned off, only allowing access to the web UI over the management VLAN network.

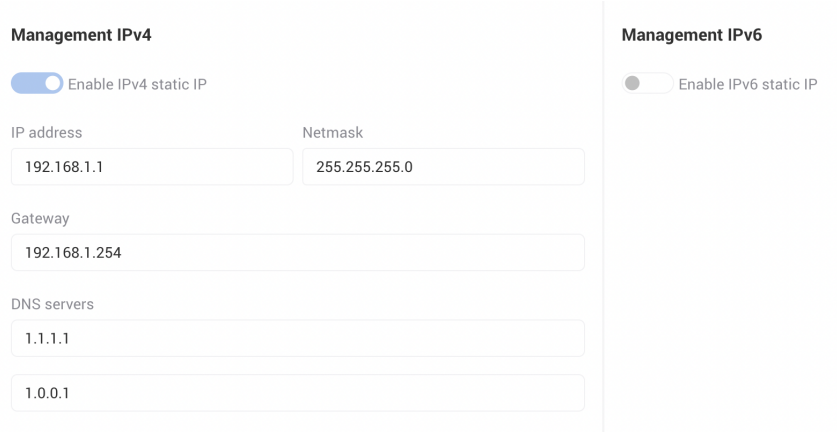
Enable Data VLAN: When Data VLAN is enabled, traffic with the specified VLAN ID received over the upstream wireless link will have the VLAN tag removed as it exits the wired ports. Similarly, traffic coming into the device over the wired ports will be tagged with the specified VLAN ID when it's sent over the wireless link.

- This feature is only available when your device is operating in station mode.
- The local web UI will be still accessible from the wired ports when data VLAN is enabled, unless management VLAN is enabled.

Management IPv4 mode options: Static or DHCP client

- **DHCP client**: If you choose DHCP client, you'll have the option of setting a fallback IPv4 address and netmask, custom DNS servers, and enabling DHCP broadcast (which requests DHCP broadcast replies from the DHCP server).

- **Static IP**: If you choose Static IP as the IP mode, you will need to manually set at least one IP (IPv4 or IPv6) for the device as shown below.



Wireless Settings

Wireless mode: Choose whether you'd like your device's 60 GHz radio to operate in access point or station mode. *Note*: if you change operating modes, your device will require a reboot to take effect.

Channel Width: Full (2 GHz) or Half (1 GHz). Please read **these important notes about half channel support** (https://tachyon-networks.freshdesk.com/support/solutions/articles/67000710571-does-the-tna-30x-support-half-channels-). *Note*: if you change channel widths, your device will require a reboot to take effect.

Channel: The available non-overlapping channels for the full 2 GHz channel width are 1-6, and 1-11 for half channel.

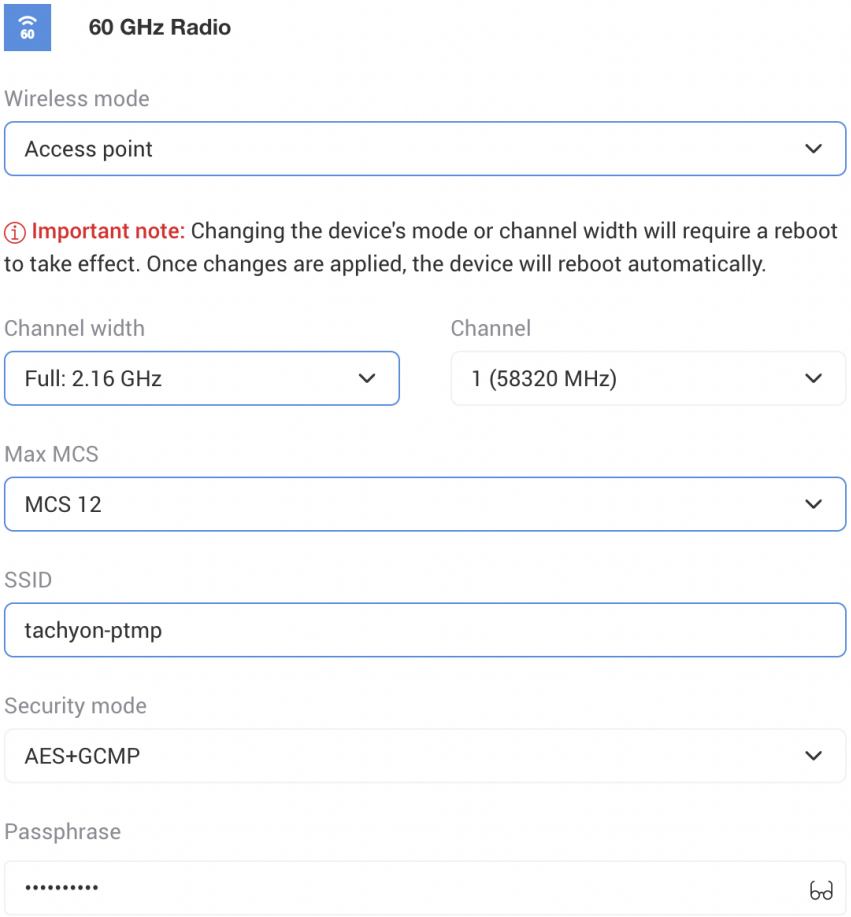
Max MCS: Data rates are dynamically selected, but you can choose to set the max MCS allowed.

- When half channel support is enabled, the max MCS allowed is MCS 9.

- Setting max MCS only affects the TX MCS rate of the current device. To set MCS for both TX And RX, you must change the max MCS value on both the AP and station sides of the link.

SSID: The radio's SSID.

Security mode: Select encryption - either open or AES+GCMP.



Station profiles

When your device is set to operate in station/client mode, additional options will be shown in the UI that allow you to input multiple connection profiles. The client will connect to the SSID/profile with the highest priority first.

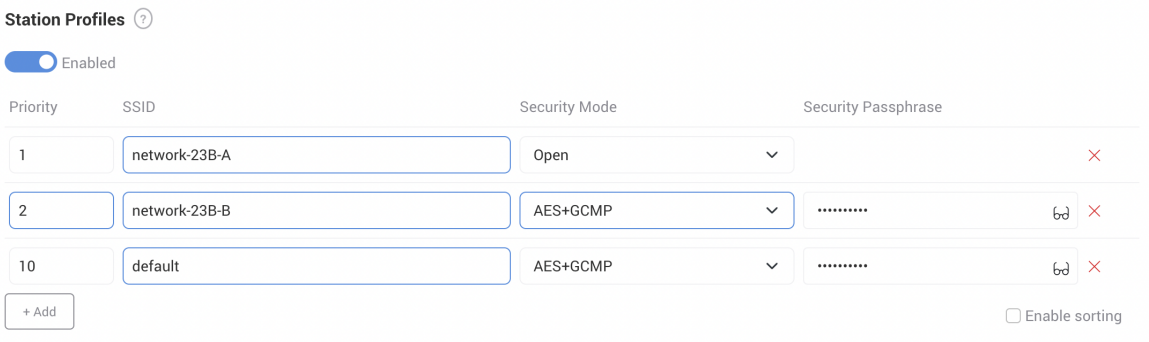
Priority: The priority of the profile. 1 is the highest priority, and 10 is the lowest. When you define multiple profiles with the same priority, the device will connect to the SSID that has the better signal.

SSID: The SSID for the connection profile.

Security: Security mode and passphrase that should be used when connecting to the specified AP.

Enable sorting: You may want to check this box to disable sorting of the profiles table while inputing profiles to keep the entries from jumping around as you change profile priorities.

These settings are available in v1.11.2+ firmwares and later.



Services Settings

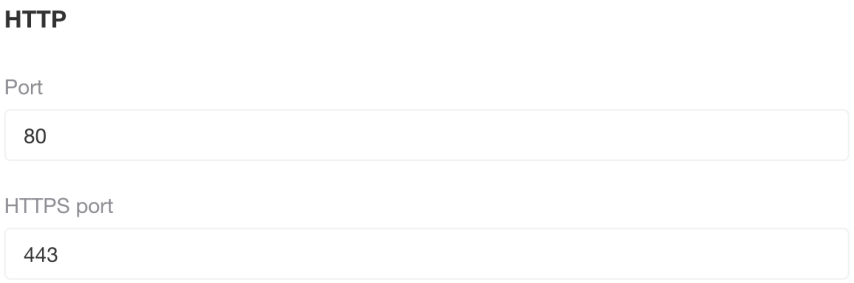
/HTTP

The settings in this section refer to the local webserver running on the device.

Port: HTTP port at which you can access the local web UI. Default is 80.

HTTPS port: HTTPS port at which you can access the local web UI. Default is 443.

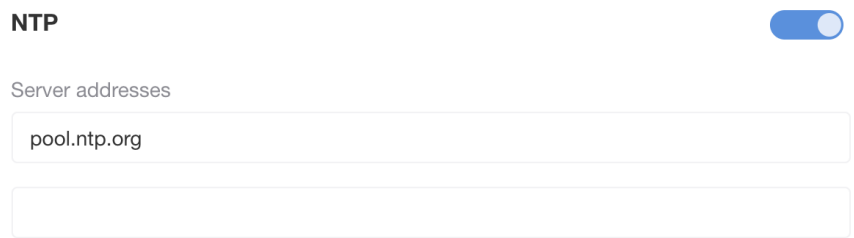
Note: the SSL certificate for the device's web server is a dynamically generated self-signed certificate. Some modern web browsers (such as Chrome) no longer accept self-signed SSL certificates by default. In order to view the HTTPS version of the web interface, you will need to use a browser that allows self-signed certificates, such as FireFox.



/NTP

Enable: Enable or disable the NTP (network time protocol) server. This server is enabled by default.

Server addresses: A list of NTP peers that the device should use when updating the local time.

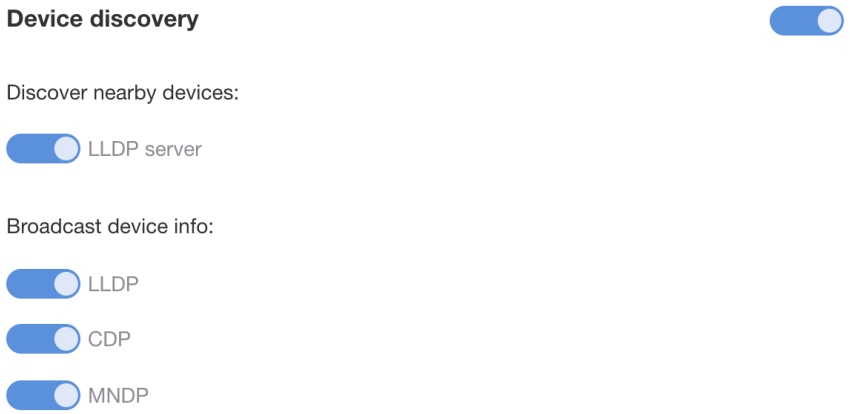


/Device discovery

Enable: Enable or disable the device discovery service for this device.

Discovery nearby devices:
Enable the LLDP (Link Layer Discovery Protocol) server in order to find nearby devices on the network. Nearby devices can be found by using the **Device discovery tool** on the **Tools** page.

Broadcast device info:
Allow this device to be discoverable over LLDP (Link Layer Discovery Protocol), CDP (Cisco Discovery Protocol), and/or MNDP (Mikrotik Neighbor Discovery Protocol).



/SNMP

Enable: Enable the local SNMP server. The SNMP server is disabled by default. The private MIB for the TNA-30x can be found **here** (https://tachyon-networks.freshdesk.com/support/solutions/articles/67000659779-tna-200-private-mib).

Protocol: Choose SNMP version: SNMPv2, SNMPv3, or dual SNMPv2 + SNMPV3.

Community *(SNMPv2 only)*: Input the community string for the SNMP server. The default value is public.

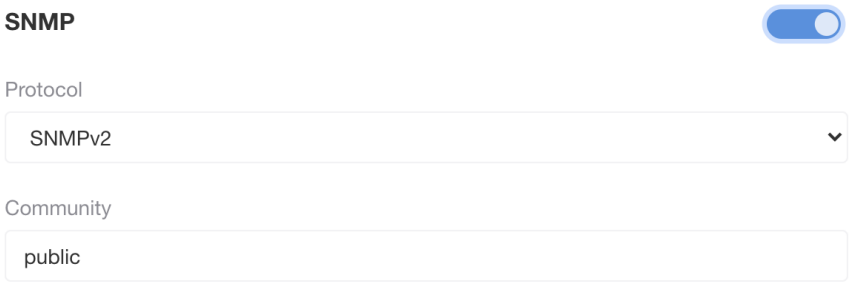
User *(SNMPv3 only)*: SNMPv3 authentication username. Length must be between 1 and 100 characters.

Password *(SNMPv3 only)*: SNMPv3 SHA+AES authentication passphrase. Length must be between 1 and 32 characters.

Here's an example demonstrating how to fetch the device's current 60GHz channel using SNMPv3 and `snmpwalk`:

```
> snmpwalk -v 3 -u <user> -A <password> -X <password> -a SHA -x AES -l authPriv <device ip> .1.3.6.1.4.1.4458.57344.2.2.1.4

SNMPv2-SMI::enterprises.4458.57344.2.2.1.4.2 = INTEGER: 1
```



/SNMP traps

Enable: Enable or SNMP traps to be sent from this device.

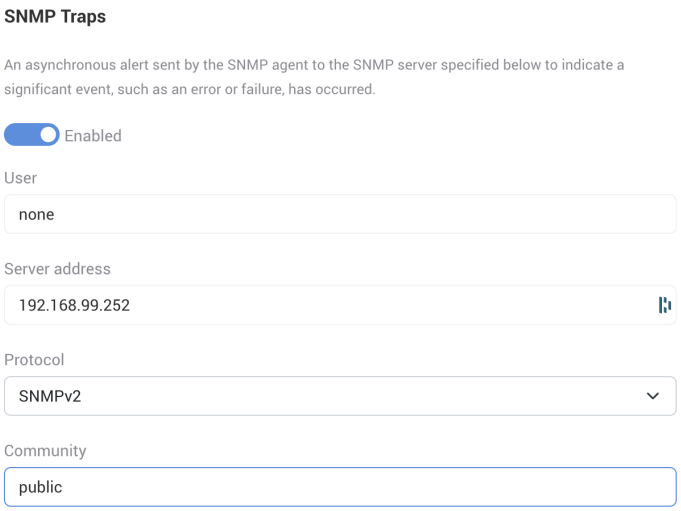
User: The username that should be included when connecting to the server specified below. If no username is required, just use a dummy value here such as "nonya".

Server address: Hostname or IP of the SNMP trap receiver.

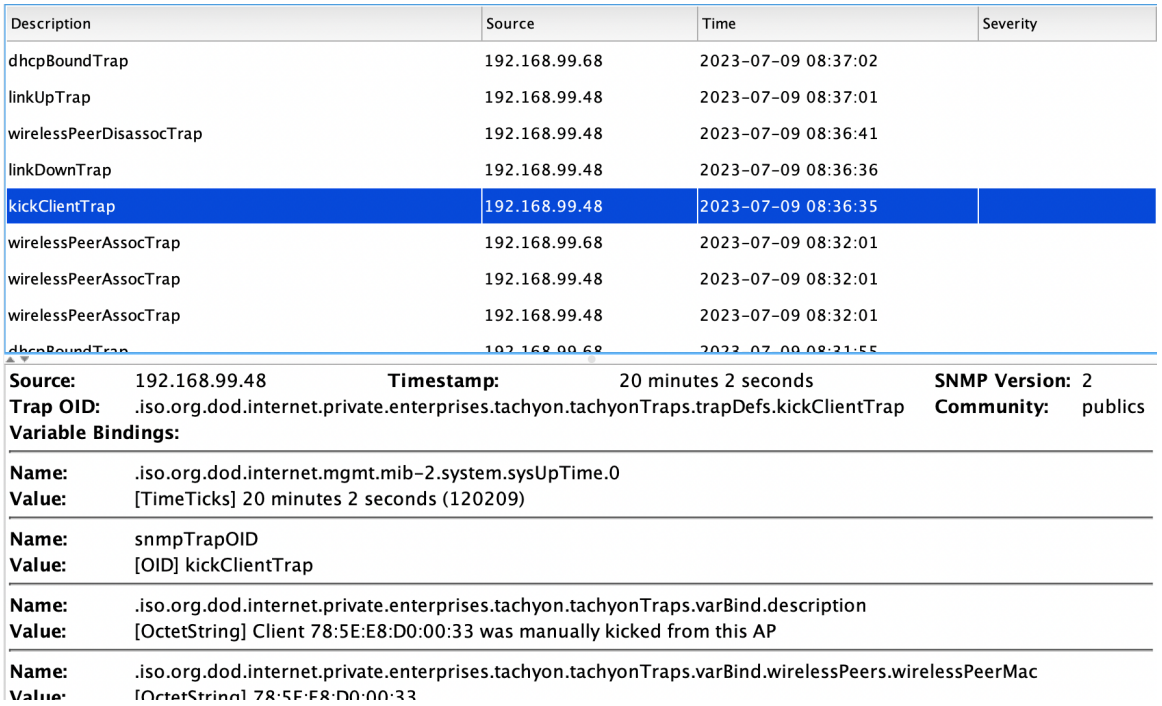
Protocol: Choose the trap version: SNMPv2 or SNMPv3

Community *(SNMPv2 only)*: Community string for SNMPv2.

Password *(SNMPv3 only)*: Password used for SNMPv3.



Once enabled, traps will be pushed to your trap server, like shown in the iReasoning MIB browser example screenshot below:



Description	Source	Time	Severity
dhcpBoundTrap	192.168.99.68	2023-07-09 08:37:02	
linkUpTrap	192.168.99.48	2023-07-09 08:37:01	
wirelessPeerDisassocTrap	192.168.99.48	2023-07-09 08:36:41	
linkDownTrap	192.168.99.48	2023-07-09 08:36:36	
kickClientTrap	192.168.99.48	2023-07-09 08:36:35	
wirelessPeerAssocTrap	192.168.99.68	2023-07-09 08:32:01	
wirelessPeerAssocTrap	192.168.99.48	2023-07-09 08:32:01	
wirelessPeerAssocTrap	192.168.99.48	2023-07-09 08:32:01	

Notes:

- The MIB that contains the Tachyon trap definitions can be found in the **TNA-30x Private MIB** (https://tachyon-networks.freshdesk.com/support/solutions/articles/67000659779-tna-30x-private-mib) article.
- Because of the nature of SNMP traps, some events might be lost before they reach your trap server. For example, client association traps are sent at association time, which could occur before the upstream data path is completely initialized, causing the trap message to be dropped.

/Ping watchdog

This service pings the specified IP address at the given interval and reboots the device after receiving a certain number of failures in a row. This service is disabled by default.

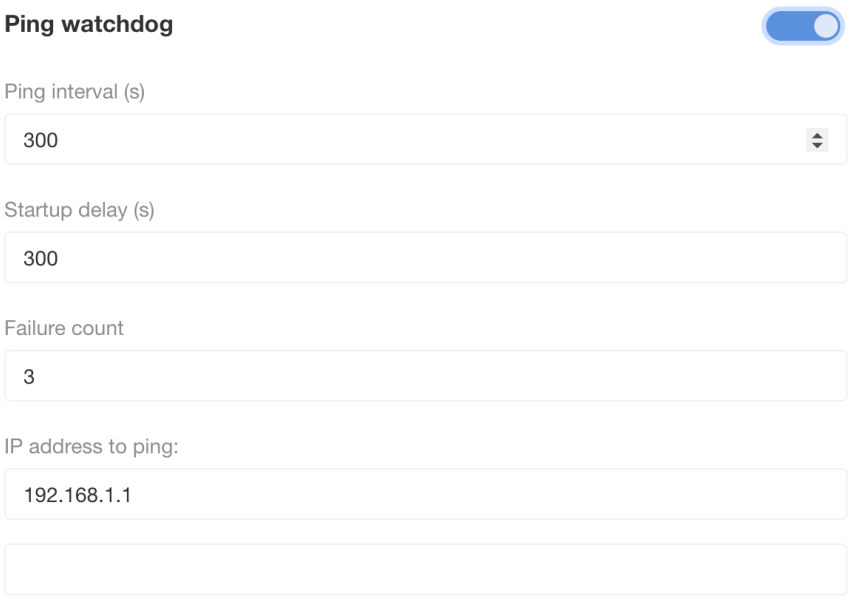
Enable: Enable the ping watchdog service.

Ping interval: How long the service should wait, in seconds, between attempts to ping the provided IP.

Startup delay: The length of time in seconds that the service should wait until it attempts the first ping.

Failure count: The maximum allowed number of failures allowed (in a row) before the device will be rebooted.

IP address to ping: The IP address that the service will attempt to ping.



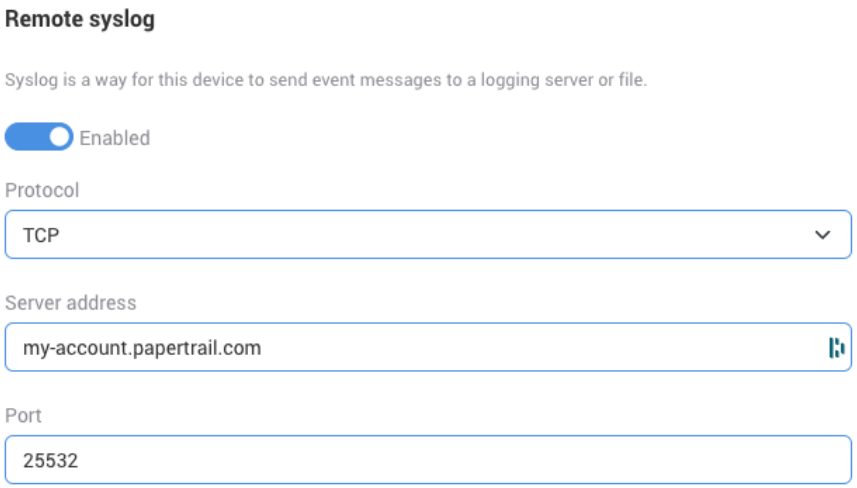
/Remote syslog

Enable: Enable or disable the remote syslog service.

Protocol: Remote syslog server protocol: TCP or UDP

Server address: IP address or hostname of the remote syslog server.

Port: Port at which the remote syslog server is running.



System Settings

/Device information

Device name: The name of this device. This field is used to populate the system name field used in the **device discovery** tool.

Device location: The physical location of this device. This free-form field is not used internally by the system, and can be set to whatever you'd like.

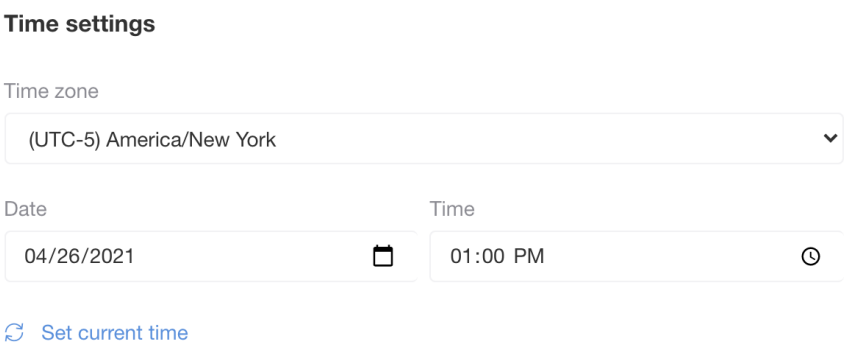
Country: Select the country where this device will be used. The country field is used to set local regulatory rules.

Hostname: The system hostname of your device. This must be a valid hostname format and only contain alphanumeric characters, periods and dashes, and must start or end in an alphanumeric character.

/Time settings

Time zone: The timezone that should be used for this device's time.

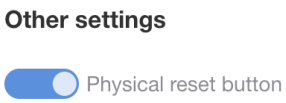
Date/time: Use the date and time fields to manually set the device's local date and time. It is not recommended that you manually set these fields - instead, use NTP.



/Other settings

Physical reset button: Enable or disable the physical reset button.

[!] **Warning**: It is not recommended that you disable the device's physical reset button. Misconfigurations could make the device become unreachable.

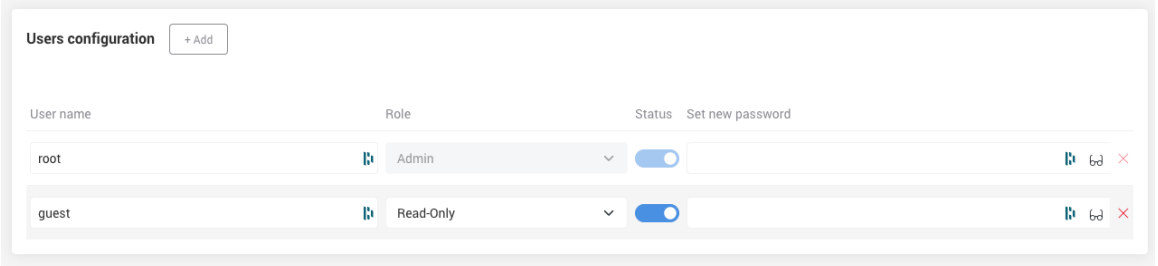


Users

The Users page gives you control over access to your device via the web UI and API.

There are currently two roles for a user:

1. **Admin**: Full access to all settings in the Web UI and all RESTful APIv1 routes
2. **Read-only**: Limited access to the Dashboard page of the web UI only, and APIv1 routes that don't affect operation of the device, such as fetching device stats.



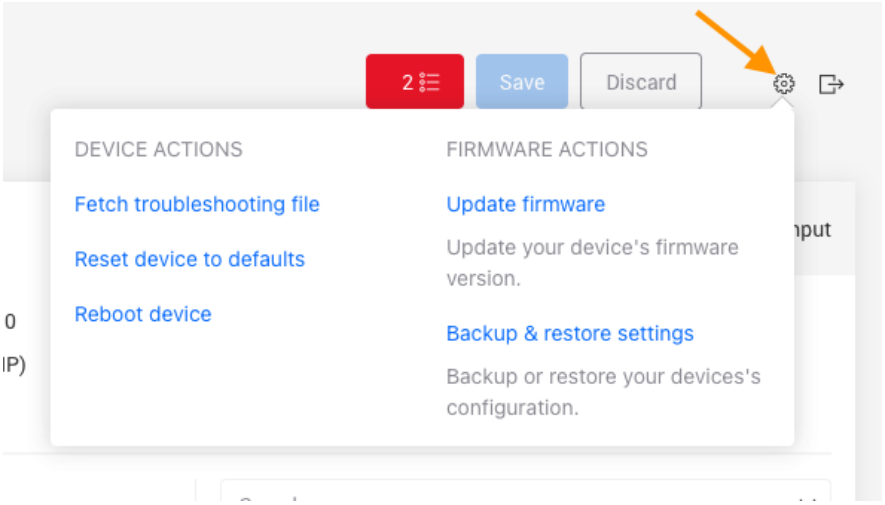
Password requirements

- Passwords must be between 5 and 32 characters long.

- As of firmware v1.11.0, you may use a subset of special characters in your user passwords.
- As of firmware v.1.11.2, you may use the following special characters: !@#$%^&*()?.><,~+_-/

System and device actions

You can find the system actions by clicking the gear icon located on the top right side of the page:



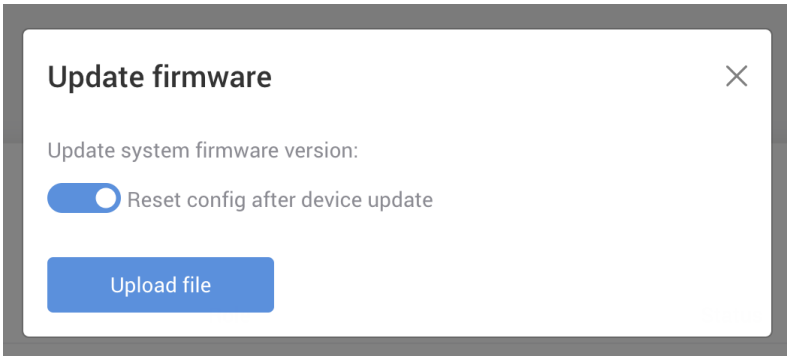
/Upgrade firmware

Select this option to upgrade or downgrade your device's firmware.

If after an upgrade attempt your device is running a previous version of firmware, it's possible that it failed to boot using the new firmware, and fell back to the previously working bootbank.

In this case, please contact support to verify you have a valid firmware image. If there was a power interruption or flicker during the upgrade, it's safe to retry the firmware upgrade assuming the device's input power is stable.

If you're downgrading your device's firmware, make sure to select the **"Reset config after device update"** option:



Warning: Do not unplug or reboot your device while firmware upgrade is in progress!

/Config backup & restore

Backup or restore the device's configuration settings.

! **Warning**: Is it currently not supported to restore the config of a device operating in AP mode on a device operating in Station mode, or visa versa.

/Reboot

Reboot your device immediately.

/Reset device

Reset your device to factory defaults. You may want to reset your device if downgrading to an older firmware.

/Fetch troubleshooting file

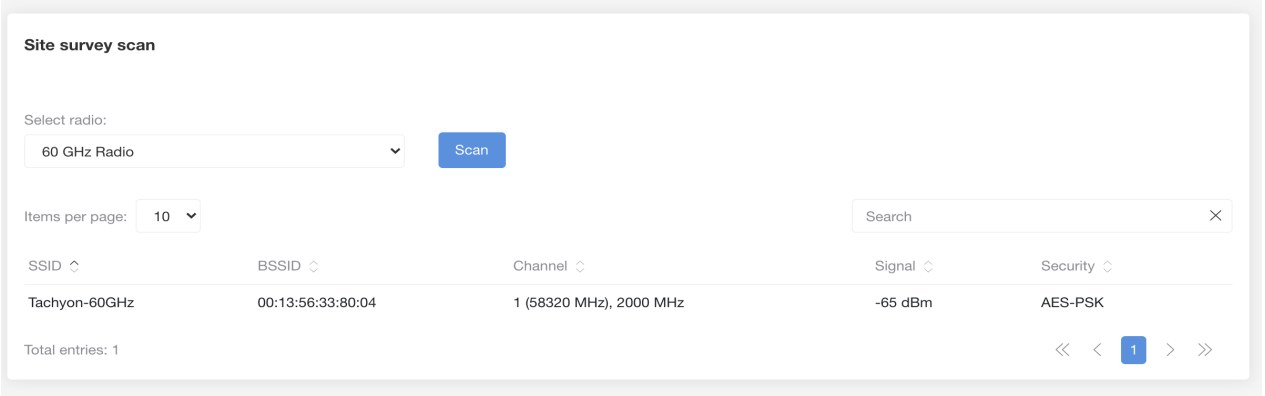
Fetch an archive of log files, configuration files, stats, and other information useful in troubleshooting any issues with the Tachyon support team.

Tools

/Site Survey

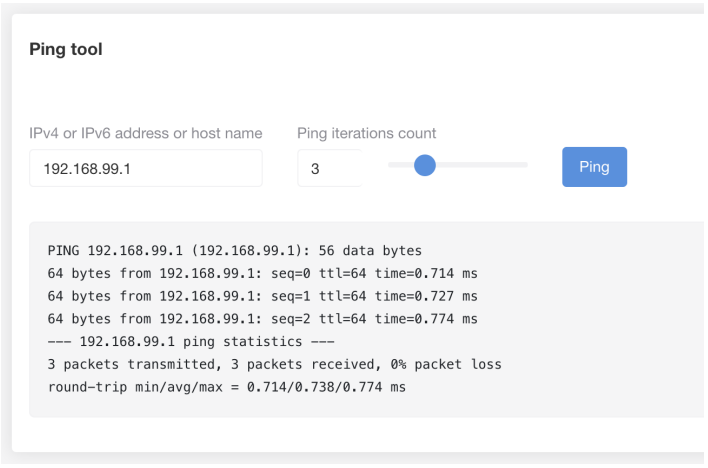
Use the site survey tool in order to view a list of other Tachyon 60GHz APs broadcasting in the nearby area.

! **Warning**: Running a site survey scan will temporarily cause your radio to become unreachable. It will come back automatically when scanning is complete.



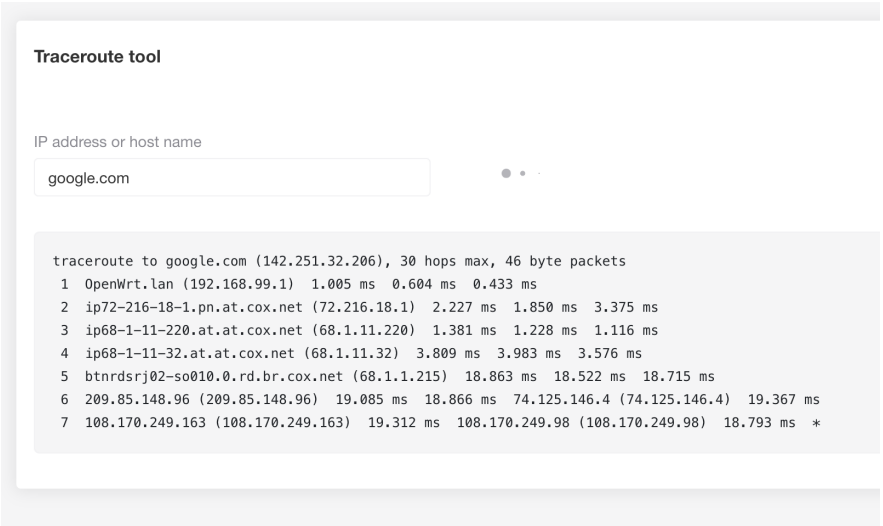
/Ping

Perform a basic ping IPv4 or IPv6 operation from the device.



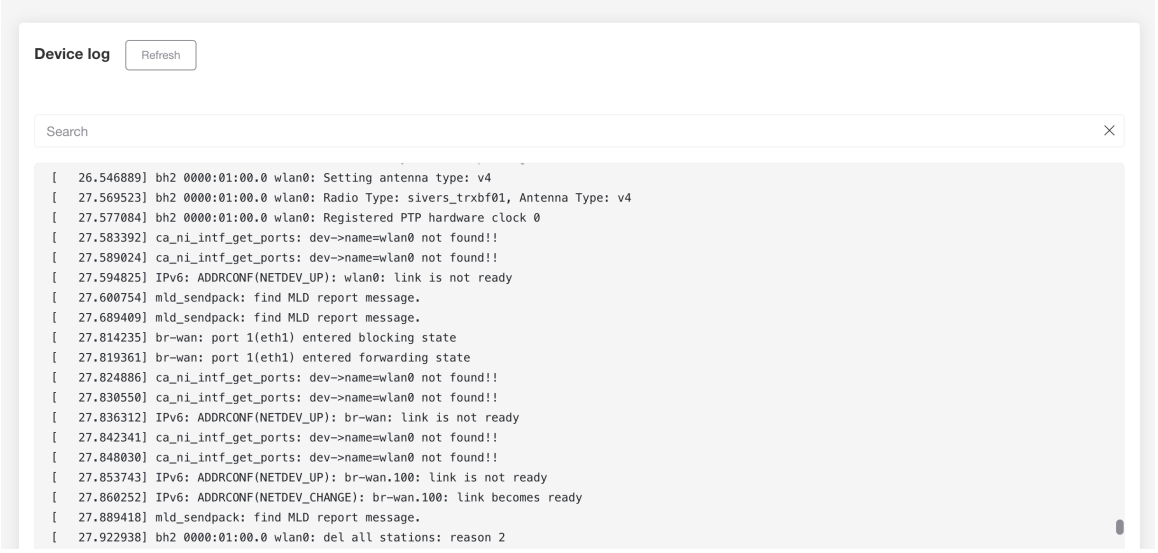
/Traceroute

Perform a basic traceroute operation from the device.



/View log

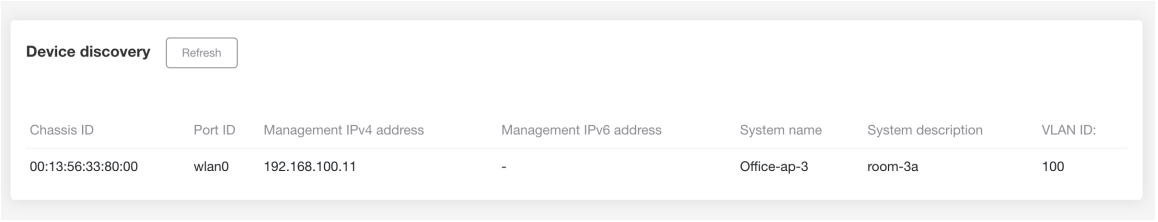
Search and view the device's `dmesg` output. Output from `logread` can be read from the console or via one of the **remote syslog** options.



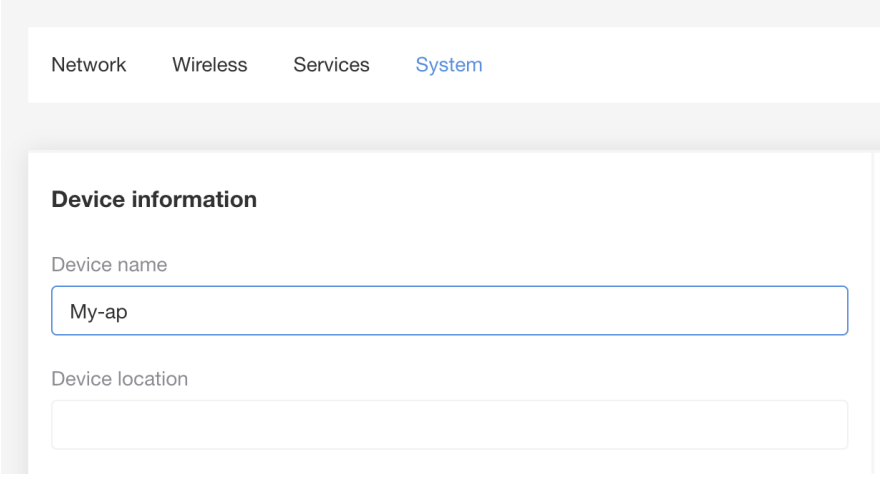
/Device discovery

Use the device discovery tool to find other devices on your network.

! **Note**: You must have **Device Discovery** enabled under the `Configuration >> Services >> Device discovery settings` page in order for your device(s) to be discoverable.

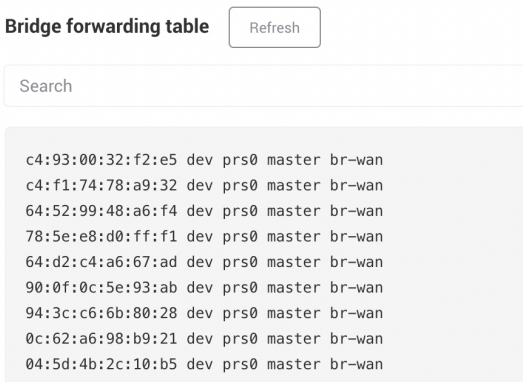


System name and description can be set under your device's system settings located at `Configuration >> System >> Device information`:



/Bridge Table

Use the bridge table tool to view the MAC addresses in the device's bridge forwarding table, as well as their associated interface and bridge.



In the example above, these MACs are behind prs0 in the br-wan bridge.

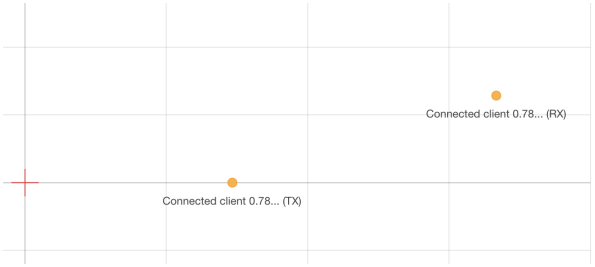
/Sector Info Tool

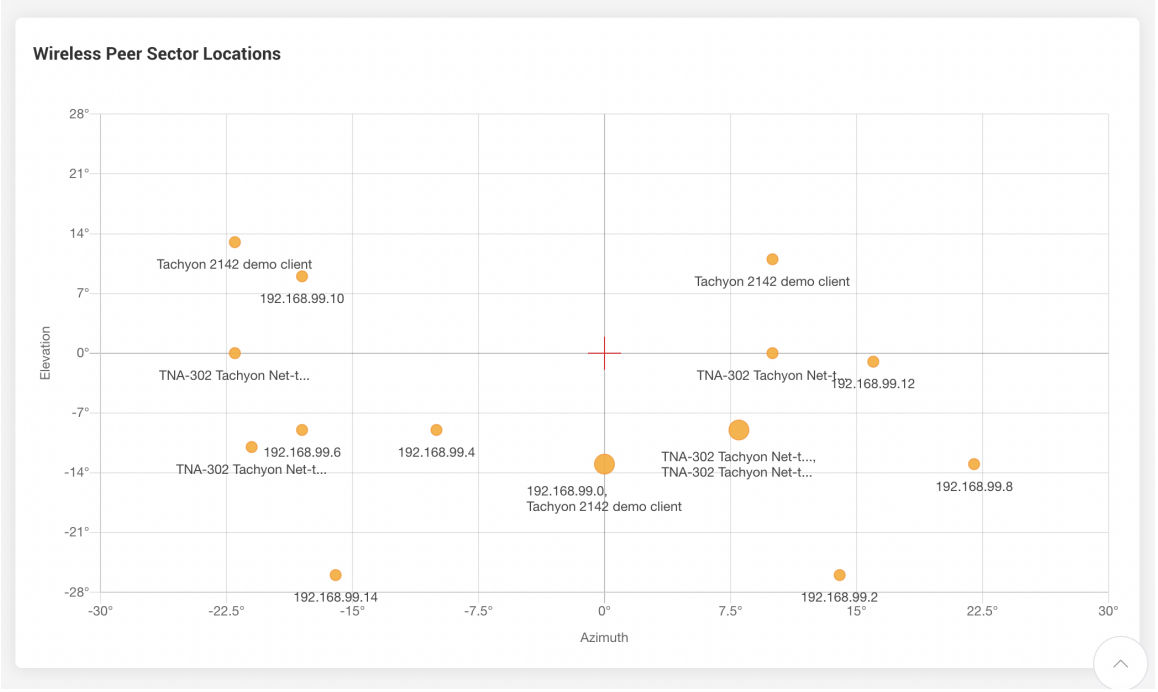
The sector tool will allow you to visually see how each peer is connected to the current device (the orange dot), which can help you determine how close connected peers are to boresight.

You can read more about TNA-30x antenna sectors (https://tachyon-networks.freshdesk.com/support/solutions/articles/67000717208-what-do-the-tna-30x-tx-rx-sector-numbers-mean-) in order to get a better understanding about what the sector IDs represent.

Notes:

- The red "X" denotes boresight for the device particular model.
- When you click on a connected peer's sector ID from the dashboard, you will only see that individual sector on the sector tool. You can click the "View all" button to view all connected peers.
- When multiple peers are connected on the same sector, the point will grow larger, a list of up to the first 3 devices connected on that sector will be shown.
- It's possible for a peer to be connected on different sectors for RX and TX. When this happens, a peer will be represented by two dots, each with a "(RX)" or "(TX)" label following the peer's name, like this:





Activity

Recent events, such as client association/disassociation, user login, DHCP events, etc can be found under the Activity page, or by clicking the calendar icon in the top right nav area.