

User Guide:

Datto AP840E

Version 0.1

Table of Contents

1. General Warnings	3
2. Product Specifications	4
3. Creating a Network on Network Manager	6
4. Mounting and Installation Instructions	13
5. Configuring a network.....	17
6. Configuring Device for Indoor Use	23
7. Monitoring, Management and Troubleshooting	24
8. Additional Resources.....	26
9. Appendix A: FCC Statement	27
10. Appendix B: IC Statement	28
11. Appendix C: Declaration of Conformity	29
12. Appendix D: CE Statements	30

Warnings

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

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

Thermal Hazard: Exposed Metal heatsink can be hot to the touch. Avoid direct physical contact with the heatsink when system is or has been operating.

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

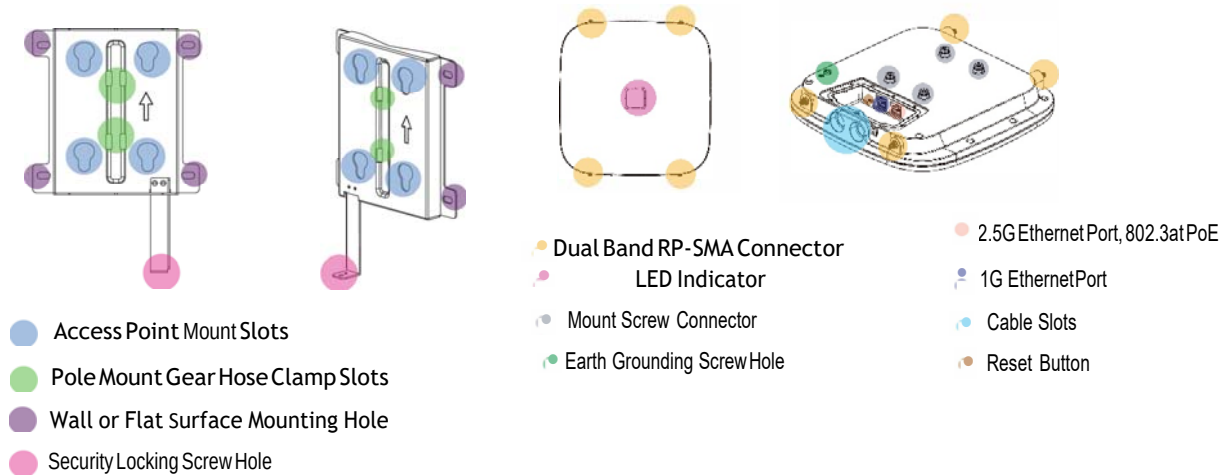
Product Specifications

OFDMA Data rate (aggregate)	3583.9 Mbps (2.4GHz - 1182 Mbps, 5GHz - 2401.9 Mbps)
OFDM Data rate (aggregate)	2333.3 Mbps (2.4GHz - 600 Mbps, 5GHz - 1733.3 Mbps)
Transfer Rate	802.11b: up to 11 Mbps 802.11a/g: up to 54 Mbps 802.11n: up to 600 Mbps 802.11ac: up to 1733.3 Mbps 802.11ax: up to 2401.9 Mbps
Radio	2.4 GHz: 4 stream, 802.11 b/g/n/ax 5 GHz: 4 stream, 802.11 a/b/g/n/ac/ax Scanning Dual Band Radio: 1 Stream Bluetooth Radio: 1 Stream
Antenna	External: 4x Dual Band Dipole RP-SMA, Patch RP-SMA antennas Internal: 1x Scanning Dual band, 1x BLE
OFDM Max users (recommended)	75–150 per AP
OFDMA Max users (recommended)	
WLAN standard	WiF6 - 802.11a/b/g/n/ac/ax
Processor	Quad Core CPU @ 2.2GHz
Memory	1GB DDR4
Ethernet Ports	1 x 2.5 Gigabit Ethernet and 1x 1Gigabit Ethernet
PoE	Standard 802.3af/at* *Difference Performance based on Power Source
DC Power Input	N/A
USB	N/A
Temperature	0–50 C
Installation Location	Outdoors or Indoors
LEDs	Tri-color LED status indicator
Hardware watchdog CPU	Yes
Size	6.5" x 6.5" x 1.2" .9 Lbs
Mounting	solid wall, solid ceiling, Pole
Warranty	Lifetime
Certifications	FCC, IC, CE, RCM

Product Specifications

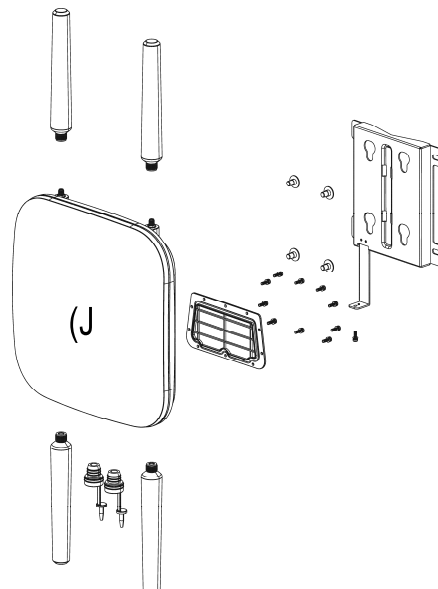
SSIDs	4
SSID to VLAN tagging	Yes
Bridge to LAN	Yes
Seamless roaming	Yes
Cloud management	Yes
Free iOS/Android apps	Yes
Zero config plug and play	Yes
Self-forming, self-healing mesh	Yes
Captive portal w/ bandwidth throttling, splash pages and user controls	Yes

Mount Plate Overview



What's in the Box

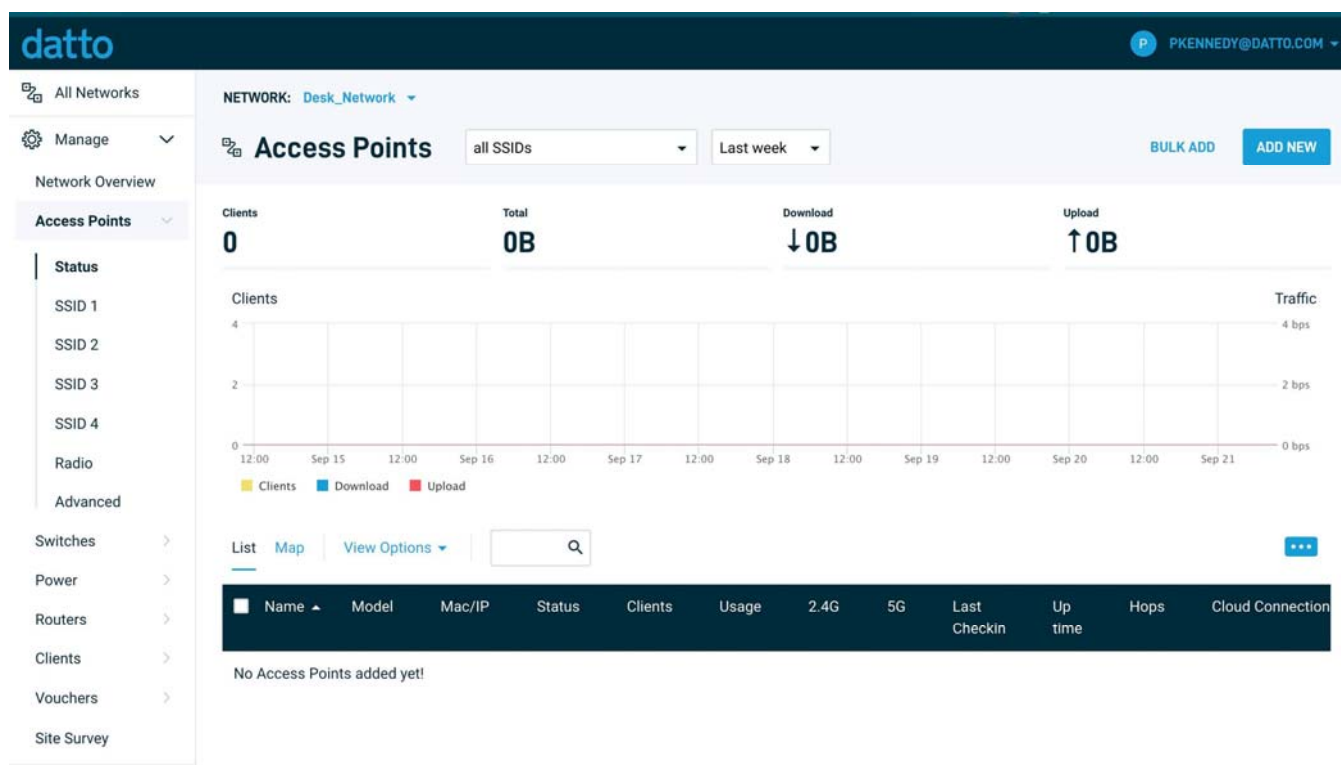
- (1) Access Point
- (4) IP55 Rated Dipole Antennas
- (1) Ruggedized Mounting Plate
- (4) Oversized Mounting Plate Screws
- (1) I/O Shield with Gasket and (10) Screws
- (2) Rubber Cable Fittings
- (1) Locking Screw
- (1) Torque Locking Screw
- (1) Torque Screw Tool
- (1) Grounding Screw
- (4) Wall Mounting Screws with Anchors



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 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).

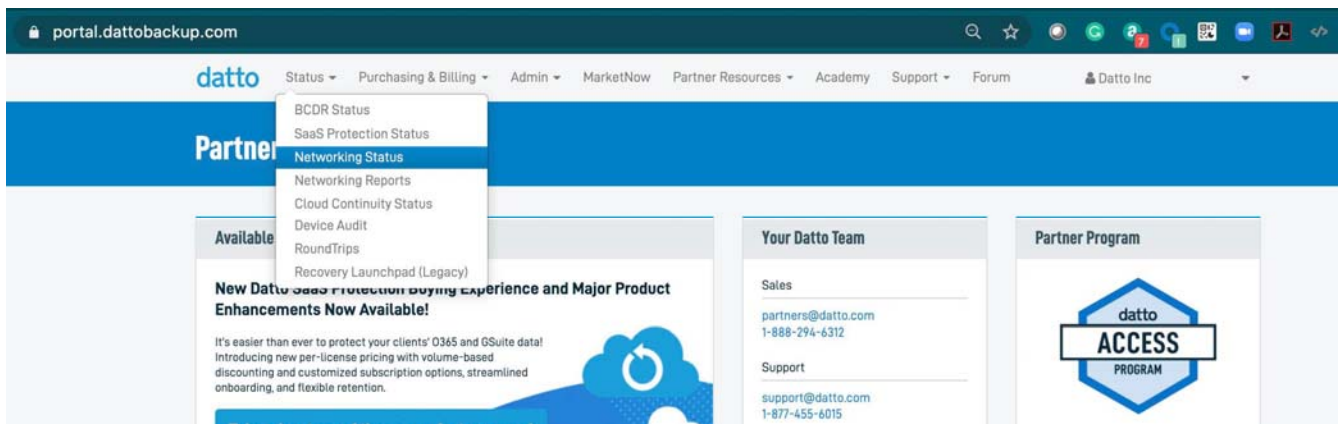
Gateway: A Network Manager-compatible router that is connected to the Internet (usually through a DSL, cable, or LAN connection).

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.

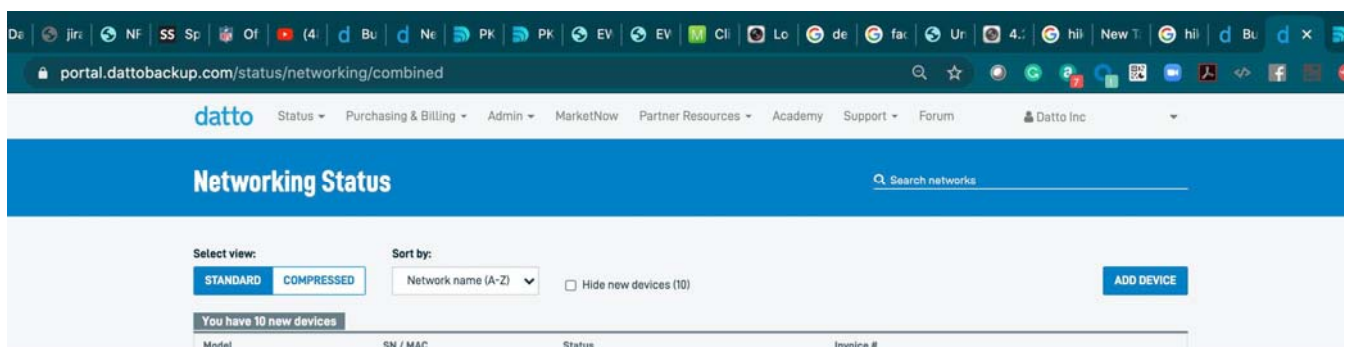
Access point: A generic name for an Network Manager-compatible router/access point which can be either a Gateway or a Repeater. You may also see these called "Nodes."

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

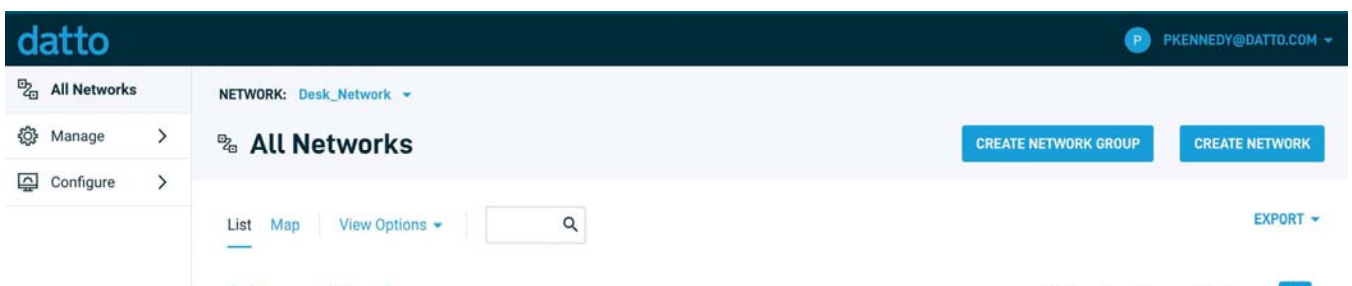
Step 1: Log into the Datto Partner Portal(datto.com) and Navigate to the Network Status Page



Then Select to Add Device, as shown in the Diagram below in the ttop right corner of the screen



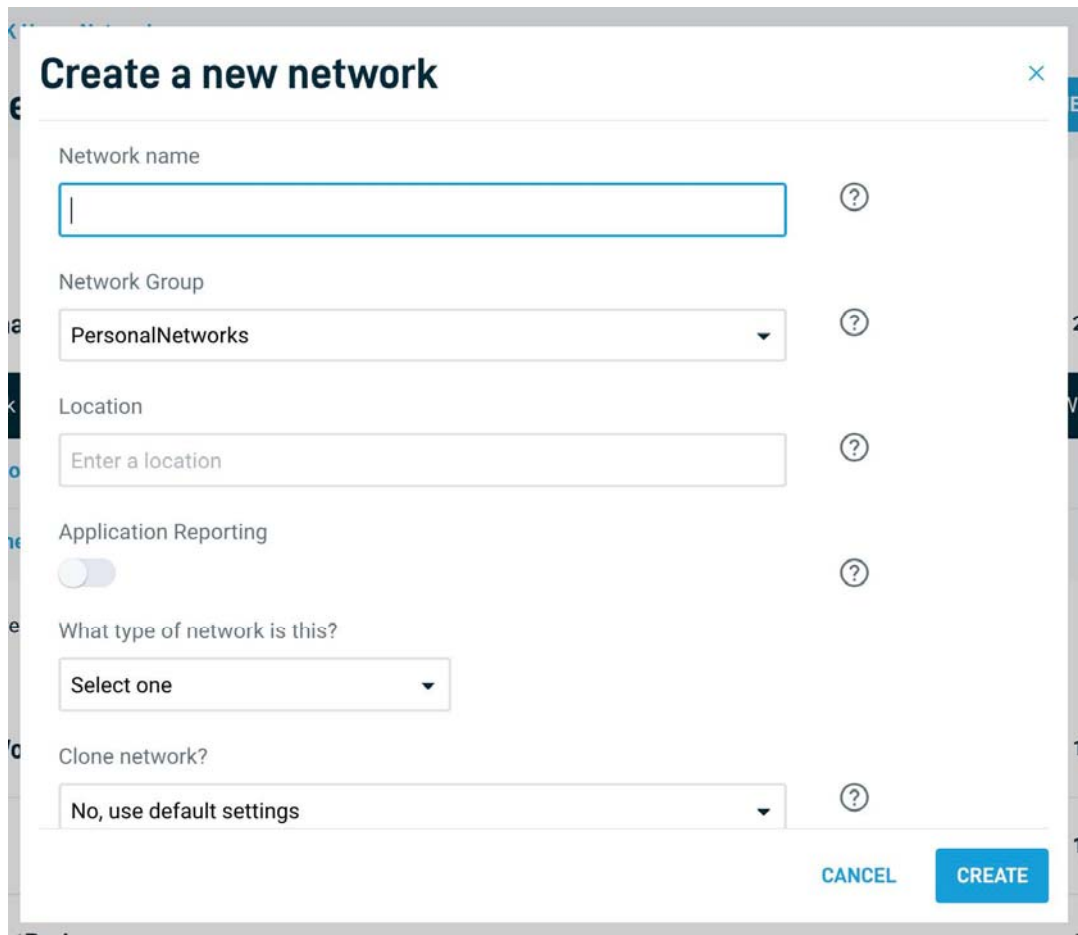
You will now be automatically redirected to the Datto Networking Manager webpage, as seen below:



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.



The screenshot shows a web form titled "Create a new network" with a close button (X) in the top right corner. The form contains several fields, each with a help icon (question mark in a circle) to its right:

- Network name:** A text input field with a cursor inside.
- Network Group:** A dropdown menu currently showing "PersonalNetworks".
- Location:** A text input field with the placeholder text "Enter a location".
- Application Reporting:** A toggle switch currently in the "off" position.
- What type of network is this?:** A dropdown menu currently showing "Select one".
- Clone network?:** A dropdown menu currently showing "No, use default settings".

At the bottom right of the form are two buttons: "CANCEL" and "CREATE".

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.

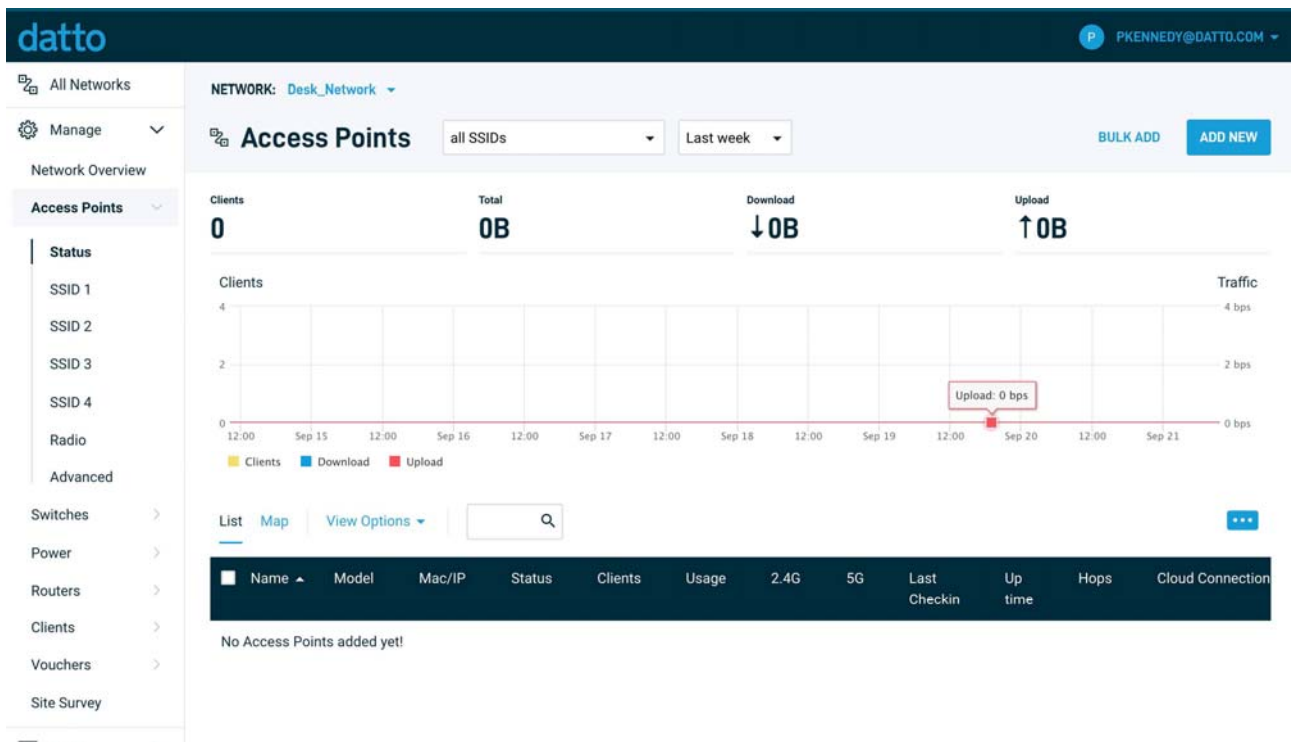
When finished, click "Create" to save your new network settings.

Step 3: Add access points to your network

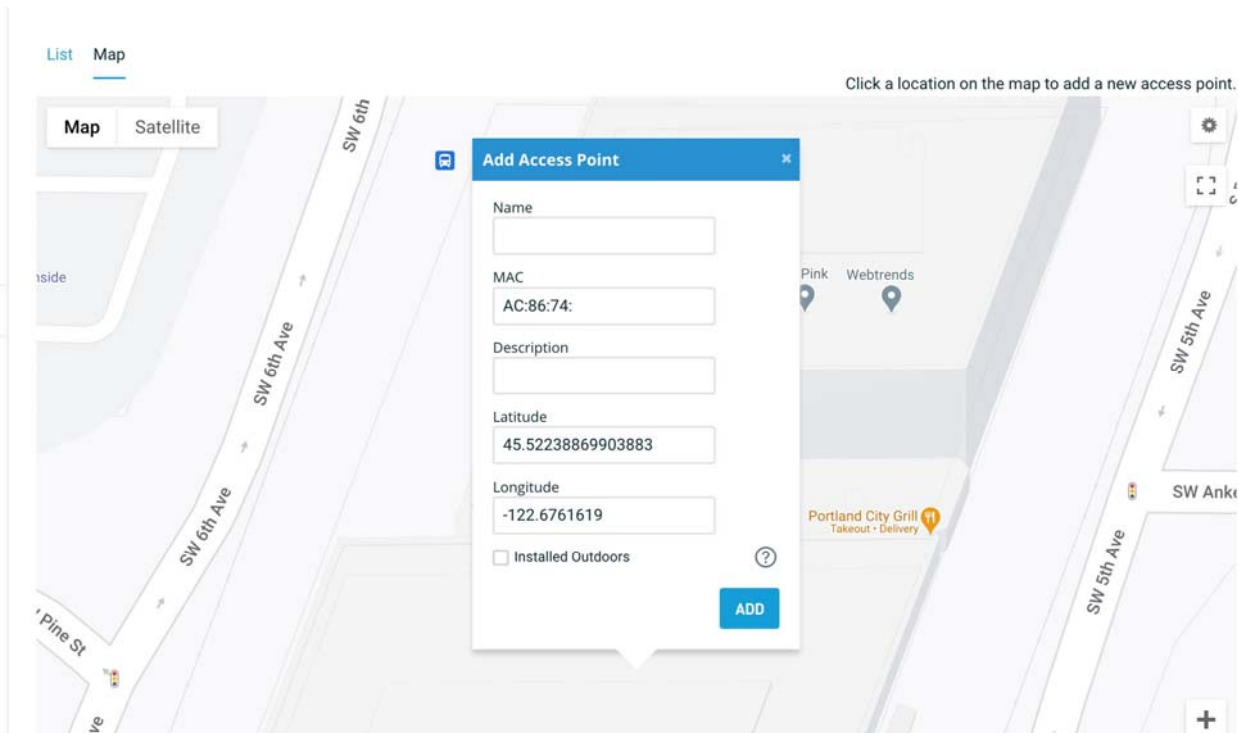
It's time to let Network Manager know which access points you want to include in the network. Adding them to Network Manager will allow you to manage and monitor the access points from anywhere.

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:

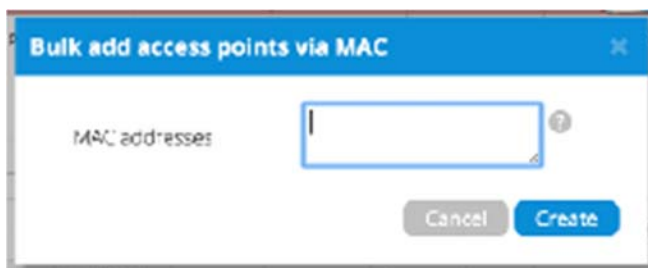
Name: Enter a name for this access point. This name is used to reference its location and will be displayed in reports. It does not affect users.

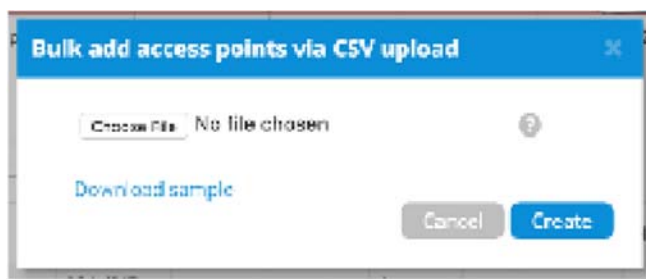
MAC address: A MAC address is a sequence of 12 numbers and the letters A-F often separated by colons (Eg: 00:02:6F:8A:B2:6E). This can be found on a label on the bottom of the router and on the side of the product box.

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:

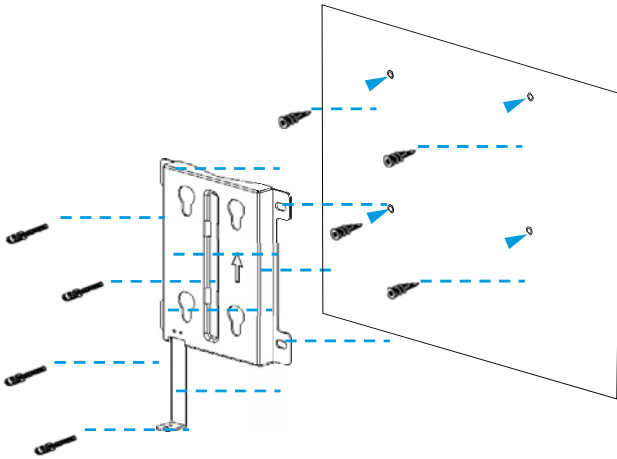
1. Place your gateway in the center of the network. For most devices, every time data is transmitted over one repeater hop, it loses half its speed. A central gateway minimizes the number of hops required.
2. Never go through more than three to four walls or floors.
3. Never go more than 50-150 feet (depending on building materials) between access points.
4. Install no more than about five repeaters to every one 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](#).

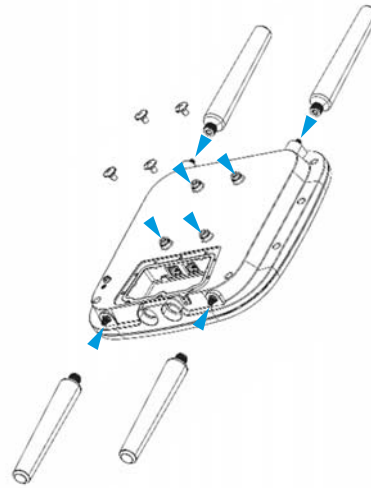
Wall or Solid Ceiling Mount

Attach the universal mounting plate to any solid surface

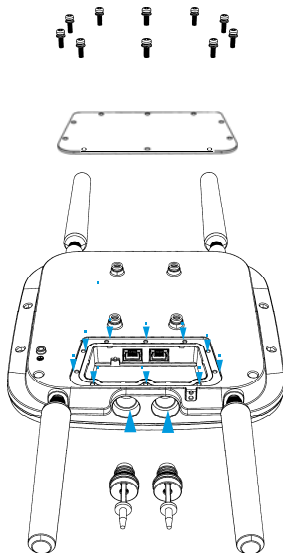
1) Mount flat side of plate to wall or ceiling, arrow on mount pointing up



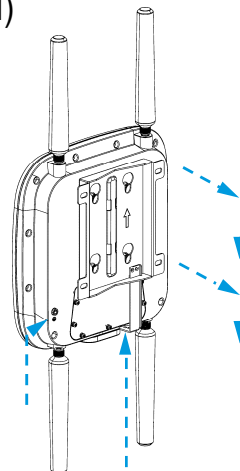
2) Screw Oversized Mount screws into Access Point, Attach antennas and Connect Ethernet cable to 2.5G Ethernet port, with 802.3at PoE source.



3) Wrap Ethernet plug with rubber wraps and insert them into the I/O plugs, Then screw on I/O Cover with gasket.



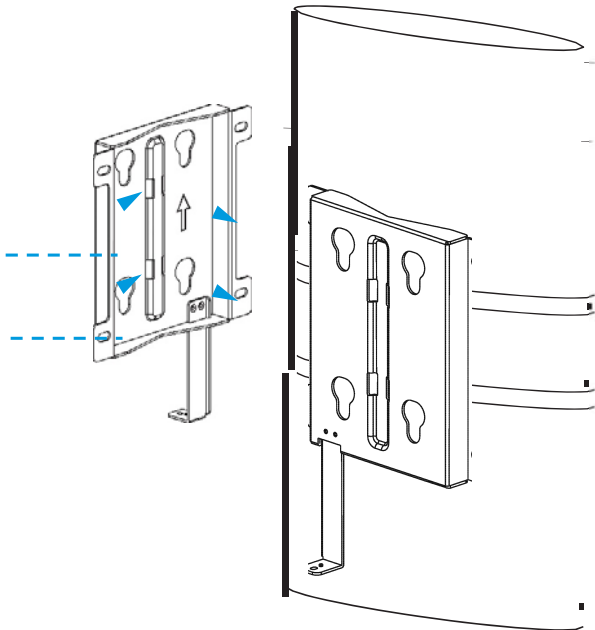
4) Align the 4 oversized screws on the AP with the mount holes and slide down, then screw in security screw and, if needed, grounding cable (Not Included)



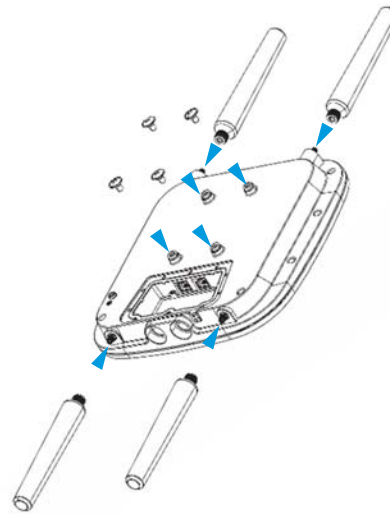
Pole Mount (Components Sold Separately)

For mounting to poles of a variety of diameters

- 1) Place clamp cabling (sold separately) through slots on Mount plate on the angled side

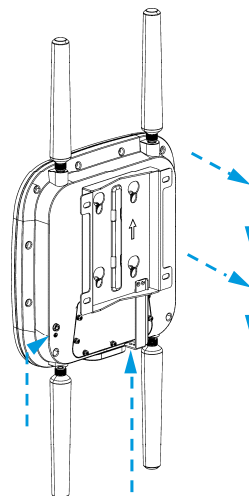
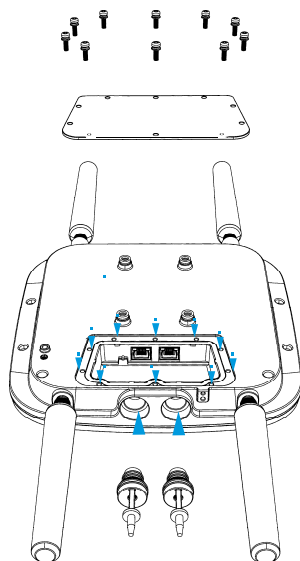


- 2) Screw Oversized Mount screws into Access Point, Attach antennas and Connect Ethernet cable to 2.5G Ethernet port, with 802.3at PoE source.



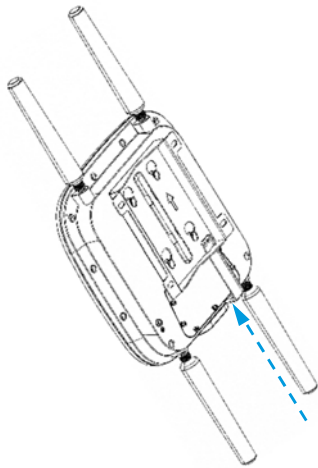
- 3) Wrap Ethernet plug with rubber wraps and insert them into the I/O plugs, Then screw on I/O Cover with gasket.

- 4) Align the 4 oversized screws on the AP with the mount holes and slide down, then screw in security screw and, if needed, grounding cable (Not Included)

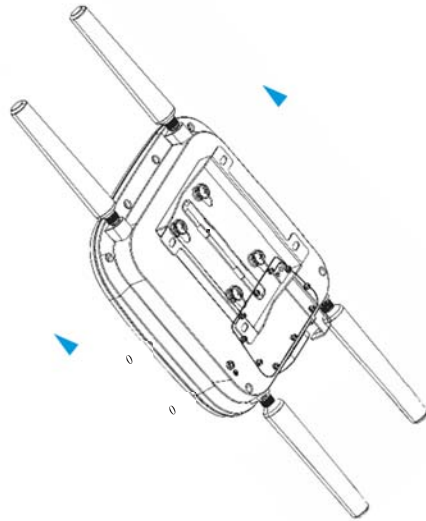


Unmounting Directions

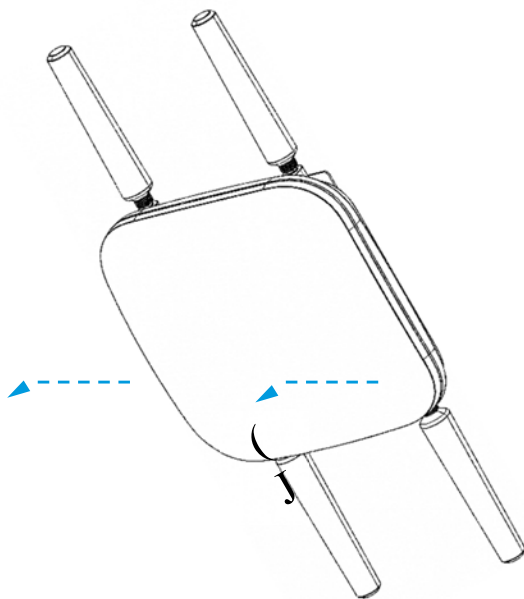
(1) To unlock, remove the security screw connected at the bottom of the mount by the I/O connections



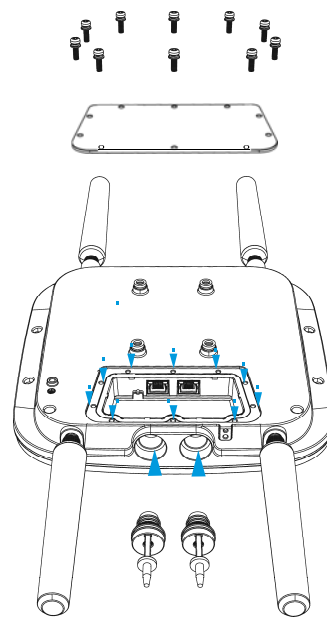
(2) Slide the access point upwards until it disengages from the mounting plate. (Away from I/O)



3) Pull the access point towards the installer

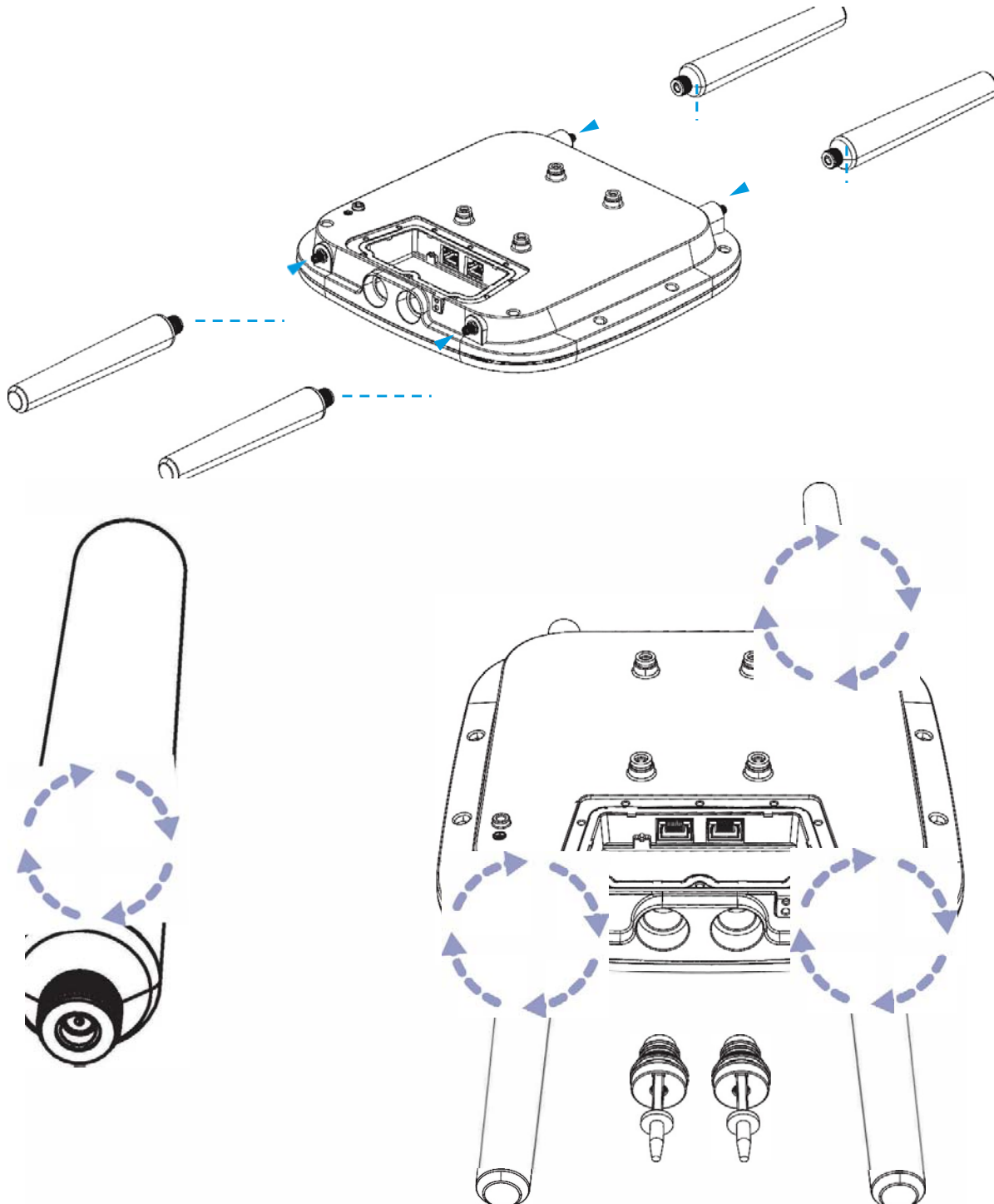


4) remove screws on I/O compartment and remove connections



Installing the Antennas

The antenna connectors all support 2.4GHz and 5GHz Antennas, and datto offers other antenna options as well.



Configuring a Network Manager 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.

How to Install Device indoors

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 user 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.

ONLINE Gateway

2 Clients

1.2GB Download

22.3MB Upload

Access point description...

Model

A42

MAC Address

cc:85:74:ab:74:80

Floorplan

None

LAN IP

192.168.128.5

Mesh IP

5.171.115.128

Firmware

6.4.8 (gg6.4.8)

Latitude

45.57103, -122.6541

Radio

Auto channel is ON

2.4GHz

Channel: 1 Width: HT20

Transmit Power: Network default

5GHz

Channel: 167 Width: VHT80

Transmit Power: Network default

Actions

Alerts

Installed Outdoors

Status LED(s)

Enable this if the access point is installed outdoors and within FCC jurisdiction. Ensures compliance with FCC regulations by reducing power.

1

2



Top: Neighbors

Neighbor	MAC	RSSI (2.4GHz)	RSSI (5GHz)
No neighbors found			

5 records per page. 0 Neighbors total.

< Previous

Next >

Save Changes

Monitoring, Management and Troubleshooting

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 AP840 Series 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

Gateway-Specific States

Repeater-Specific States

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 Indoor Environment:

Appendix A:

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 or more 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 45cm between the radiator & your body.

Non-modification Statement: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the 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.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

This device and its 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.

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

Appendix B: 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 45cm 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 FCC 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.

Appendix C:

Industry Canada Statement

Canada, Industry Canada (IC) Notices

This device complies with Canada licence-exempt RSS standard(s).

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Canada, avis d'Industry Canada (IC)

Cet appareil est conforme avec industrie Canada exemptes de licence RSS standard(s).

Son fonctionnement est soumis aux deux conditions suivantes: (1) cet appareil ne doit pas causer d'interférence et (2) cet appareil doit accepter toute interférence, notamment les interférences qui peuvent affecter son fonctionnement.

Radio Frequency (RF) Exposure Information

The radiated output power of the Wireless Device is below the Industry Canada (IC) radio frequency exposure limits. The Wireless Device should be used in such a manner such that the potential for human contact during normal operation is minimized.

This device has also been evaluated and shown compliant with the IC RF Exposure limits under mobile exposure conditions (antennas are greater than 52cm from a person's body).

Informations concernant l'exposition aux fréquences radio (RF)

La puissance de sortie émise par l'appareil de sans fil est inférieure à la limite d'exposition aux fréquences radio d'industrie Canada (IC). Utilisez l'appareil de sans fil de façon à minimiser les contacts humains lors du fonctionnement normal.

Ce périphérique a également été évalué et démontre conforme aux limites d'exposition aux RF d'IC dans des conditions d'exposition à des appareils mobiles (antennes sont supérieures à 52cm à partir du corps d'une personne).

This radio transmitter [**IC: 23500-DNWAP840E**] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Le présent émetteur radio [**IC: 23500-DNWAP840E**] a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

Approved antenna(s) list :

Manufacturer	Model	Antenna Type	Max Gain (dBi)	Impedance (Ω)
Nienyi	NYS4436	Dipole	3.5 (2.4~2.4835GHz) 6.5 (5.15~5.85GHz)	50
TerraWave	M6060060MP1D43620	Patch	6(2.4~2.4835GHz) 6(5.15~5.85GHz)	50

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) for devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit;

(iii) for devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate;

(iv) 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) pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e;

(iii) pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée, selon le cas;

(iv) 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.

Appendix D: 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 52cm 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 52 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 defines 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 dépasse pas les limites en vigueur. La violation de cette règle peut conduire à de sérieuses pénalités fédérales.

For Outdoor Environment:

Appendix E:

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 or more 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 45cm between the radiator & your body.

Non-modification Statement: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the 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 its 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.

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

Appendix F: 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 45cm 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 FCC 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.

Appendix G:

Industry Canada Statement

Canada, Industry Canada (IC) Notices

This device complies with Canada licence-exempt RSS standard(s).

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Canada, avis d'Industry Canada (IC)

Cet appareil est conforme avec industrie Canada exemptes de licence RSS stanard(s).

Son fonctionnement est soumis aux deux conditions suivantes: (1) cet appareil ne doit pas causer d'interference et (2) cet appareil doit accepter toute interference, notamment les interferences qui peuvent affecter son fonctionnement.

Radio Frequency (RF) Exposure Information

The radiated output power of the Wireless Device is below the Industry Canada (IC) radio frequency exposure limits. The Wireless Device should be used in such a manner such that the potential for human contact during normal operation is minimized.

This device has also been evaluated and shown compliant with the IC RF Exposure limits under mobile exposure conditions (antennas are greater than 52cm from a person's body).

Informations concernant l'exposition aux frequences radio (RF)

La puissance de sortie emise par l'appareil de sans fil est inferieure a la limite de'exposition aux frequences radio d'industry Canada (IC). Utilisez l'appareil de sans fil de facon a minimiser les contacts humains lors du fonctionnement normal.

Ce peripherique a egalement ete evalue et demontre conforme aux limites d'exposition aux RF d'IC dans des conditions d'exposition a des appareils mobiles (antennes sont superieures a 52cm a partirdu corps d'une personne).

This radio transmitter [**IC: 23500-DNWAP840E**] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Le présent émetteur radio [**IC: 23500-DNWAP840E**] a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

Approved antenna(s) list :

Manufacturer	Model	Antenna Type	Max Gain (dBi)	Impedance (Ω)
Nienyi	NYS4436	Dipole	3.5 (2.4~2.4835GHz) 6.5 (5.15~5.85GHz)	50
TerraWave	M6060060MP1D43620	Patch	6(2.4~2.4835GHz) 6(5.15~5.85GHz)	50

Caution :

- (i) for devices with detachable antenna(s), the maximum antenna gain permitted for devices in the bands 5250-5350 MHz and 5470-5725 MHz shall be such that the equipment still complies with the e.i.r.p. limit;
- (ii) for devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits as appropriate;
- (iii) 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) pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis pour les dispositifs utilisant les bandes de 5 250 à 5 350 MHz et de 5 470 à 5 725 MHz doit être conforme à la limite de la p.i.r.e;
- (ii) pour les dispositifs munis d'antennes amovibles, le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5 725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée, selon le cas;
- (iii) 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.

Appendix H:

Instructions d'installation professionnelle

1.) Installation

Ce produit est destiné à un usage spécifique et doit être installé par un personnel qualifié maîtrisant les radiofréquences et les règles s'y rapportant. L'installation et les réglages ne doivent pas être modifiés par l'utilisateur final.

2.) Emplacement d'installation

En usage normal, afin de respecter les exigences réglementaires concernant l'exposition aux radiofréquences, ce produit doit être installé de façon à respecter une distance de 52cm entre l'antenne émettrice et les personnes.

3.) Antenne externe.

Utiliser uniquement les antennes approuvées par le fabricant. L'utilisation d'autres antennes peut conduire à un niveau de rayonnement essentiel ou non essentiel dépassant les niveaux limites définies par ISED, ce qui est interdit.

4.) Procédure 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 dépasse pas les limites en vigueur. La violation de cette règle peut conduire à de sérieuses pénalités fédérales.

Appendix I:

EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

Safety

- EN 60950-1: 2006
- EN 60950-1/A1: 2010
- EN 60950-1/A11: 2009
- EN 60950-1/A12: 2011
- EN60950-1/A2:2013

MPE

- EN 50385:2002
Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

Radio

- EN 300 328 V1.9.1:2015
Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2.4GHz ISM band and using wide band modulation techniques; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive

EMC

- EN 301 489-1 V1.9.2:2011
Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- EN 301 489-17 V2.2.1:2012
Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment; Part 17: Specific conditions for Broadband Data Transmission Systems

Appendix J:

C € 0560

 Český [Czech]	<i>Datto</i> tímto prohlašuje, že tento [<i>typ zařízení</i>] je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
 Dansk [Danish]	Undertegnede <i>Datto</i> erklærer herved, at følgende udstyr [<i>udstyrets typebetegnelse</i>] overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
 Deutsch [German]	Hiermit erklärt <i>Datto</i> , dass sich das Gerät [<i>Gerätetyp</i>] in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
 Eesti [Estonian]	Käesolevaga kinnitab <i>Datto</i> seadme [<i>seadme tüüp = type of equipment</i>] vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
 English	Hereby, <i>Datto</i> , declares that this <i>wireless router</i> is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
 Español [Spanish]	Por medio de la presente <i>Datto</i> declara que el [<i>clase de equipo</i>] cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
 Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ <i>Datto</i> ΔΗΛΩΝΕΙ ΟΤΙ [<i>type of equipment</i>] ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EK.
 Français [French]	Par la présente <i>Datto</i> déclare que l'appareil [<i>type d'appareil</i>] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
 Italiano [Italian]	Con la presente <i>Datto</i> dichiara che questo [<i>tipo di apparecchio</i>] è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo <i>Datto</i> deklarē, ka [<i>type of equipment / iekārtas tips</i>] atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo <i>Datto</i> deklaruoja, kad šis [<i>equipment type</i>] atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
 Nederlands [Dutch]	Hierbij verklaart <i>Datto</i> dat het toestel [<i>type van toestel</i>] in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
 Malti [Maltese]	Hawnhekk, <i>Datto</i> jiddikjara li dan [<i>il-mudel tal-prodott</i>] jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Direttiva 1999/5/EC.
 Magyar [Hungarian]	Alulírott, <i>Datto</i> nyilatkozom, hogy a [<i>... típus</i>] megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.

 Polski [Polish]	Niniejszym <i>Datto</i> oświadcza, że <i>[nazwa wyrobu]</i> jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
 Português [Portuguese]	<i>Datto</i> declara que este <i>[tipo de equipamento]</i> está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
 Slovensko [Slovenian]	<i>Datto</i> izjavlja, da je ta <i>[tip opreme]</i> v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
 Slovenský [Slovak]	<i>Datto</i> týmto vyhlasuje, že <i>[typ zariadenia]</i> spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
 Suomi [Finnish]	<i>Datto</i> vakuuttaa täten että <i>[type of equipment = laitteen tyyppimerkintä]</i> tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
 Svenska [Swedish]	Härmed intygar <i>Datto</i> att denna <i>[utrustningstyp]</i> står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.