User Guide:

Datto AP440

Version 1.2

July 30, 2021

Table of Contents

1. <u>**General Warnings:**</u>

Electrical Hazard: Only qualified, instructed, or skilled personnel should perform installation, repair, or disassembly procedures

Risque électrique : Seul le personnel qualifié, instruit ou qualifié doit effectuer les procédures d'installation, de réparation ou de démontage

WARNING: 24V Passive PoE is not supported on this device, do not attempt to use, Damage can result

AVERTISSEMENT : le PoE passif 24 V n'est pas pris en charge sur cet appareil, n'essayez pas de l'utiliser, des dommages peuvent en résulter

Restriction Statement:

The 5150-5350-MHz band is allocated for indoor use only in

EU member countries and Canada.

BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV

LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	UK

2. Product Specifications

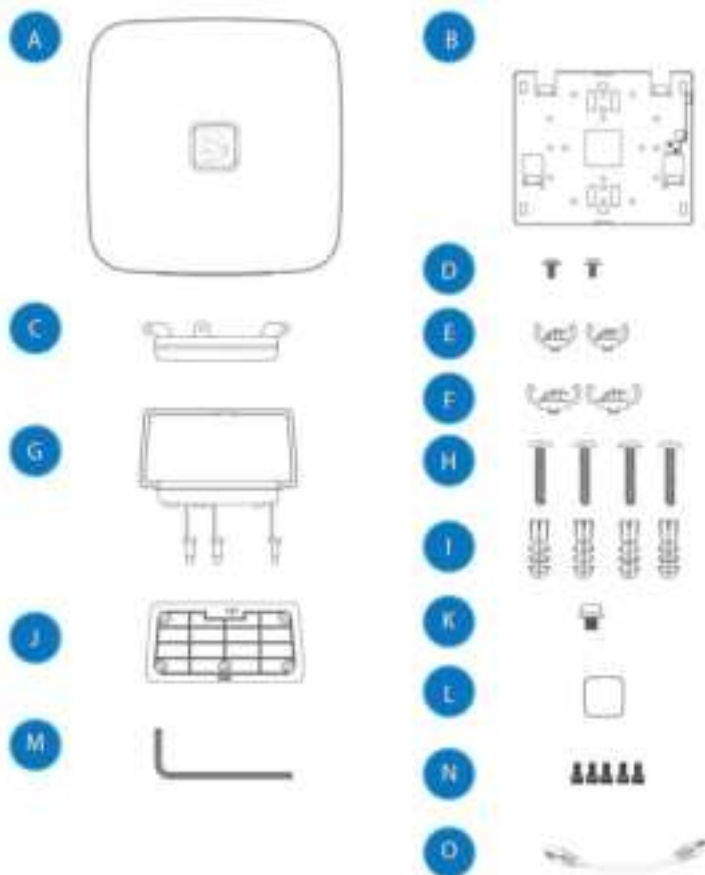|	
OFDMA Data Rate (Aggregate)	1774.5 Mbps (2.4GHz: 573.5 Mbps, 5GHz: 1201 Mbps)
OFDM Data Rate (Aggregate)	1166.7 Mbps (2.4GHz: 300Mbps, 5GHz: 866.7 Mbps)
Transfer Rate	802.11b: Up to 11 Mbps 802.11a/g: Up to 54 Mbps 802.11n: Up to 300 Mbps 802.11ac: Up to 866.7 Mbps 802.11ax: Up to 1201 Mbps
Radio	2.4 GHz: 2 stream, 802.11 b/g/n/ax 5 GHz: 2 stream, 802.11 a/b/g/n/ac/ax Scanning Dual Band Radio: 1 Stream Receive
Antenna	2x Internal Dual band Antenna
OFDMA Max Users (Recommended)	200 -250 Users per AP
OFDM Max Users (Recommended)	75-150 Users per AP
WLAN Standard	WiFi6 – 802.11a/b/g/n/ac/ax
Processor	Quad Core CPU @ 1.8GHz
Memory	1GB DDR3
Ethernet Ports	2x 10/100/1000 Mbps RJ45 Ethernet Ports
PoE	1x 802.3AF/AT Standard PoE input
DC Power Input	12V, 2.5A DC Power input
USB	1x USB 2.0
Operating Temperature	-20C ~ 50C
Installation Environment	Indoor or Outdoor Installation
LEDs	Tri-Color LED Status Indicator
Hardware CPU Watchdog	Yes
Size	7.3" x 7.3" x 1.6" (186mm x 186mm x 40mm)
Mounting	Solid Wall, Solid Ceiling, Ethernet Junction box, Pole, T-Rail
Warranty	Lifetime
Certifications	FCC, IC, CE, RCM, UL
SSIDs	4
SSID to VLAN Tagging	Yes
Bridge to LAN	Yes
Seamless Roaming	Yes
Cloud Management	Yes
Free iOS/Android App	Yes
Zero Config Plug and Play	Yes
Self-forming, Self-healing Mesh	Yes
Captive Portal w/ Bandwidth throttling, splashpages, and user controls	Yes

3. Product Overview

Reset
USB 2.0
12V DC, 2.5A Power Input
Ground
LED Indicator
1G Ethernet Port
1G Ethernet Port, 802.3at PoE Input
Kensington Lock Mount

4. Included Accessories

A
B
C
D
E
F
G
H
I
J
K
L
M
N
O

A (1) Access Point

B (1) Mounting Bracket

C (1) Indoor I/O Cover

D (2) M3-10 T-rail Clip Screws

E (2) 9/16" T-Rail Clips

F (2) 15/16" T-Rail Clips

G (1) I/O Port Gasket

H (4) M4-25 Drywall Screws

I (4) Drywall Anchors

J (1) I/O Port Cover

K (1) M4-6 Grounding Screw

L (1) Blank LED Tab

M (1) Allen and Torque Combo Tool

N (5) M3-8 I/O Port Cover Screws

O (1) 12" Ethernet Cable

Drywall Screw Dimensions:
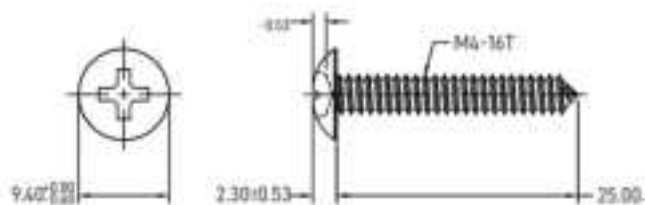
Drywall Anchor Dimensions:
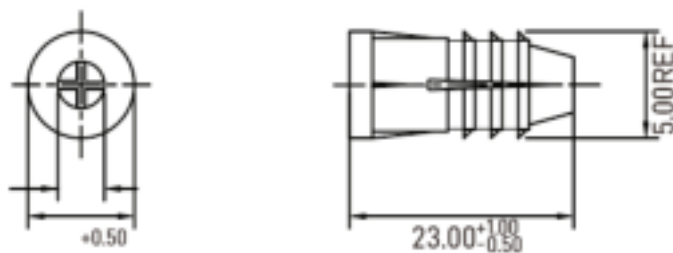
5. Mounting and Installation Instructions

5.1 How to Assemble the I/O Port Cover and Gasket for IP54:

1. Plug in a rounded Ethernet cable into the Far right Ethernet Port with 802.3AT poe input supported
2. Wrap the Gasket around the Ethernet cable, align with the I/O cover spacing and push gasket into place.
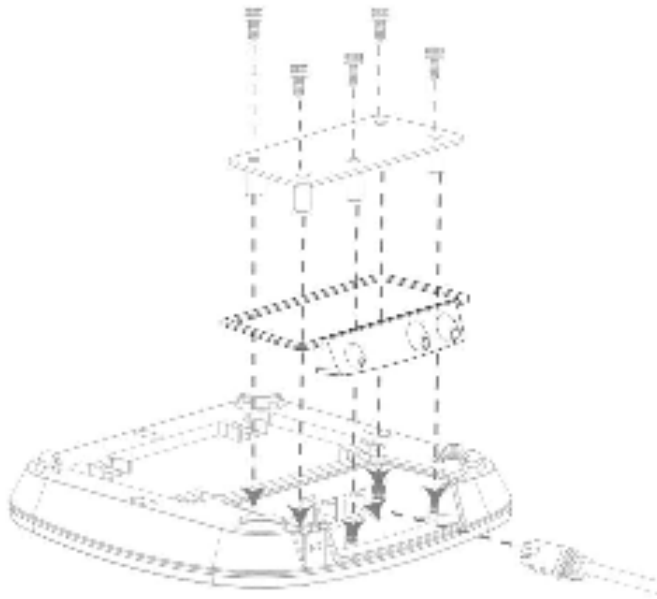
3. Place the I/O port cover in place over the Gasket and leveraging the provided Allen and Torque tool, screw the 5 Hex screws into place
4. Once Done you will want to use the plugs and fill the unused I/O Holes
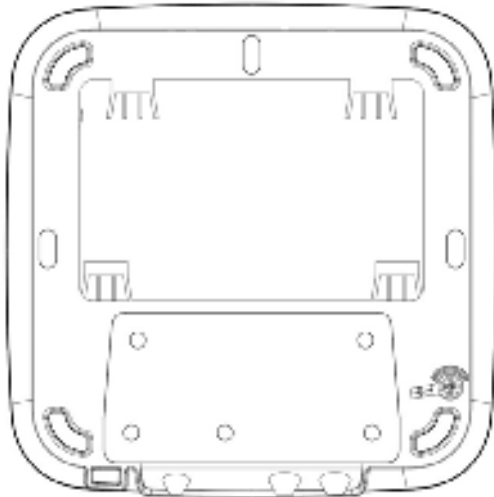
5. For Best Sealing and protection of Product, do not mount the device with the Ethernet cables facing upwards towards the sky.

5.2 How to Assemble the I/O Edge Cover:

1) Align the I/O Cover with the side of the Housing, and align the 3 mounting holes with the 3 screw mounts on the AP440 Housing
2) Using the Provided I/O Cover screws, screw the 3 screws in place using the provided Allen and Torque L-Tool
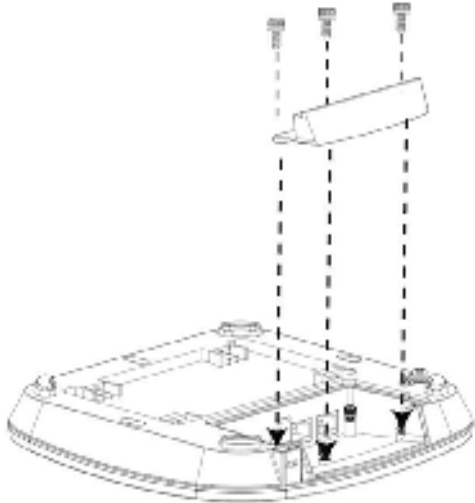
3) Now when routing the cables route up and through the Mounting bracket
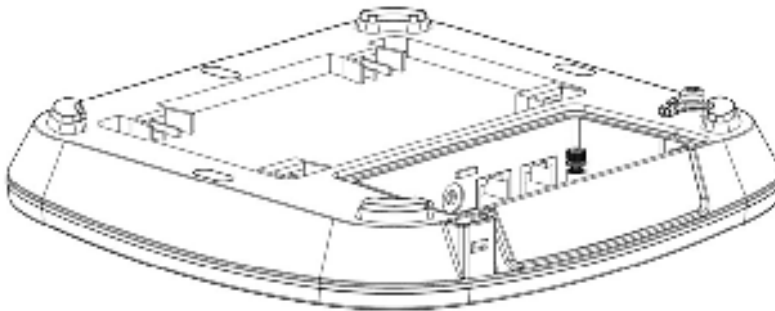
5.3 How to Mount to an Ethernet Junction Box:

    1)   Install the Flat side of the mounting plate to the Junction Box:
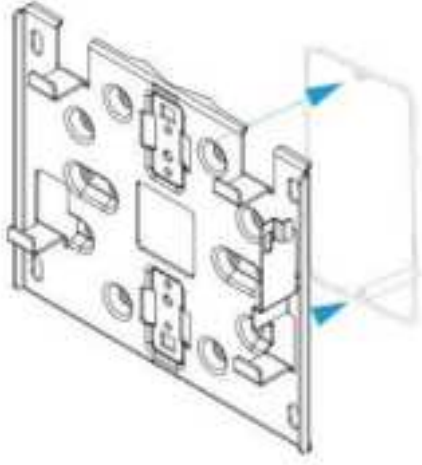
    2)   Connect the Ethernet Cable to the Access Point Ethernet Port with 802.3AF/AT PoE input
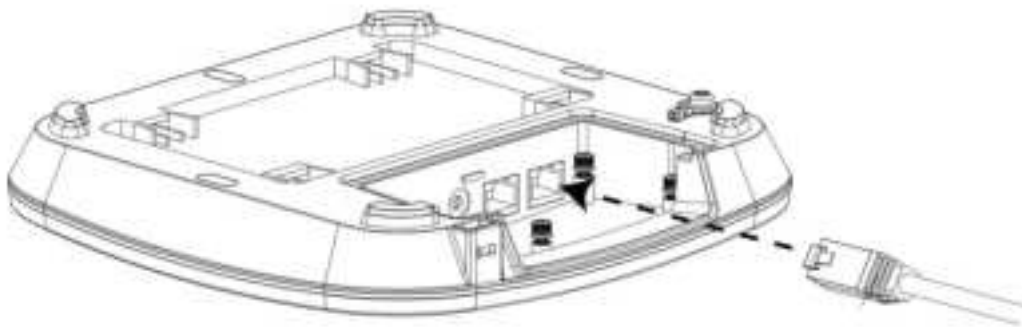
    3)   Alternatively you can supply power to the device using the 12V DC Power input

    4)   Install the Access Point on the mounting plate and lock into place

5.4 How to Mount to a Flat Surface (Wall or Ceiling):

1) Install the flat side of the Mounting plate on the wall or solid ceiling with wall screws and anchors

2) Connect the Ethernet Cale to the Access Point Ethernet Port with 802.3AT PoE input

3) Alternatively you can supply power to the device using the 12V DC Power input
4) Install the I/O Port Cover and Gasket if installed outdoors
5) Install the Access Point on the mounting plate and lock into place
6) Attach Grounding Cable to the Grounding Point on the Access point and screw in provided Grounding screw if installed outdoors

5.5 How to Mount to a Pole:

NOTES:

- Metal Hose Clamp is not included in the packaging and must be purchased Separately
- Always use a 0.5" thick Stainless Steel Hose Clamp and Not a Plastic one
- The system supports being mounting to a pole of diameter 0.75"(19mm) up to 6"(152.4mm).

1) Install Clamp Cabling through the slots on the Mounting Plate.
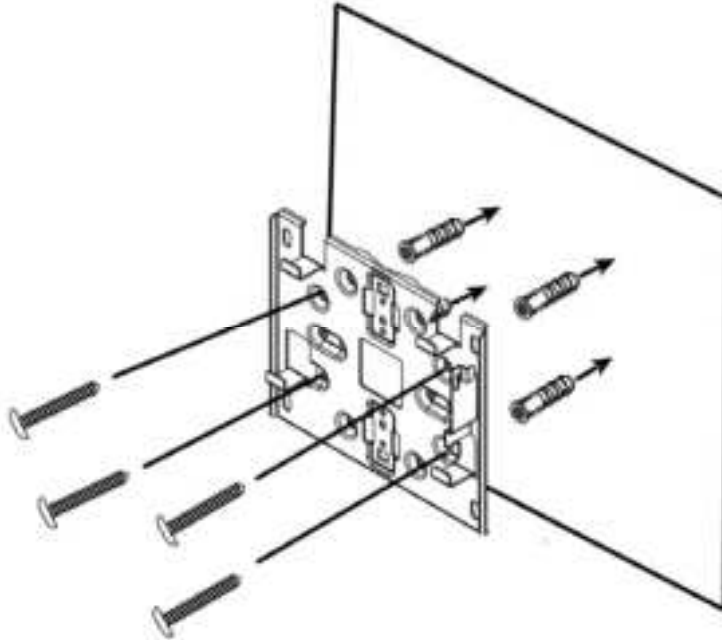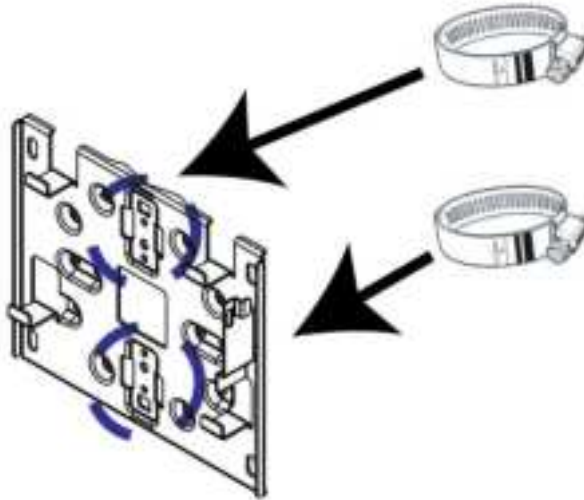

2) Connect the Ethernet Cable to the Access Point Ethernet Port with 802.3AF/AT PoE input
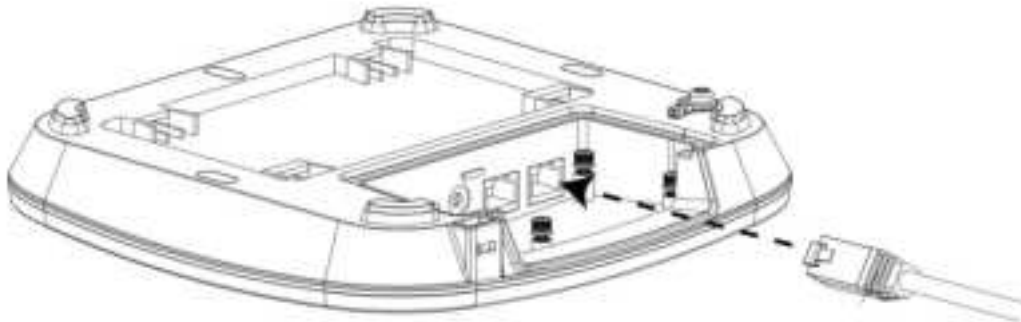
3) Alternatively you can supply power to the device using the 12V DC Power input
4) Install the I/O Port Cover and Gasket if installed outdoors
5) Install the Access Point on the mounting plate and lock into place
6) Attach Grounding Cable to the Grounding Point on the Access point and screw in provided Grounding screw

5.6 How to Mount to T-Rails

1) Install the Desired T-Rail Clip set in the Mounting Plate. Secure Clips with T-Rail Screws.
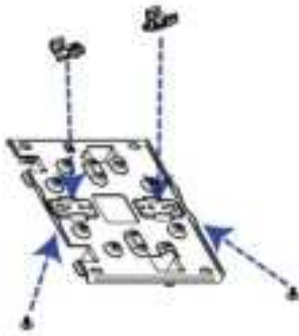
2) Install the mounting plate by pressing both clips on the ceiling T-rail until fully engaged
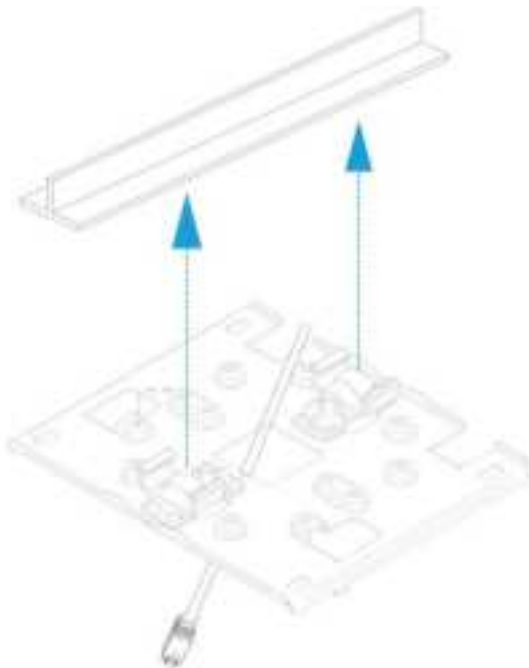
3) Connect the Ethernet Cable to the Access Point Ethernet Port with 802.3AF/AT PoE input, and assemble I/O Cover and Gasket for outdoor installations
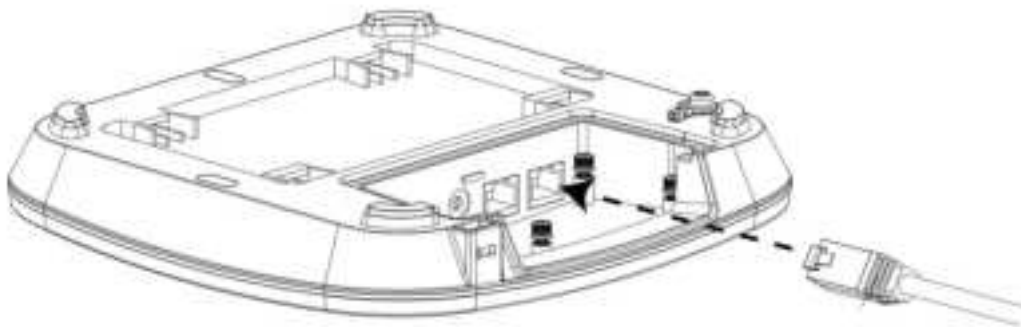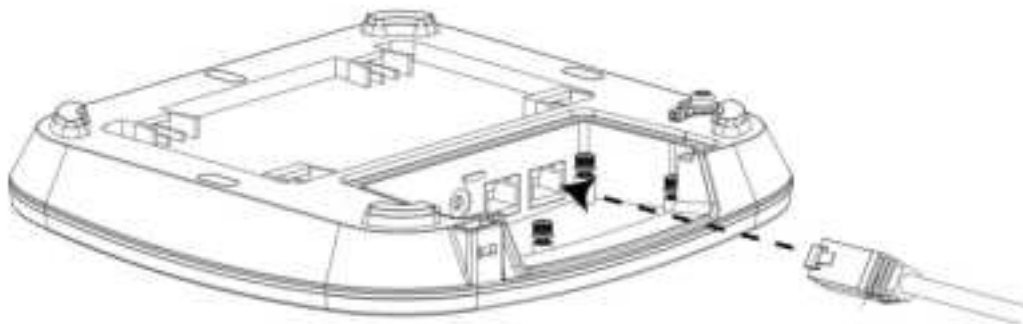
4) Alternatively you can supply power to the device using the 12V DC Power input
5) Install the Access Point on the mounting plate and lock into place

6. Creating a Network on Network Manager

Overview: what we're doing

This guide is intended to help you set up your first cloud-managed wireless mesh network with Datto Network Manager. Network Manager is a cloud-based network controller that makes it easy for anyone to build, manage, and monitor wireless networks from anywhere in the world.
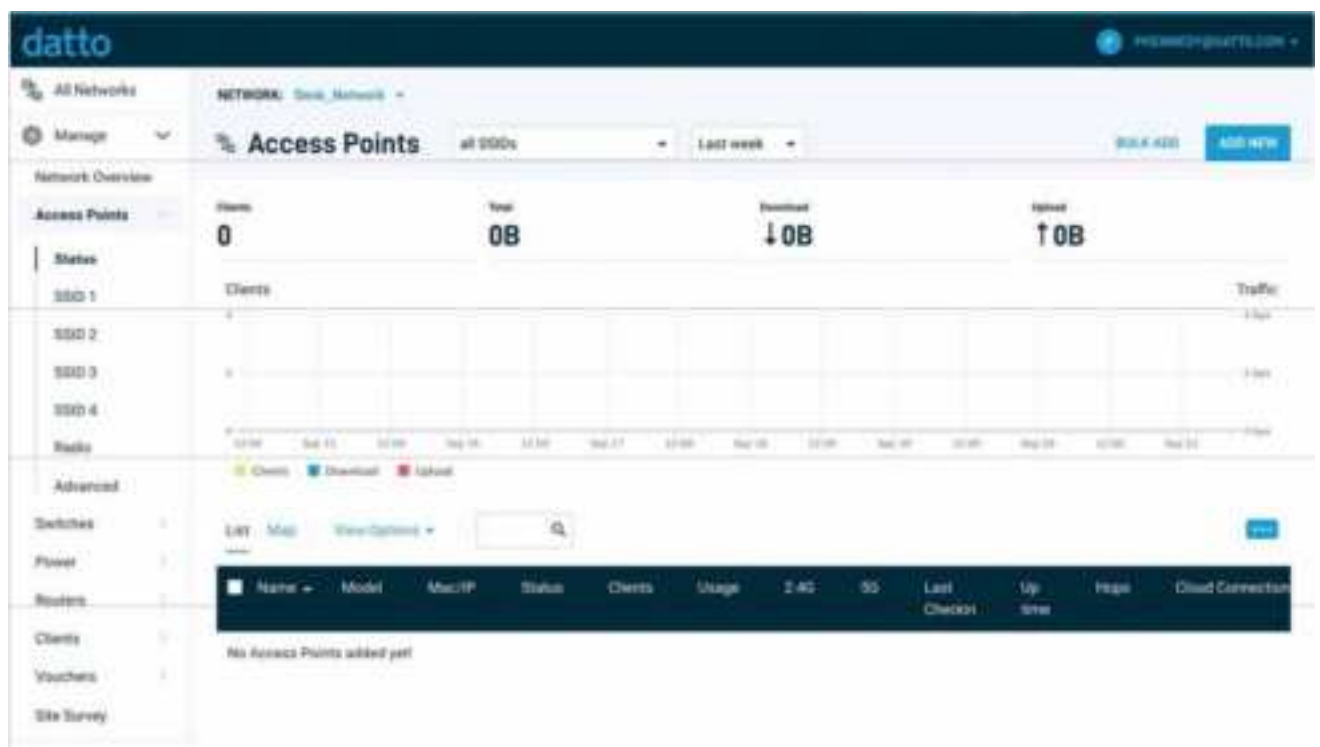
This guide will assist you in setting up a new network on the Datto Network Manager web application. For easier, faster setup, use the Datto Networking for iOS or Datto

Networking apps. No matter which version you start with, you can switch between the web and mobile apps seamlessly.

Here's what's about to happen:

1. Log into your Datto Partner Portal

2. We'll create a new network on Network Manager.

3. We'll add access points to the network.

4. We'll physically install the access points.

5. We'll do some basic network configuration.

This guide is not intended to cover every aspect of Network Manager. To learn more about planning your network, view the Datto Knowledge Base (kb.datto.com)

What you'll need

To set up your network, you'll need the following:

1. One or more Datto Network Manager-compatible wireless devices, such as the AP440, AP840 or AP840E

2. An Internet connection with at least one Ethernet port available on your modem or router

3. one Ethernet cable and a 802.3at POE source
4. A computer with a browser pointed to datto.com, or an iOS or Android device running the Datto Network Manager App

Terminology

We'll make this process as easy and nontechnical as possible. Here are a few key words that will help.

Network: A group of computers or devices that can talk to each other (in our case, wirelessly). **Gateway:** A Network Manager-compatible router that is connected to the Internet (usually through a DSL, cable, or LAN connection).

Repeater: A Network Manager-compatible router that is not connected to the Internet that repeats the signals from local computers and other access points to the gateway.

Access point: A generic name for an Network Manager-compatible router/access point which can be either a Gateway or a Repeater. You may also see these called "Nodes."

All Datto Networking Access Points configure themselves: they become gateways or repeaters depending on if they are connected to the Internet or not.

Step 1: Log into the Datto Partner Portal(datto.com) and Navigate to the Network Status Page

Then Select to Add Device, as shown in the Diagram below in the ttop right corner of the screen
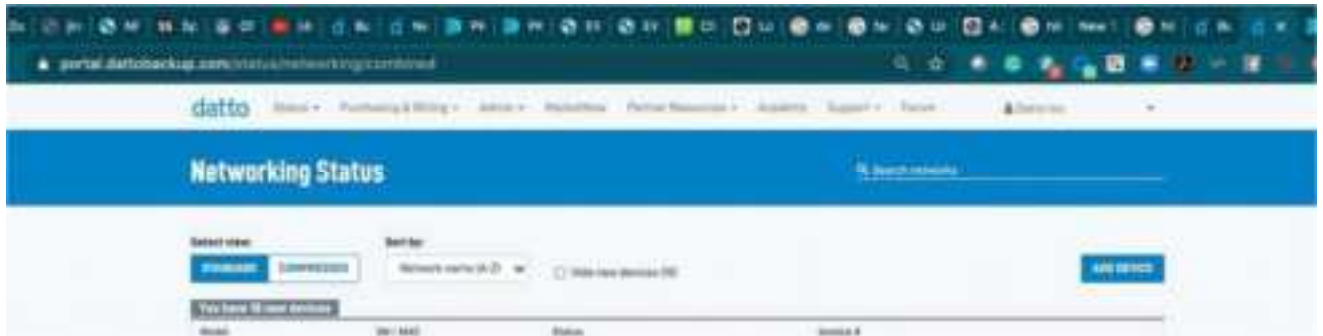
You will now be automatically redirected to the Datto Networking Manager webpage, as seen below:

Now you may create new network to add this device to, or navigate to the network you would like to add this device to. For this guide we will be setting up a new Network. So click "Create Network"

Step 2: Create a new network

You'll automatically be taken to a page, similar to the one below, to create your first network.

Fill in the following information:

Network name: This is the name you want to give this specific network. You will use this name to make changes to the network, display reports, etc.

Password: This is the password for local administrators and should be different from your master account login. This limits access and prevents users from making changes to your network.

Email: Enter your email address or the address of a local administrator to contact. We will never share this with others.

Network Location: Enter a street address for the first access point. To add access points, you will be shown a map that you click on to place access points. By entering an address here, you will be centered on the correct location for your network.

Email for Notifications: Enter the email addresses, separated by spaces, for all people you'd like to receive "outage" notifications. These are sent hourly.

When finished, click "Create" to save your new network settings.

Step 3: Add access points to your network

It's time to let Network Manager know which access points you want to include in the network. Adding them to Network Manager will allow you to manage and monitor the access points from anywhere.

Navigate to the Manage > Access Points screen.

There are three options to add access points to your network: click the "Add New" button to add access points one at a time by clicking on a map, or use the down arrow to the right of that to add access points in bulk.

If you add access points the default way, you'll be taken to the Map tab of the Access Points page. A Google map, centered on the address you entered when you created the network, will show a popup to enter your first access point. You can often (depending on location) click the "Satellite" view button and zoom in for a closer look.
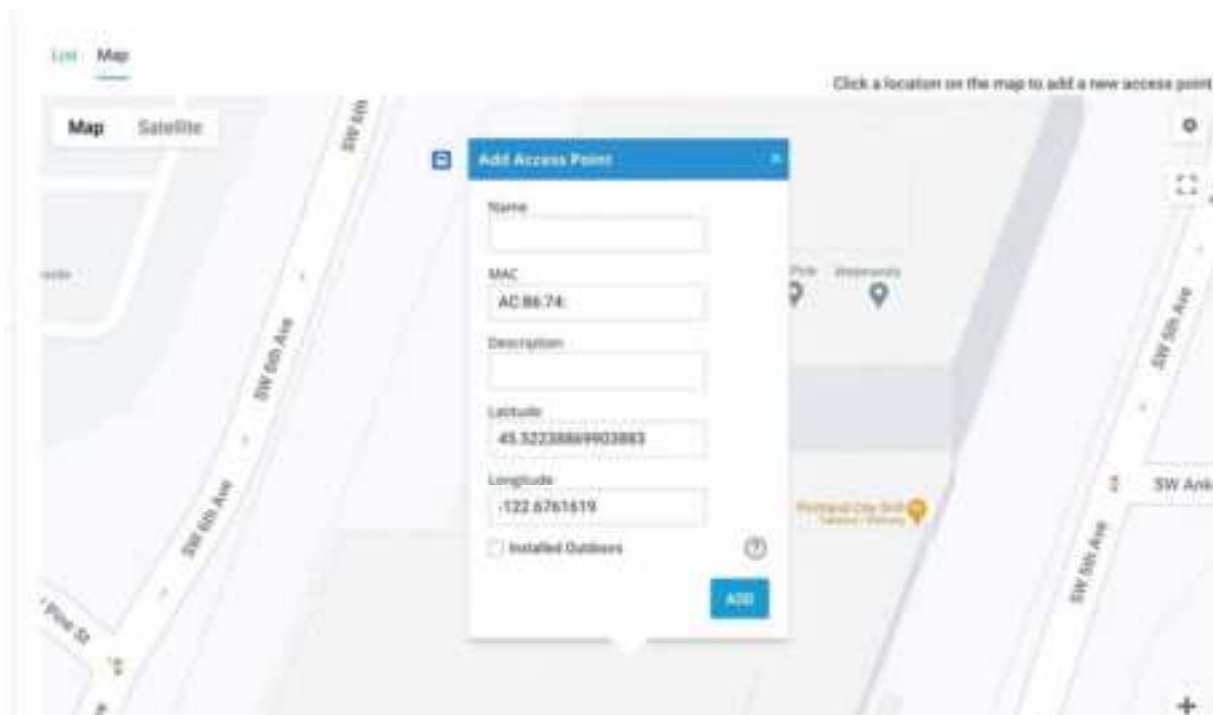
Fill in the following information:

Name: Enter a name for this access point. This name is used to reference its location and will be displayed in reports. It does not affect users.

MAC address: A MAC address is a sequence of 12 numbers and the letters A-F often separated by colons (Eg: 00:02:6F:8A:B2:6E). This can be found on a label on the bottom of the router and on the side of the product box.

Description: You can enter optional descriptive text that will be shown on the reports. This is typically used to keep notes on where the access point is installed, etc.

Click "Add" and repeat the process for each additional access point.

If you need to add a large number of access points, you may want to add them in bulk. You can do so two ways: by entering the MAC addresses in a text field (one per line), or by uploading a list of access points (along with optional name, location, channel overrides, etc.) in a CSV file.

For both of these options, your access points will be added to the map based on your network location (similar to how the Datto Networking iOS and Android apps add access points). You can reposition these access points on the map after adding them.

When adding by CSV, the CSV file must be in a specific format. You can download a sample CSV file here.

Step 4: Install the access points

Once your access points are added to Network Manager, it's time to install them. If you're using an enclosure, video installation guides are available here.

First, connect your Gateway unit to the Internet with an Ethernet cable. This can be plugged in directly to your high-speed modem (if it has a single Ethernet port, power cycle it first), or it can be fed from a router or switch. If it can get an Internet connection through the cable, it'll connect to Datto Network Manager. Once the Ethernet cable is plugged in, connect power.

The Ethernet cable (PoE device) must be connected only to PoE networks that is SELV circuit and without routing to the outside plant.

Next, plug in additional access points as either gateways (connected to Ethernet) or repeaters, connected only to power.

When mounting Datto access points directly onto a wall, use a minimum 30 mm screw length.

To ensure strong, consistent signal coverage, follow these guidelines:

1. Place your gateway in the center of the network. For most devices, every time data is transmitted over one repeater hop, it loses half its speed. A central gateway minimizes the number of hops required.

2. Never go through more than three to four walls or floors.

3. Never go more than 50-150 feet (depending on building materials) between access points.

4. Install no more than about five repeaters to everyone gateway.

Once all access points are plugged in, you should see them turn green on the Network Manager Status page in about 5 to 15 minutes. For more detailed information on planning and optimizing your network, see the Network Planning Guide.

7. Configuring A Network

Your network should now be up and running, but there's a lot we can do to customize it to meet your specific needs. We'll walk you through the most common settings here.

Configure > General Settings

The General Settings tab controls network-wide settings. This will be partially filled in with the information you used to create the network.

Location: This defaults to the first address you entered when setting up the network. You can change it at any time. Note that the location only determines where your access point appears on the map; radio settings will be based on the IP address of the access point.

Network name: The login name for this network on the dashboard, and also the login ID to access this network individually by a site administrator. This is NOT your master login. This allows you to give access to only the network settings for that network without allowing access to your master account.

Time Zone: Used in displaying the local time on reports.

AM/PM time: Used in displaying the local time on reports.

Display Name: Used to display a more descriptive name (other than the login ID) on reports. **Password:** The administrator password for this network. Again, this is only for this network and is not your master login password. It is also not the password your users will use to connect to the network.

Disable Limited View: If unchecked, users will be able to see a limited view of the network status. The password will still be required to change any network settings.

Email: Your email in case we need to contact you. We will not share this with others. **Notification Email:** The email address notifications will be sent to if enabled. You can list multiple email addresses, separated by spaces.

Email Alerts: Select this box to send notifications of network outages each hour to the email addresses you entered above.

Network notes: Enter any unique notes for this installation you'd like to be able to refer to later. **Configure > SSID 1, 2, 3...**

Each device can broadcast four unique SSIDs that users can connect to. Each of these SSIDs are controlled independently in Network Manager. Typically users have a mix of public SSIDs - with splash pages, bandwidth throttling, DNS filtering and client isolation - and private SSIDs, with WPA Enterprise authentication and access to LAN resources and other clients. When we created your network, we set the first SSID to be public and the second SSID to be private, but you can adjust these any way you wish.

We'll go through most of the features you may want to enable or change. You can also learn more about voucher access, pay networks and more by following the links at the end of this document. *Common Settings*

SSID name: The name you'd like users to see and connect to with their device. You can also check the box below to use each access point's name for its SSID instead.

Enable: When selected, this SSID will broadcast on all access points in this network. When deselected, it won't broadcast but your settings will be saved.

Visible: When enabled, this SSID will advertise itself publicly so users can select it from their list of available networks. When disabled, users must enter the SSID name manually.

Band Use this to limit what bands the SSID is broadcast on. *Note:* Selecting the 'only' options in a network with single radio devices (like the OM2P) may cause the SSID to not be broadcast at all.

Authentication: Enable this to authenticate users with WPA-PSK or WPA-Enterprise at the time they connect to the SSID. This isn't required if you wish to authenticate users on a splash page.

WPA Pre-shared key (Password): If you would like to secure your network with a password, enter it here. It must be eight characters or longer and contain no spaces.

WPA Enterprise: Uses 802.1x authentication that requires a unique username and password for each user.

Captive Portal Settings

Bandwidth Throttling: Enable and set download/upload limits to set the maximum speeds users will get when connected to your network. You may want to set these to between 10 and 25 per cent of the speed of your Internet connection, ensuring that one or two users can't consume the entire available bandwidth.

Splash Page/Splash Page Type: Enable or disable a page users will see before connecting to your network. You can set this to Custom (hosted by Datto), Facebook WiFi, or a hosted remotely version for advanced users.

Splash Page Authentication: Choose Network Manager, RADIUS or HTTP Authentication. Read more here.

Client Force Timeout: Minutes client is idle (Idle Timeout) before showing splash page, or minutes between showing splash page regardless of activity (Force Timeout) for non-voucher access. 1 day=1440.

Require voucher: Require a valid voucher on splash pages. If unchecked, allows you to provide a basic tier of service at the rates and durations above and (optionally) faster service using vouchers or PayPal.

Redirect URL: The page to display after the splash page. Leave blank to display the user's requested page.

Include user data in redirect URL: If set, additional information specific to the request is added as URL parameters when the final redirect occurs. The parameters node mac, client_mac, and client_url will be set to the MAC addresses of the Access Point and Client, and the original request URL, respectively.

Block Unauthenticated Users: Block all ports until a client device has been authenticated. If unchecked, only browsing is blocked. When selected, unauthenticated users trying to access https websites will not be redirected to the splash page.

White List: MAC addresses, one per line that will NOT see the splash page, if enabled. Useful for game consoles that do not have a browser.

Walled Garden: Sites and resources (images and files for the splash page, etc.) users can visit prior to authentication.

Blocked Devices MAC addresses that are blocked from this network.

Blocked Message Message to display on the splash page to users who are blocked

Availability

Schedule WiFi A WiFi schedule allows you to enable or disable each SSID for specific times of the day. The SSID will be enabled or disabled upon checkin to Datto Network Manager, typically within five minutes of the times specified. This schedule will control the SSID only if Enabled for the SSID.

Advanced Settings

Band Steering Attempts to connect clients to the 5Ghz band when possible in order to best utilize available bandwidth. Band Steering is only available when "Band" is set to "Both - Combined SSID".

802.11r Fast BSS transition (FT), attempts to reduce handoff delay in situations where an end device is roaming from one AP to another. This is useful in applications such as VoIP calls that must maintain continuity of connection. This option is only available if the SSID has WPA authentication enabled.

Block LAN Access: Prevents users on this wireless network from accessing your wired LAN.

Client isolation: Prevents your wireless users from being able to access each other's computers and common for public networks. Unchecking this box will allow you to do things like share a printer attached to the network, but will also allow malicious users access to other users on the network. Uncheck this ONLY if you know all users have a firewall enabled on their computers.

DNS Intercept this must be enabled for Alternate DNS, Blocked Devices, Blocked Message and Splash Page functionality to work

SMTP Redirect: Alternate SMTP server IP address for your network. This allows users to send SMTP email by using your ISP's SMTP server.

Alternate DNS: Alternate DNS server IP addresses, one per line, for this SSID. This setting will override your network-wide Alternate DNS settings on this SSID. This allows you to use services such as OpenDNS for content filtering, client tracking and more.

Access Control List: MAC addresses allowed to use this Access Point, one per line. All other users (MAC addresses) will not be able to browse on this access point. Leave blank to allow all MAC addresses (recommended).

Bridge to LAN: Each SSID can be bridged to the LAN for access to local LAN resources.

Bridge to VLAN: Each SSID can be tagged with a number from 2-4094 so you can control traffic flow within your LAN. Using a VLAN automatically bridges the SSID to the LAN.

PayPal Item ID: You can require guests to pay for all service or enhanced service through PayPal.
See the guides at the end of this document.

Configure > Radio

The Radio settings controls network-wide access point settings. The main items you'll want to set are Channels and Internet Check.

Channels: Auto Channel will let Network Manager optimize channel settings daily for your network, taking into consideration mesh repeaters, nearby access points, and sources of interference. Auto Channel respects the Maintenance Window setting in Configure > Maintenance to avoid disruptions during critical times. If Auto is selected then the ability to specify channels, on either a per-network or per-access point basis, is disabled.

Manual lets you specify a single channel per band to use for all access points. You can override individual access points in Manage > Access Points.

Internet Check: When selected, the wireless network will only be available when there is an active Internet connection. This allows access points to recover quickly when they lose a connection and is the recommended setting. When deselected, the wireless network will stay up even when there is no Internet connection. This allows local resources such as printers and shared drives to continue to function, but access points may take longer to recover when they lose a connection.

Configure > Maintenance

Automatic Upgrades: When enabled, your network will automatically upgrade to the latest firmware version as new stable upgrades become available.

Maintenance window: Select the period of time each day when Network Manager can perform maintenance on your network. This maintenance includes firmware upgrades and Auto Channel scanning and configuration.

Configure > Display

The Display section allows you to customize the look and feel of Network Manager, and enable external embeds.

Display Name: Used to display a more descriptive name on reports. When none is entered, the network name will be used.

Update Logo: Load your own logo to replace the Network Manager logo in the top left corner of the application.

Allow Read-Only: Click to enable the password-free read-only view of the network status. When enabled, read-only view can be accessed by entering just the network name in Network Manager without a password. The password will still be required to change any network settings.

Enable 12 Hour Display: Check to display time in 12 hour (am/pm) format.

External embeds: Use the HTML snippet to embed Network Manager reporting pages on an external site like a client portal.

Configure > Advanced

The Advanced Settings page has a variety of settings that most users won't change. This section will touch on the more common settings.

AP Mesh When disabled, this turns off meshing on your APs. Mesh Encryption must be enabled.

Mesh Encryption: Encrypts all mesh traffic with WPA2 protection. Access points not belonging to this network won't be able to join the mesh due to the encryption.

Alternate DNS: Alternate DNS server IP address for your network, such as OpenDNS. OpenDNS provides several additional features such as content filtering that you may find helpful. This setting applies to all SSIDs and can be overridden by setting an Alternate DNS for each individual SSID.

Presence Reporting Settings to configure exporting presence data about wireless clients. Commonly used for location analytics. Note that this feature will be part of a paid package of services in the future. Learn more

Status LED(s) When disabled, this turns off LED lights on your APs

Share Vouchers: When enabled, vouchers created on this network will be usable on all other networks under this account.

Bridge wired clients: When a wired client is connected to an access point, it will use settings from this SSID.

Application Reporting (DPI) Disabling this will cause application data (pie chart and table) in the clients page to not be displayed and application data in the networks overview page to display all traffic as 'unclassified'.

IGMP Proxy When enabled multicast traffic will be allowed over the LAN. When disabled multicast traffic will be blocked from entering the LAN **Roaming VLANs** Provides seamless roaming to all SSIDs that aren't bridged to the LAN. Requires that your Switch already be configured to utilize our VLANs. To learn more about setting this feature up, click here. Not compatible with Client Isolation.

Bridge SSID: Select an SSID to bridge to the LAN. This gives clients access to LAN resources such as file servers and printers, disables NAT and lets your LAN assign all client DHCP addresses. You can bridge additional SSIDs by using a VLAN tag on each SSID settings page.

Delete Network: Select to delete this network from Network Manager.

8. <u>**Configuring a Device for Indoor or Outdoor Installation**</u>

This access point can be configured as an indoor model in addition to an outdoor model and mounted to any wall, ceiling, or pole. When the device is installed indoor, the user should navigate to the specific Access Point management page, and the use can click after reviewing the warning that the device is actually installed indoors. Once that has been processed in the cloud your available 2.4GHz and 5GHz radios should update to the indoor limits to be selected from. This should only be enabled when the device is actually installed indoors.
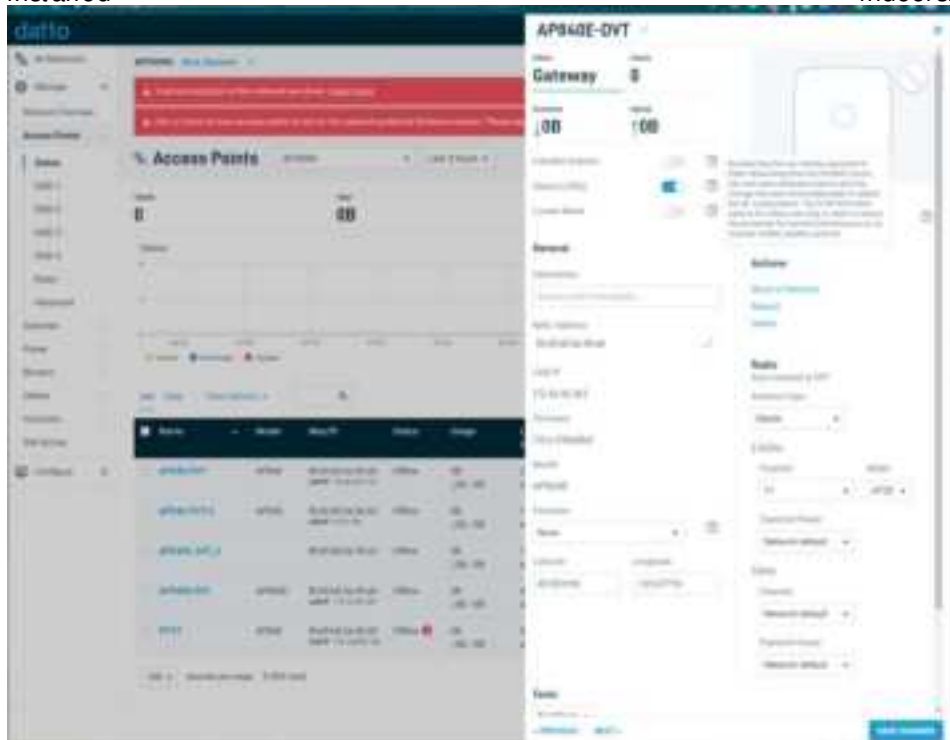
9. <u>Monitoring, Management, and Troubleshooting</u>

With your network running and customized, you can now monitor its usage and status by selecting the Network Status link. Here's an overview of the tools available:

Network Usage graph at the top of the page shows the number of users on SSID#1 and the amount of upload and download traffic.

Node Map shows the nodes relationship to each other on a map.

Node List gives details on each individual node.

Node Outages Chart shows the check-in status of a node using colors.

STATE	COLOR
Cloud check-in succeeded	Solid Teal
IP acquired via DHCP, but inet test is failing	Flash Purple

Users List shows all users connected to the network.

Network Diagram shows how all nodes relate to each other.

STATE	COLOR
Checkin performed, mesh speed <= 2Mbps	Flash Green
Orphan mode	Flash (Yellow), then Green
Lonely mode	Flash (Red), then Green
checkin performed, mesh speed >2Mbps	Solid Green

You can use each of these tools to see how your network is doing and troubleshoot issues.

Troubleshooting in Datto Network Manager

Have you have created a strong, healthy network? While there are plenty of diagnostic tools available, the following two are most telling:

On the Node Outages Chart: dark/light green indicate a gateway/repeater is online and hasn't missed a check-in, yellow indicates a node has lost contact with the mesh and is in lonely/orphan mode, pink is when a node needs re-pairing (update of network settings), and gray indicates it's down, offline or has missed check-ins.

On the Node Map: (click on a node, then select **Neighbors**) all nodes will have at least one

(preferably two) connections with an RSSI of 17 or more. If not, you need to reposition your node closer to the others or in a better line through fewer walls. You may need to add new nodes.

On the Node List: the number of Hops should be three or less (fewer is better). If not, you need to add additional gateways or reposition nodes.

Troubleshooting with your device with lights
The LED on your device can tell you a lot about how that device is functioning. The meaning of the LED light for the AP440 is as follows:

Common States (Gateway and Repeater)

STATE	COLOR
Boot loader	Solid Purple
Booting Up	Solid Yellow
Firmware upgrade (node is executing the firmware upgrade)	Solid Red
Cloud check-in failure	Flash White
Key re-pair	Flash Yellow
Configuration change AP not ready	Solid White
Net failure - no default route	Flash Red

10. Additional Resources

To learn more about planning and optimizing your network, download the Datto Network Planning Guide.

To learn more about Datto's splash page feature, download the Using the Splash Page Editor Guide.

To learn more about Datto's vouchers feature, download the Using Vouchers in Network Manager Guide.

To learn more about integrating vouchers with PayPal, download the Using PayPal in Network Manager Guide.

For any information or datasheets please log into the Datto Partner Portal and view the Corresponding KB articles at help.datto.com

11. Appendix A: FCC Statements
Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 22 cm between the radiator & your body.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Caution: This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This device and it's antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

Devices will not permit operations on channels 120-132 for 11a and 11n/a which overlap the 5600 - 5650 MHz band.

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

Only Trained and Qualified Professionals should be allowed to install, replace or service this equipment. No User-Serviceable parts inside. To Avoid Risk of electric shock, do not open. Installation of the equipment must comply with local and national electrical codes.

FCC Professional Installation Instructions:

1. Installation Personnel
   This product is designed for a specific application and needs to be installed by a qualified professional who has RF and related rule knowledge. The General User shall not attempt to install or change the settings.

2. Installation Location
   The product shall be installed at a location where the radiating antenna can be kept 22 cm away from nearby person in normal operating condition to meet regulatory RF exposure requirements

3. External Antenna
   Use only the antennas which have been approved by the applicant. The non-approved antenna(s) may produce unwanted spurious or excessive RF emissions which may lead to the violation of FCC limit and is prohibited.

4. Installation Procedure
   Please refer to the User's Manual for the installation procedure details

5. Warning
   Please carefully select the installation position and make sure that the final output power does not exceed the limit set in relevant rules. The violation of the rule could lead to serious federal penalty.

12. Appendix B: IC Statements

Canada, Industry Canada (IC) Notices
This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:
(1) This device may not cause interference.
(2) This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :
(1) L'appareil ne doit pas produire de brouillage;
(2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Caution :

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) where applicable, antenna type(s), antenna models(s), and worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in section 6.2.2.3 shall be clearly indicated.

Avertissement:

Le guide d'utilisation des dispositifs pour réseaux locaux doit inclure des instructions précises sur les restrictions susmentionnées, notamment :

(i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) lorsqu'il y a lieu, les types d'antennes (s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3, doivent être clairement indiqués

Radiation Exposure Statement:
This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with greater than 26 cm between the radiator & your body.

Déclaration d'exposition aux radiations:
Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à plus de 26 cm entre le radiateur et votre corps.

Professional installation instruction

1. Installation personal

    This product is designed for specific application and needs to be installed by a qualified personal who has RF and related rule knowledge. The general user shall not attempt to install or change the setting.

2. Installation location

    The product shall be installed at a location where the radiating antenna can be kept 26 cm from nearby person in normal operation condition to meet regulatory RF exposure requirement.

3. External antenna

    Use only the antennas which have been approved by the applicant. The non-approved antenna(s) may produce unwanted spurious or excessive RF transmitting power which may lead to the violation of ISED limit and is prohibited.

4. Installation procedure

    Please refer to user's manual for the detail.

5. Warning

    Please carefully select the installation position and make sure that the final output power does not exceed the limit set force in relevant rules. The violation of the rule could lead to serious federal penalty.

Instructions d'installation professionnelle

1. Installation
   Ce produit est destine a un usage specifique et doit etre installe par un personnel qualifie maitrisant les radiofrequences et les regles s'y rapportant. L'installation et les reglages ne doivent pas etre modifies par l'utilisateur final.

2. Emplacement d'installation
   En usage normal, afin de respecter les exigences reglementaires concernant l'exposition aux radiofrequences, ce produit doit etre installe de facon a respecter une distance de 26 cm entre l'antenne emettrice et les personnes.

3. Antenn externe.
   Utiliser uniiquement les antennes approuvees par le fabricant. L'utilisation d'autres antennes peut conduire a un niveau de rayonnement essentiel ou non essentiel depassant les niveaux limites definis par ISED, ce qui est interdit.

4. Procedure d'installation
   Consulter le manuel d'utilisation.

5. Avertissement
   Choisir avec soin la position d'installation et s'assurer que la puissance de sortie ne depasse pas les limites en vigueur. La violation de cette regle peut conduire a de serieuses penalites federales.

13. Appendix C: Declaration of Conformity

Hereby, Datto, Inc, declares that the radio equipment type AP440 is in compliance with Directive 2014/53/EU issues by the Commission of the European Community. The full text of the EU declaration of conformity is available at the following internet address: help.datto.com

A minimum Separation distance of 20 cm must be maintained between the user's body and the device, including the antenna during body-worn operation to comply with the RF exposure requirements in Europe.

The following Test methods have been applied in order to prove conformity with the essential requirements of the EU Directive 2014/53/EU.

Radio:
- EN 300 328
- EN 301 893

RF Exposure:
- EN 50385
- EN 62311

EMC:
- EN 301 489-1
- EN 301 489-17

Emissions:
- EN 55024
- EN 55032
- EN 55035

Safety:
- EN 62368-1
- EN 60950-22
- IEC 60529
-

14. Appendix D: CE Statements

Simplified EU Declaration of Conformity:

Cesky[Czech]	Datto tímto prohlašuje, že tento bezdrátový přístupový bod AP440 je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53 / EU

Dansk[Danish]	Datto erklærer hermed, at dette trådløse adgangspunkt AP440 er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i direktiv 2014/53 / EU
Deutsch[German]	Hiermit erklärt Datto, dass dieser drahtlose Zugangspunkt AP440 den grundlegenden Anforderungen und anderen relevanten Bestimmungen der Richtlinie 2014/53 / EU entspricht
Eesti[Estonian]	Käesolevaga deklareerib Datto, et see traadita pääsupunkt AP440 on - oluliste nõuete ja muude asjakohaste sätete järgimine Direktiiv 2014/53 / EU
English	Hereby, Datto, declares that this wireless Access Point AP440 is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU
Español[Spanish]	Por la presente, Datto declara que este punto de acceso inalámbrico AP440 cumple con los requisitos esenciales y otras disposiciones relevantes de la Directiva 2014/53 / EU.
Ελληνική [Greek]	Με το παρόν, η Datto, δηλώνει ότι αυτό το ασύρματο σημείο πρόσβασης AP440 συμμορφώνεται με τις βασικές απαιτήσεις και άλλες σχετικές διατάξεις της οδηγίας 2014/53 / EU
Français [French]	Par la présente, Datto déclare que ce point d'accès sans fil AP440 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53 / EU.
Italiano[Italian]	Con la presente, Datto, dichiara che questo Access Point wireless AP440 è conforme ai requisiti essenziali e ad altre disposizioni pertinenti della Direttiva 2014/53 / EU.
Latviski[Latvian]	Ar šo Datto paziņo, ka šis bezvadu piekļuves punkts AP440 atbilst Direktīvas 2014/53 / EU pamatprasībām un citiem attiecīgajiem noteikumiem
Lietuvių[Lithuanian]	Šiuo, Datto pareiškia, kad šis belaidis prieigos taškas AP440 atitinka esminius Direktyvos 2014/53 / ES reikalavimus ir kitas susijusias nuostatas
Nederlands[Dutch]	Hierbij verklaart Datto dat dit draadloze toegangspunt AP440 in overeenstemming is met de essentiële vereisten en andere relevante bepalingen van richtlijn 2014/53 / EU
Malti[Maltese]	Hawnhekk, Datto, jiddikjara li dan il-Punt ta 'Aċċess bla fili AP440 huwa konformi mar-rekwiżiti essenzjali u dispożizzjonijiet rilevanti oħra tad-Direttiva 2014/53 / EU
Magyar[Hungarian]	Ezennel a Datto kijelenti, hogy ez az AP440 vezeték nélküli hozzáférési pont megfelel a 2014/53 / EU irányelv alapvető követelményeinek és egyéb vonatkozó rendelkezéseinek

Polski[Polish]	Niniejszym Datto oświadcza, że ten bezprzewodowy punkt dostępowy AP440 jest zgodny z zasadniczymi wymaganiami i innymi odpowiednimi postanowieniami dyrektywy 2014/53 / EU
Português[Portuguese]	Por meio deste, Datto declara que este Ponto de Acesso sem fio AP440 está em conformidade com os requisitos essenciais e outras disposições relevantes da Diretiva 2014/53 / EU
Slovensko [Slovenian]	Datto izjavlja, da je ta brezžična dostopna točka AP440 v skladu z bistvenimi zahtevami in drugimi ustreznimi določbami Direktive 2014/53 / EU
Slovensky [Slovak]	Týmto spoločnosť Datto vyhlasuje, že tento bezdrôtový prístupový bod AP440 je v súlade so základnými požiadavkami a ďalšími príslušnými ustanoveniami smernice 2014/53 / EÚ.
Suomi [Finnish]	Täten Datto vakuuttaa, että tämä langaton tukiasema AP440 on direktiivin 2014/53 / EU olennaisten vaatimusten ja muiden asiaankuuluvien säännösten mukainen.
Svenska [Swedish]	Härmed förklarar Datto att denna trådlösa åtkomstpunkt AP440 överensstämmer med de väsentliga kraven och andra relevanta bestämmelser i direktiv 2014/53 / EU