Monitor the

Omada SDN Controller Network

Full version of Omada SDN Controller User Guide is available at **https://www.tp-link.com/support/download/omada-software-controller**

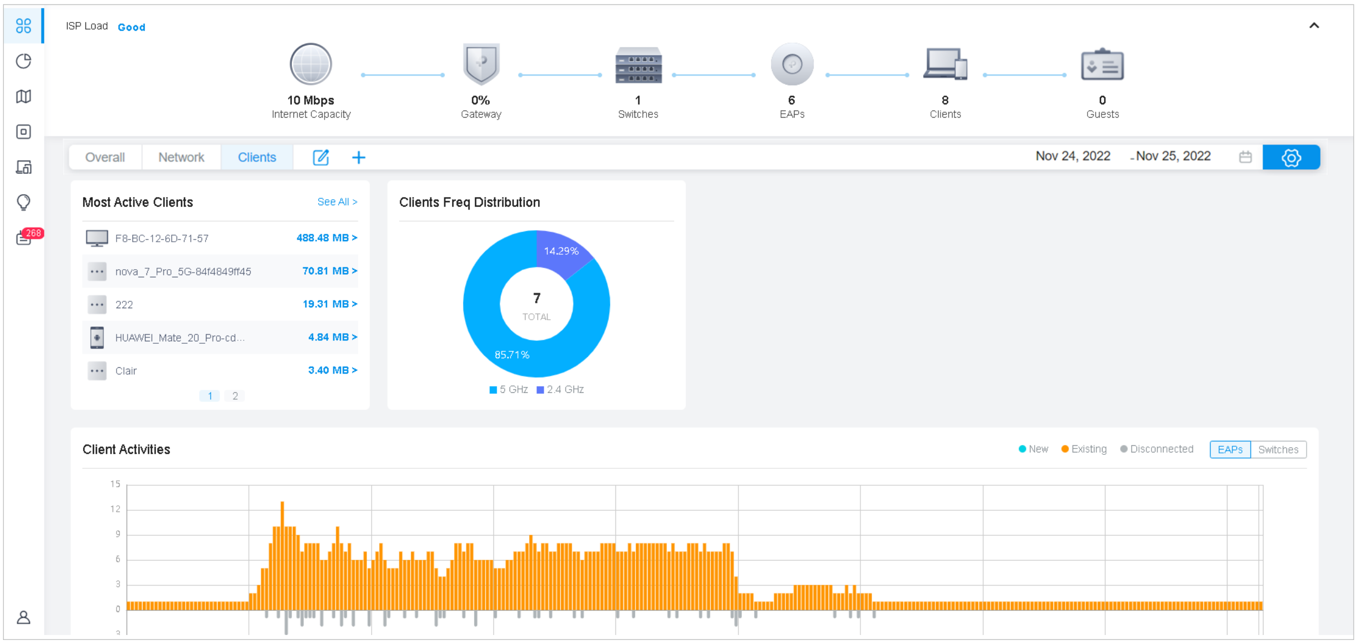
CONTENTS

1.Monitor and Manage the Clients

1. 1 View the Status of Network with Dashboard

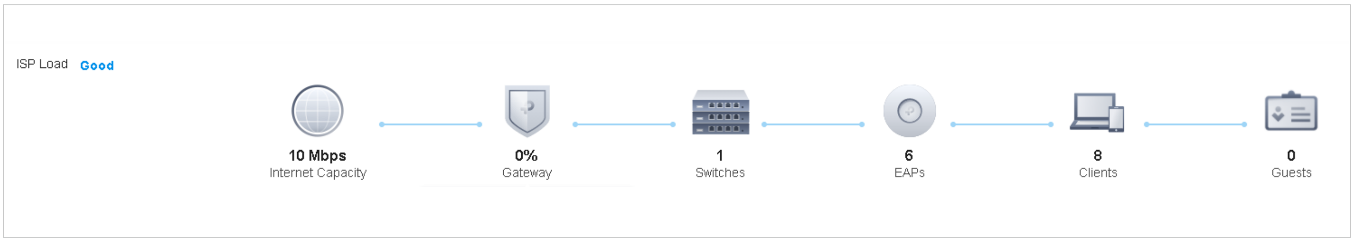
1. 1. 1 Page Layout of Dashboard

Dashboard is designed for a quick real-time monitor of the site network. An overview of network topology is at the top of Dashboard, and the below is a tab bar followed with customized widgets.

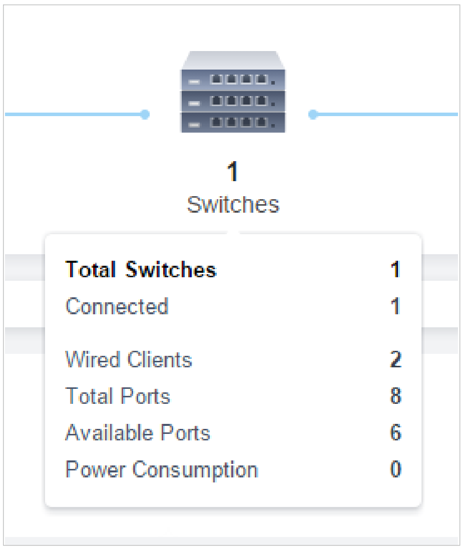


Topology Overview

Topology Overview on the top shows the status of ISP Load and numbers of devices, clients and guests. ISP Load has four statuses: Unknown, Good, Medium, Poor.



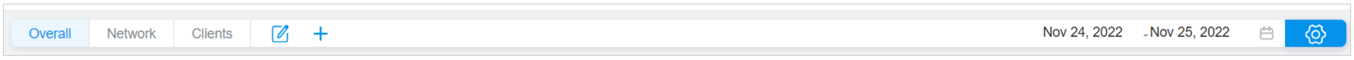
You can hover the cursor over the gateway, switch, AP, client or guest icons to check their status. For detailed information, click the icon here to jump to the Devices or Clients section.



Total Switches	1
Connected	1
Wired Clients	2
Total Ports	8
Available Ports	6
Power Consumption	0

Tab Bar

You can customize the widgets displayed on the tab for Dashboard page. Three tabs are created by default and cannot be deleted.



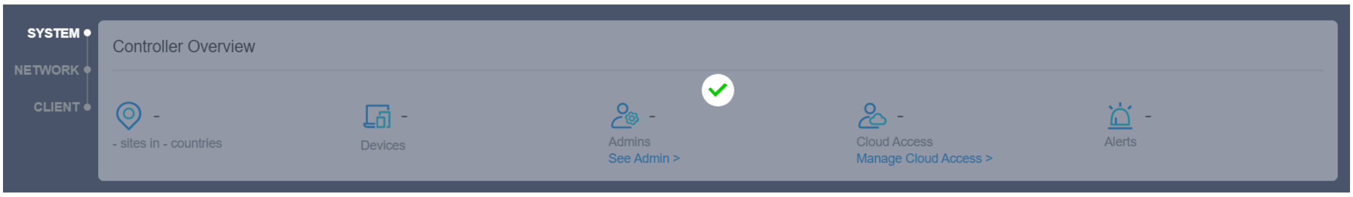
Overview	Displays Controller Overview and Association Failures by default.
Network	Displays Alerts, Wi-Fi Traffic Distribution, Wi-Fi Summary and Traffic Activities by default.
Clients	Displays Most Active Clients, Clients Freq Distribution, and Client Activities by default.

In the tab bar, you can take the following action to edit the tabs and customize the widget to be displayed.

✎	Click the icon to edit the tabs. For the default tabs, you can reset them to the default settings. For a created tab, you can edit its name or delete it.
+	Click the icon and enter the name in the pop-up window to create a new tab.
Nov 24, 2022 - Nov 25, 2022 📅	Click the date to display a calendar. To quickly display the statistics of today, yesterday, last 24 hours, or last several days, click the default date/period at the right side in the calendar. To display the statistics of a specific date, click the date twice in the calendar. To display the statistics of a specific time range, click the start date and end date in the calendar.
⚙	Click a tab and then click the widget in the pop-up page to add it to this tab or remove it.

1. 1. 2 Explanation of Widgets

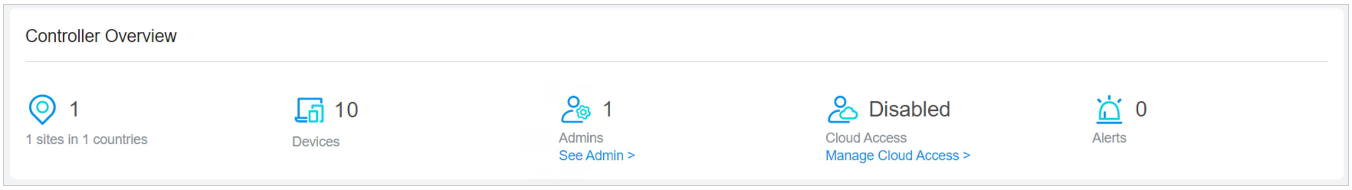
The widgets are divided into three categories: System, Network and Client. You can click the ⚙ icon to add or remove the widgets.



System	Controller Overview
Network	Alerts, ISP Load, VPNs, Most Active EAPs, Most Active Switches,Wi-Fi Traffic Distribution, Wi-Fi Summary, Switching Summary, Traffic Distribution, Client Distribution, Traffic Activities, Retried Rate/Dropped Rate, Top Devices Usage, PoE Utilization, Top Interference
Client	Most Active Clients, Longest Client Uptime, Clients Freq Distribution, Client Activities, Clients Association Activities, Association Failures, Clients SSID Distribution, Clients with on Boarding Times, Clients with RSSI

System

The Controller Overview widget in System displays the general information about the controller, including sites, devices, Admin accounts, Cloud Access, and alerts. You can click See Admin to view and manage Admin accounts, or click Manage Cloud Access to configure cloud access. For details, refer to 9 Manage Administrator Accounts of Omada SDN Controller.

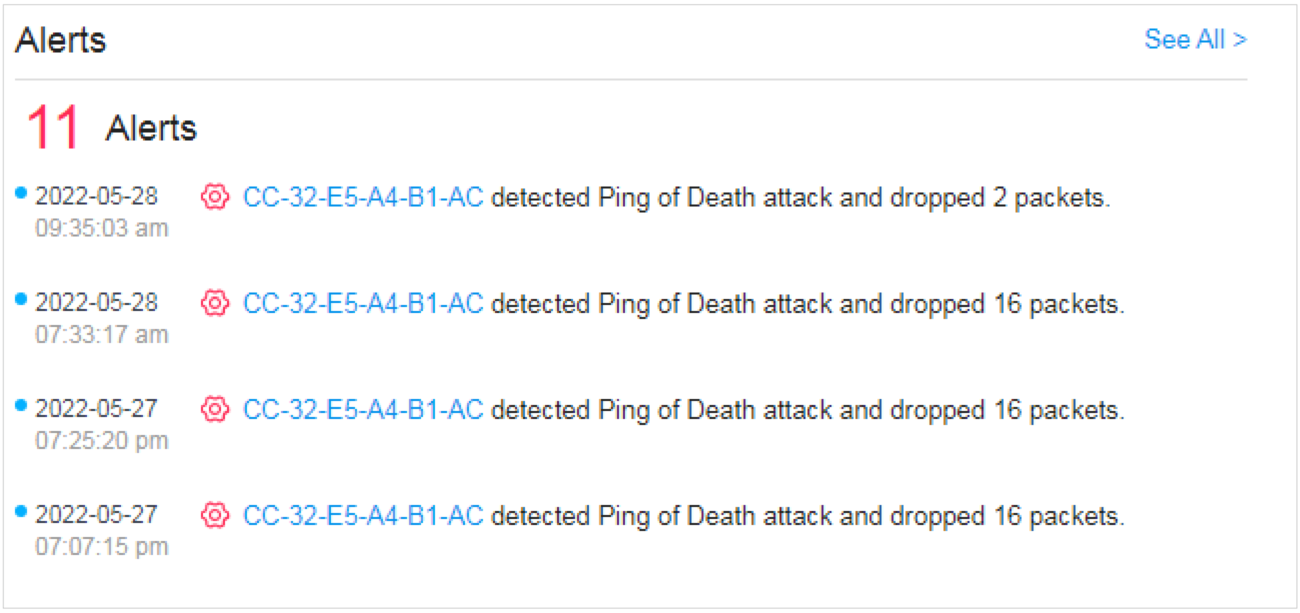


Network

Widgets in Network use lists and charts to illustrate the traffic status of wired and wireless networks in the site, including traffic statistics, the most active devices, VPN connection, distribution, **PoE utilization**, and interference.

- **Alerts**

  The Alerts widget displays the total number of unarchived alerts happened in the site and details of the latest five. To view all the alerts and archive them, click See All to jump to Log > Alerts. To specify events appeared in Alerts, go to Log > Notifications and configure the events as the Alert level. For details, refer to 8. 6 View and Manage Logs.



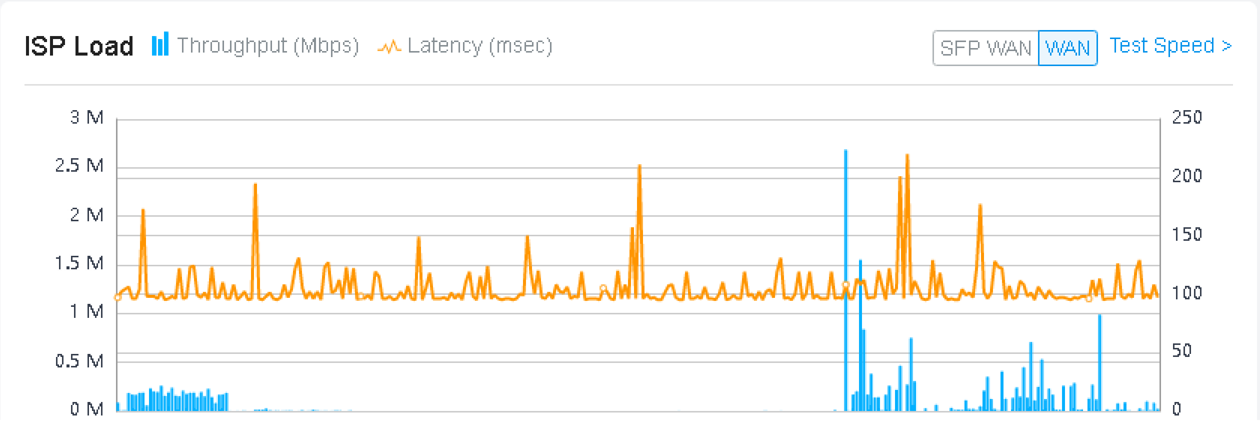
Alerts See All >

11 Alerts

- 2022-05-28 09:35:03 am CC-32-E5-A4-B1-AC detected Ping of Death attack and dropped 2 packets.
- 2022-05-28 07:33:17 am CC-32-E5-A4-B1-AC detected Ping of Death attack and dropped 16 packets.
- 2022-05-27 07:25:20 pm CC-32-E5-A4-B1-AC detected Ping of Death attack and dropped 16 packets.
- 2022-05-27 07:07:15 pm CC-32-E5-A4-B1-AC detected Ping of Death attack and dropped 16 packets.

- **ISP Load**

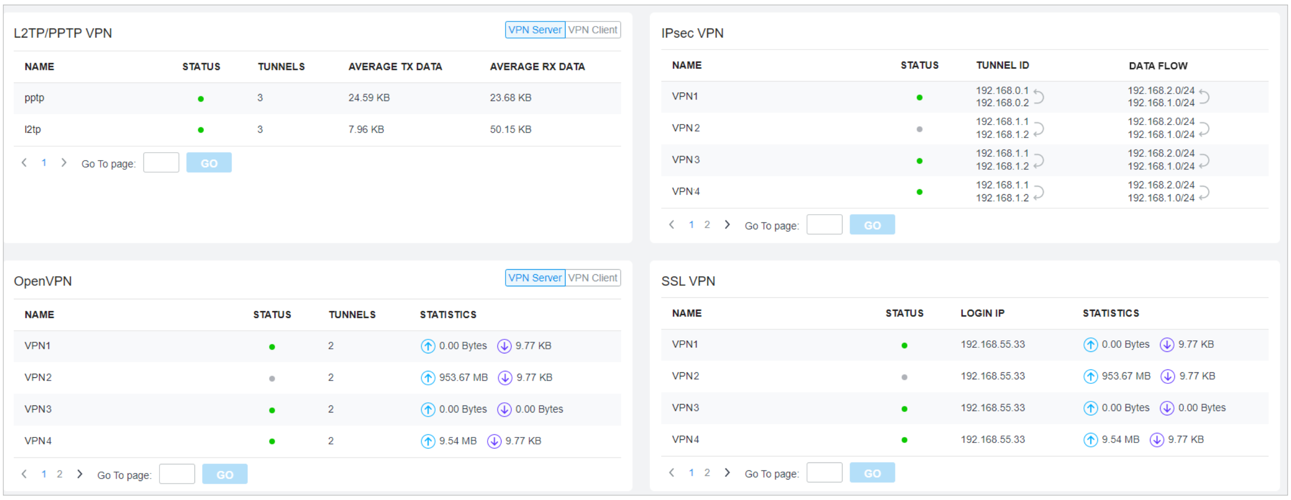
ISP Load use a line chart to display the throughput and latency of gateway's WAN port within the time range. Click the tab on the right to view the statistics of each WAN port and move the cursor on the line chart to view specific values of throughput and latency. For detailed statistics of certain gateway's WAN port within a time range, refer to 8. 2 View the Statistics of the Network.



To test the current download and unload speed and the latency of WAN port, click Test Speed on the widget to display the speed test result.

- **VPNs**

VPNs displays the information of VPN servers and VPN clients. Click the corresponding tab to display the statistics.



L2TP/PPTP VPN

NAME	STATUS	TUNNELS	AVERAGE TX DATA	AVERAGE RX DATA
pptp	●	3	24.59 KB	23.68 KB
l2tp	●	3	7.96 KB	50.15 KB

IPsec VPN

NAME	STATUS	TUNNEL ID	DATA FLOW
VPN1	●	192.168.0.1 192.168.0.2	192.168.2.0/24 192.168.1.0/24
VPN2	●	192.168.1.1 192.168.1.2	192.168.2.0/24 192.168.1.0/24
VPN3	●	192.168.1.1 192.168.1.2	192.168.2.0/24 192.168.1.0/24
VPN4	●	192.168.1.1 192.168.1.2	192.168.2.0/24 192.168.1.0/24

OpenVPN

NAME	STATUS	TUNNELS	STATISTICS
VPN1	●	2	↑ 0.00 Bytes ↓ 9.77 KB
VPN2	●	2	↑ 953.67 MB ↓ 9.77 KB
VPN3	●	2	↑ 0.00 Bytes ↓ 0.00 Bytes
VPN4	●	2	↑ 9.54 MB ↓ 9.77 KB

SSL VPN

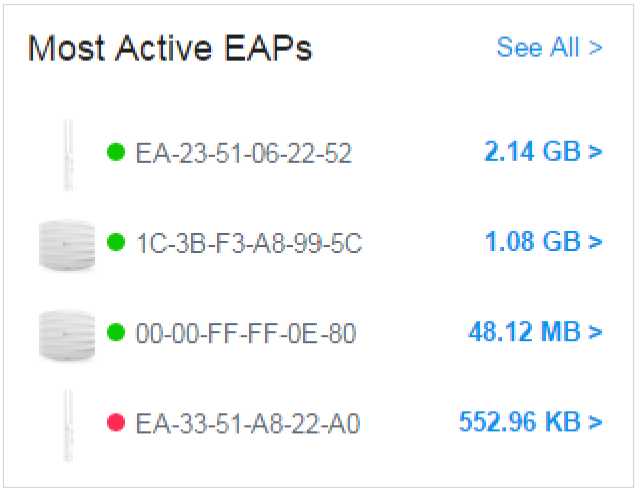
NAME	STATUS	LOGIN IP	STATISTICS
VPN1	●	192.168.55.33	↑ 0.00 Bytes ↓ 9.77 KB
VPN2	●	192.168.55.33	↑ 953.67 MB ↓ 9.77 KB
VPN3	●	192.168.55.33	↑ 0.00 Bytes ↓ 0.00 Bytes
VPN4	●	192.168.55.33	↑ 9.54 MB ↓ 9.77 KB

Name	Displays the name of VPN server/client.
Status	Displays the connection status of VPN server/client.
Tunnels	Displays the number of VPN tunnels for the VPN server.
Average Tx Data	Displays the average transmitted traffic of the VPN serve/client.
Average Rx Data	Displays the average received traffic of the VPN serve/client.
Statistics	Displays the upstream and downstream traffic of the VPN server/client.
Login IP	Displays the login IP of the SSL VPN.
Tunnel ID	Displays the direction of the IPSec VPN tunnel.
Data Flow	Displays the data flow of the IPSec VPN tunnel.

- **Most Active EAPs/Most Active Switches**

These two widgets can display, respectively, 15 most active EAPs and switches in the site based on the total number of traffic within the time range. Only the devices that has been adopted by the controller will be displayed.

To view all the devices discovered by the controller, click See All to jump to the Devices section. You can also click the traffic number in the widget to open the device's Properties window for further configurations and monitoring. For details, refer to 6 Configure and Monitor Omada Managed Devices.

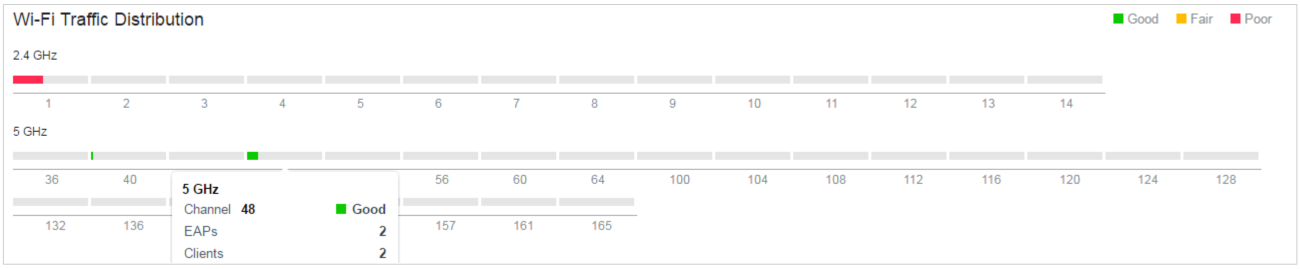


Most Active EAPs See All >

- ● EA-23-51-06-22-52 2.14 GB >
- ● 1C-3B-F3-A8-99-5C 1.08 GB >
- ● 00-00-FF-FF-0E-80 48.12 MB >
- ● EA-33-51-A8-22-A0 552.96 KB >

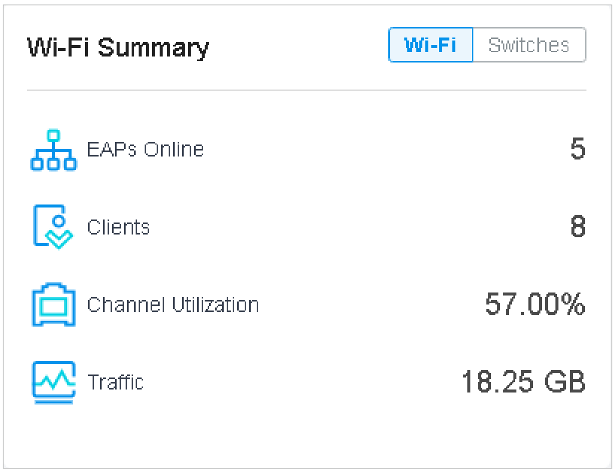
- **Wi-Fi Traffic Distribution**

The Wi-Fi Traffic Distribution widget displays channel distribution of all connected EAPs in the site. Good, Fair, and Poor are used to describe channel status which indicates channel interference from low to high. You can hover your cursor over the band to view the number of EAPs and clients on the channel.



- **Wi-Fi Summary**

The Wi-Fi Summary widget summarizes the real-time status of wireless networks in the site, including the number of connected EAPs and clients, the channel utilization, and the total number of traffic within the time range.

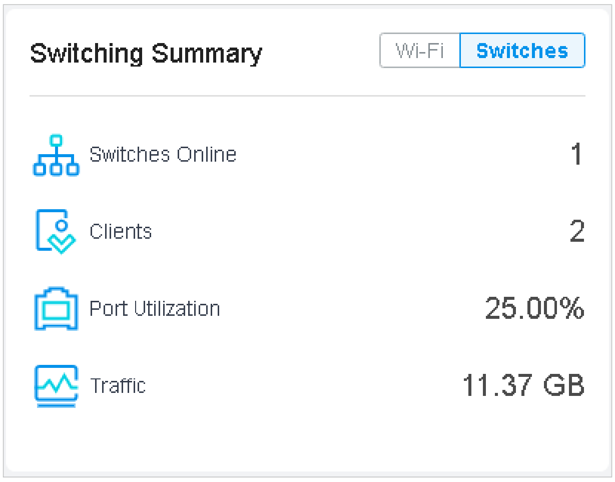


Wi-Fi Summary Wi-Fi Switches

EAPs Online	5
Clients	8
Channel Utilization	57.00%
Traffic	18.25 GB

- **Switching Summary**

  The Switching Summary widget summarizes the real-time status of switches in the site, including the number of connected switches and clients, the port utilization, and the total amount of traffic within the time range.

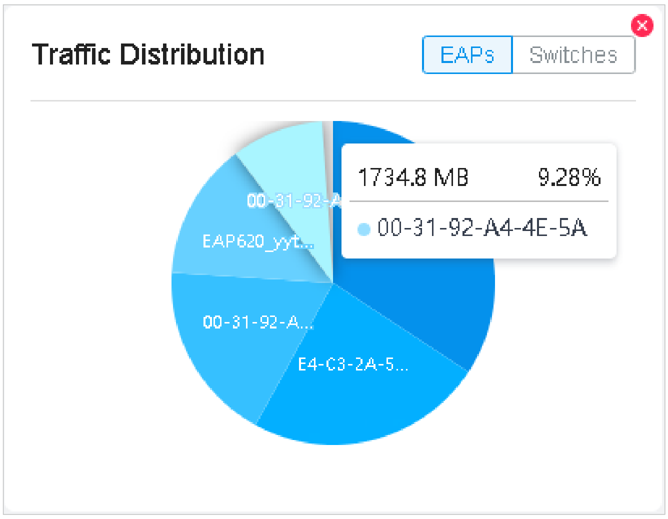


Switching Summary

Switches Online	1
Clients	2
Port Utilization	25.00%
Traffic	11.37 GB

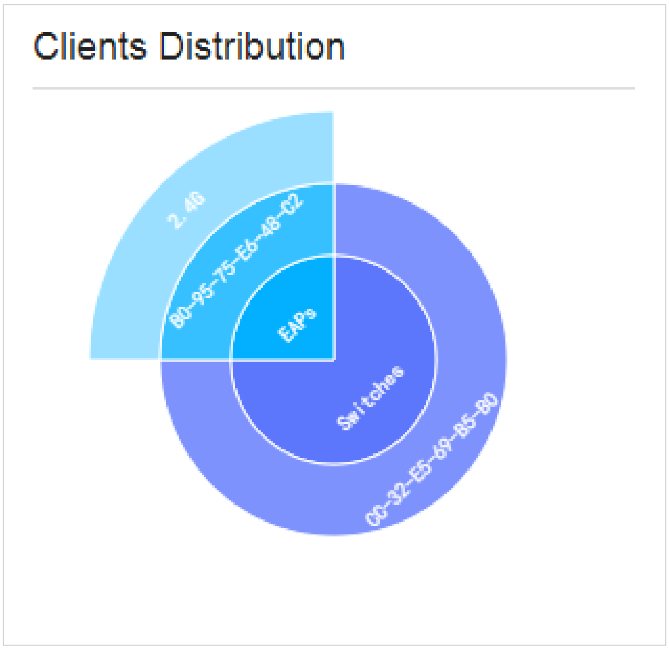
- **Traffic Distribution**

  The Traffic Distribution widget uses a pie chart to display the traffic distribution on EAPs and switches in the site within the time range. Click the tab to display the statistic of EAPs or switches, and click the slice to view the total number of traffic, its proportion, and the device name.



- **Client Distribution**

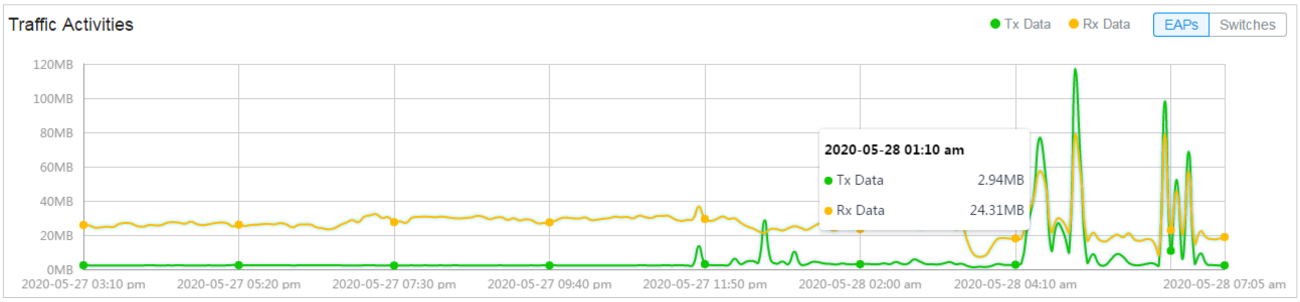
  The Client Distribution widget uses a sunburst chart to display the real-time distribution of connected clients in the site. The chart has up to three levels. The inner circle is divided by the device category the clients connected to, the middle is by the device name, and the outer is by the frequency band. You can hover the cursor over the slice to view specific values.



- **Traffic Activities**

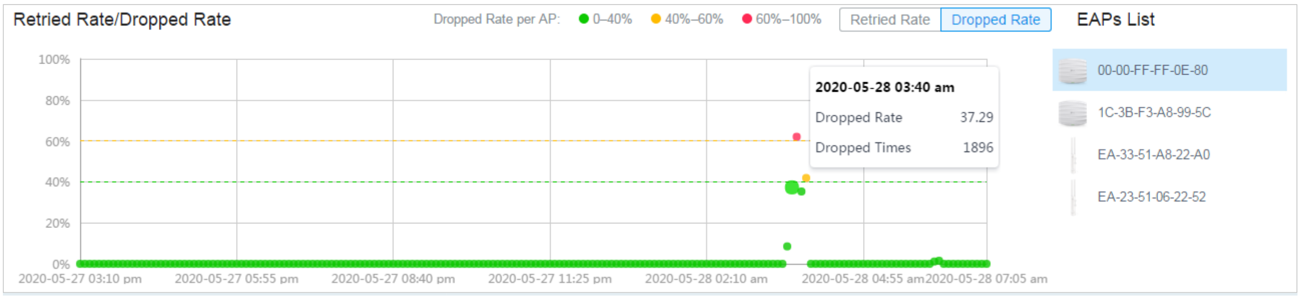
  The Traffic Activities widget displays the Tx and Rx data of EAPs and switches within the time range. Only activities of the devices in the connected status currently will be counted.

  Click the tab to display the statistic of EAPs or switches, and move the cursor on the line chart to view specific values of traffic. For detailed statistics of certain devices within a time range, refer to 8. 2 View the Statistics of the Network.



- **Retried Rate/Dropped Rate**

  The Retried Rate/Dropped Rate widget displays the rate of retried and dropped packets of the connected EAPs within the time range. Select an AP from the list and click the tab to display the chart of retried rate or dropped rate. You can move the cursor on the point to view specific values.



2020-05-28 03:40 am

Dropped Rate 37.29

Dropped Times 1896

00-00-FF-FF-0E-80

1C-3B-F3-A8-99-5C

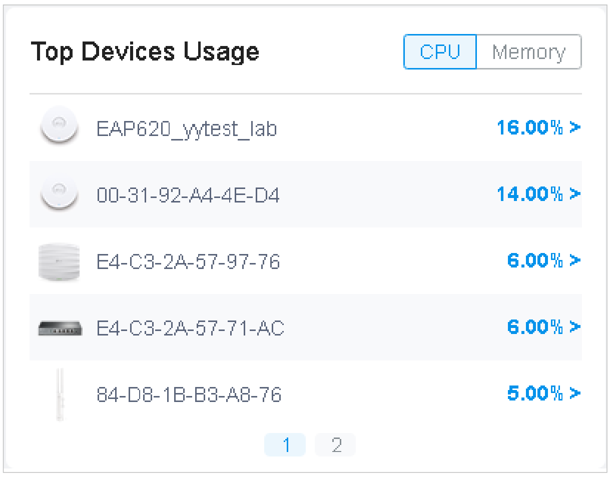
EA-33-51-A8-22-A0

EA-23-51-06-22-52

Retried Rate	Displays the percentage of packets that needed to be re-sent because they were corrupted upon arriving at the proper destination.
Dropped Rate	Displays the percentage of packets that were dropped before reaching their intended destination.

- **Top Devices Usage**

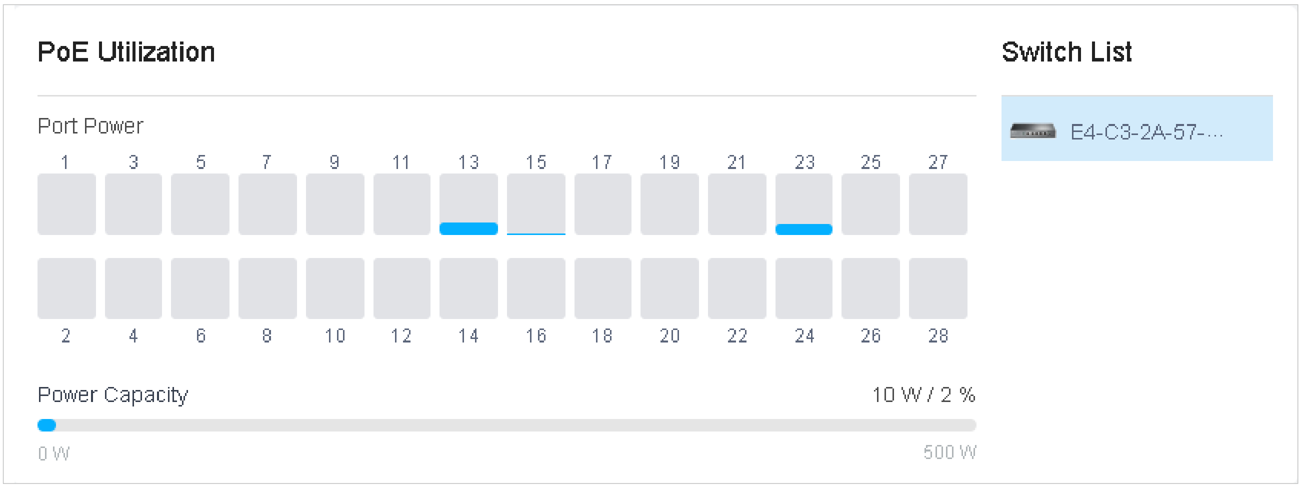
  The Top Devices Usage widget displays the CPU utilization and memory utilization of devices within the time range. Click the tab to select the CPU or memory for display. Click the traffic number in the widget to open the device's Properties window for further configurations and monitoring. For details, refer to 6 Configure and Monitor Omada Managed Devices.



EAP620_yytest_lab	16.00% >
00-31-92-A4-4E-D4	14.00% >
E4-C3-2A-57-97-76	6.00% >
E4-C3-2A-57-71-AC	6.00% >
84-D8-1B-B3-A8-76	5.00% >

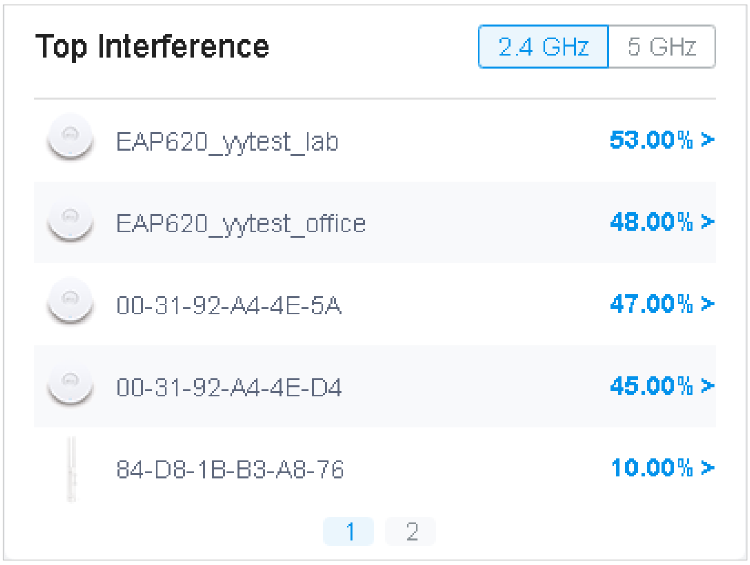
- **PoE Utilization**

  The PoE Utilization widgets describes the PoE utilization of a switch. Select a switch from the switch list to display the ports connected to PoE devices. You can hover the cursor over a certain port to view specific values. The bar below displays the current power capacity provided by PoE and its proportion of the PoE budget.



- **Top Interference**

  The Top Interference widget displays the environment interference of wireless products. Click the tab to select the 2.4 GHz band or 5 GHz band. Click the traffic number in the widget to open the device's Properties window for further configurations and monitoring. For details, refer to 6 Configure and Monitor Omada Managed Devices.



Top Interference

2.4 GHz | 5 GHz

EAP620_yytest_lab	53.00% >
EAP620_yytest_office	48.00% >
00-31-92-A4-4E-5A	47.00% >
00-31-92-A4-4E-D4	45.00% >
84-D8-1B-B3-A8-76	10.00% >

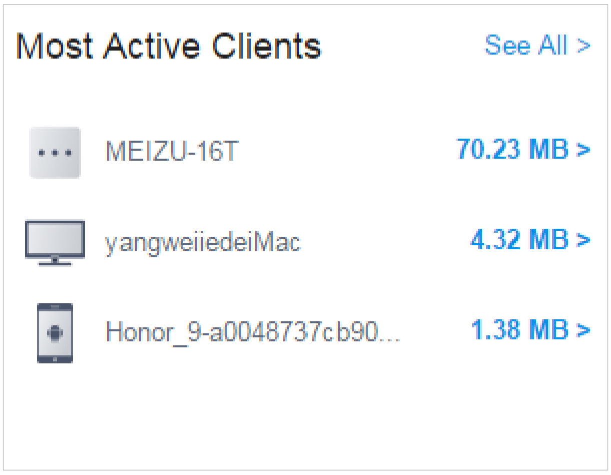
Client

Widgets in Clients use lists and charts to illustrate the traffic status of wired and wireless clients in the site, including the most active clients, activity statistics and distribution.

- **Most Active Clients**

  The Most Active Clients widget can display 15 most active clients. Only the clients in the connected status currently will be displayed.

To view all the clients connected to the network, click See All to jump to the Clients section. You can also click the traffic number in the widget to open the client's Properties window for further configurations and monitoring. For details, refer to 7.1 Manage Wired and Wireless Clients in Clients Page.



Most Active Clients See All >

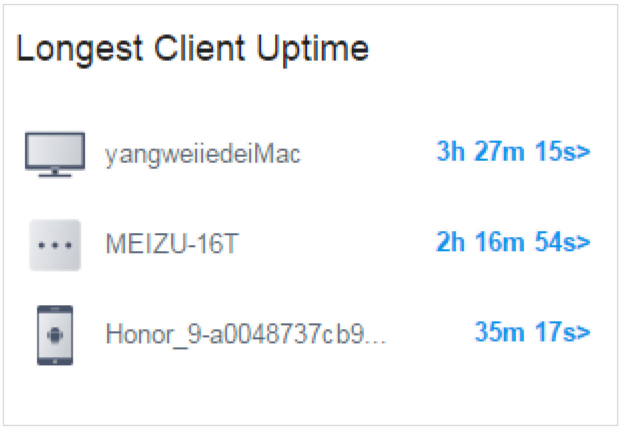
MEIZU-16T 70.23 MB >

yangweiiedeiMac 4.32 MB >

Honor_9-a0048737cb90... 1.38 MB >

- **Longest Client Uptime**

  The Longest Client Uptime widget can display up to15 clients sorted by the uptime. Only the clients in the connected status currently will be displayed. You can also click the uptime in the widget to open the client's Properties window for further configurations and monitoring. For details, refer to 7.1 Manage Wired and Wireless Clients in Clients Page.



Longest Client Uptime

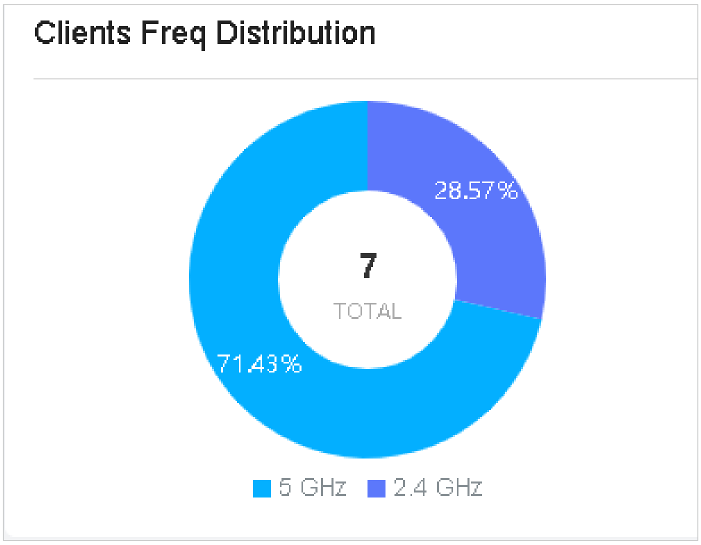
yangweiiedeiMac 3h 27m 15s>

MEIZU-16T 2h 16m 54s>

Honor_9-a0048737cb9... 35m 17s>

- **Clients Freq Distribution**

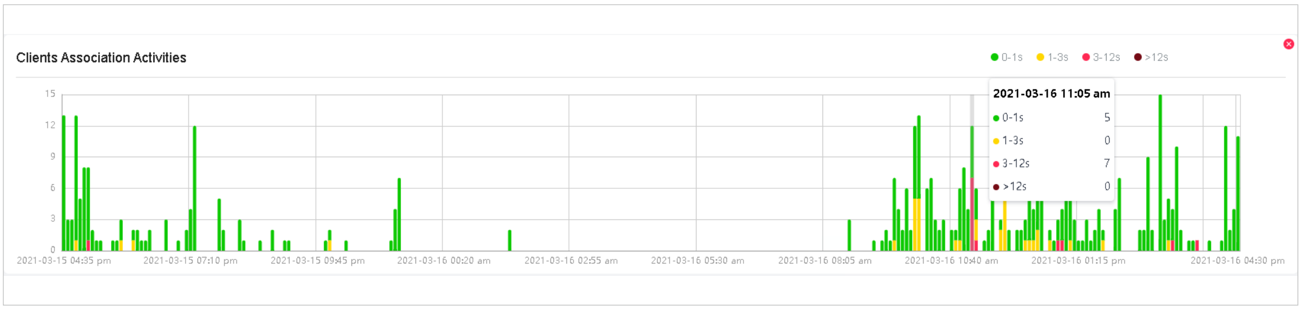
  The Clients Freq Distribution widget uses a donut chart to display the distribution of wireless clients connected to the 5 GHz band and 2.4 GHz band in the site. The chart has two levels. The inner circle shows the total number of wireless clients, and the outer displays the proportion of clients that connect to the two bands. You can hover the cursor over the slice to view the number of clients in 2.4 GHz or 5 GHz band.



- **Clients Association Activities**

  The Clients Association Activities widget displays how the number of client connected to EAPs changes over time and the duration during which the clients communicate with the EAPs. In the stacked chart, you can easily compare the total number of clients and analyze the variation of each time period.

  The total value of a column shows the total number of clients connected to EAPs in this time period, and the segments in four colors represents the client number of different durations in specific time.

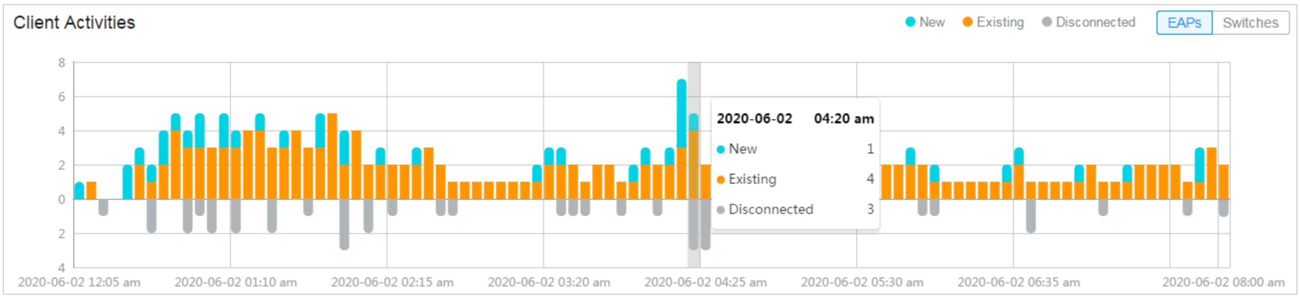


- **Client Activities**

  The Client Activities widget displays how the number of connected client changes over time within the time range. In the stacked chart, you can easily compare the total number of clients and analyze the variation of each time period.

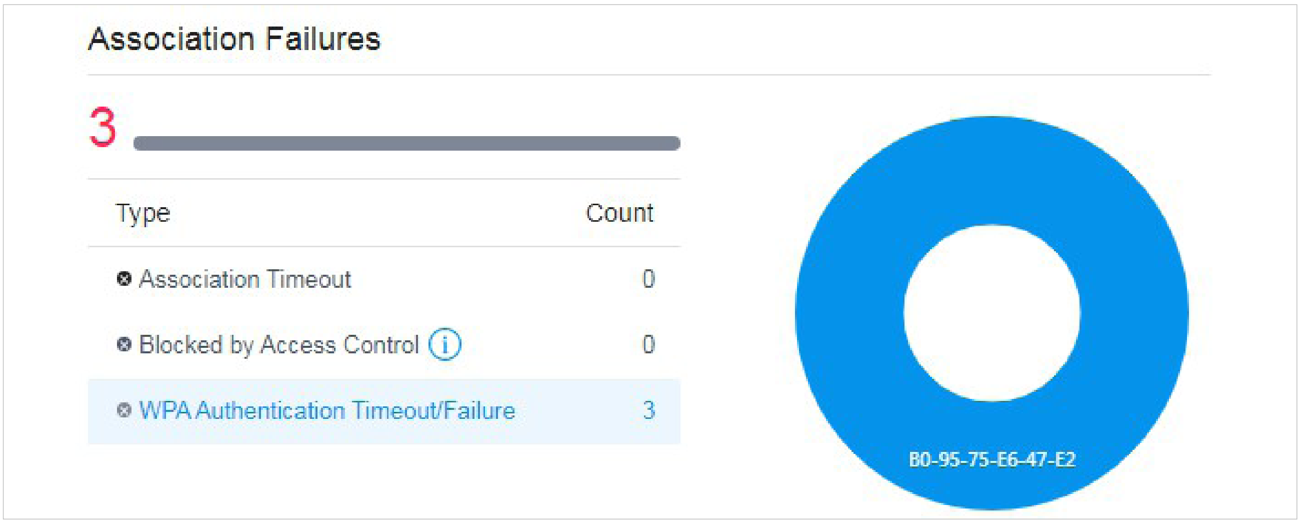
  The total value of a column shows the total number of connected clients in this time period, and the segments in three colors shows the change of client number compared with the last time period.

Blue represents the newly connected clients, orange is the clients have been connected in the last period, and gray is the newly disconnected clients.



- **Association Failures**

The Association Failures widget list three failure types and the times of clients failed to connect to the EAPs' networks in the site. A single bar is next to the count to show the proportion of the three failure reasons using gray colors from dark to light. Click the reason in the list to view the distribution of failures on EAPs.



Association Failures

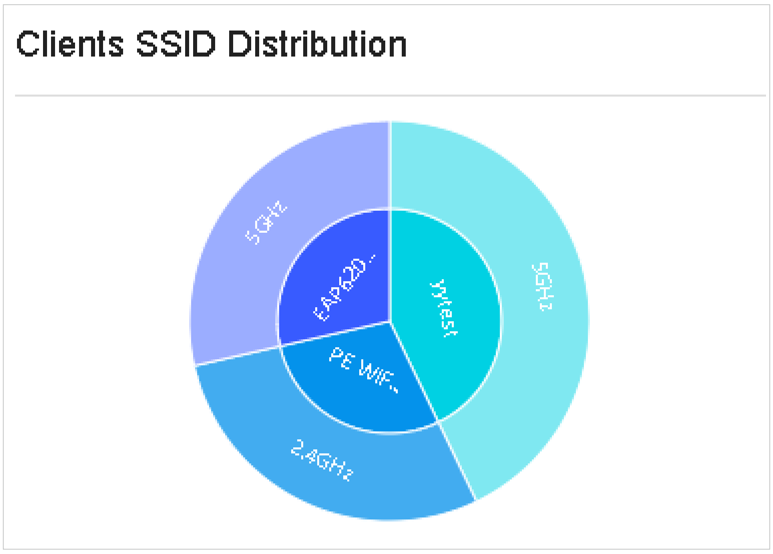
3

Type	Count
Association Timeout	0
Blocked by Access Control ⓘ	0
WPA Authentication Timeout/Failure	3

Association Timeout	The connection failed because of session timeout.
Blocked by Access Control	The connection failed because the client has been blocked. For details about blocked clients, refer to 8. 5. 1 Known Clients.
WPA Authentication Timeout/Failure	The connection failed because the client did not pass the authentication due to authentication timeout or wrong password.

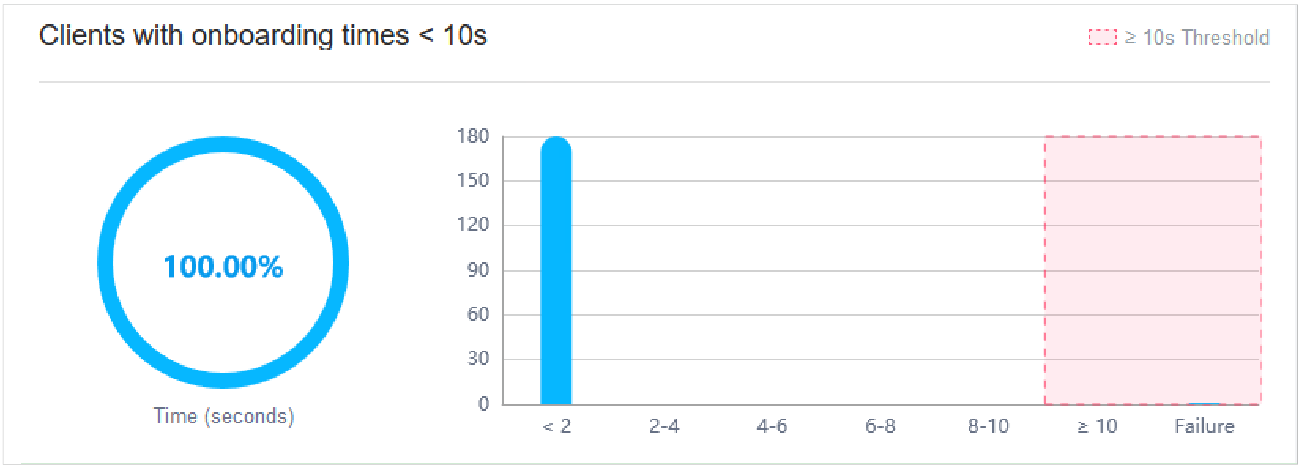
- **Clients SSID Distribution**

The SSID Distribution widget uses a sunburst chart to display the distribution of wireless clients connected to the different SSIDs in the site. The chart has two levels. The inner circle is divided by the EAP's SSID that the clients connected to, and the outer is by the frequency band. You can hover the cursor over the slice to view the number of clients connected to the SSID in 2.4 GHz or 5 GHz band. Click a certain SSID to further display the statistics of its band frequency distribution.



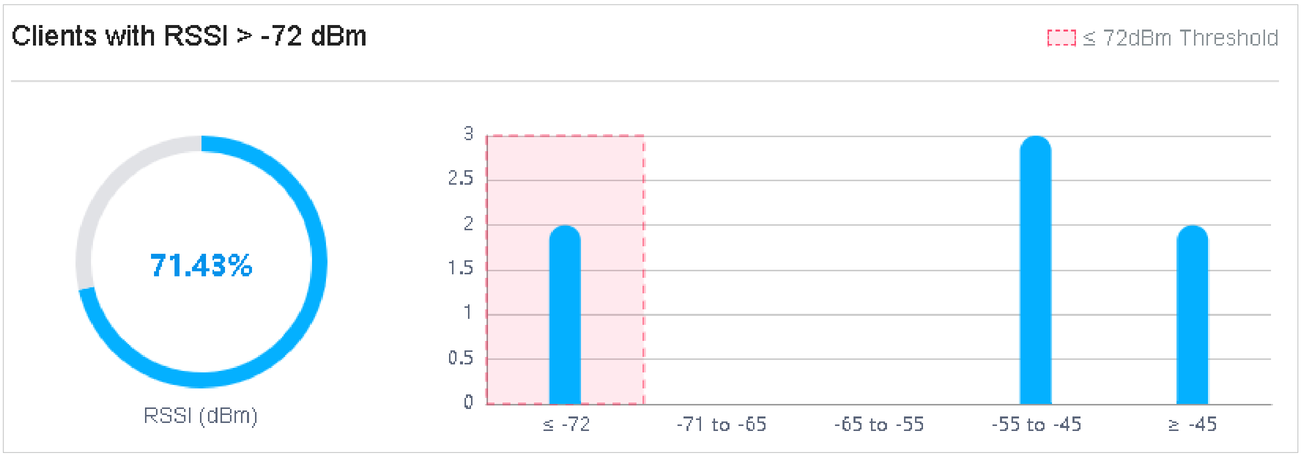
- **Clients with on Boarding Times**

  The Clients with on Boarding Times widget describes the time wireless clients uses when connecting to a certain SSID. The donut chart on the left shows the proportion of clients that uses less than 10 seconds to connect to the devices. The line graph on the right displays the number of clients according to the different time that the clients takes to connect to the SSIDs.



- **Clients with RSSI**

  The Clients with RSSI widget describes the RSSI (Received Signal Strength Indication) that wireless clients experience in the environment. RSSI is a negative value measuring the power level being received after any possible loss at the antenna and cable level. The higher the RSSI value, the stronger the signal. The donut chart on the left shows the proportion of clients whose RSSI value is bigger than -72 dBm. The line graph on the right displays the number of clients according to the different range values of RSSI.



1. 2 View the Statistics of the Network

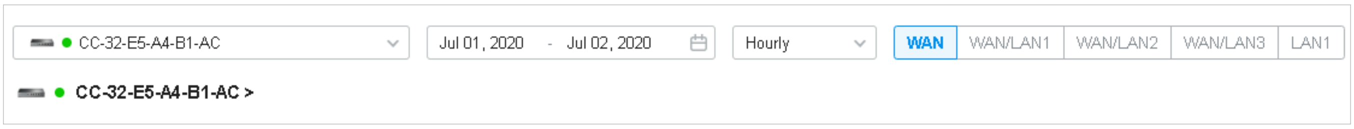
Statistics provides a visual representation of device data in Omada SDN Controller. You can easily monitor the network traffic and performance under the following tabs, Performance, Switch Statistics, and Speed Test Statistics.

1. 2. 1 Performance

In Performance, you can view the device performance in a specified period by graphs, such as user counts, CPU and memory usage, and transmitted and received packets. The graphs vary due to the device type and status.

Tab Bar

The tabs and calendar on the top are used to specify the displayed statistics, and the legends on the right account for elements in the graphs.



switch	Click to select a device from the drop-down list to view its statistics. The tabs vary due to the type of the selected device.
Jul 06 , 2020 - Jul 07 , 2020	Click the date to display a calendar. Click a specific date twice in the calendar for the widgets to display its statistics. To display the statistic of a time range, click the start date and end date in the calendar, or directly select the time range on the right. The available time range is restricted by the time interval. Before selecting a long time range, select Hourly or Daily as the time interval.
Hourly	Select 5 minutes, Hourly, or Daily to specify the time interval of the data. When selecting a long time range, a longer time interval is recommended for a better view.
WAN WAN/LAN1 WAN/LAN2 WAN/LAN3 LAN1	(For gateway) Click to select the port of gateway on the tab to view the statistics.
All 2.4 GHz 5 GHz	(For AP) Click to select the band of the AP to view the statistics.

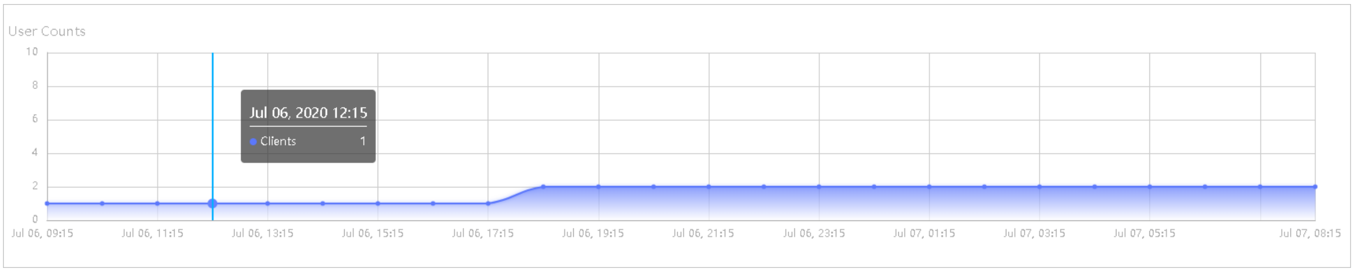
Statistical Graphs

Statistical graphs vary according to the type of devices. The chart below shows the statistical graphs which correspond to the gateway, switch, and AP.

Gateway	User Counts, Usage, Traffic, Packets
Switch	User counts, Usage
AP	User Counts, Usage, Traffic, Packets, Dropped, Errors, Retries

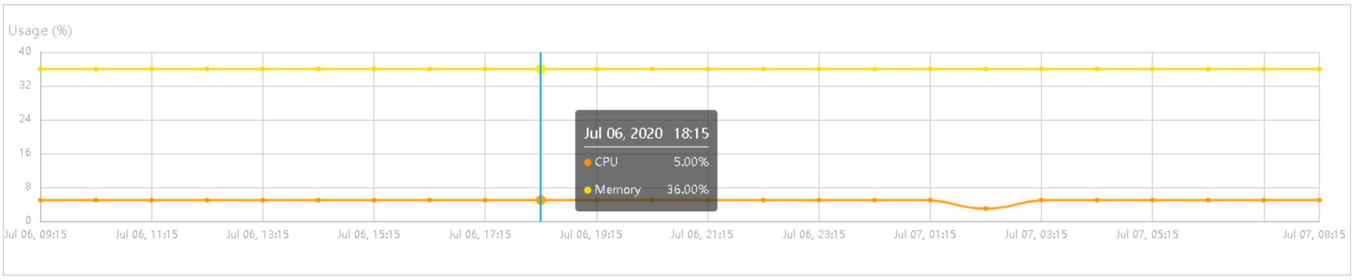
- **User Counts**

The User Counts graph displays the number of users connected to the devices during the selected time range. Hover the cursor over the line to display the specific values.



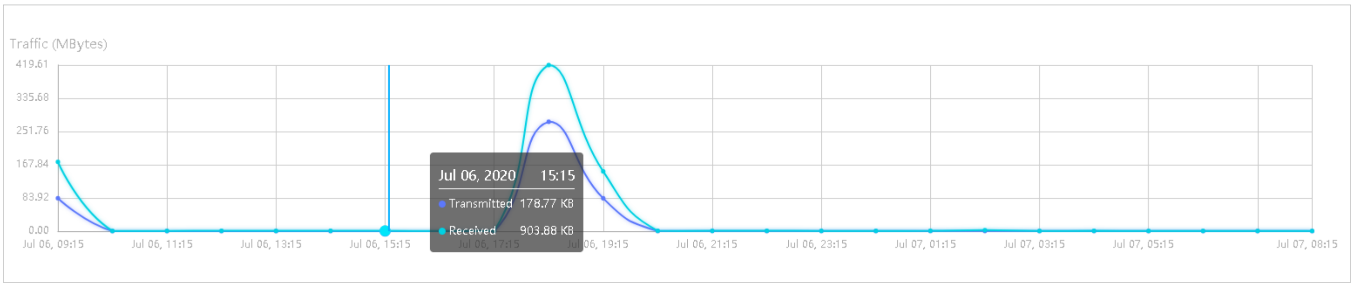
- **Usage**

The Usage graph uses the orange line and yellow line to display the percentage of CPU usage and used memory during the selected time range, respectively. Hover the cursor over the lines to display the specific values.



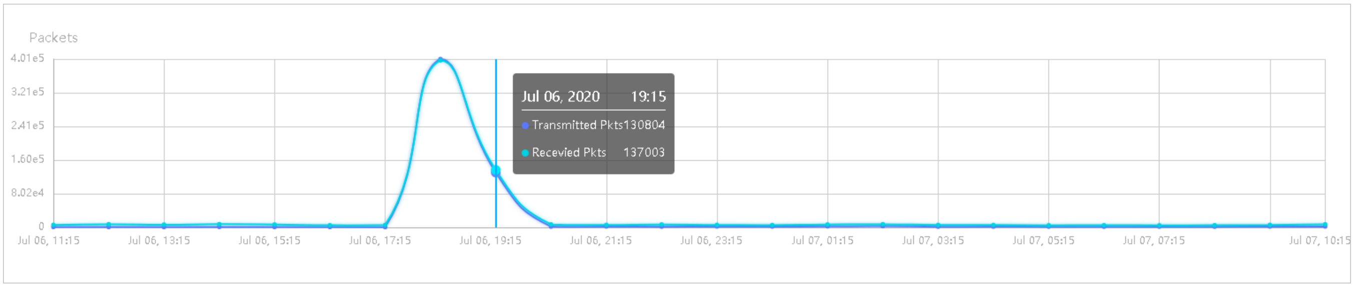
- **Traffic**

The Traffic graph uses the dark blue line and light blue line to display the bytes of data transmitted and received during the selected time range, respectively. Hover the cursor over the lines to display the specific values.



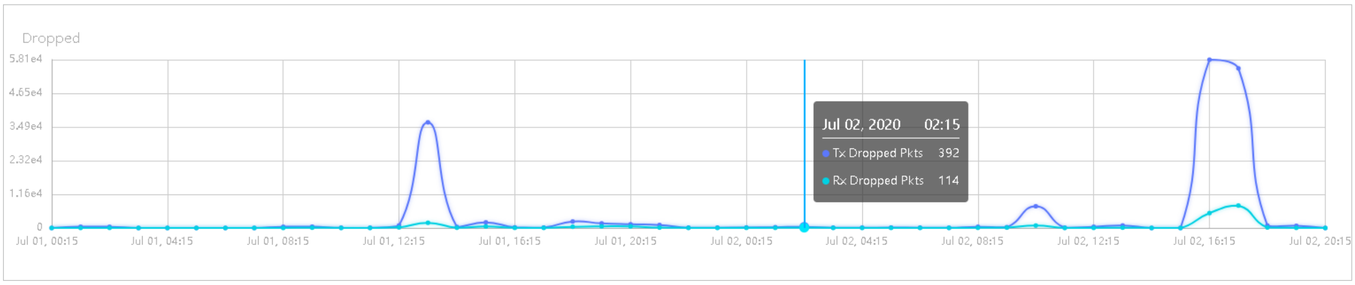
Packets

The Packets graph uses the dark blue line and light blue line to display the number of packets transmitted and received during the selected time range, respectively. Hover the cursor over the lines to display the specific values.



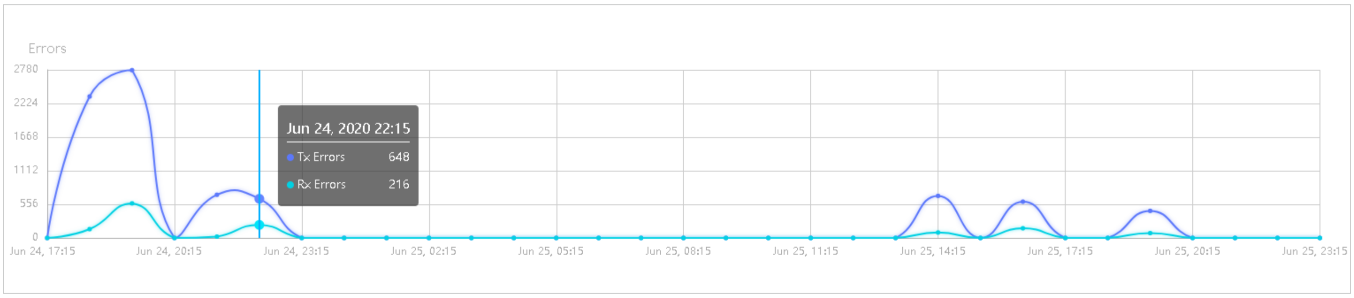
Dropped

The Dropped graph uses the dark blue line and light blue line to display the number of dropped Tx packets and Rx packets during the selected time range, respectively. Hover the cursor over the lines to display the specific values.



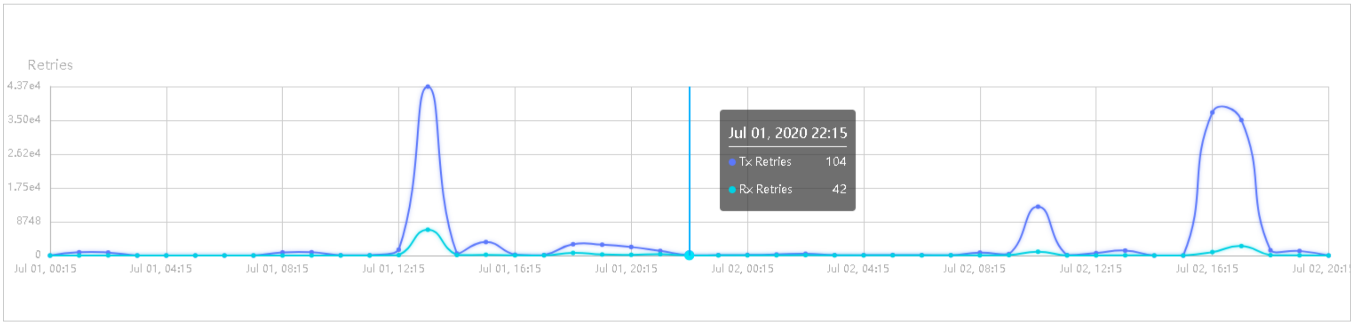
Errors

The Errors graph uses the dark blue line and light blue line to display the number of error packets sent to AP and received by AP during the selected time range, respectively. Hover the cursor over the line to display the specific values.



- **Retries**

The Retries graph uses the dark blue line and light blue line to display the number of times that the data packets are transmitted again and received again during the selected period, respectively. Hover the cursor over the lines to display the specific values.

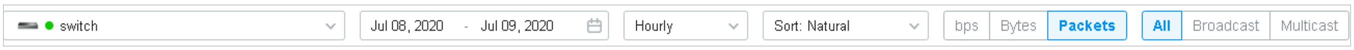


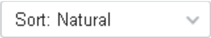
1. 2. 2 Switch Statistics

In Switch Statistics, you can view the current status of ports and their traffic statistics of the selected switch in the specified time range via a monitor panel and graphs.

Tab Bar

The tabs and calendar on the top are used to specify the displayed statistics, and the legends on the right account for elements in the graphs.

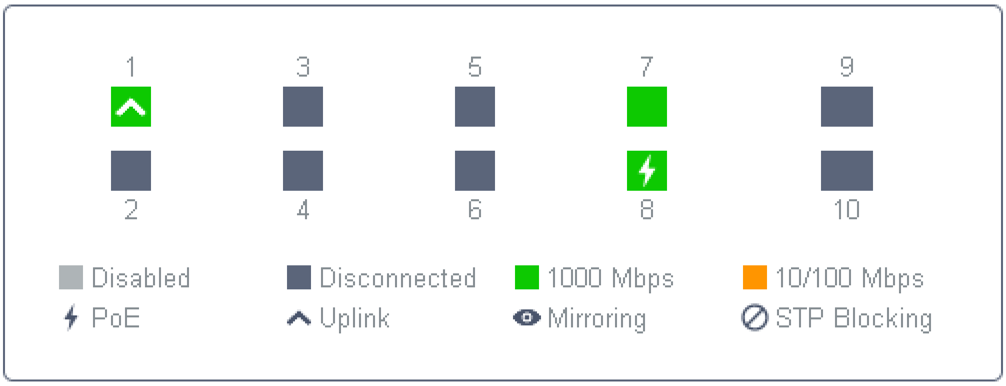


switch	Click to select a switch from the drop-down list to view its statistics.
Jul 06, 2020 - Jul 07, 2020	Click the date to display a calendar. Click a specific date twice in the calendar for the widgets to display its statistics. To display the statistic of a time range, click the start date and end date in the calendar, or directly select the time range on the right. The available time range is restricted by the time interval. Before selecting a long time range, select Hourly or Daily as the time interval.
Hourly	Select 5 minutes, Hourly, or Daily to specify the time interval of the data. When selecting a long time range, a longer time interval is recommended for a better view.
 Sort: Natural	Select Natural, Transmitted, Received, or All to specify the graph order of ports. Natural: Displays the line graphs in ascending order of the port number. Transmitted: Displays the line graphs in descending order based on the traffic volume of transmitted packets. Received: Displays the line graphs in descending order based on the traffic volume of received packets. All: Displays the line graphs in descending order based on the total traffic volume of transmitted and received packets.

	Select bps, Bytes or Packets to specify the data type and measuring unit. bps: Displays the traffic rate in bps. Bytes: Displays the traffic statistics in Bytes. Packets: Displays the total number of packets.
	If you select Packet, click the tab to specify which type of packet statistics to be displayed. All: Displays statistics of all packets, including broadcast and multicast packets. Broadcast: Displays statistics of broadcast packets only. Multicast: Displays statistics of multicast packets only.

Monitor Panel

The monitor panel below the tab bar displays the current status of the ports on the selected switch.

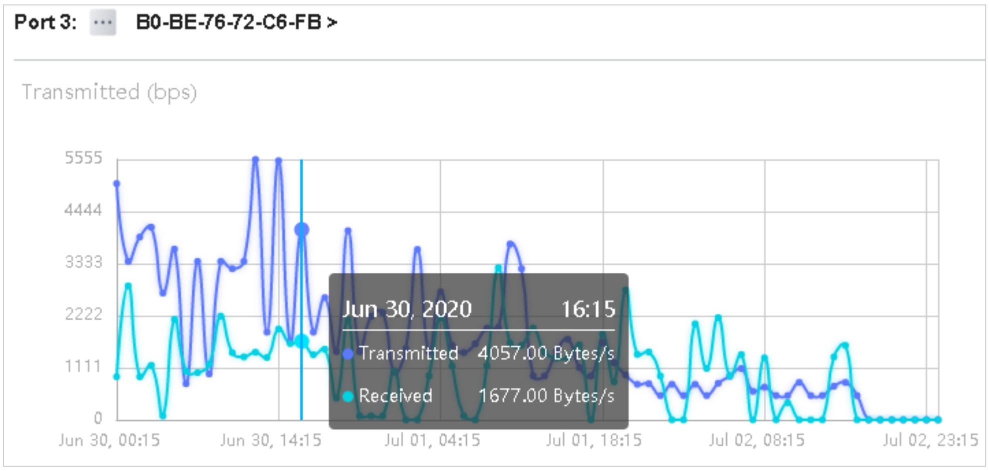


▨ Disabled	The port profile is Disable. To enable it, refer to 6. 3 Configure and Monitor Switches.
■ Disconnected	The port is enabled but connects to no devices or clients.
🟩 1000 Mbps	The port is running at 1000 Mbps.
🟧 10/100 Mbps	The port is running at 10/100 Mbps.
ϟ PoE	A PoE port connected to a powered device (PD).
^ Uplink	An uplink port connected to WAN.
👁 Mirroring	A mirroring port that is mirroring another switch port.
⊘ STP Blocking	A port in the Blocking status in Spanning Tree. It receives and sends BPDU (Bridge Protocal Data Unit) packets to maintain the spanning tree. Other packets are dropped.

Statistical Graphs

Statistical graphs below the monitor panel display the traffic statistics of active ports.

You can specify the data type and measuring unit by clicking the bps Bytes Packets tab. The dark blue and light blue are used to indicate the transmitted and received statistics, respectively. Hover the cursor over the lines to display the specific values. To view and configure the device connected to the port, click the device name beside the port number.



Port 3: ··· B0-BE-76-72-C6-FB >

Transmitted (bps)

Jun 30, 2020 16:15

Transmitted 4057.00 Bytes/s

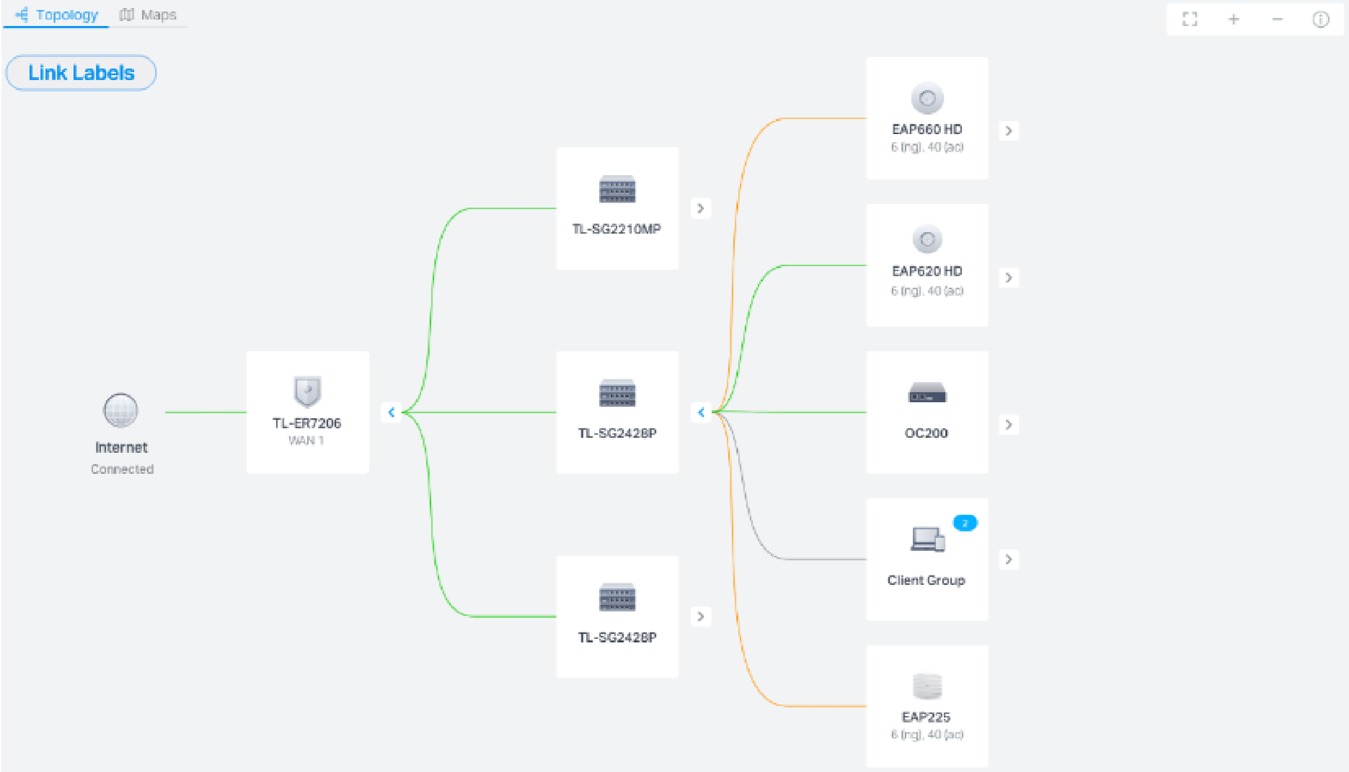
Received 1677.00 Bytes/s

1. 3 Monitor the Network with Map

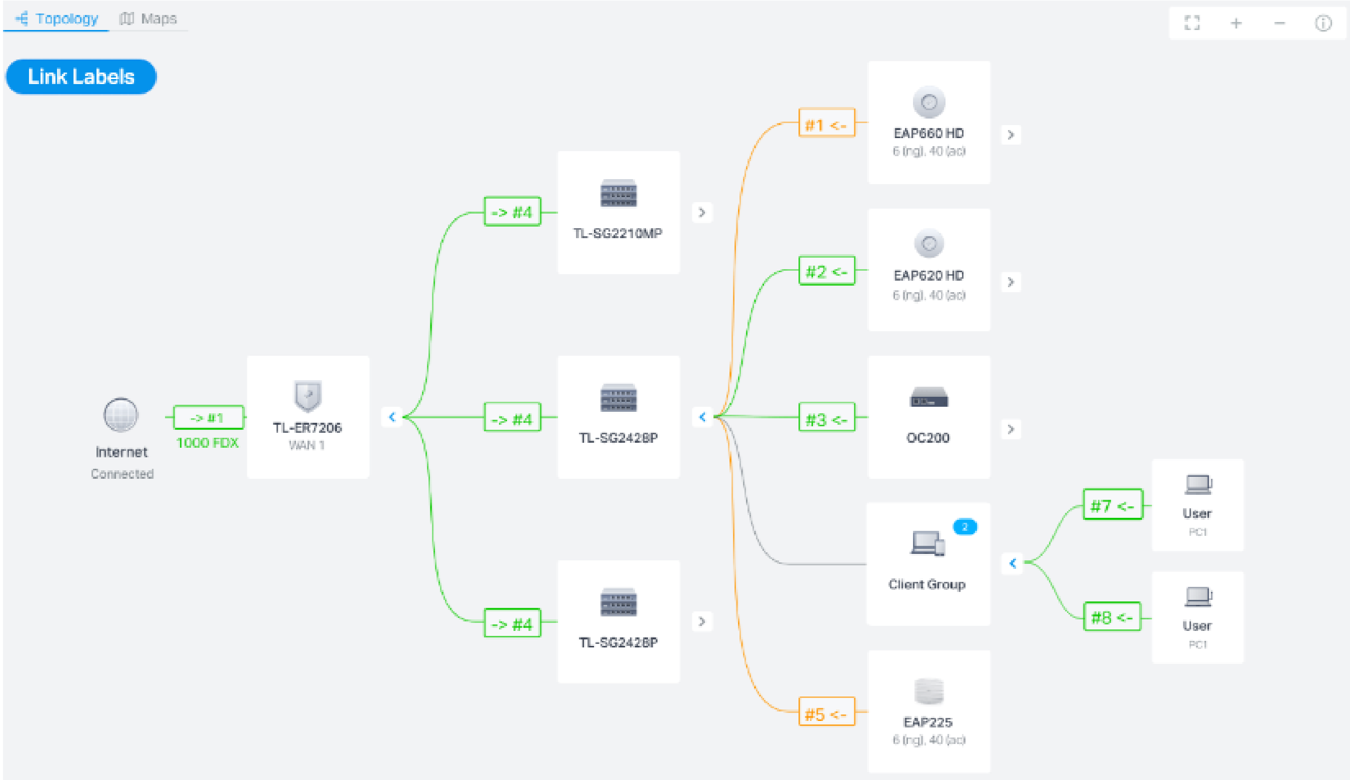
With the Map function, you can look over the topology and device provisioning of network in Topology, customizes a visual representation of your network in Heat Map, and visually display the geographic location of each device and site in Device Map and Site Map.

1. 3. 1 Topology

Go to Map > Topology, and you can view the topology generated by the controller automatically. You can click the icon of devices to open the Properties window. For detailed configuration and monitoring in the Properties window, refer to 6 Configure and Monitor Omada Managed Devices.



For a better overview of the network topology, you can control the display of branches, the size of the diagram, and the link labels.



- **Display of Branches**

  The default view shows the all devices connected by solid and dotted lines. Click the icon of the client group to view clients connected to the same device. Click the nods ⊕ to unfold or ⊖ to fold the branches.

- **Diagram Size**

  Click the icons at the right corner to adjust the size of the topology and view the legends.

⛶	Click to fit the topology to the web page.
+	Click to zoom in the topology.
−	Click to zoom out the topology.
ⓘ	Click to view the meaning of lines in the topology. Solid and dotted lines are used to indicate wired and wireless connections, respectively, and four colors are used to indicate the link speed.

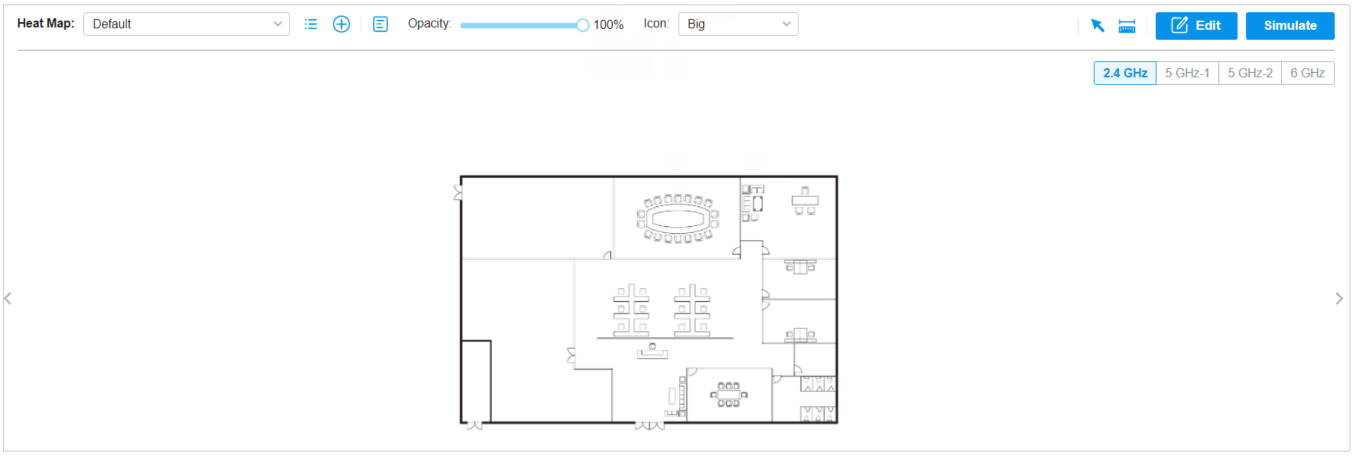
- **Link Labels**

Click Link Labels at the left corner, and labels will appear to display the link status. Information on the labels varies due to the link connections.

-> WAN1 1000 FDX	(For the WAN port of router connected to the internet) Displays the port name, link speed and duplex type.
#7 <->#8 1000 FDX	(For simple wired connections) Displays the connected port number, link speed, and duplex type. Note that only the switch's port number can be displayed in the label.
LAG1#4,5 <->LAG2#7,8 1000 FDX	(For Link Aggregation) Displays the LAG ID, port number of LAG members, LAG speed, and duplex type.
↑360Mbps ↓400Mbps 100% (-35dBm)	(For wireless connections between APs) Displays the negotiation rate of uplink and downlink and the RSSI (displayed in percentage and dBm).
48 5 GHz Free Wi-Fi	(For wireless connections between clients) Displays the connected SSID, wireless channel of AP, and its signal strength.

1. 3. 2 Heat Map

Go to Map > Heat Map, and a default map is shown as below. You can upload your local map images and add devices and different types of walls to customize a visual representation of your network.



Heat Map: Default

Opacity: 100%

Icon: Big

Click the following icons to add, edit, and select the map. After selecting a map, click and drag in the devices from the Devices list to place it on the map according to the actual locations.

Map: TP-Link	Click to select a map from the drop-down list to place the devices.

☰	Click to edit maps in the pop-up window. Click ✎ to edit the description and layout of the map. Click 🗑 to delete the map.
⊕	Click to add a map. In the pop-up window, enter the description, select the layout, and upload an image in the .jpg, .jpeg, .gif, .png, .bmp, .tiff format.
Opacity: ━━━○ 100%	Adjust the opacity of the map.
Icon: Small ⌄	Click to select the icon size displayed on the map.
↖	Click to use the selection tool to select the elements including walls and devices on the map.
📏	Click to use the measurement tool. Draw a line on the map to measure the actual distance according to the map scale.
✎ Edit	Click to edit the elements including walls and devices on the map.
Simulate	Click to simulate the network heat map. Note: It is required to click Simulate to generate a new heat map after editing elements on the map.
⛶	Click to fit the map to the web page.
+	Click to zoom in the map.
—	Click to zoom out the map.
10.73m	Click to set the map scale. Draw a line on the map by clicking and dragging, and then define the distance of the line.
⚙	Click to set the default height of the added devices and the information displayed on the map.
↗	Click to export the network coverage report.

Configuration

To generate a visual representation and heat map of your network, follow these steps:

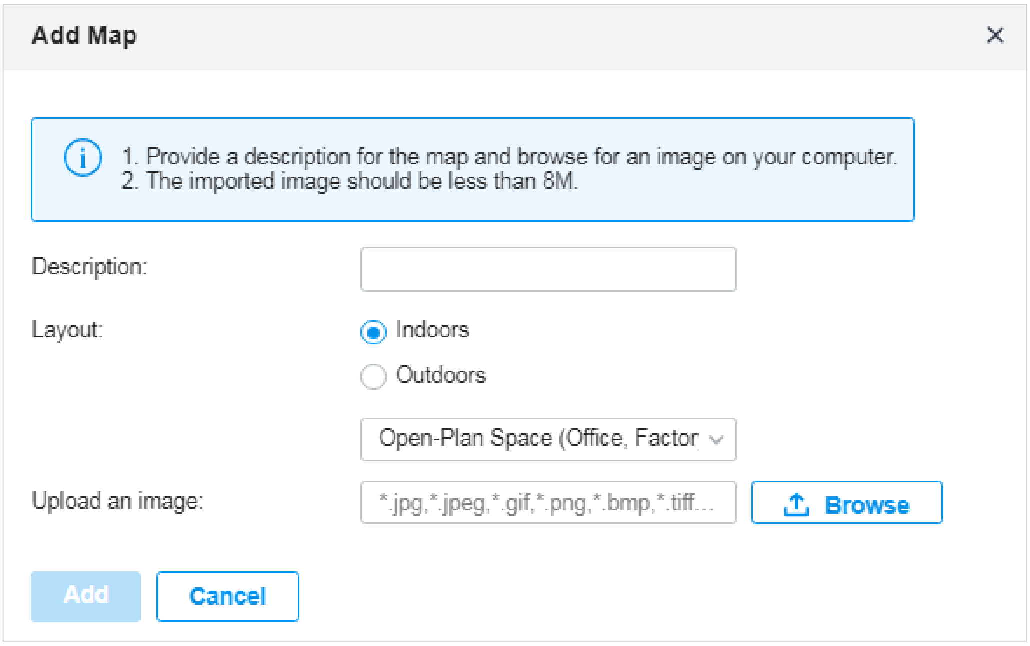
1) Add a map and configure the general parameters for the map.

2) Add devices and walls, and configure the parameters.

3) View simulation results.

Add Map > Add Devices and Walls > View and Export Results

1. Go to Map > Heat Map and click ⊕ to add a new map. Then click Add.



Add Map ×

1. Provide a description for the map and browse for an image on your computer.
2. The imported image should be less than 8M.

Description:

Layout: ● Indoors ○ Outdoors

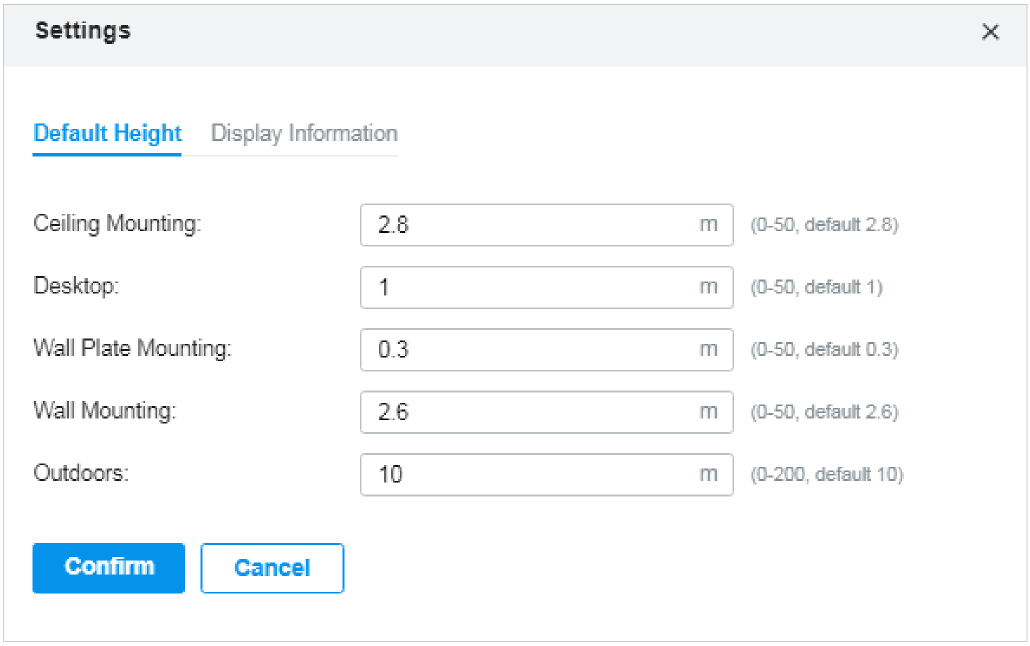
Open-Plan Space (Office, Factor

Upload an image: *.jpg,*.jpeg,*.gif,*.png,*.bmp,*.tiff... Browse

Description	Enter a description for the map.
Layout	Select the general layout of the map, which will make the simulation more accurate.
Upload an image	Upload the map in the .jpg, .jpeg, .gif, .png, .bmp, .tiff, .dxf format.

2. Click 10.73m on the upper right to set a map scale. Draw a line on the map by clicking and dragging, and then define the distance of the line.

3. Click ⚙ to set the default height of the added devices and the information displayed on the map. Then click Confirm.



Settings

Default Height | Display Information

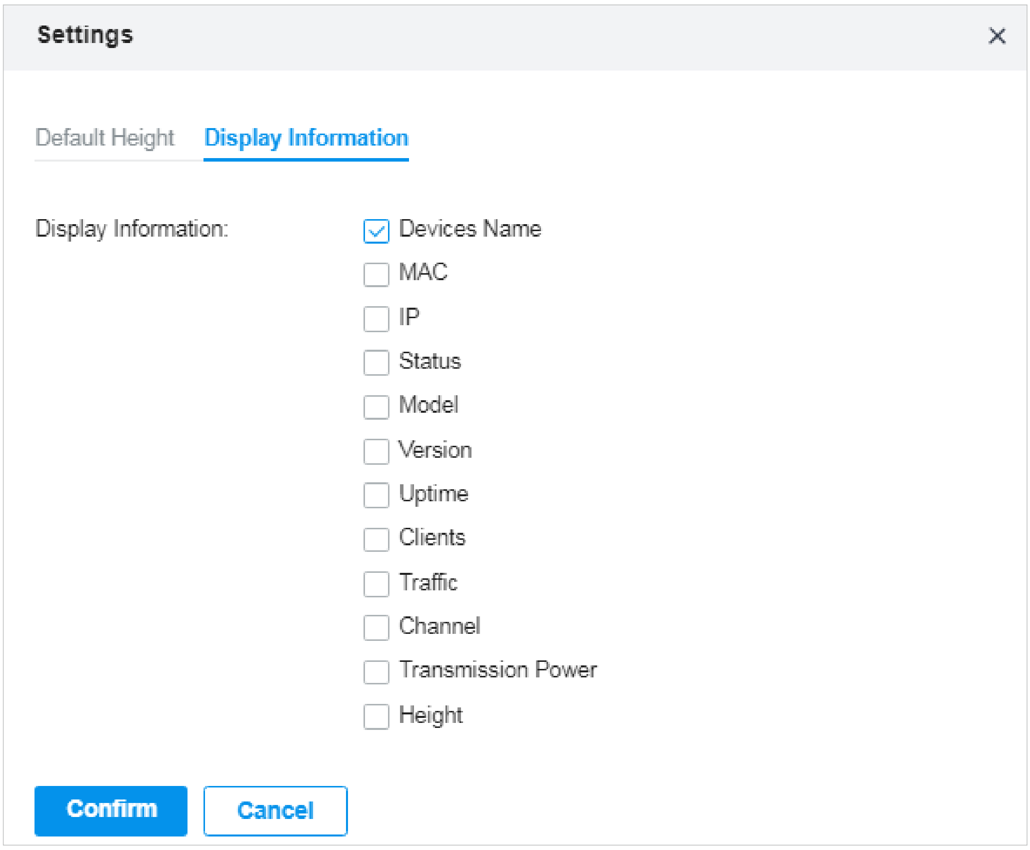
Ceiling Mounting: 2.8 m (0-50, default 2.8)

Desktop: 1 m (0-50, default 1)

Wall Plate Mounting: 0.3 m (0-50, default 0.3)

Wall Mounting: 2.6 m (0-50, default 2.6)

Outdoors: 10 m (0-200, default 10)



Settings

Default Height | Display Information

Display Information:

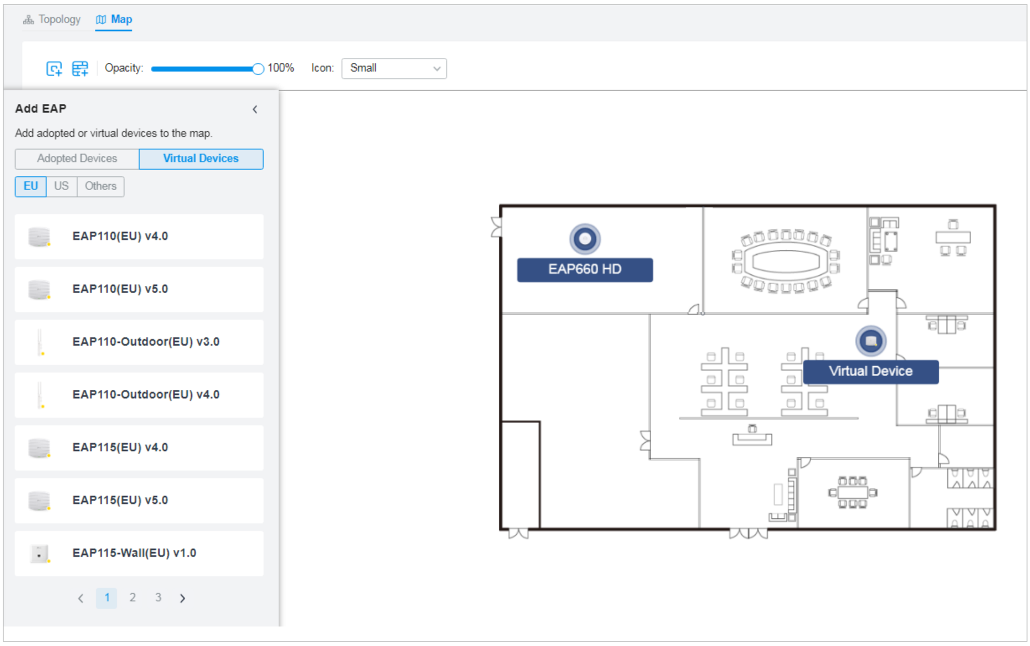
☑ Devices Name
□ MAC
□ IP
□ Status
□ Model
□ Version
□ Uptime
□ Clients
□ Traffic
□ Channel
□ Transmission Power
□ Height

Default Height	Specify the default height for devices. You can change the height for individual device later.
Display Information	Select the information you want to see on the map.

Add Map | **Add Devices and Walls** | View and Export Results

1. Click Edit to enter the editing status of the map.

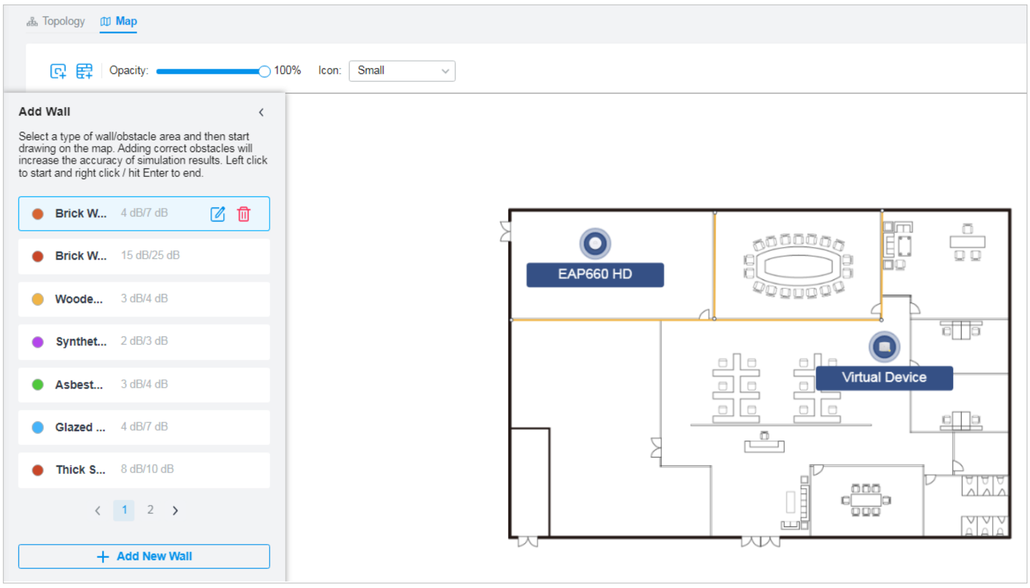
2. Click on the upper left, and the list of adopted devices and virtual devices will appear. Drag the devices to the desired place on the map.


Add EAP

Add adopted or virtual devices to the map.

3. Click on the upper left. Select a type of wall/obstacle area and then start drawing on the map. Left click to start and right click / hit Enter to end.

You can also edit the details parameters of the walls and obstacles, delete, and add walls. Adding correct obstacles will increase the accuracy of simulation results.


Add Wall

Select a type of wall/obstacle area and then start drawing on the map. Adding correct obstacles will increase the accuracy of simulation results. Left click to start and right click / hit Enter to end.

Brick W...	4 dB/7 dB
Brick W...	15 dB/25 dB
Woode...	3 dB/4 dB
Synthet...	2 dB/3 dB
Asbest...	3 dB/4 dB
Glazed ...	4 dB/7 dB
Thick S...	8 dB/10 dB

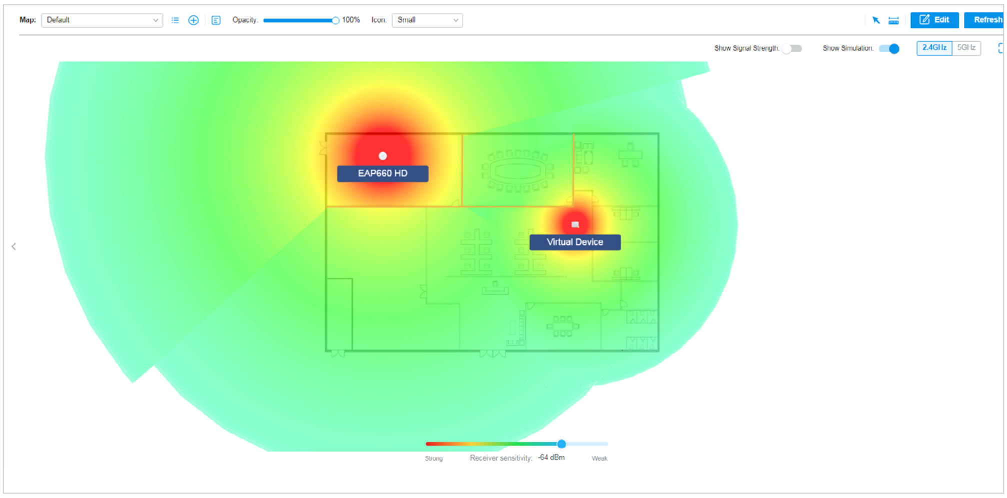
4. Click Done to exit the editing status of the map.

Add Map > Add Devices and Walls > **View and Export Results**

Note:

It is required to click Simulate to generate a new heat map after editing elements on the map.

1. Click **Simulate** to generate the heat map. You can adjust the receiver sensitivity, show signal strength, and view the simulation results according to your needs.



Show Signal Strength: ○	Enable the feature, and you can move the cursor to view the signal strength of a specific location.
Show Simulation: ●	Enable or disable the display of simulation results on the map.
2.4GHz | 5GHz	Select 2.4GHz or 5GHz to view the simulation results of the band.
⛶	Click and follow the instruction to specify an area to view the signal strength and the corresponding percentage.
Strong Receiver sensitivity: -60 dBm Weak	Adjust the receiver sensitivity, and the new settings will take effect after refreshing the simulation.

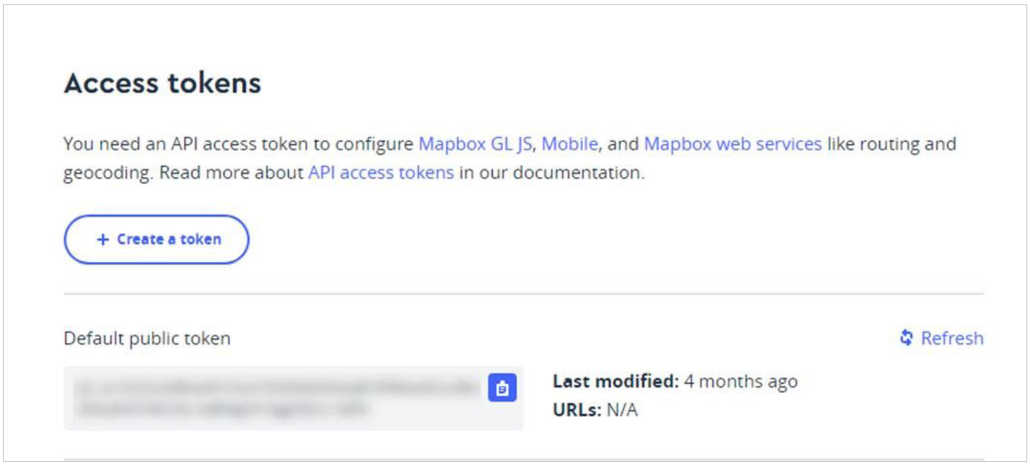
2. (Optional) If you want to export a network coverage report, click ↗ on the upper right to export a report in .docx format.

1. 3. 3 Device Map

Prerequisite

A valid Mapbox API Access Token is required to use the Device Map function.

Visit https://www.mapbox.com, register an account, and obtain the default token on the account page.



Access tokens

You need an API access token to configure Mapbox GL JS, Mobile, and Mapbox web services like routing and geocoding. Read more about API access tokens in our documentation.

Default public token

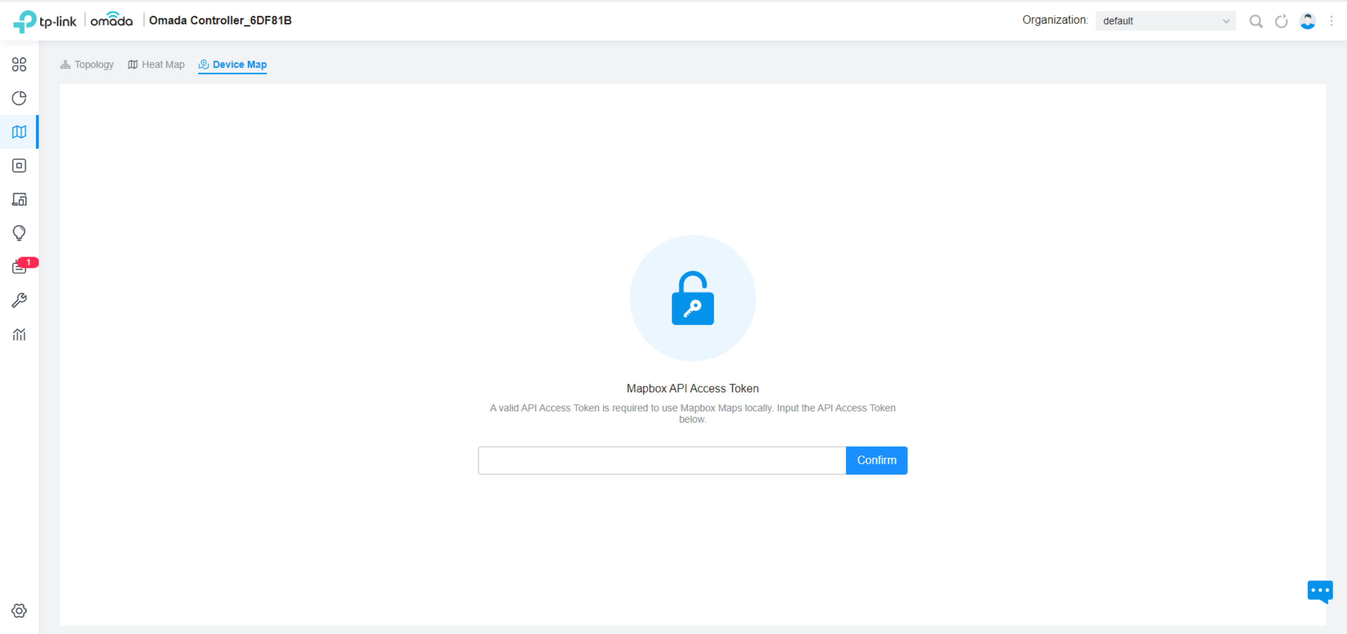
[redacted]

Last modified: 4 months ago

URLs: N/A

Configuration

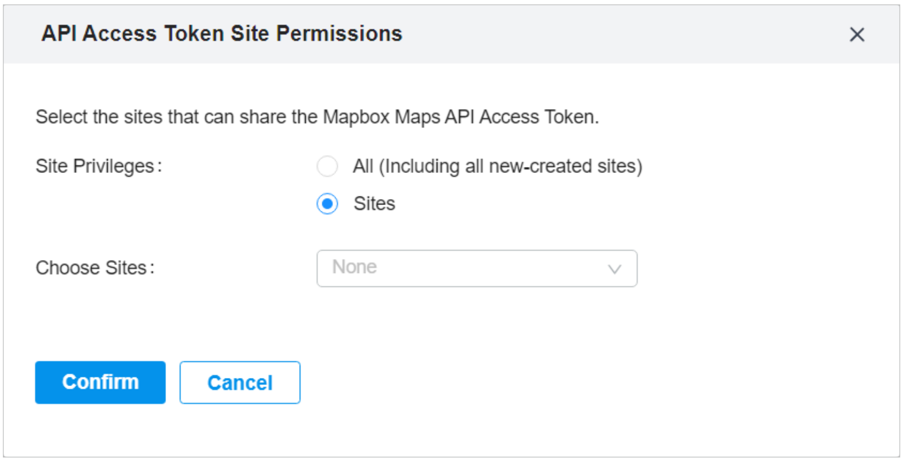
1. Select a site from the drop down list of Organization in the top-right corner. Go to Map > Device Map.
2. Enter the Mapbox API Access Token you obtained, then click Confirm.



Mapbox API Access Token

A valid API Access Token is required to use Mapbox Maps locally. Input the API Access Token below.

3. Select the sites that can share the token, then click Confirm.



API Access Token Site Permissions ✕

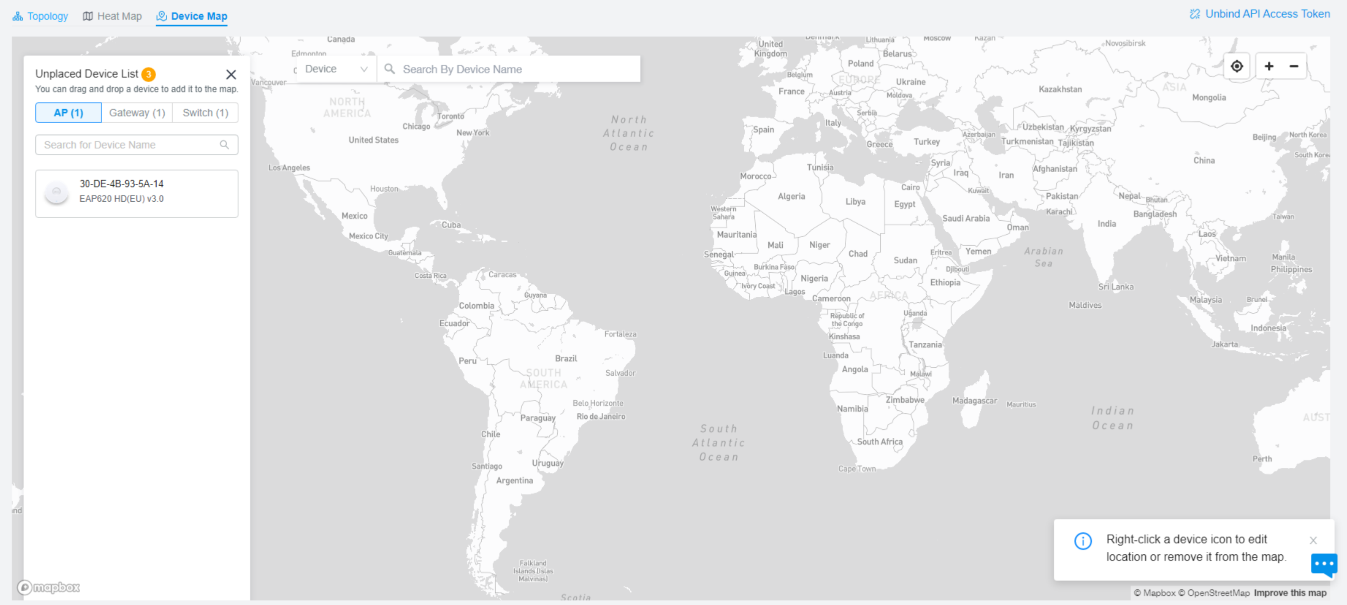
Select the sites that can share the Mapbox Maps API Access Token.

Site Privileges: ○ All (Including all new-created sites) ● Sites

Choose Sites: None

Confirm Cancel

4. Use the map to manage your devices.



Unplaced Device List 3

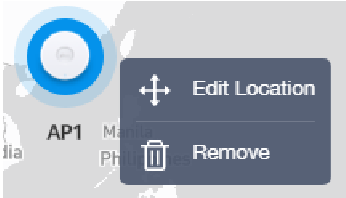
You can drag and drop a device to add it to the map.

30-DE-4B-93-5A-14
EAP620 HD(EU) v3.0

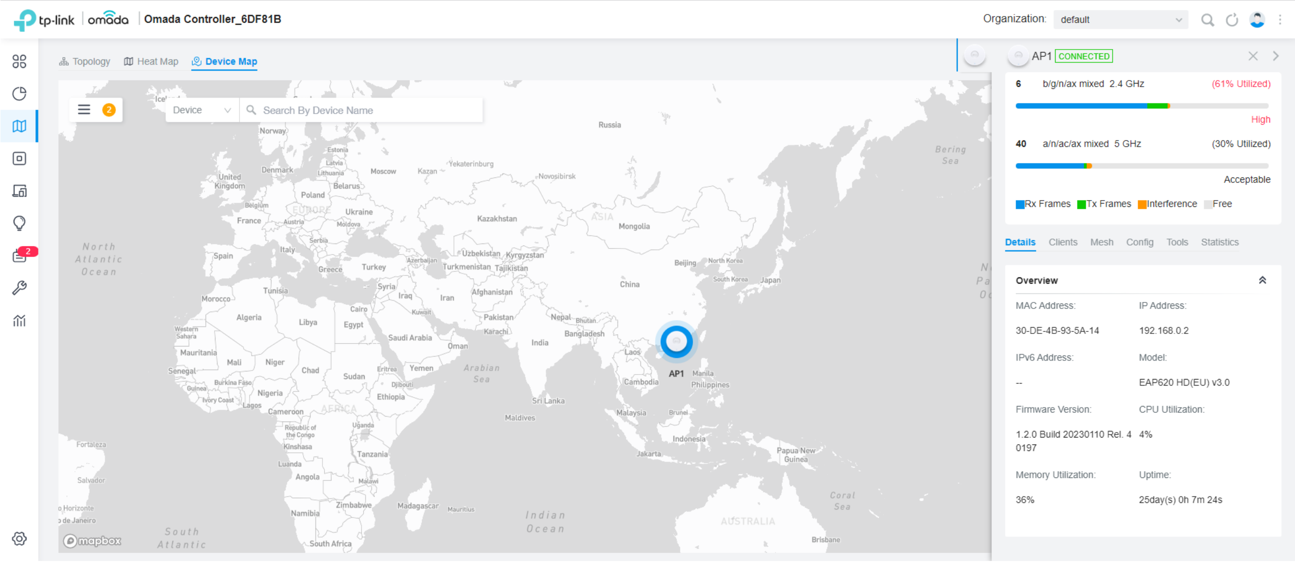
Right-click a device icon to edit location or remove it from the map.

Unplaced Device List	Display a list of sites that are not marked on the map. You can drag and drop a site to add it to the map.
Search bar	Select a catogary and enter the keyword to search for a site or address.
⊙	Locate to current location.
+ −	Zoom in and zoom out the map.

Right-click a device icon to edit location or remove it from the map.



Click a device icon to view device info and edit settings.



AP1 CONNECTED

6 b/g/n/ax mixed 2.4 GHz (61% Utilized)

High

40 a/n/ac/ax mixed 5 GHz (30% Utilized)

Acceptable

🟦Rx Frames 🟩Tx Frames 🟧Interference ▢Free

Overview

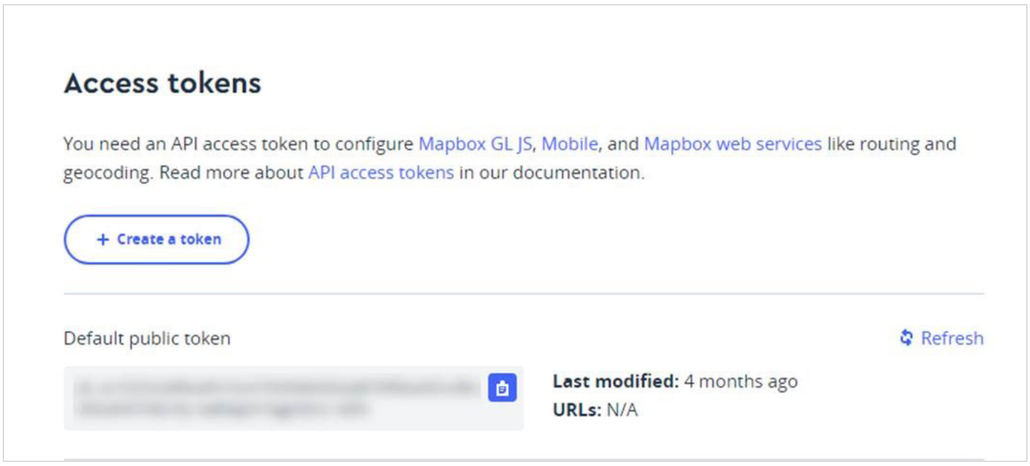
MAC Address:	IP Address:
30-DE-4B-93-5A-14	192.168.0.2
IPv6 Address:	Model:
--	EAP620 HD(EU) v3.0
Firmware Version:	CPU Utilization:
1.2.0 Build 20230110 Rel. 40197	4%
Memory Utilization:	Uptime:
36%	25day(s) 0h 7m 24s

1.3.4 Site Map

Prerequisite

A valid Mapbox API Access Token is required to use the Site Map function.

Visit https://www.mapbox.com, register an account, and obtain the default token on the account page.



Access tokens

You need an API access token to configure Mapbox GL JS, Mobile, and Mapbox web services like routing and geocoding. Read more about API access tokens in our documentation.

+ Create a token

Default public token

↻ Refresh

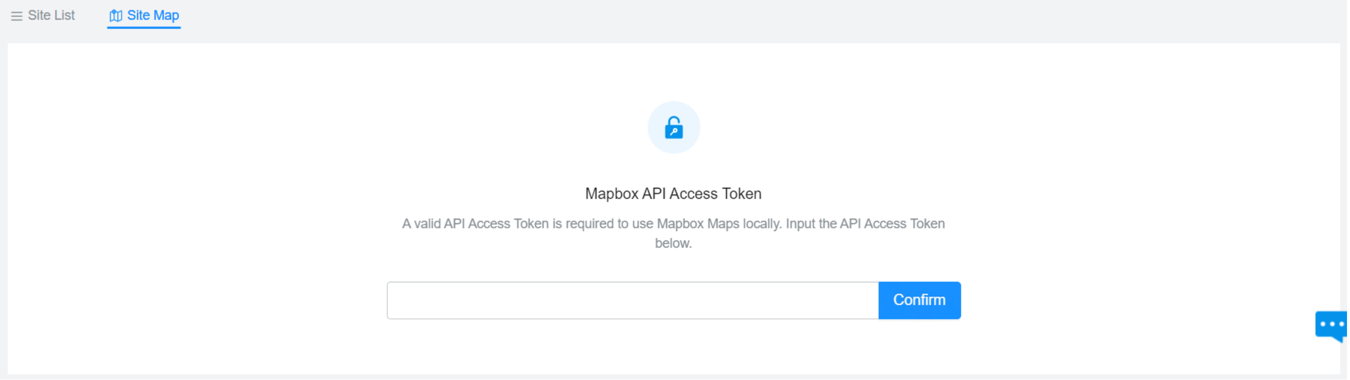
[redacted]

Last modified: 4 months ago

URLs: N/A

Configuration

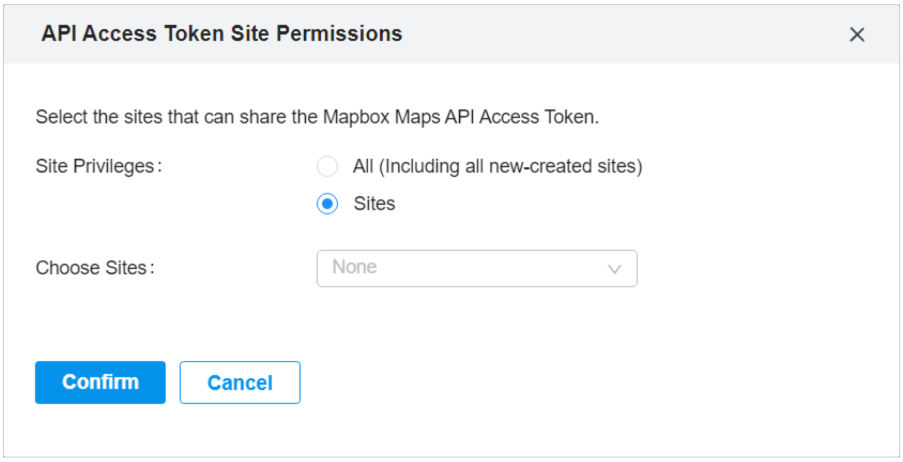
1. Select Global from the drop down list of Organization in the top-right corner. Go to Dashboard > Site Map.
2. Enter the Mapbox API Access Token you obtained, then click Confirm.



Mapbox API Access Token

A valid API Access Token is required to use Mapbox Maps locally. Input the API Access Token below.

3. Select the sites that can share the token, then click Confirm.



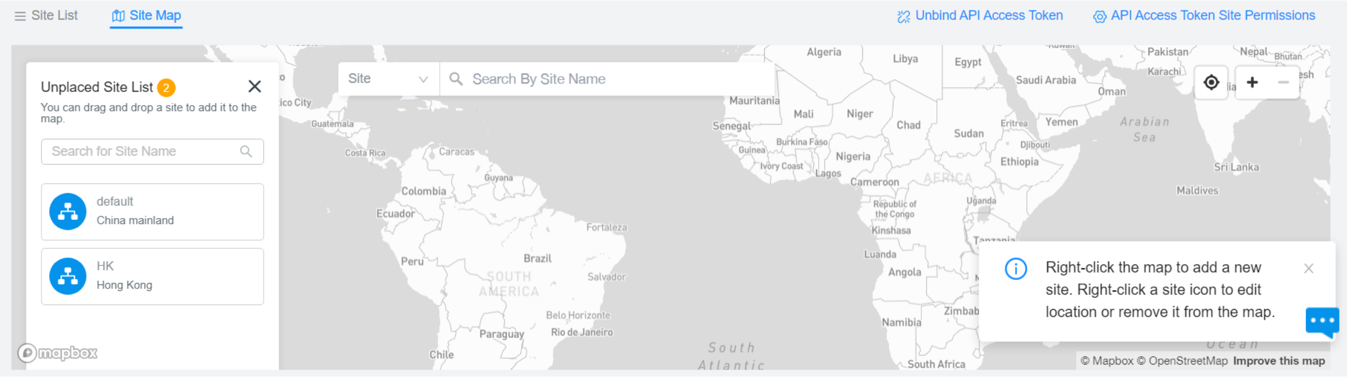
API Access Token Site Permissions

Select the sites that can share the Mapbox Maps API Access Token.

Site Privileges: ○ All (Including all new-created sites) ● Sites

Choose Sites: None

4. Use the map to manage your sites.



Unplaced Site List 2

You can drag and drop a site to add it to the map.

default
China mainland

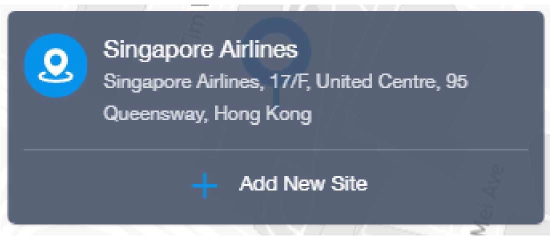
HK
Hong Kong

Right-click the map to add a new site. Right-click a site icon to edit location or remove it from the map.

Unplaced Site List	Display a list of sites that are not marked on the map. You can drag and drop a site to add it to the map.
Search bar	Select a catogary and enter the keyword to search for a site or address.

⊙	Locate to current location.
+ −	Zoom in and zoom out the map.

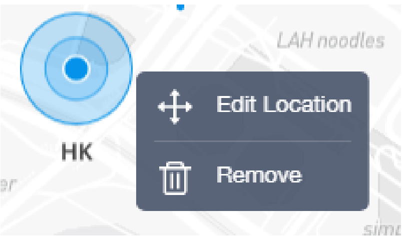
Right-click the map to add a new site.



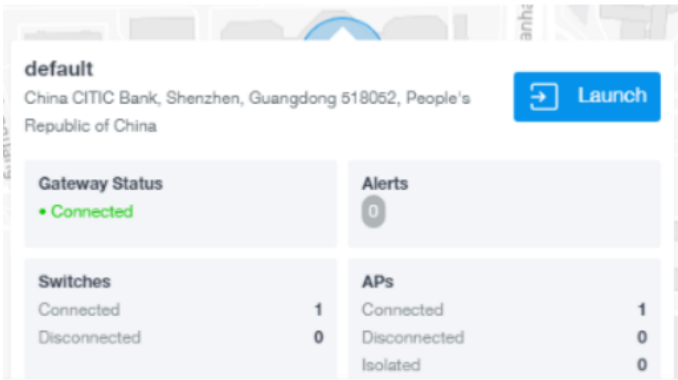
Singapore Airlines

Singapore Airlines, 17/F, United Centre, 95 Queensway, Hong Kong

Right-click a site icon to edit location or remove it from the map.



Click a site to view site info, and click Launch to access the site.



default

China CITIC Bank, Shenzhen, Guangdong 518052, People's Republic of China

Gateway Status
• Connected

Alerts
0

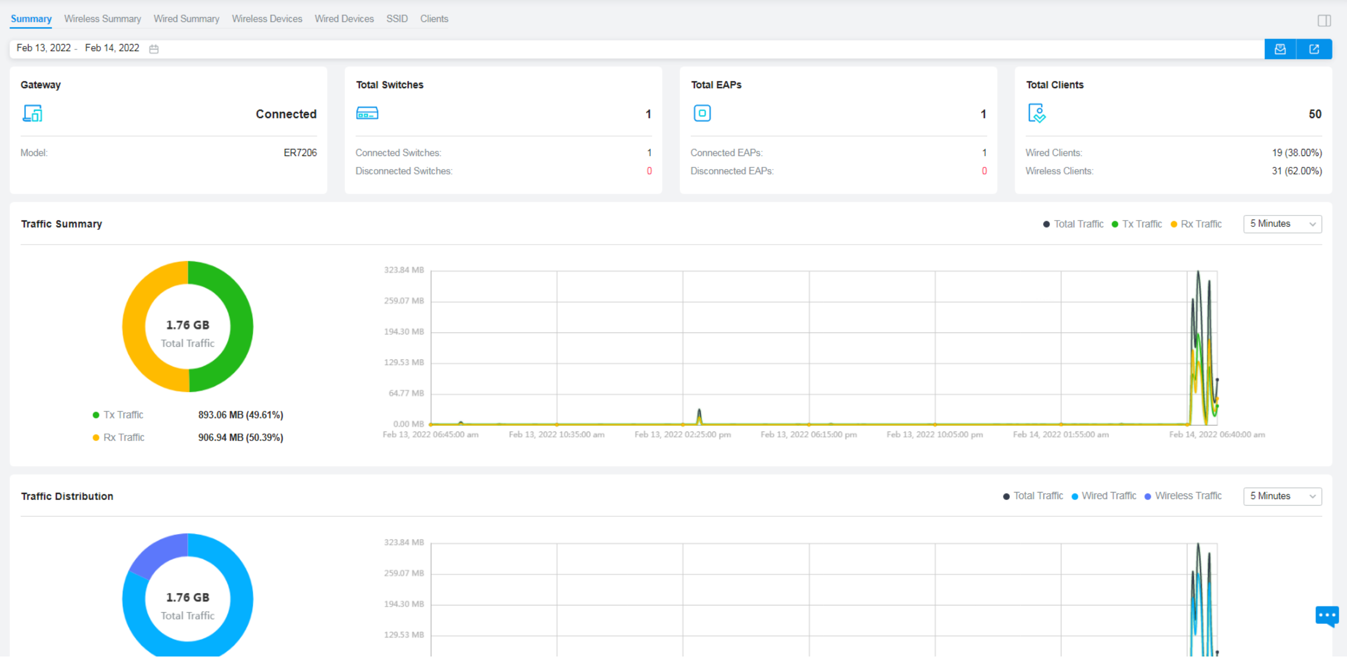
Switches
Connected 1
Disconnected 0

APs
Connected 1
Disconnected 0
Isolated 0

1. 4 Monitor the Network with Reports

Network Report shows the statistics of various network indicators and their changes over time, helping network administrators to intuitively and comprehensively understand the current and historical operating status of their network. Thus, it facilitates network administrators to decide whether the controller and devices needs to be upgraded and optimized. It also provides network administrators and SI with data support for reporting network conditions.

Go to Reports, and you can view the connection data of the devices in the topology and the statistics of various network indicators and their changes over time. Click the tabs on the top to view the statistics of specific section of the network.



Gateway: Connected
Model: ER7206

Total Switches: 1
Connected Switches: 1
Disconnected Switches: 0

Total EAPs: 1
Connected EAPs: 1
Disconnected EAPs: 0

Total Clients: 50
Wired Clients: 19 (38.00%)
Wireless Clients: 31 (62.00%)

Tx Traffic 893.06 MB (49.61%)
Rx Traffic 906.94 MB (50.39%)

Summary	Display the statistics summary of the whole network.
Wireless Summary	Display the wireless statistics summary of the whole network, including data related to APs, wireless clients, and wireless traffic.
Wired Summary	Display the wired statistics summary of the whole network, including data related to gateway, switches, wired clients, and wired traffic.
Wireless Devices	Display details of APs in the network, including AP Traffic, CPU Utilization, Memory Utilization, Total Clients, Alerts, and Reboot Times.
Wired Devices	Display details of gateway and switches in the network, including Traffic, CPU Utilization, Memory Utilization, Total Clients, Alerts, and Reboot Times.
SSID	Display the statistics of SSIDs in the network, including Traffic, Total Clients, and Activities.
Clients	Display the statistics of Clients in the network, including Distribution, Client Activities, and Client Numbers.

When you are accessing the controller locally, you can export the network report or send the report via email by clicking the icons on the upper right.

✉	Click to send the report via email. Both Send Now and Send Schedule are available.
↗	Click to export and the network report locally. Note that for Linux system, please install Chromium before exporting the network report and make sure you can run Chromium as root.

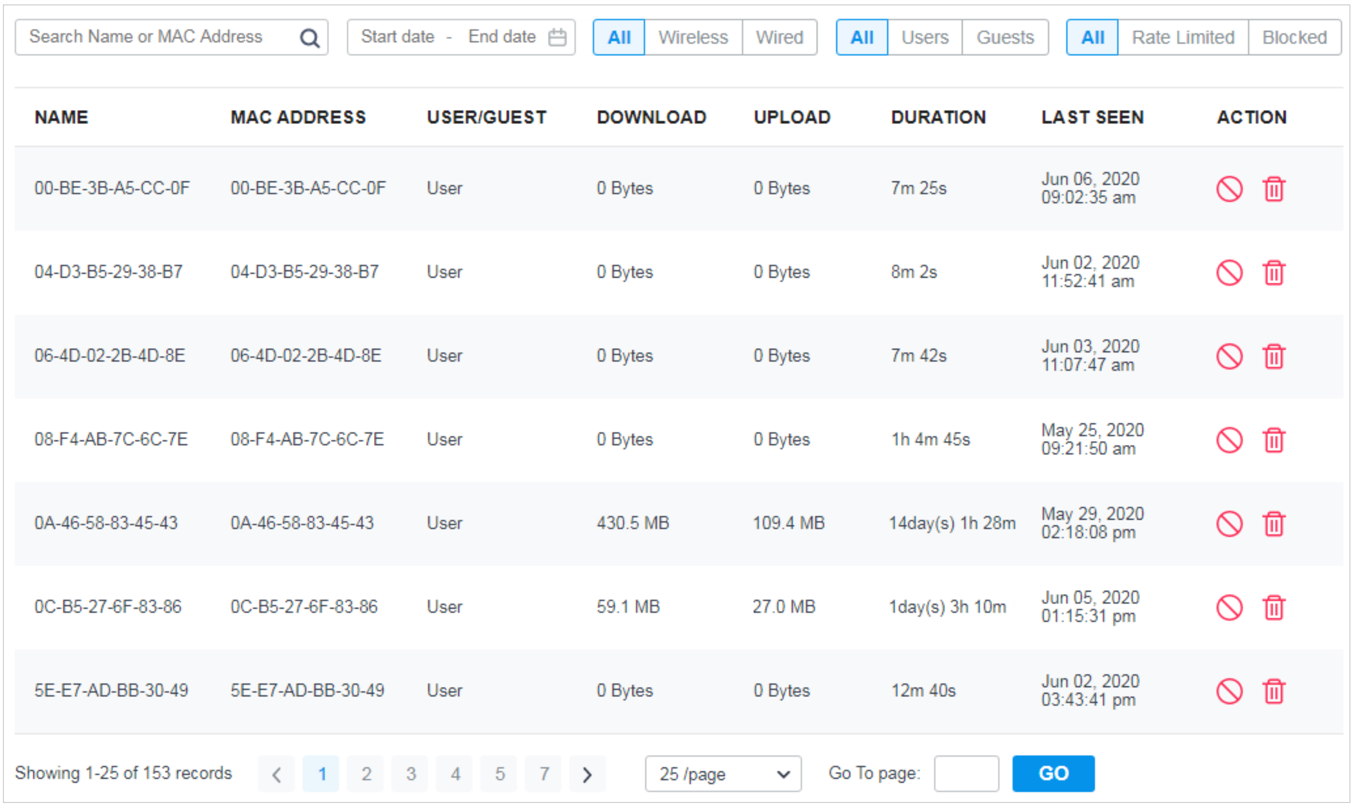
1. 5 View the Statistics During Specified Period with Insight

In the Insight page, you can monitor the site history of connected clients, portal authorizations, and rouge APs. For a better monitoring, you can specify the time period and classify the clients and APs.

1. 5. 1 Known Clients

In Known Clients, a table lists all clients that connected to the network before in the site.

In the table, you can view the client's basic information, role and connection statistics, including download and upload traffics, connection duration, and the last time it connected to the network.

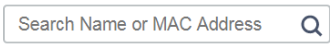
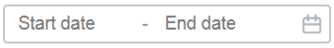


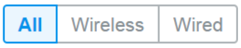
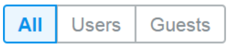
Search Name or MAC Address | Start date - End date | All | Wireless | Wired | All | Users | Guests | All | Rate Limited | Blocked

NAME	MAC ADDRESS	USER/GUEST	DOWNLOAD	UPLOAD	DURATION	LAST SEEN	ACTION
00-BE-3B-A5-CC-0F	00-BE-3B-A5-CC-0F	User	0 Bytes	0 Bytes	7m 25s	Jun 06, 2020 09:02:35 am	⊘ 🗑
04-D3-B5-29-38-B7	04-D3-B5-29-38-B7	User	0 Bytes	0 Bytes	8m 2s	Jun 02, 2020 11:52:41 am	⊘ 🗑
06-4D-02-2B-4D-8E	06-4D-02-2B-4D-8E	User	0 Bytes	0 Bytes	7m 42s	Jun 03, 2020 11:07:47 am	⊘ 🗑
08-F4-AB-7C-6C-7E	08-F4-AB-7C-6C-7E	User	0 Bytes	0 Bytes	1h 4m 45s	May 25, 2020 09:21:50 am	⊘ 🗑
0A-46-58-83-45-43	0A-46-58-83-45-43	User	430.5 MB	109.4 MB	14day(s) 1h 28m	May 29, 2020 02:18:08 pm	⊘ 🗑
0C-B5-27-6F-83-86	0C-B5-27-6F-83-86	User	59.1 MB	27.0 MB	1day(s) 3h 10m	Jun 05, 2020 01:15:31 pm	⊘ 🗑
5E-E7-AD-BB-30-49	5E-E7-AD-BB-30-49	User	0 Bytes	0 Bytes	12m 40s	Jun 02, 2020 03:43:41 pm	⊘ 🗑

Showing 1-25 of 153 records < 1 2 3 4 5 7 > 25 /page Go To page: GO

A search bar, a time selector and three tabs are above the table for searching and filtering.

 Search Name or MAC Address	Enter the client name or MAC address to search the clients.
 Start date - End date	Filter the clients based on Last Seen. Click the selector to open the calendar. Click a specific date twice in the calendar to display the records on the day. To display the records of a time range, click the start date and end date in the calendar.

  	Click the tabs to filter the clients listed in the table. The three tabs can take effect simultaneously. All/Wireless/Wired: Click All to display both wireless and wired clients. Click Wireless or Wired to display wireless or wired clients only. All/Users/Guests: Click All to display both users and guests. Click Users or Gusets to display users or guests only. Guests are users connected to the wireless guest network. To configure guest network, refer to 4. 4 Configure Wireless Networks. All/Rate Limited/Blocked: Click All to display both rate limited and blocked clients. Click Rate Limited or Blocked to display rate limited or blocked clients only. To configure Rate Limit, refer to 4. 8. 3 Rate Limit. To block the clients, click the 🚫 icon in the table.

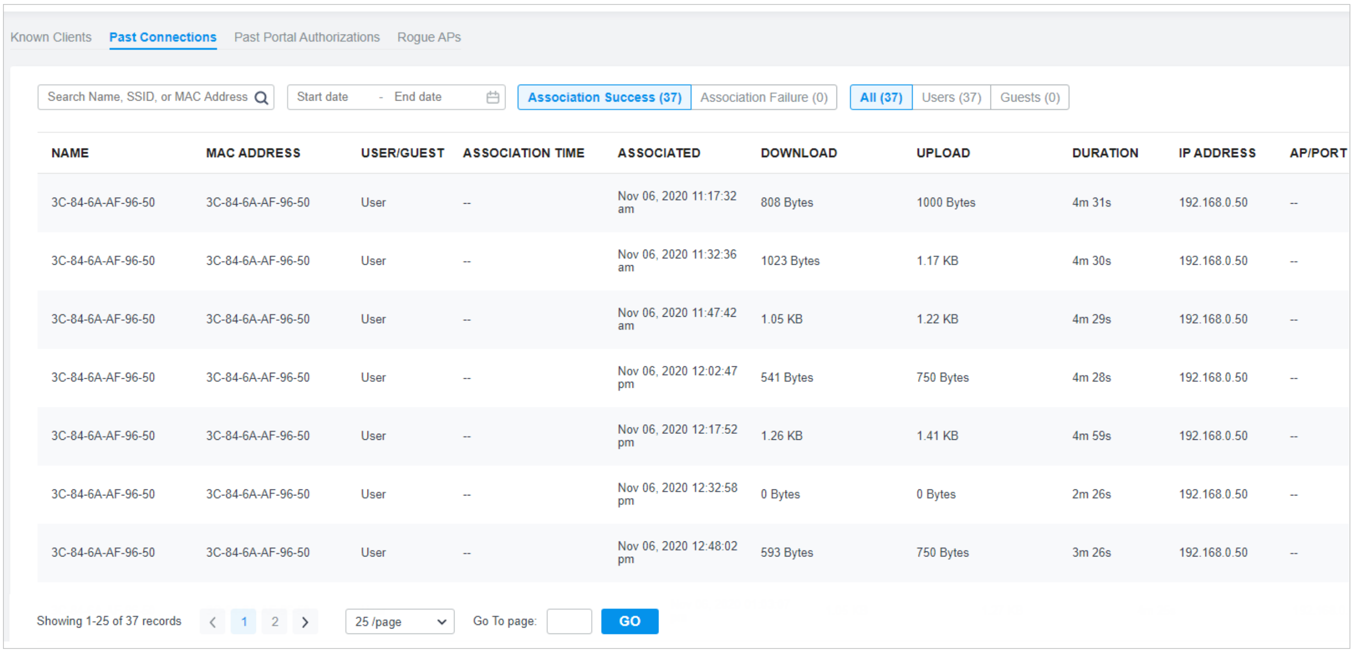
You can also take actions to block or forget the client. For detailed monitor and management, click the entry in the table to open the Properties window of the client. For more details, refer to 7. 1. 2 Using the Clients Table to Monitor and Manage the Clients.

🚫	(For unblocked clients) Click to block the client in the site. Once blocked, the client is banned from connecting to the network in the site.
🔗	(For blocked clients) Click to unblock the client in the site.
🗑	Click to forget the client. Once forget, all statistics and history of the client in the site are dropped.

1. 5. 2 Past Connections

In Past Connections, a table displays information about previous client connection sessions.

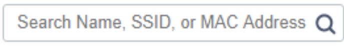
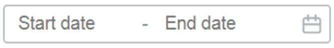
In the table, you can view the client's name, MAC address, association time and duration, download and upload traffic, IP address, and the network/port it connected to.



NAME	MAC ADDRESS	USER/GUEST	ASSOCIATION TIME	ASSOCIATED	DOWNLOAD	UPLOAD	DURATION	IP ADDRESS	AP/PORT
3C-84-6A-AF-96-50	3C-84-6A-AF-96-50	User	--	Nov 06, 2020 11:17:32 am	808 Bytes	1000 Bytes	4m 31s	192.168.0.50	--
3C-84-6A-AF-96-50	3C-84-6A-AF-96-50	User	--	Nov 06, 2020 11:32:36 am	1023 Bytes	1.17 KB	4m 30s	192.168.0.50	--
3C-84-6A-AF-96-50	3C-84-6A-AF-96-50	User	--	Nov 06, 2020 11:47:42 am	1.05 KB	1.22 KB	4m 29s	192.168.0.50	--
3C-84-6A-AF-96-50	3C-84-6A-AF-96-50	User	--	Nov 06, 2020 12:02:47 pm	541 Bytes	750 Bytes	4m 28s	192.168.0.50	--
3C-84-6A-AF-96-50	3C-84-6A-AF-96-50	User	--	Nov 06, 2020 12:17:52 pm	1.26 KB	1.41 KB	4m 59s	192.168.0.50	--
3C-84-6A-AF-96-50	3C-84-6A-AF-96-50	User	--	Nov 06, 2020 12:32:58 pm	0 Bytes	0 Bytes	2m 26s	192.168.0.50	--
3C-84-6A-AF-96-50	3C-84-6A-AF-96-50	User	--	Nov 06, 2020 12:48:02 pm	593 Bytes	750 Bytes	3m 26s	192.168.0.50	--

Showing 1-25 of 37 records

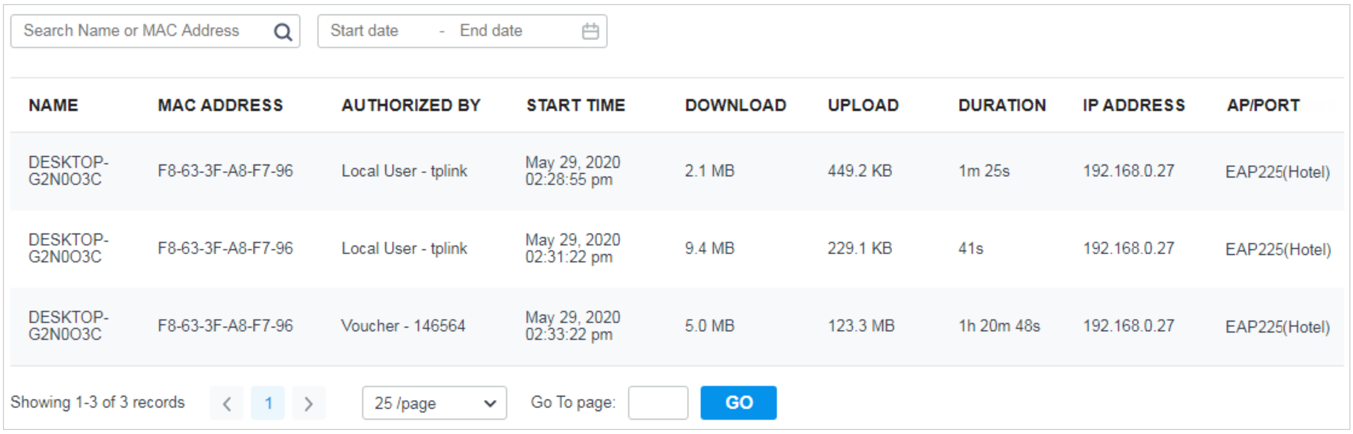
A search bar and a time selector are above the table for searching and filtering.

 Search Name, SSID, or MAC Address	Enter the client name, SSID or MAC address to search the clients.
 Start date - End date	Filter the clients based on Start Time. Click the selector to open the calendar. Click a specific date twice in the calendar to display client connection sessions on the day. To display the client connection sessions during a time range, click the start date and end date in the calendar.

1. 5. 3 Past Portal Authorizations

In Past Portal Authorization, a table lists all clients that passed the portal authorization before.

In the table, you can view the client's name, MAC address, authorization credential, uplink and downlink traffics, authorization time and duration, IP address, and the network/port it connected to. For detailed monitoring and management, refer to 7. 2 Manage Client Authentication in Hotspot Manager.



Search Name or MAC Address | Start date - End date

NAME	MAC ADDRESS	AUTHORIZED BY	START TIME	DOWNLOAD	UPLOAD	DURATION	IP ADDRESS	AP/PORT
DESKTOP-G2N0O3C	F8-63-3F-A8-F7-96	Local User - tplink	May 29, 2020 02:28:55 pm	2.1 MB	449.2 KB	1m 25s	192.168.0.27	EAP225(Hotel)
DESKTOP-G2N0O3C	F8-63-3F-A8-F7-96	Local User - tplink	May 29, 2020 02:31:22 pm	9.4 MB	229.1 KB	41s	192.168.0.27	EAP225(Hotel)
DESKTOP-G2N0O3C	F8-63-3F-A8-F7-96	Voucher - 146564	May 29, 2020 02:33:22 pm	5.0 MB	123.3 MB	1h 20m 48s	192.168.0.27	EAP225(Hotel)

Showing 1-3 of 3 records < 1 > 25 /page Go To page: GO

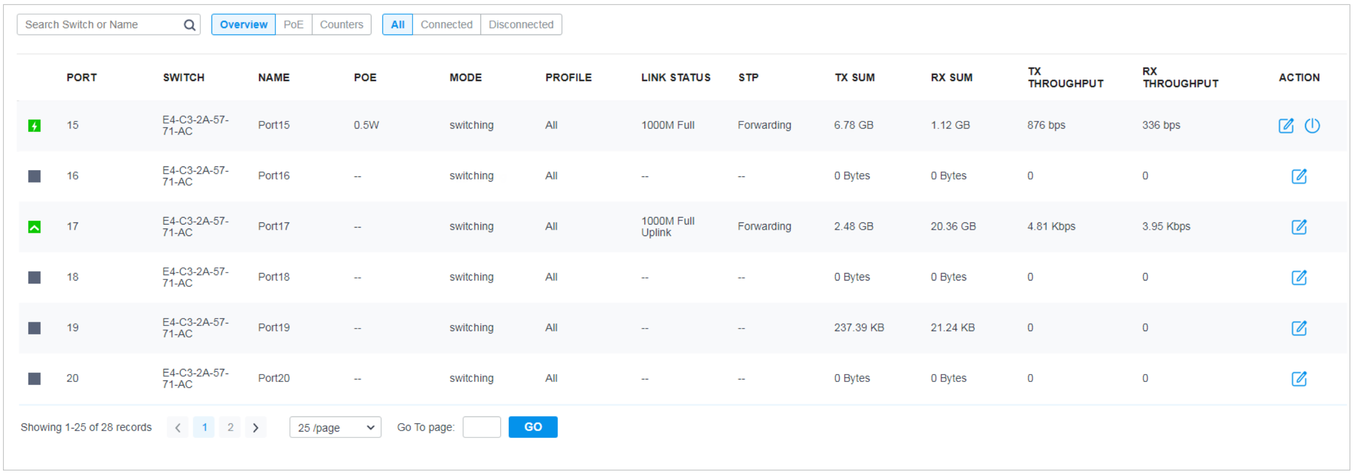
A search bar and a time selector are above the table for searching and filtering.

Search Name or MAC Address	Enter the client name or MAC address to search the clients.
Start date - End date	Filter the clients based on Start Time. Click the selector to open the calendar. Click a specific date twice in the calendar to display the clients authorized on the day. To display the clients authorized during a time range, click the start date and end date in the calendar.

1. 5. 4 Switch Status

In Switch Status, a table displays information about the status of the switches managed by the controller.

In the table, you can view the ports, PoE status, mode, and traffic activity of the switches.

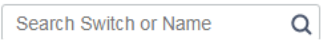
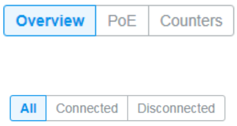


Search Switch or Name | Overview | PoE | Counters | All | Connected | Disconnected

	PORT	SWITCH	NAME	POE	MODE	PROFILE	LINK STATUS	STP	TX SUM	RX SUM	TX THROUGHPUT	RX THROUGHPUT	ACTION
⚡	15	E4-C3-2A-57-71-AC	Port15	0.5W	switching	All	1000M Full	Forwarding	6.78 GB	1.12 GB	876 bps	336 bps	✎ ⏻
■	16	E4-C3-2A-57-71-AC	Port16	--	switching	All	--	--	0 Bytes	0 Bytes	0	0	✎
▲	17	E4-C3-2A-57-71-AC	Port17	--	switching	All	1000M Full Uplink	Forwarding	2.48 GB	20.36 GB	4.81 Kbps	3.95 Kbps	✎
■	18	E4-C3-2A-57-71-AC	Port18	--	switching	All	--	--	0 Bytes	0 Bytes	0	0	✎
■	19	E4-C3-2A-57-71-AC	Port19	--	switching	All	--	--	237.39 KB	21.24 KB	0	0	✎
■	20	E4-C3-2A-57-71-AC	Port20	--	switching	All	--	--	0 Bytes	0 Bytes	0	0	✎

Showing 1-25 of 28 records < 1 2 > 25 /page Go To page: GO

A search bar and two tabs are above the table for searching and filtering. You can also click the icons in the Action column for quick operation.

	Enter the switch or name to search.
	Click the tabs to filter the switch ports listed in the table. The two tabs can take effect simultaneously. Overview/PoE/Counters: Click Overview to display the general status of each port. Click PoE to display the PoE configurations and status of each port. Click Counters to display TX and RX rates for each port. All/Connected/Disconnected: Filter the ports by their link status. Click All to display information of all ports. Click Connected or Disconnected to display all connected or disconnected ports.
✎	Click to edit the configurations of the port.
⏻	(Only for the PoE port that is connected to a PD) Click the button and the port will stop to supply power to the connected PD momentarily in order to reboot the PD.

The listed information when you select Overview on the first tab is explained as follows.

Port	Display the port number and status of the port . 🟧 10/100 Mbps: The port is running at 10/100 Mbps. 🟩 1000 Mbps: The port is running at 1000 Mbps. 🟦 2.5 Gbps: The port is running at 2.5 Gbps. 🟦 10 Gbps: The port is running at 10 Gbps. ⬜ Disabled: The port is disabled. ⬛ Disconnected: The port is enabled but connects to no devices or clients. ⚡ PoE: The PoE port is connected to a powered device (PD). ^ Uplink: The port is an uplink port connected to WAN. 👁 Mirroring: The port is a mirroring port that is mirroring another switch port. ⊘ STP Blocking: The port is in the Blocking status in Spanning Tree. It receives and sends BPDU (Bridge Protocal Data Unit) packets to maintain the spanning tree. Other packets are dropped.
Switch	Display the MAC address or the alias of the switch.
Name	Display the name of the port.
PoE	Display the PoE status of the port. --: PoE is disabled _W: Display the power output of the port in watts.

Mode	Display the operation mode of the port. Switching: The default mode. Mirroring: The network traffic of this port will receive the mirrored traffic from its mirrored port. Aggregating: The port is a part of an aggregate link
Profile	Display the switch port profile that takes effect on the port.
Link Status	Display the connection speed and duplex mode of the port.
STP	Display the Spanning Tree Protocol (STP) mode.
TX Sum	Display the amount of transmitted data.
RX Sum	Display the amount of received data.
TX Throughput	Display the transmit throughput rate.
RX Throughput	Display the receive throughput rate.

The listed information when you select PoE on the first tab is explained as follows.

Port	Display the port number and status of the port . 🟧 10/100 Mbps: The port is running at 10/100 Mbps. 🟩 1000 Mbps: The port is running at 1000 Mbps. 🟦 2.5 Gbps: The port is running at 2.5 Gbps. 🟦 10 Gbps: The port is running at 10 Gbps. ◻ Disabled: The port is disabled. ⬛ Disconnected: The port is enabled but connects to no devices or clients. ⚡ PoE: The PoE port is connected to a powered device (PD). ⌃ Uplink: The port is an uplink port connected to WAN. 👁 Mirroring: The port is a mirroring port that is mirroring another switch port. ⊘ STP Blocking: The port is in the Blocking status in Spanning Tree. It receives and sends BPDU (Bridge Protocal Data Unit) packets to maintain the spanning tree. Other packets are dropped.
Switch	Display the MAC address or the alias of the switch.
Name	Display the name of the port.

PoE	Display the PoE status of the port. --: PoE is disabled _W: Display the power output of the port in watts.
PD Class	Display the power requirement of the PD connected to the PoE port.
Power	Display the power output of the port in watts.
Voltage	Display the voltage output in volts.
Current	Display the current output in amperes.

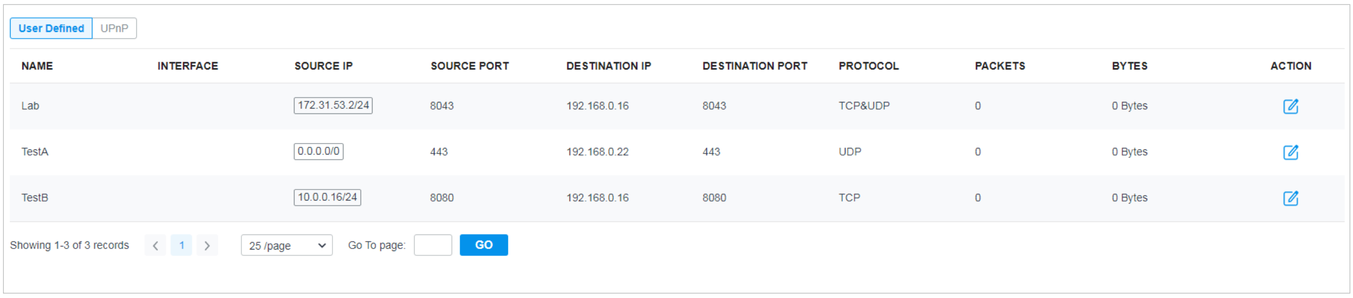
The listed information when you select Counters on the first tab is explained as follows.

Port	Display the port number and status of the port . 🟧 10/100 Mbps: The port is running at 10/100 Mbps. 🟩 1000 Mbps: The port is running at 1000 Mbps. 🟦 2.5 Gbps: The port is running at 2.5 Gbps. 🟦 10 Gbps: The port is running at 10 Gbps. ⬜ Disabled: The port is disabled. ⬛ Disconnected: The port is enabled but connects to no devices or clients. ⚡ PoE: The PoE port is connected to a powered device (PD). ^ Uplink: The port is an uplink port connected to WAN. 👁 Mirroring: The port is a mirroring port that is mirroring another switch port. ⊘ STP Blocking: The port is in the Blocking status in Spanning Tree. It receives and sends BPDU (Bridge Protocal Data Unit) packets to maintain the spanning tree. Other packets are dropped.
Switch	Display the MAC address or the alias of the switch.
TX Bytes	Display the number of transmitted bytes.
TX Frames	Display the number of transmitted frames.
TX Multicast	Display the number of transmitted multicast packets.
TX Broadcast	Display the number of transmitted broadcast packets.
TX Errors	Display the number of transmitted error packets.
RX Bytes	Display the number of received bytes.
RX Frames	Display the number of received frames.

RX Multicast	Display the number of received multicast packets.
RX Broadcast	Display the number of received broasdcast packets.
RX Errors	Display the number of received error packets.

1. 5. 5 Port Forwarding Status

In Port Forwarding Status, a table displays information about the port forwarding entries used by the gateway managed by the controller.



NAME	INTERFACE	SOURCE IP	SOURCE PORT	DESTINATION IP	DESTINATION PORT	PROTOCOL	PACKETS	BYTES	ACTION
Lab		172.31.53.2/24	8043	192.168.0.16	8043	TCP&UDP	0	0 Bytes	✎
TestA		0.0.0.0/0	443	192.168.0.22	443	UDP	0	0 Bytes	✎
TestB		10.0.0.16/24	8080	192.168.0.16	8080	TCP	0	0 Bytes	✎

Showing 1-3 of 3 records

A tab is above the table for filtering. You can also click the icons in the Action column for quick operation.

User Defined | UPnP	Click the tab to filter the port forwarding entries listed in the table. User-defined/UPnP: Click User Defined to display the port forwarding entries created by the user. Click UPnP to display the UPnP port forwarding entries.
✎	Click to edit the configurations of the port forwarding entry.

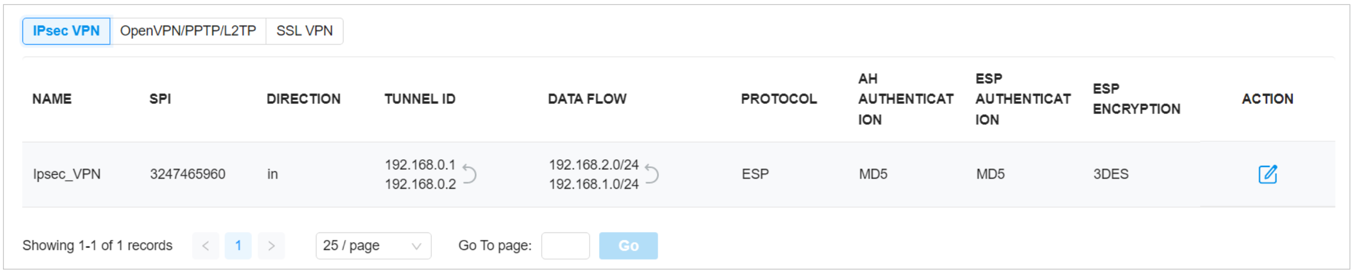
The listed information is explained as follows.

Name	Display the name of the port forwarding entry.
Interface	Display the WANs used by the port forwarding entry.
Source IP	(Only for user-defined entries) Display the source IP address. A specific IP address/Mask: The specified source IP address. 0.0.0.0/0: All IP addresses are set as the source IP address.
Source Port	The traffic through the source port, also known as internal port, will be forwarded to the LAN.
Destination IP	Display the destination IP address, and it will receive the forwarded port traffic.
Destination Port	Display the destination port, also known as internal port, that will receive the forwarded traffic.
Protocol	Display the protocol that will be forwarded.

Packets	Display the number of transferred packets.
Bytes	Display the number of transferred bytes.
Lease Duration	(Only for UPnP port forwarding) Display the uptime of the port forwarding entry.

1.5.6 VPN Status

In VPN Status, a table displays the existing VPN tunnels and corresponding information.



IPsec VPN | OpenVPN/PPTP/L2TP | SSL VPN

NAME	SPI	DIRECTION	TUNNEL ID	DATA FLOW	PROTOCOL	AH AUTHENTICATION	ESP AUTHENTICATION	ESP ENCRYPTION	ACTION
Ipsec_VPN	3247465960	in	192.168.0.1 192.168.0.2	192.168.2.0/24 192.168.1.0/24	ESP	MD5	MD5	3DES	✎

Showing 1-1 of 1 records < 1 > 25 / page Go To page: Go

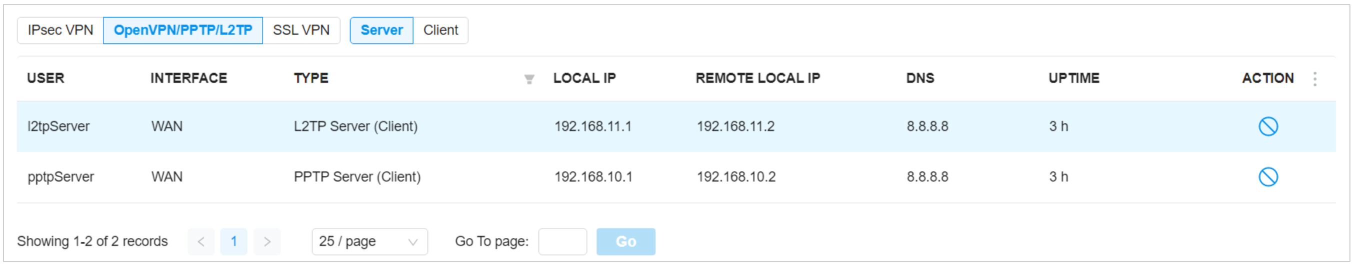
A tab is above the table for filtering. You can also click the icons for quick operation.

IPsec VPN | OpenVPN/PPTP/L2TP | SSL VPN	Click the tab to filter the routing information listed in the table. When you select OpenVPN/PPTP/L2TP, you can further choose Server or Client.
✎	Click to configure the entry.
▼	(Only for OpenVPN/PPTP/L2TP) Filter the entries.
⊘	(Only for OpenVPN/PPTP/L2TP) Click to terminate the VPN tunnel.
⋮	(Only for OpenVPN/PPTP/L2TP) Click to choose more listed information to be displayed in the table.
⊘	(Only for SSL VPN) Click to lock out the user. You can click View Locked Out Users to manage the locked out users.
⛓	(Only for SSL VPN) Click to disconnect the user.

The listed information of IPsec VPN table is explained as follows.

Name	Display the name of the IPsec VPN entry.
SPI	Display the Security Parameter Index of VPN.
Direction	Display the direction of the VPN process.
Tunnel ID	Display the local and remote IP address/name. The arrow indicates the traffic direction.

Data Flow	Display local and remote subnet. The arrow indicates the direction.
Protocol	Display the authentication and encryption protocol of the entry.
AH Authentication	Display checksum algorithms of the entry.
ESP Authentication	Display the algorithms for ESP authentication.
ESP Encryption	Display the algorithms for ESP encryption.

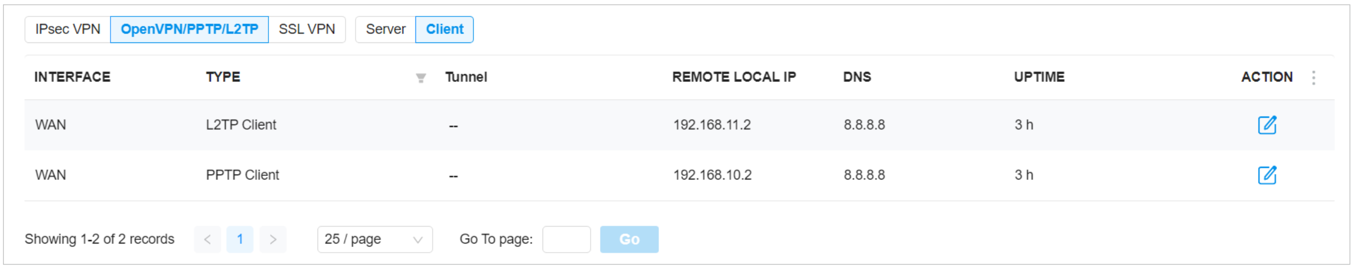


USER	INTERFACE	TYPE	LOCAL IP	REMOTE LOCAL IP	DNS	UPTIME	ACTION
l2tpServer	WAN	L2TP Server (Client)	192.168.11.1	192.168.11.2	8.8.8.8	3 h	⊘
pptpServer	WAN	PPTP Server (Client)	192.168.10.1	192.168.10.2	8.8.8.8	3 h	⊘

The listed information of OpenVPN/PPTP/L2TP (Server) table is explained as follows (some information listed below is hidden by default). You can further filter the entries based on their type.

User	Display the username of the remote user.
Interface	Display the interface that the traffic goes through.
Type	Display the connection type.
Local IP	Display the local IP address of the VPN tunnel.
Remote Local IP	Display the IP address of the remote user of the VPN tunnel.
DNS	Display the DNS address of the VPN tunnel.
Download Pkts	Display the amount of data downloaded as packets.
Download Bytes	Display the amount of data downloaded as bytes.
Upload Pkts	Display the amount of data uploaded as bytes.
Upload Bytes	Display the amount of data uploaded as bytes.

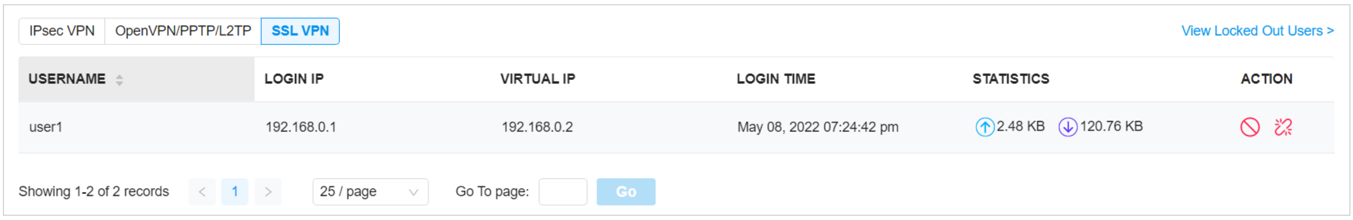
Uptime	Display the time duration that the VPN tunnel has been active.



INTERFACE	TYPE	Tunnel	REMOTE LOCAL IP	DNS	UPTIME	ACTION
WAN	L2TP Client	--	192.168.11.2	8.8.8.8	3 h	
WAN	PPTP Client	--	192.168.10.2	8.8.8.8	3 h	

The listed information of OpenVPN/PPTP/L2TP (Client) table is explained as follows (some information listed below is hidden by default). You can further filter the entries based on their type.

Interface	Display the interface that the traffic goes through.
Tunnel	Display the name of the VPN client.
Type	Display the connection type.
Remote Local IP	Display the IP address of the remote user of the VPN tunnel.
DNS	Display the DNS address of the VPN tunnel.
Download Pkts	Display the amount of data downloaded as packets.
Download Bytes	Display the amount of data downloaded as bytes.
Upload Pkts	Display the amount of data uploaded as bytes.
Upload Bytes	Display the amount of data uploaded as bytes.
Uptime	Display the time duration that the VPN tunnel has been active.



USERNAME	LOGIN IP	VIRTUAL IP	LOGIN TIME	STATISTICS	ACTION
user1	192.168.0.1	192.168.0.2	May 08, 2022 07:24:42 pm	↑2.48 KB ↓120.76 KB	

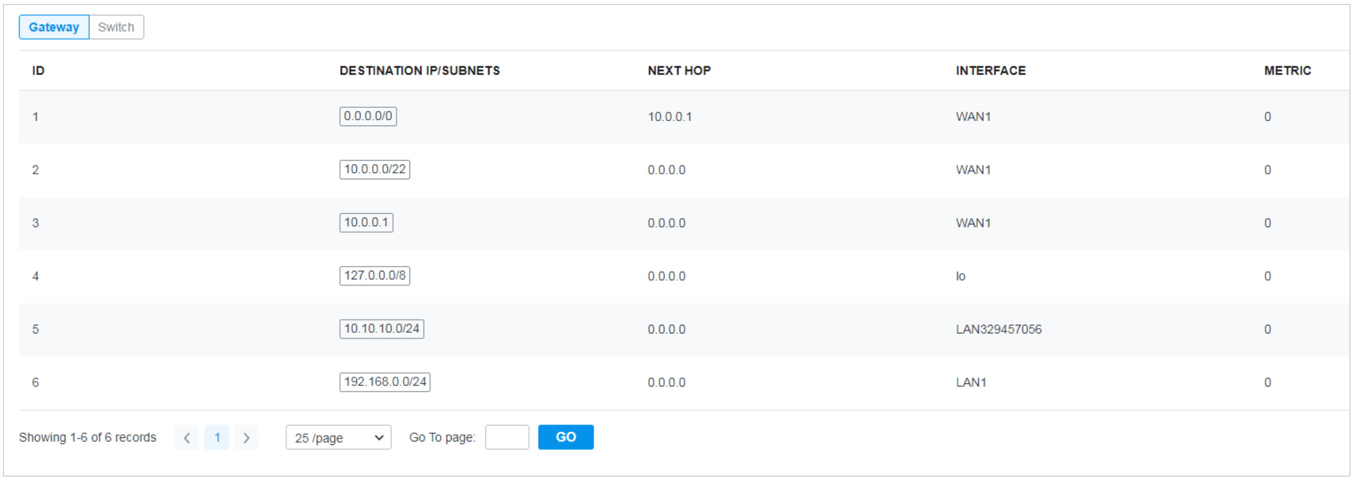
The listed information of SSL VPN table is explained as follows.

Username	Display the username of the remote user.

Login IP	Display the login IP address of the remote user.
Virtual IP	Display the virtual IP address of the remote user.
Login Time	Display the login time of the remote user.
Statistics	Display the upload and download traffic of the remote user.

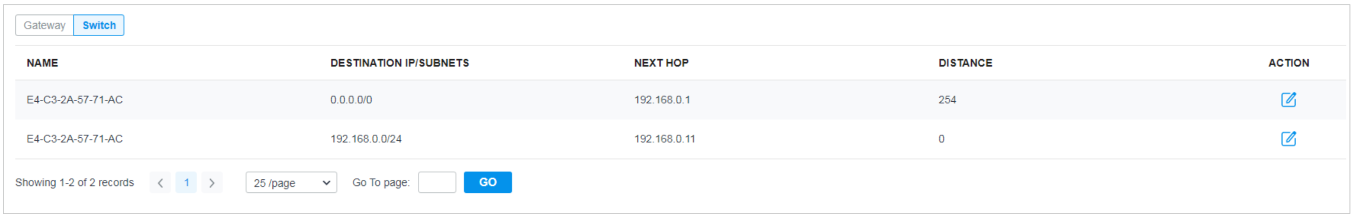
1. 5. 7 Routing Table

Routing Table displays information of routing entries that have taken effect.



ID	DESTINATION IP/SUBNETS	NEXT HOP	INTERFACE	METRIC
1	0.0.0.0/0	10.0.0.1	WAN1	0
2	10.0.0.0/22	0.0.0.0	WAN1	0
3	10.0.0.1	0.0.0.0	WAN1	0
4	127.0.0.0/8	0.0.0.0	lo	0
5	10.10.10.0/24	0.0.0.0	LAN329457056	0
6	192.168.0.0/24	0.0.0.0	LAN1	0

Showing 1-6 of 6 records



NAME	DESTINATION IP/SUBNETS	NEXT HOP	DISTANCE	ACTION
E4-C3-2A-57-71-AC	0.0.0.0/0	192.168.0.1	254	✎
E4-C3-2A-57-71-AC	192.168.0.0/24	192.168.0.11	0	✎

Showing 1-2 of 2 records

A tab is above the table for filtering. You can also click the icons in the Action column for quick operation.

Gateway Switch	Click the tab to filter the routing information listed in the table. Gateway/Switch: Click to display the routing information of the gateway or the switch.
✎	(Only for switch) Click to configure the static routes.

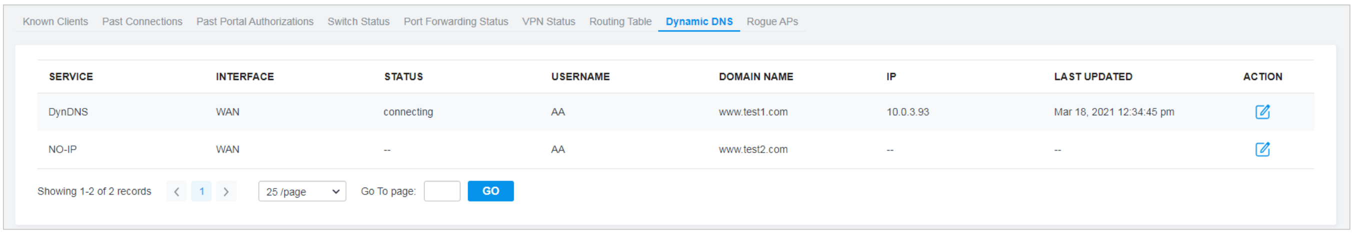
The listed information is explained as follows.

Destination IP/Subnets	Display the destination IP addresses of the routing entry..
Next Hop	Display the IP address of the next hop.
Interface	(Only for Gateway) Display the interface that the traffic of the entry goes through.

Metric	(Only for Gateway) Display the number of hops before reaching the destination. Generally, if there are a few routing entries with the same destination, the routing with the lowest metric will be used.
Distance	(Only for Switch) Display the administrative distance of the routing entry. It is used to decide the priority among routes to the same destination. Among routes to the same destination, the route with the lowest distance value will be used.

1. 5. 8 Dynamic DNS

In Dynamic DNS, a table displays information about the uses of the dynamic DNS services. You can click ✎ in the Action column to edit the entry.



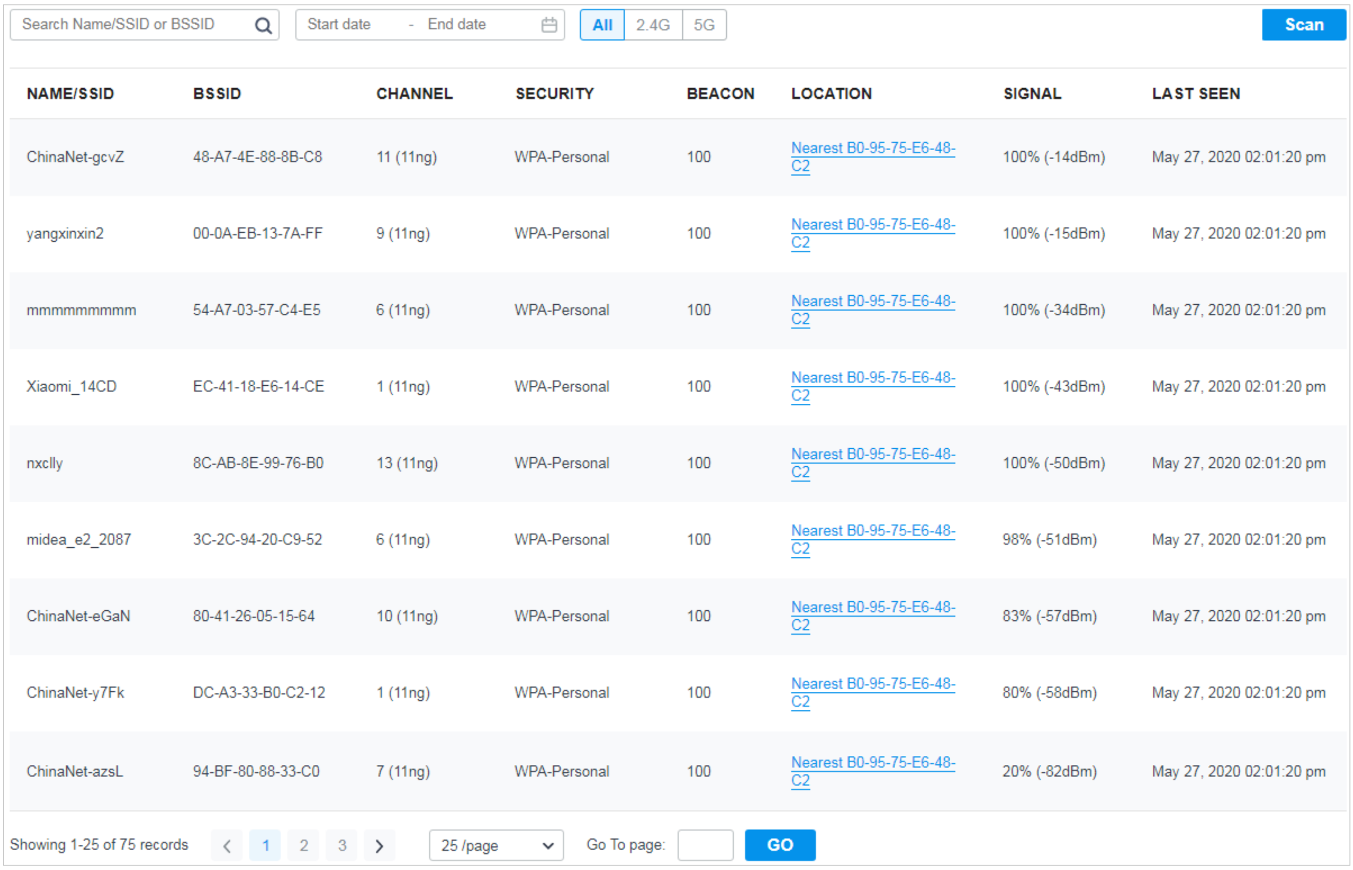
SERVICE	INTERFACE	STATUS	USERNAME	DOMAIN NAME	IP	LAST UPDATED	ACTION
DynDNS	WAN	connecting	AA	www.test1.com	10.0.3.93	Mar 18, 2021 12:34:45 pm	✎
NO-IP	WAN	--	AA	www.test2.com	--	--	✎

Showing 1-2 of 2 records < 1 > 25 /page Go To page: GO

Service	Display the name of the DDNS service.
Interface	Display the WANs used by the DDNS entry.
Status	Display the status of the latest DDNS update.
Username	Display the username of the DDNS account.
Domain Name	Display domain name registered with the DDNS service.
IP	Display the IP address of the domain name.
Last Updated	Display the time when the IP address of the domain name was last updated.

1. 5. 9 Rogue APs

A rogue AP is an access point that has been installed on a secure network without explicit authorization from a system administrator. In Rogue APs, you can scan rogue APs and view the rogue APs scanned before.



NAME/SSID	BSSID	CHANNEL	SECURITY	BEACON	LOCATION	SIGNAL	LAST SEEN
ChinaNet-gcvZ	48-A7-4E-88-8B-C8	11 (11ng)	WPA-Personal	100	Nearest B0-95-75-E6-48-C2	100% (-14dBm)	May 27, 2020 02:01:20 pm
yangxinxin2	00-0A-EB-13-7A-FF	9 (11ng)	WPA-Personal	100	Nearest B0-95-75-E6-48-C2	100% (-15dBm)	May 27, 2020 02:01:20 pm
mmmmmmmmm	54-A7-03-57-C4-E5	6 (11ng)	WPA-Personal	100	Nearest B0-95-75-E6-48-C2	100% (-34dBm)	May 27, 2020 02:01:20 pm
Xiaomi_14CD	EC-41-18-E6-14-CE	1 (11ng)	WPA-Personal	100	Nearest B0-95-75-E6-48-C2	100% (-43dBm)	May 27, 2020 02:01:20 pm
nxclly	8C-AB-8E-99-76-B0	13 (11ng)	WPA-Personal	100	Nearest B0-95-75-E6-48-C2	100% (-50dBm)	May 27, 2020 02:01:20 pm
midea_e2_2087	3C-2C-94-20-C9-52	6 (11ng)	WPA-Personal	100	Nearest B0-95-75-E6-48-C2	98% (-51dBm)	May 27, 2020 02:01:20 pm
ChinaNet-eGaN	80-41-26-05-15-64	10 (11ng)	WPA-Personal	100	Nearest B0-95-75-E6-48-C2	83% (-57dBm)	May 27, 2020 02:01:20 pm
ChinaNet-y7Fk	DC-A3-33-B0-C2-12	1 (11ng)	WPA-Personal	100	Nearest B0-95-75-E6-48-C2	80% (-58dBm)	May 27, 2020 02:01:20 pm
ChinaNet-azsL	94-BF-80-88-33-C0	7 (11ng)	WPA-Personal	100	Nearest B0-95-75-E6-48-C2	20% (-82dBm)	May 27, 2020 02:01:20 pm

Showing 1-25 of 75 records < 1 2 3 > 25 /page Go To page: GO

Search Name or MAC Address	Enter the client name or MAC address to search the clients.
Start date - End date	Filter the rogue APs based on Last Seen. Click the selector to open the calendar. Click a specific date twice in the calendar to display the rogue APs scanned on the day. To display the scanned AP during a time range, click the start date and end date in the calendar.
All 2.4G 5G	Click the tab to filter the rogue APs listed in the table based on the frequency band.
Scan	Click to scan rogue APs. It may take several minutes, and the wireless service may be influenced during scanning.
BSSID	A string with a similar form as MAC address to recognize access points.
Channel	Displays the operation channel and standard of the rogue AP.
Security	Displays the security strategy of the rogue AP.
Beacon	Displays the beacon interval of the rogue AP. Beacons are transmitted periodically by the EAP to announce the presence of a wireless network for the clients, and the interval means how often the AP send a beacon to clients.
Location	Displays the managed AP nearest to the rogue AP. You can click the nearest AP to open its Properties window.

Signal	Displays the signal strength in percentage and dBm).
Last Seen	Display the last time that the rogue AP was scanned by the controller.

1. 6 View and Manage Logs

The controller uses logs to record the activities of the system, devices, users and administrators, which provides powerful supports to monitor operations and diagnose anomalies. In the Logs page, you can conveniently monitor the logs in 8. 6. 1 Alerts and 8. 6. 2 Events, and configure their notification levels in 8. 6. 3 Notifications.

All logs can be classified from the following four aspects.

- **Occurred Hierarchies**

  Two categories in occurred hierarchies are Controller and Site, which indicate the log activities happened, respectively, at the controller level and in the certain site. Only Master Administrators can view the logs happened at the controller level.

- **Notifications**

  Two categories in notifications are Event and Alert, and you can classify the logs into them by yourself.

- **Severities**

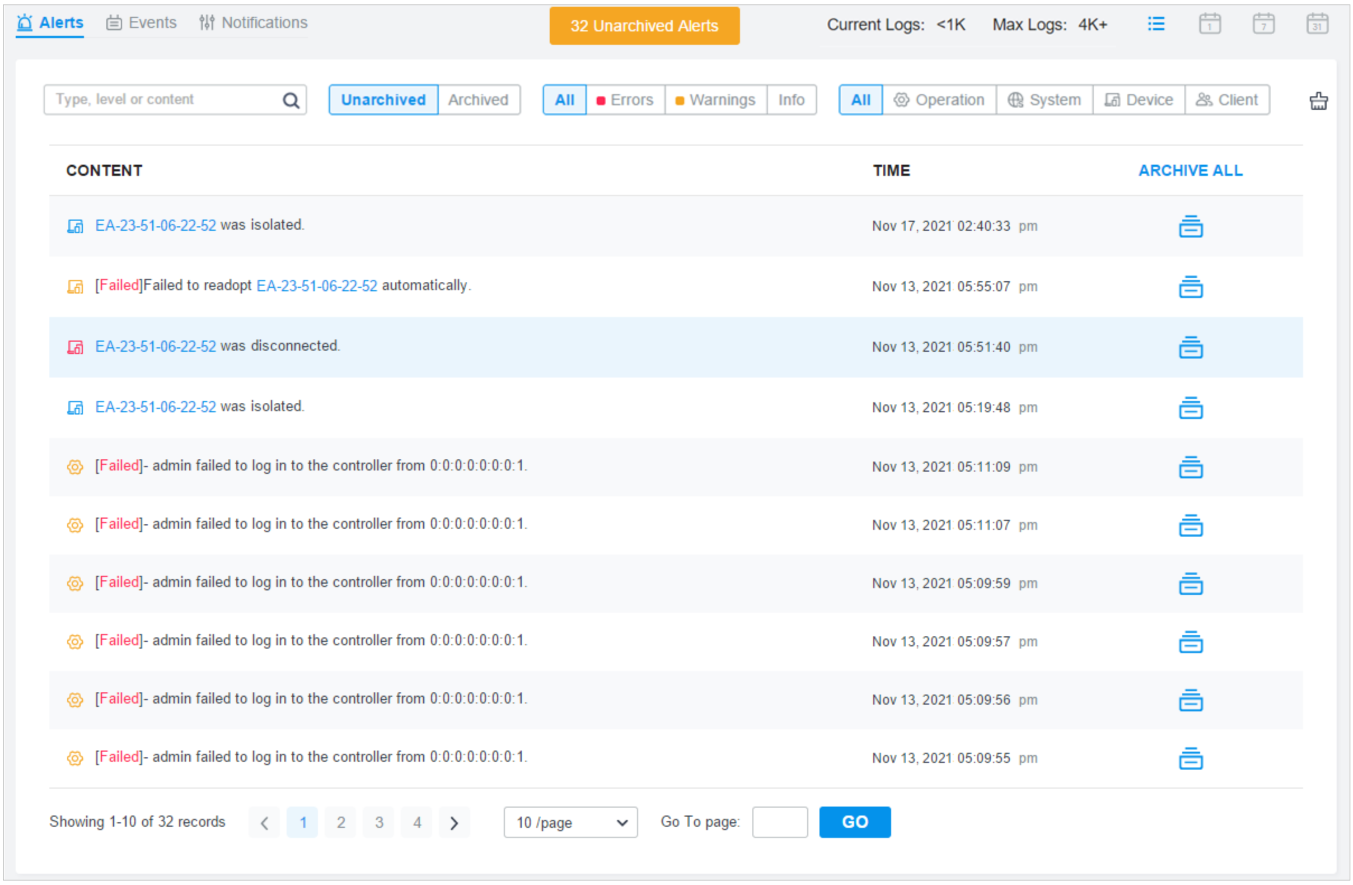
  Three levels in severities are Error, Warning, and Info, whose influences are ranked from high to low.

- **Contents**

  Four types in contents are Operation, System, Device, and Client, which indicate the log contents relating to.

1. 6. 1 Alerts

Alerts are the logs that need to be noticed and archived specially. You can configure the logs as Alerts in Notifications, and all the logs configured as Alerts are listed under the Alerts tab for you to search, filter, and archive.



CONTENT	TIME	ARCHIVE ALL
EA-23-51-06-22-52 was isolated.	Nov 17, 2021 02:40:33 pm	▤
[Failed]Failed to readopt EA-23-51-06-22-52 automatically.	Nov 13, 2021 05:55:07 pm	▤
EA-23-51-06-22-52 was disconnected.	Nov 13, 2021 05:51:40 pm	▤
EA-23-51-06-22-52 was isolated.	Nov 13, 2021 05:19:48 pm	▤
[Failed]- admin failed to log in to the controller from 0:0:0:0:0:0:0:1.	Nov 13, 2021 05:11:09 pm	▤
[Failed]- admin failed to log in to the controller from 0:0:0:0:0:0:0:1.	Nov 13, 2021 05:11:07 pm	▤
[Failed]- admin failed to log in to the controller from 0:0:0:0:0:0:0:1.	Nov 13, 2021 05:09:59 pm	▤
[Failed]- admin failed to log in to the controller from 0:0:0:0:0:0:0:1.	Nov 13, 2021 05:09:57 pm	▤
[Failed]- admin failed to log in to the controller from 0:0:0:0:0:0:0:1.	Nov 13, 2021 05:09:56 pm	▤
[Failed]- admin failed to log in to the controller from 0:0:0:0:0:0:0:1.	Nov 13, 2021 05:09:55 pm	▤

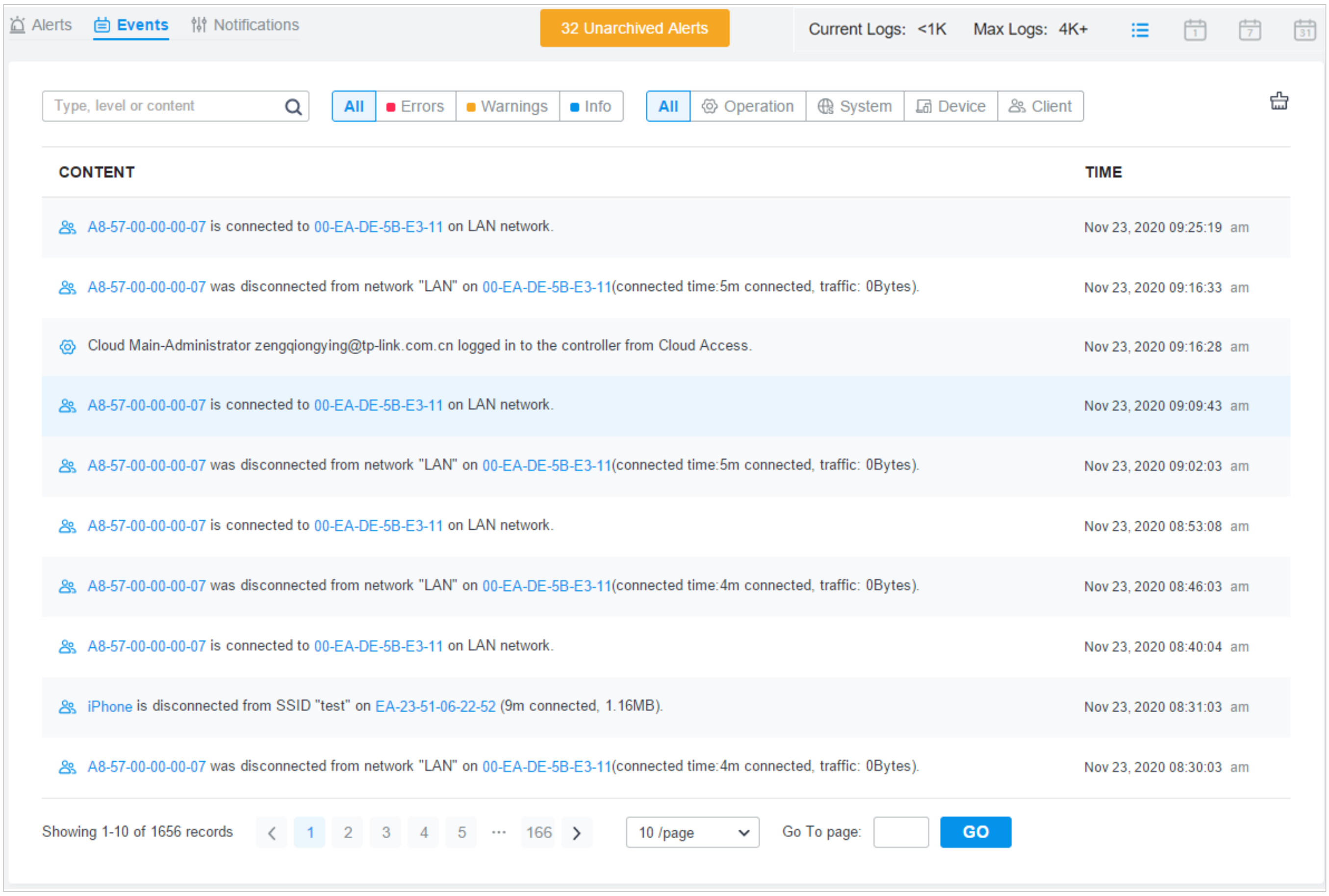
Showing 1-10 of 32 records ‹ 1 2 3 4 › 10 /page Go To page: GO

☰ 1 7 31	Click to change the view mode for a better overview. ☰: Displays the logs in a table. 1/7/31: Displays the logs in a day/week/month. To change the time, click ‹ or ›. To jump back to the current one, click Today/This Week/This Month.
Type, level or content 🔍	Enter the content types, severity levels, or key words to search the logs.
Unarchived Archived All Errors Warnings	Click the tabs to filter the logs listed in the table. The two tabs can take effect simultaneously. Unarchived/Archived: Click the tab to filter the unarchived and archived logs. You can click ▤ and Archive All to archive a single log and all, respectively. All/Errors/Warnings: Click All to display logs in both Error, Warning, and Info levels. Click Errors or Warnings to display logs in Error or Warning levels only.
Content	Displays the log types and detailed message. You can click the device name, client name to open its Properties window for detailed information.

Time	Displays when the activity happened.
Archive All	Click to archive all unarchived logs.
☰	Click to archive the log entry.
🗑	Click and select the log types to delete the corresponding alert logs. Once deleted the archived alerts cannot be recovered. The unarchived alerts cannot be deleted.

1. 6. 2 Events

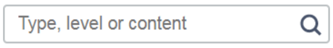
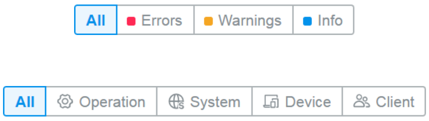
Events are the logs that can be viewed but have no notifications. You can configure the logs as Events in Notifications, and all the logs configured as Events are listed under the Events tab for you to search and filter.



CONTENT	TIME
A8-57-00-00-00-07 is connected to 00-EA-DE-5B-E3-11 on LAN network.	Nov 23, 2020 09:25:19 am
A8-57-00-00-00-07 was disconnected from network "LAN" on 00-EA-DE-5B-E3-11(connected time:5m connected, traffic: 0Bytes).	Nov 23, 2020 09:16:33 am
Cloud Main-Administrator zengqiongying@tp-link.com.cn logged in to the controller from Cloud Access.	Nov 23, 2020 09:16:28 am
A8-57-00-00-00-07 is connected to 00-EA-DE-5B-E3-11 on LAN network.	Nov 23, 2020 09:09:43 am
A8-57-00-00-00-07 was disconnected from network "LAN" on 00-EA-DE-5B-E3-11(connected time:5m connected, traffic: 0Bytes).	Nov 23, 2020 09:02:03 am
A8-57-00-00-00-07 is connected to 00-EA-DE-5B-E3-11 on LAN network.	Nov 23, 2020 08:53:08 am
A8-57-00-00-00-07 was disconnected from network "LAN" on 00-EA-DE-5B-E3-11(connected time:4m connected, traffic: 0Bytes).	Nov 23, 2020 08:46:03 am
A8-57-00-00-00-07 is connected to 00-EA-DE-5B-E3-11 on LAN network.	Nov 23, 2020 08:40:04 am
iPhone is disconnected from SSID "test" on EA-23-51-06-22-52 (9m connected, 1.16MB).	Nov 23, 2020 08:31:03 am
A8-57-00-00-00-07 was disconnected from network "LAN" on 00-EA-DE-5B-E3-11(connected time:4m connected, traffic: 0Bytes).	Nov 23, 2020 08:30:03 am

Showing 1-10 of 1656 records

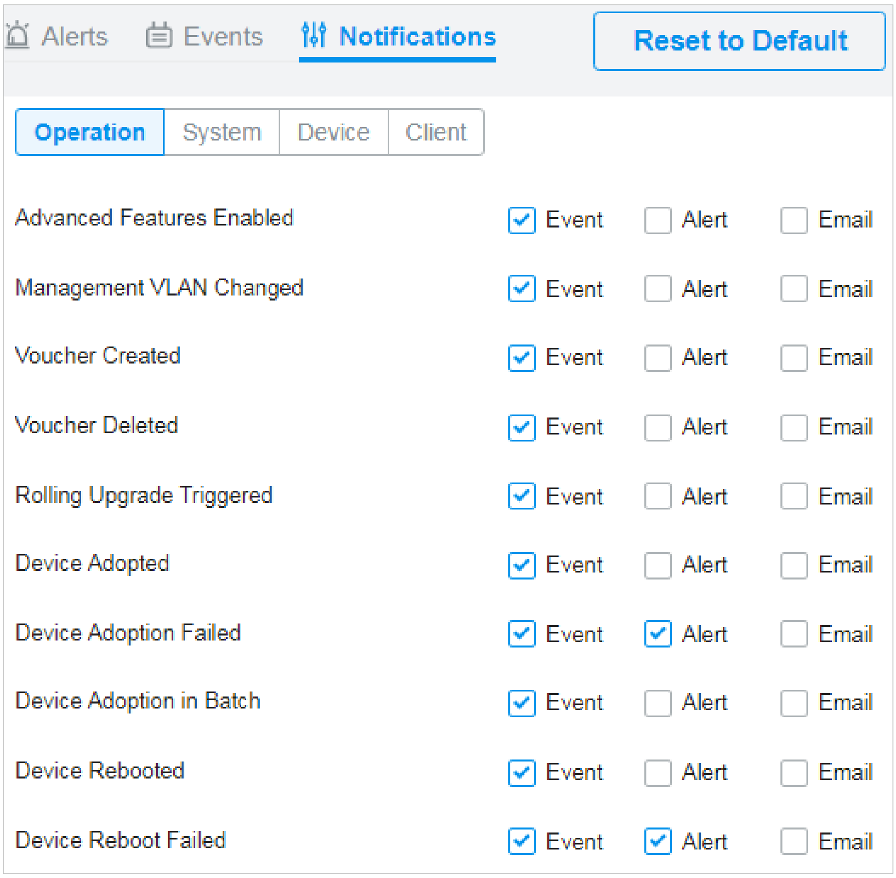
☰ 1 7 31	Click to change the view mode. ☰: Displays the logs in a table. 1/7/31: Displays the logs in a day/week/month. To change the time, click < or >. To jump back to the current one, click Today/This Week/This Month.

 Type, level or content	Enter the content types, severity levels, or key words to search the logs.
🗑	Click and select the log types to delete the corresponding event logs.
 All | Errors | Warnings | Info All | Operation | System | Device | Client	Click the tabs to filter the logs listed in the table. The two tabs can take effect simultaneously. All/Errors/Warnings/Info: Click All to display logs in both Error and Warning levels. Click Errors, Warnings or Info to display logs in the corresponding level only. All/Operation/System/Device/Client: Click All to display all types of logs. Click Operation or System or Device or Client to display the corresponding type of logs only.
Content	Displays the log types and detailed message. You can click the device name, client name to open its Properties window for detailed information.
Time	Displays when the activity happened.

1. 6. 3 Notifications

In Notifications, you can find all kinds of activity logs classified by the content and specify their notification categories as Event and Alert for the current site. Also, you can enable Email for the logs.

With proper configurations, the controller will send emails to the administrators when it records the logs.



Advanced Features Enabled	☑ Event	□ Alert	□ Email
Management VLAN Changed	☑ Event	□ Alert	□ Email
Voucher Created	☑ Event	□ Alert	□ Email
Voucher Deleted	☑ Event	□ Alert	□ Email
Rolling Upgrade Triggered	☑ Event	□ Alert	□ Email
Device Adopted	☑ Event	□ Alert	□ Email
Device Adoption Failed	☑ Event	☑ Alert	□ Email
Device Adoption in Batch	☑ Event	□ Alert	□ Email
Device Rebooted	☑ Event	□ Alert	□ Email
Device Reboot Failed	☑ Event	☑ Alert	□ Email

To specify the logs as Alert/Event, click the corresponding checkboxes of logs and click Apply. The following icons and tab are provided as auxiliaries.

Reset to Default	Click to reset all notification configurations in the current site to the default.
Operation | System | Device | Client	Click the tabs to display the configurations of corresponding log types.
□ Event □ Alert	Enable the checkboxes to specify the activity logs as Events/Alerts, and then the recorded logs will be displayed under the Events/Alerts tab. If both of them are disabled, the controller will not record the activity logs.
□ Email	Enable the checkboxes to specify the activity logs as alert logs. With proper settings in Site and Admin, the controller can send emails to notify the administrators and viewers of the site's alert logs once generated.
↻	This icon appears when the configuration of a log is changed but has not been applied. Click it to reset the configuration of the log to the default.

The Email checkboxes are used to enable Alert Emails for the logs. To make sure the administrators and viewers can receive alert emails of the site, follow the following steps:

1) Enable Mail Server

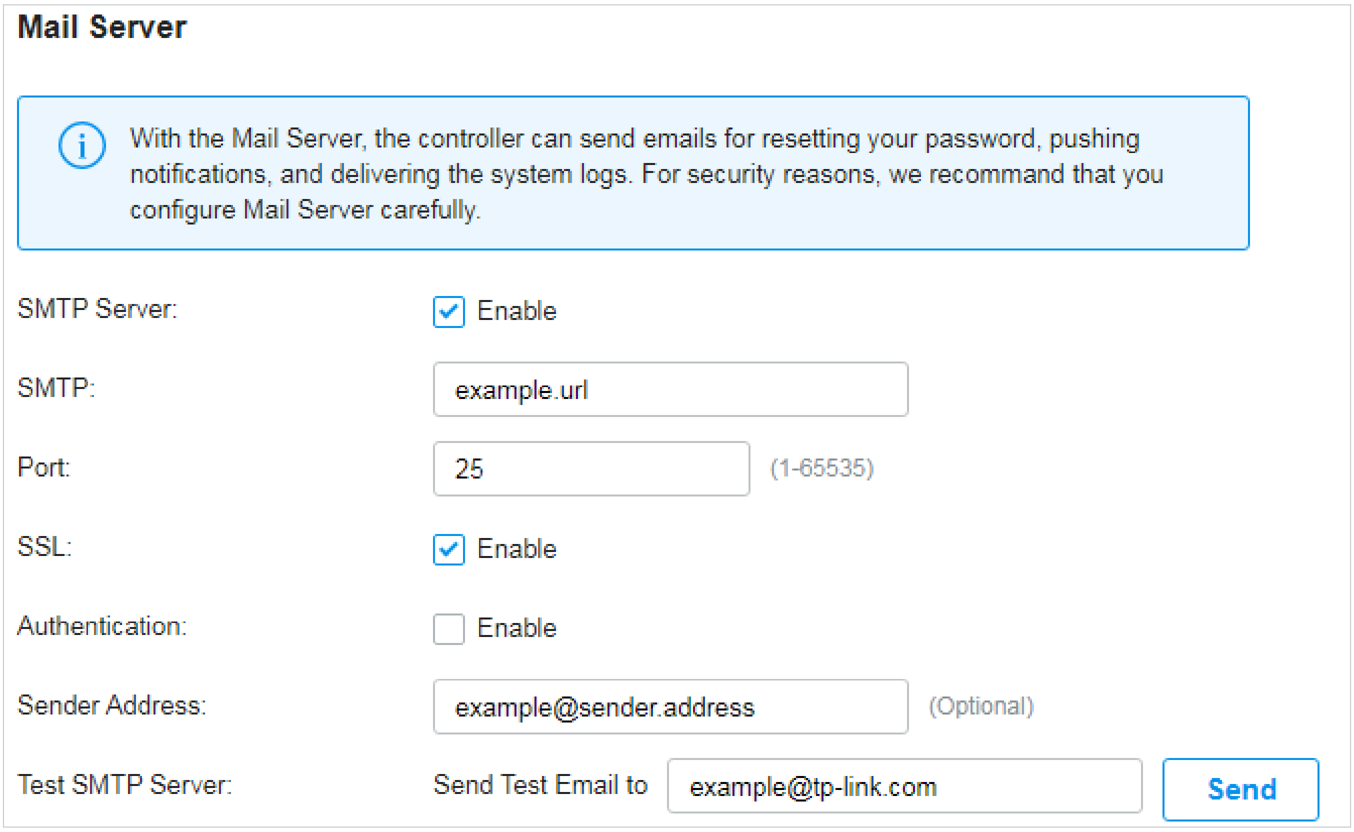
2) Enable Alert Emails in Site

3) Enable Alert Emails in Admin

4) Enable Alert Emails in Logs

Enable Mail Server > Enable Alert Emails in Site > Enable Alert Emails in Admin

Go to Settings > Controller. In the Mail Server section, enable SMTP Server and configure the parameters. Then click Save.



Mail Server

With the Mail Server, the controller can send emails for resetting your password, pushing notifications, and delivering the system logs. For security reasons, we recommand that you configure Mail Server carefully.

SMTP Server: ☑ Enable

SMTP: example.url

Port: 25 (1-65535)

SSL: ☑ Enable

Authentication: □ Enable

Sender Address: example@sender.address (Optional)

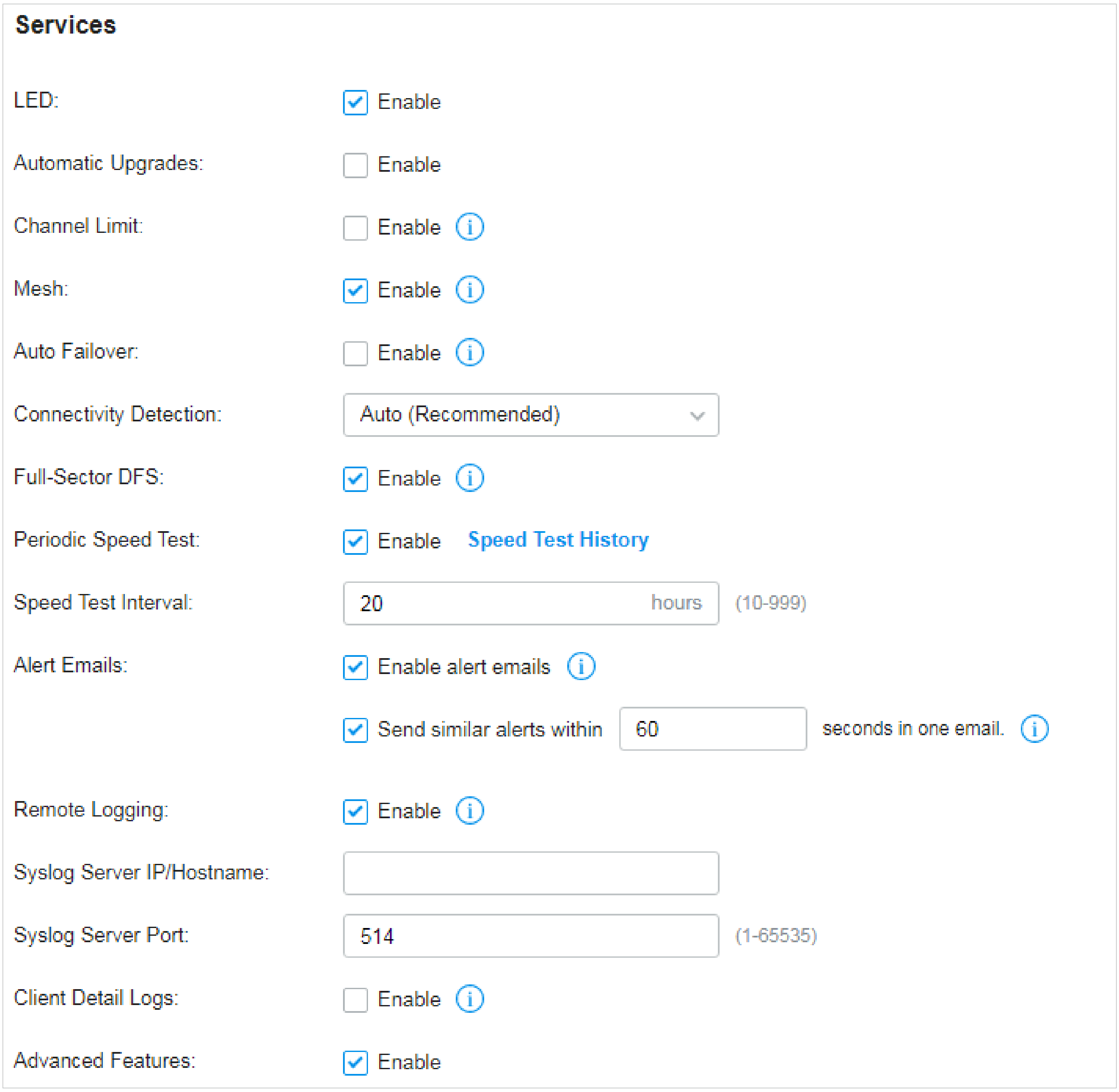
Test SMTP Server: Send Test Email to example@tp-link.com

SMTP	Enter the URL or IP address of the SMTP server according to the instructions of the email service provider.
Port	Configure the port used by the SMTP server according to the instructions of the email service provider.
SSL	Enable or disable SSL according to the instructions of the email service provider. SSL (Secure Sockets Layer) is used to create an encrypted link between the controller and the SMTP server.
Authentication	Enable or disable Authentication according to the instructions of the email service provider. If Authentication is enabled, the SMTP server requires the username and password for authentication.
Username	Enter the username for your email account if Authentication is enabled.
Password	Enter the password for your email account if Authentication is enabled.
Sender Address	(Optional) Specify the sender address of the email.

Test SMTP Server	Test the Mail Server configuration by sending a test email to an email address that you specify.

Enable Mail Server → **Enable Alert Emails in Site** → Enable Alert Emails in Admin

5. Go to Settings > Site and enable Alert Emails in the Services section.



Services

LED: ☑ Enable

Automatic Upgrades: □ Enable

Channel Limit: □ Enable ⓘ

Mesh: ☑ Enable ⓘ

Auto Failover: □ Enable ⓘ

Connectivity Detection: Auto (Recommended)

Full-Sector DFS: ☑ Enable ⓘ

Periodic Speed Test: ☑ Enable Speed Test History

Speed Test Interval: 20 hours (10-999)

Alert Emails: ☑ Enable alert emails ⓘ

☑ Send similar alerts within 60 seconds in one email. ⓘ

Remote Logging: ☑ Enable ⓘ

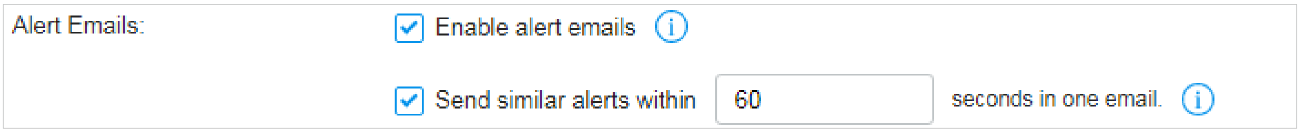
Syslog Server IP/Hostname:

Syslog Server Port: 514 (1-65535)

Client Detail Logs: □ Enable ⓘ

Advanced Features: ☑ Enable

6. (Optional) On the same page, enable Send similar alerts within seconds in one email and specify the time interval. When enabled, the similar alerts generated in each time period are collected and sent to administrators and viewers in one email.



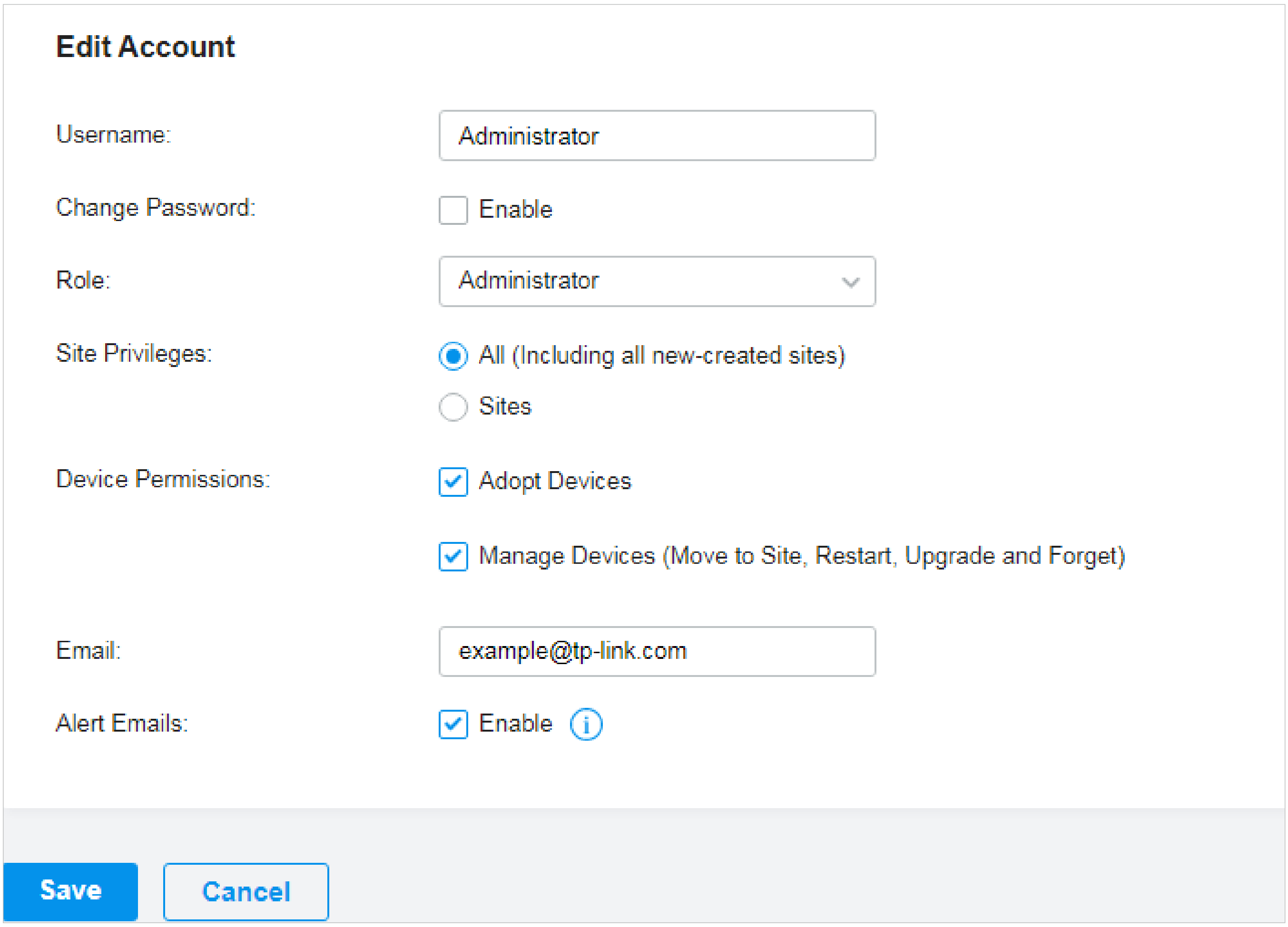
Alert Emails: ☑ Enable alert emails ⓘ

☑ Send similar alerts within 60 seconds in one email. ⓘ

7. Click Apply.

Enable Alert Emails in Site | **Enable Alert Emails in Admin** | Enable Alert Emails in Logs

Go to Admin and configure Alert Emails for the administrators and viewers to receive the emails. Click + Add New Admin Account to create an account or click ✎ to edit an account. Enter the email address in Email and enable Alert Emails. Click Create or Apply.

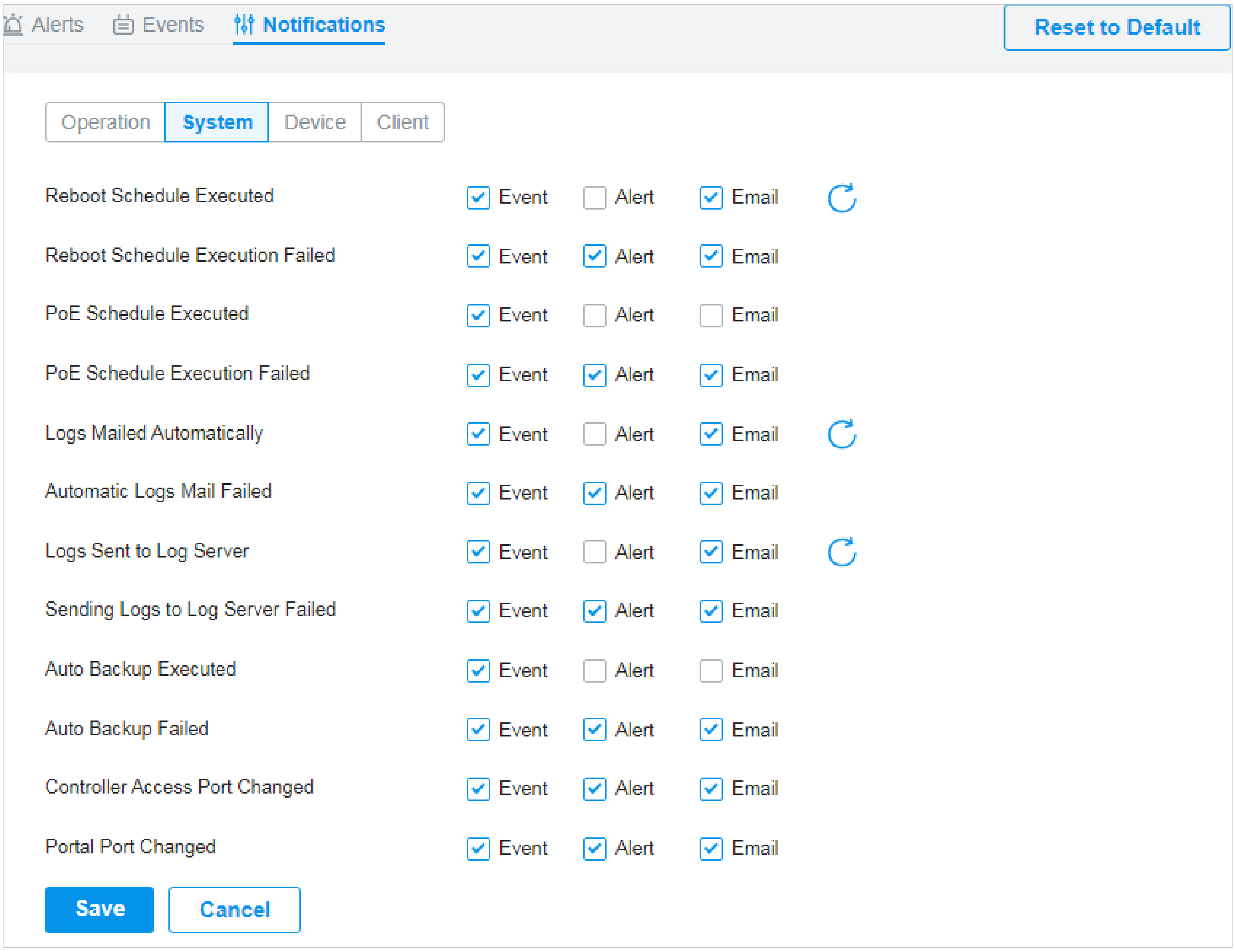


Edit Account

Username:	Administrator
Change Password:	□ Enable
Role:	Administrator
Site Privileges:	● All (Including all new-created sites) ○ Sites
Device Permissions:	☑ Adopt Devices ☑ Manage Devices (Move to Site, Restart, Upgrade and Forget)
Email:	example@tp-link.com
Alert Emails:	☑ Enable ⓘ

Enable Alert Emails in Site > Enable Alert Emails in Admin > **Enable Alert Emails in Logs**

Go to Logs and click Notifications. Click a tab of content types and enable Email for the activity logs that the controller emails administrators. Click Save.



Reboot Schedule Executed	☑ Event	□ Alert	☑ Email	↻
Reboot Schedule Execution Failed	☑ Event	☑ Alert	☑ Email	
PoE Schedule Executed	☑ Event	□ Alert	□ Email	
PoE Schedule Execution Failed	☑ Event	☑ Alert	☑ Email	
Logs Mailed Automatically	☑ Event	□ Alert	☑ Email	↻
Automatic Logs Mail Failed	☑ Event	☑ Alert	☑ Email	
Logs Sent to Log Server	☑ Event	□ Alert	☑ Email	↻
Sending Logs to Log Server Failed	☑ Event	☑ Alert	☑ Email	
Auto Backup Executed	☑ Event	□ Alert	□ Email	
Auto Backup Failed	☑ Event	☑ Alert	☑ Email	
Controller Access Port Changed	☑ Event	☑ Alert	☑ Email	
Portal Port Changed	☑ Event	☑ Alert	☑ Email	

1. 7 Monitor the Network with Tools

The controller provides many tools for you to analyze your network:

- **Network Check**

  Test the device connectivity via ping or traceroute.

- **Packet Capture**

  Capture packets for network troubleshooting.

- **Terminal**

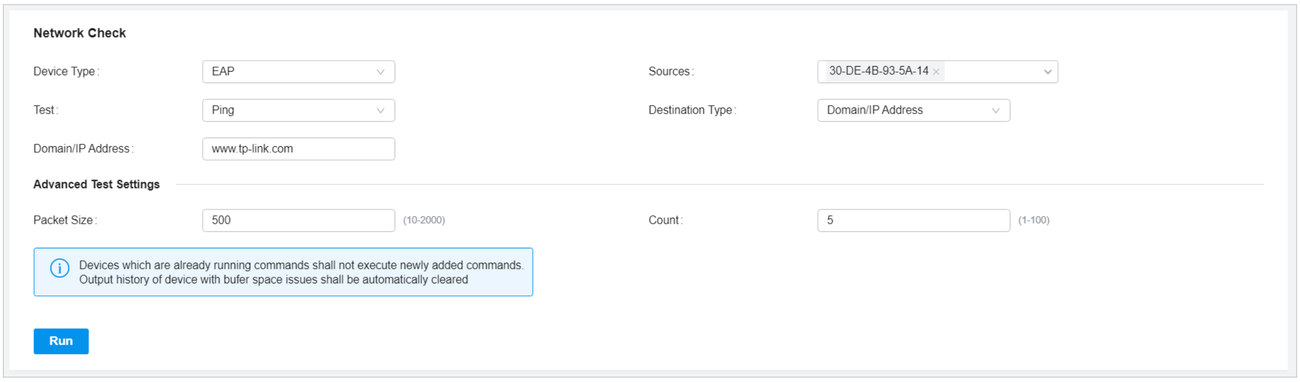
  Open Terminal to execute CLI or Shell commands.

Note:

Firmware updates are required for earlier Omada devices to support these tools.

1. 7. 1 Network Check

1. In the Site view, go to Tools > Network Check.
2. Configure the test parameters.



Network Check

Device Type: EAP

Sources: 30-DE-4B-93-5A-14

Test: Ping

Destination Type: Domain/IP Address

Domain/IP Address: www.tp-link.com

Advanced Test Settings

Packet Size: 500 (10-2000)

Count: 5 (1-100)

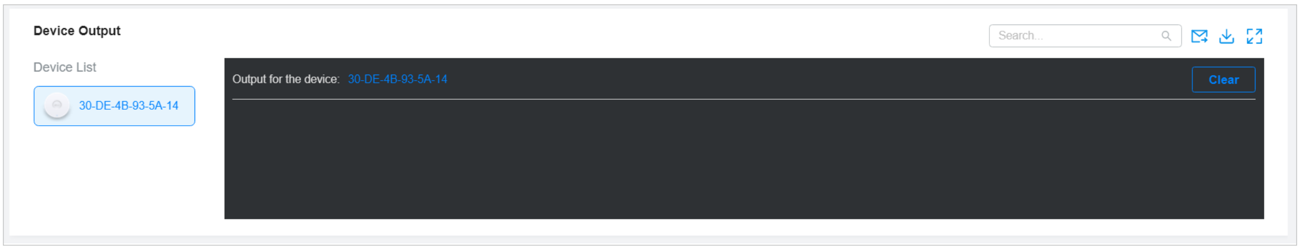
Devices which are already running commands shall not execute newly added commands.
Output history of device with bufer space issues shall be automatically cleared

Device Type	Select the type of device(s) to perform a test: EAP or Switch.
Sources	Select one or multiple devices to perform a test.
Test	Choose the Ping or Traceroute tool to test the device connectivity. Ping: Test the connectivity between the specified sources and destination, and measure the round-trip time. Traceroute: Display the route (path) the specified sources have passed to reach the specified destination, and measure transit delays of packets across an Internet Protocol network.
Destination Type	Select the destination type and specify the Domain/IP Address or Client to ping. Client is unavailable in the traceroute test or when multiple AP devices perform the ping test.
Packet Size	When Test Type is Ping, specify the size of ping packets.
Count	When Test Type is Ping, specify the number of ping packets.

ⓘ Note:

- Devices which are already running commands shall not execute newly added commands.
- Output history of device with buffer space issues shall be automatically cleared.

3. Click Run to perform the test. You can view the test result in the Device Output section.



Device Output

Device List

30-DE-4B-93-5A-14

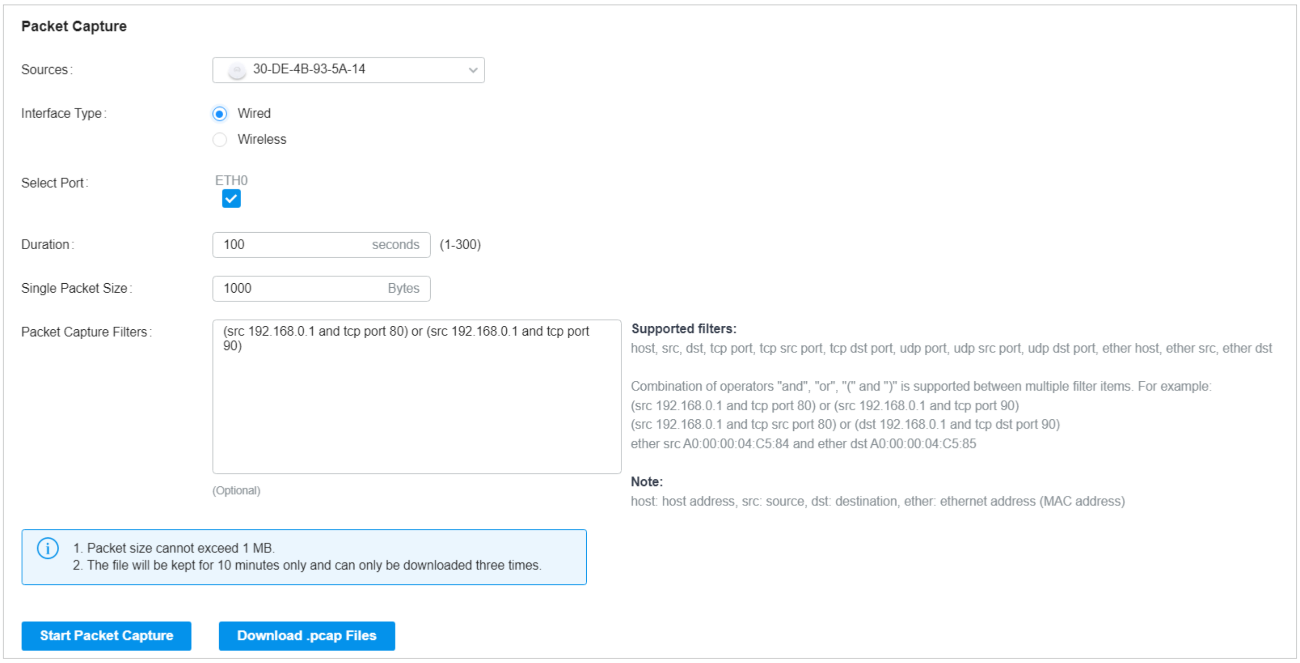
Output for the device: 30-DE-4B-93-5A-14

✉	Click to email the test logs to a mailbox.
⤓	Click to download the test logs locally.
⤢ / ⤡	Zoom out and zoom in the display area.

1.7.2 Packet Capture

1. In the Site view, go to Tools > Packet Capture.

2. Configure the parameters for packet capture.



Packet Capture

Sources: 30-DE-4B-93-5A-14

Interface Type: ● Wired ○ Wireless

Select Port: ETH0 ☑

Duration: 100 seconds (1-300)

Single Packet Size: 1000 Bytes

Packet Capture Filters: (src 192.168.0.1 and tcp port 80) or (src 192.168.0.1 and tcp port 90)

(Optional)

Supported filters:
host, src, dst, tcp port, tcp src port, tcp dst port, udp port, udp src port, udp dst port, ether host, ether src, ether dst

Combination of operators "and", "or", "(" and ")" is supported between multiple filter items. For example:
(src 192.168.0.1 and tcp port 80) or (src 192.168.0.1 and tcp port 90)
(src 192.168.0.1 and tcp src port 80) or (dst 192.168.0.1 and tcp dst port 90)
ether src A0:00:00:04:C5:84 and ether dst A0:00:00:04:C5:85

Note:
host: host address, src: source, dst: destination, ether: ethernet address (MAC address)

1. Packet size cannot exceed 1 MB.
2. The file will be kept for 10 minutes only and can only be downloaded three times.

Sources	Select the source device to capture packets.
Interface Type	Select the Wired interface type and specify the Port, or select the Wireless interface type and specify the Band and SSID / Interface.
Duration	Specify the duration for packet capture.

Single Packet Size	Specify the size of a single captured packet. It cannot exceed 1 MB.
Packet Capture Filters	Enter the filters to capture packets. Supported filters include: host, src, dst, tcp port, tcp src port, tcp dst port, udp port, udp src port, udp dst port, ether host, ether src, ether dst Combination of operators “and”, “or”, “(“ and “)” is supported between multiple filter items. For example: (src 192.168.0.1 and tcp port 80) or (src 192.168.0.1 and tcp port 90) **Note:** host: host address, src: source, dst: destination, ether: ethernet address (MAC address)

3. Click Start Packet Capture to capture packets. After packets are captured, you can click Download .pcap Files to download them.

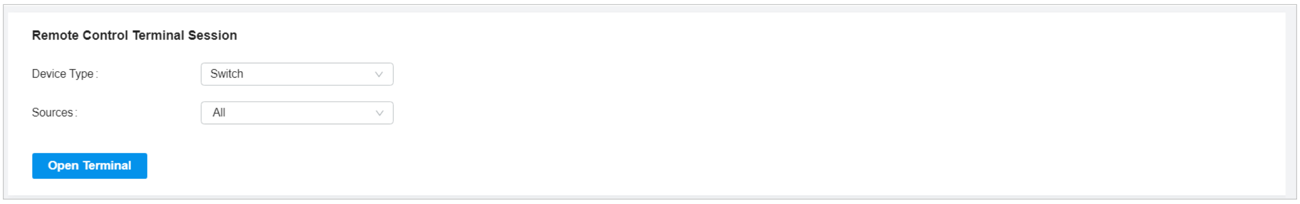
ⓘ Note:

The file will be kept for 10 minutes only and can only be downloaded three times.

1. 7. 3 Terminal

1. In the Site view, go to Tools > Terminal.

2. Configure the parameters.



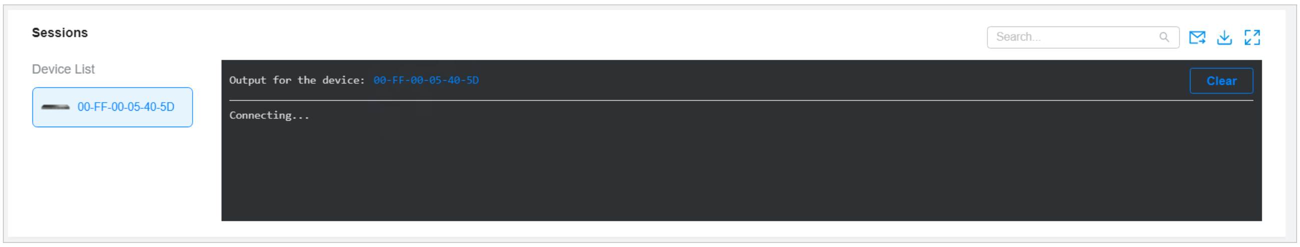
Remote Control Terminal Session

Device Type : Switch

Sources : All

Device Type	Select the type of device(s) to test: EAP or Switch.
Sources	Select one or multiple devices to test.

3. Click Open Terminal. Now you can run CLI or Shell commands.



Sessions

Device List

00-FF-00-05-40-5D

```
Output for the device: 00-FF-00-05-40-5D
Connecting...
```

✉	Click to email the test logs to a mailbox.
⤓	Click to download the test logs locally.
⤢ / ⤡	Zoom out and zoom in the display area.