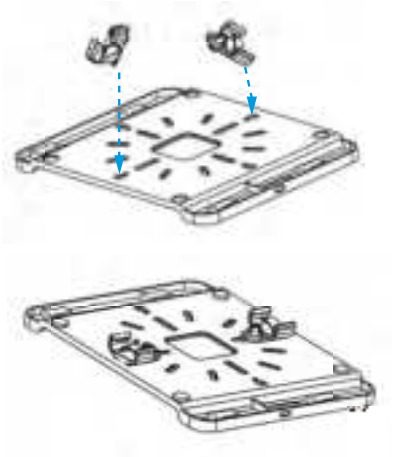
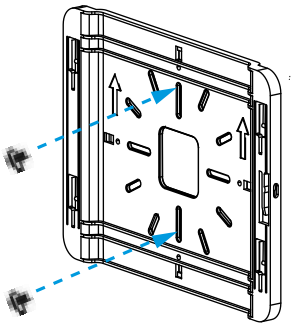
T-Rail Ceiling Mount

For attaching to drop ceiling T-Rail or other T-Rail System.

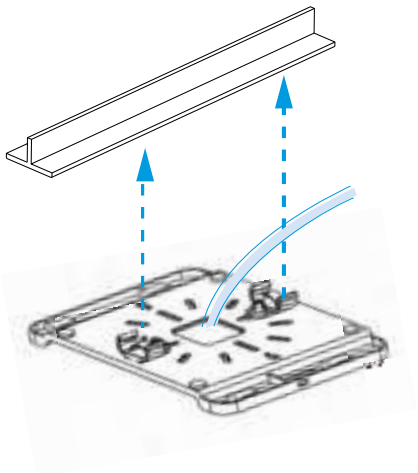
1)Place Desired T-Rail clip set into mounting plate. clips facing away from each other then lay flat



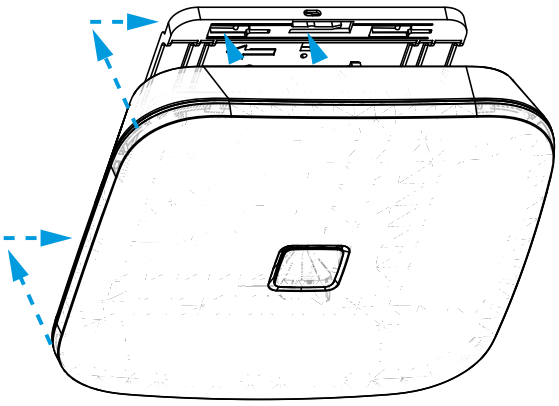
2) Flip over Mount and Screw in screws toto T-Rail Clips



3) Install the mounting plate on the T-rail by tightening both sides until secure



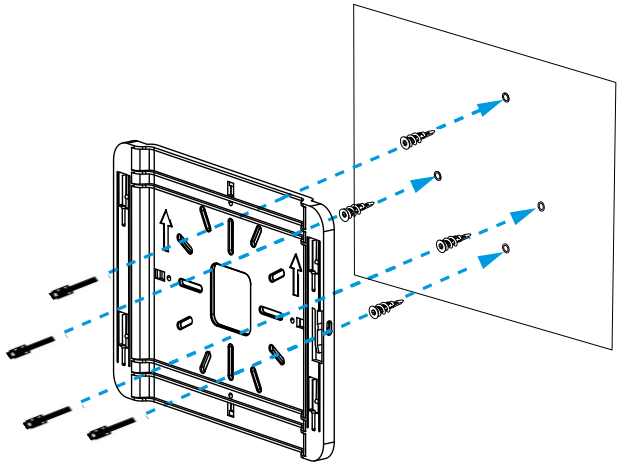
4) Align the 4 posts on the AP with the plate then Slide device toward I/O Ports to lock in place.



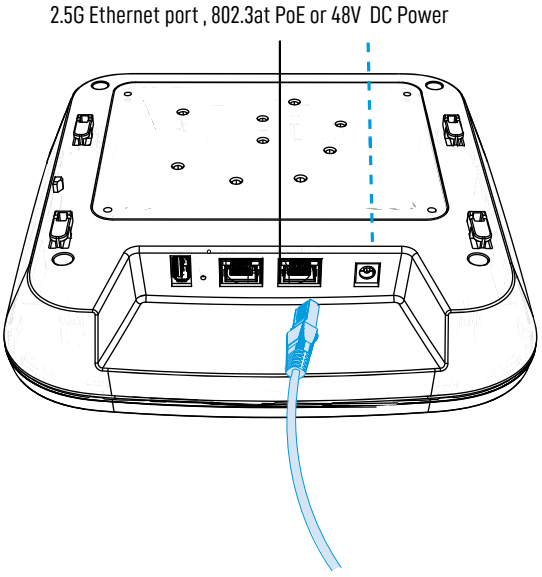
Wall or Solid Ceiling Mount

Attach the universal mounting plate to any solid surface

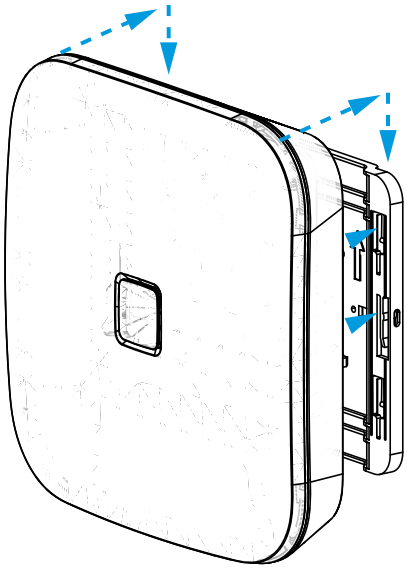
1) Mount flat side of plate to wall or ceiling.



2) Connect ethernet cable to device (2.5G Ethernet)



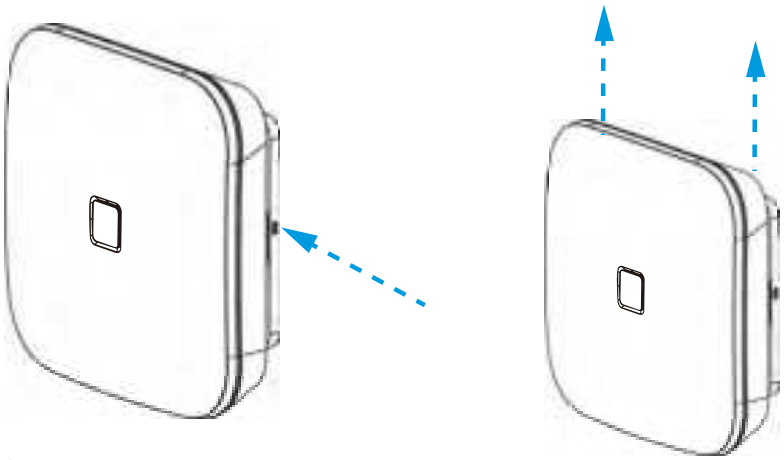
3) Align the 4 posts on the AP with the plate then Slide device toward I/O Ports to lock in place.



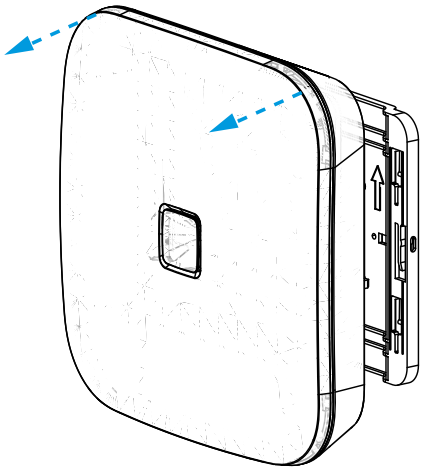
Unmounting Directions

(1) To unlock, insert a small, flat screwdriver into the Mount Release Hole on the side of the mounting plate.

(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 and disconnect cables



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. 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 Datto, 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, 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 Datto 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.

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

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.

Appendix A:

FCC Professional Installation Instruction

1. Installation Personnel

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 44 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 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 B:

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 44cm 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.

Operational Frequency Ranges: Operation in the 5.15-5.25 Hz band are restricted to indoor Usage only. Devices will not permit operations on channels 120-132 for 11a and 11n/a which overlap the 5600-5650MHz band.

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.

Appendix C:
IC Professional Installation Instruction

1. Installation Personnel

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 52 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.

IC 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 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.

Appendix D:

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 apparel 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 fonctionment.

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

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 partir du corps d'une personne).

Appendix E:
EU Declaration of Conformity

Hereby, Datto, Inc, declares that the radio equipment type AP840 is in compliance with Directive 2014/53/EU issues by the Commission of the European Community. The full text of thje EU declaration of conformity is available at the following internet address: kb.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.

Safety
- EN 62368-1

Radio
- EN 300 328 V2.1.1
- EN 301 893 v2.1.1

MPE
- EN 62311
- EN 50385:2002

EMC
- EN 301 489-1 V2.1.1
- EN 301 489-17 V2.2.1
- EN 55032
- EN 55024
- EN 55035

Frequency Range (MHz)	Mean E.I.R.P Limit (dBm)	Mean E.I.R.P Density Limit (dBm/MHz)
2412 to 2462	20	10
5150 to 5350*	23	10
5470 to 5725*	30 (see note)	17 (see note)
5745 to 5825**	30	50

* Secondary devices without radar interference detection shall comply with the limits for the 5250 MHz-5350 MHz frequency range. Operations in the 5.15-5.35GHz band are restricted to indoor usage only.
**Only where permitted by governing body.

Channels are selected uniformly and randomly among all channels available in the operating country or all channels of the selected subband using the systems random number generator. Previously detected unavailable channels are excluded from the selection. This applies for channels selected after a radar event (channel switch), and the initial channel. The user may override the initial channel using the user interface.

Appendix F:

CE 0560

Česky [Czech]	Datto tímto prohlašuje, že tento bezdrátový přístupový bod AP840 je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53 / EU
Dansk [Danish]	Datto erklærer hermed, at dette trådløse adgangspunkt AP840 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 AP840 den grundlegenden Anforderungen und anderen relevanten Bestimmungen der Richtlinie 2014/53 / EU entspricht
Eesti [Estonian]	Käesolevaga deklareerib Datto, et see traadita pääsupunkt AP840 on - oluliste nõuete ja muude asjakohaste sätete järgimine Direktiiv 2014/53 / EU
English	Hereby, *Datto,* declares that this *wireless Access Point AP840* 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 AP840 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 AP840 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 AP840 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 AP840 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 AP840 atbilst Direktīvas 2014/53 / EU pamatprasībām un citiem attiecīgajiem noteikumiem
Lietuvių [Lithuanian]	Šiuo, Datto pareiškia, kad šis belaidis prieigos taškas AP840 atitinka esminius Direktyvos 2014/53 / ES reikalavimus ir kitas susijusias nuostatas
Nederlands [Dutch]	Hierbij verklaart Datto dat dit draadloze toegangspunt AP840 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 AP840 huwa konformi mar-rekwiżiti essenzjali u dispożizzjonijiet rilevanti oħra tad-Direttiva 2014/53 / EU
Magyar [Hungarian]	Ezennel a Datto kijelenti, hogy ez az AP840 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 AP840 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 AP840 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 AP840 v skladu z bistvenimi zahtevami in drugimi ustreznimi določbami Direktive 2014/53 / EU
Slovensky [Slovak]	Týmto spoločnosť Datto vyhlasuje, že tento bezdrôtový prístupový bod AP840 je v súlade so základnými požiadavkami a ďalšími príslušnými ustanoveniami smernice 2014/53 / EÚ.
Suomi [Finnish]	Täten Datto vakuuttaa, että tämä langaton tukiasema AP840 on direktiivin 2014/53 / EU olennaisten vaatimusten ja muiden asiaankuuluvien säännösten mukainen.
Svenska [Swedish]	Härmed förklarar Datto att denna trådlösa åtkomstpunkt AP840 överensstämmer med de väsentliga kraven och andra relevanta bestämmelser i direktiv 2014/53 / EU