



MAST DIGITAL AC50 Wi-Tek Smart Cloud Cube Mini AP Controller User Guide

[Home](#) » [MAST DIGITAL](#) » MAST DIGITAL AC50 Wi-Tek Smart Cloud Cube Mini AP Controller User Guide 



Wi-Tek AC50 Cloud Cube Configuration

This guide will run through how to configure Wi-Tek Access Points via the WI-AC50 Cloud Cube Controller and setup of the remote tunnel link via the Wi-Tek Cloud portal for remote management.

In this guide we will be configuring the WI-AP217-3PBUN which includes the following items:

- 3x WI-AP217 Dual band 1200Mbps 802.11ac Access Points
- 1x WI-PS305G 4 Port GB PoE Switch
- 1x WI-AC50 Cloud Cube



Note: The following steps will apply to each bundle except for the 5Ghz band configuration with the WI-AP210 bundles as these are 2.4Ghz only.

Contents

- [1 Initial Connection](#)
- [2 Documents / Resources](#)
- [3 Related Posts](#)

Initial Connection

We recommend laying everything out locally during the initial configuration, this will make troubleshooting any issues a lot easier.

All Wi-Tek devices come set with a fallback IP of **'192.168.1.88'** – This is used if there is no network router with DHCP connected or if DHCP fails to issue an IP address to each device.

If you are connecting all the devices to the switch in one go, make sure you are also connected to the network router, you will end up with IP conflicts otherwise. You will need to use an IP scanner to find the DHCP issued IP address of the WI-AC50 Cloud Cube.

If you are setting up without a network router, ensure you only connect one device at a time and change the devices IP address before doing any configuration. This will also require setting your laptop to a static IP address, more on this below.



In this guide we will be configuring without the use of a network router.

Step 1 – Connecting the Cube and Laptop

Simply connect the WI-AC50 Cloud Cube to a PoE port on the switch via the included patch lead and connect your laptop to one of the uplink ports.

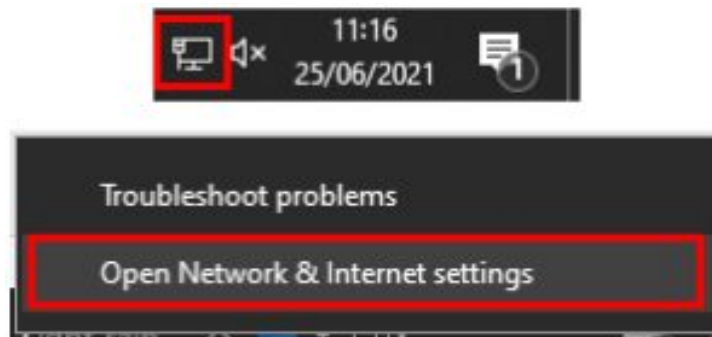


Now we need to set our laptop to a static IP address to be able to communicate with the cube.

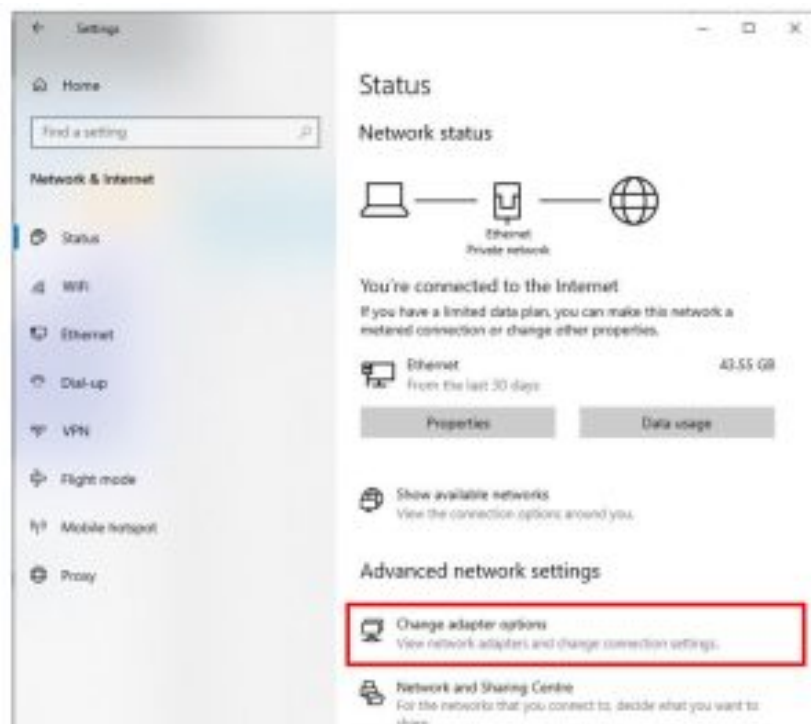
Step 2 – Putting your laptop on a Static IP

Now we have everything connected and powered on, to be able to talk to the AP we need to set our laptop on a static IP address in the same range.

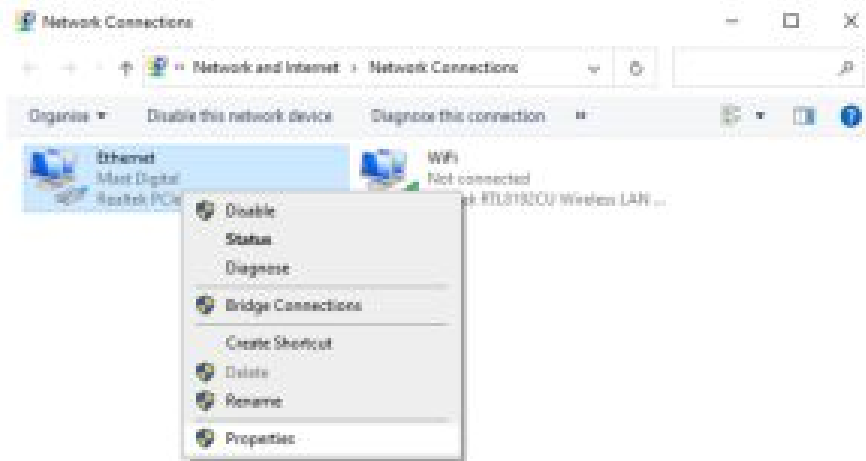
To do this, right click on the network icon in the bottom right and click 'Open Network & Internet Settings'



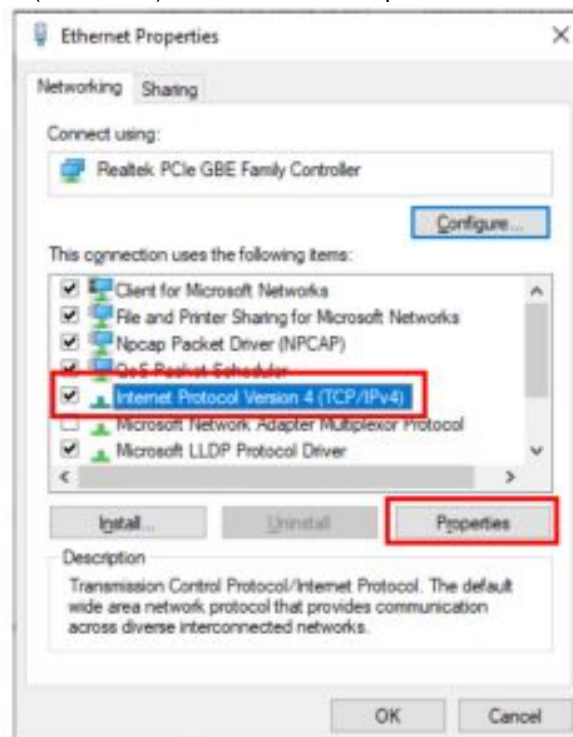
From here select 'Change adapter options'



From here right click your Ethernet adapter and select 'Properties'.



Select 'Internet Protocol Version 4 (TCP/IPv4)' and click the 'Properties' button.



Select 'Use the following IP address:' and enter the following details.



Click 'OK' and then 'CLOSE'.

Your laptop is now set on a static IP address in the same range as the access points and cloud cube controller.

Note: If the network the system is going to be installed in is not on the '192.168.1.x' range, for example Sky / Virgin that use '192.168.0.x', once you have changed all the devices into this range you will need to re-adjust your laptop to be in the same range to continue configuration.

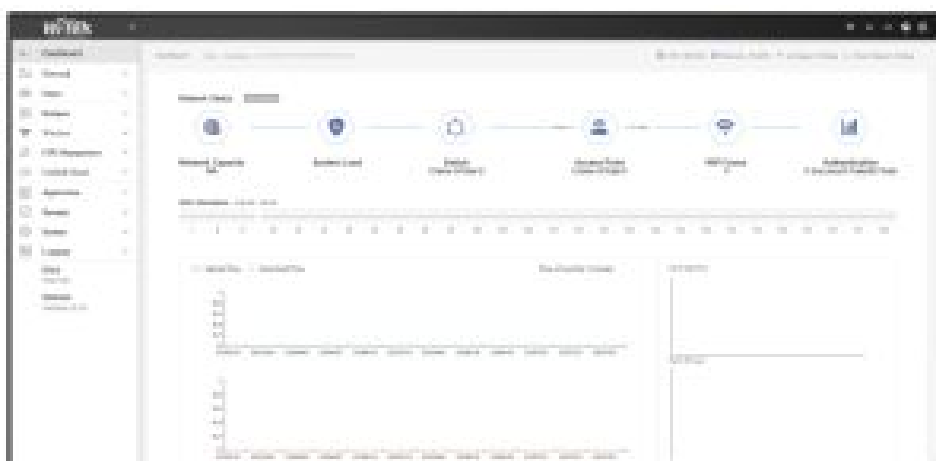
Step 3 – Logging into the Controller

Open Internet Explorer and enter '192.168.1.88' into the address bar. This will take you to the login page of the controller.

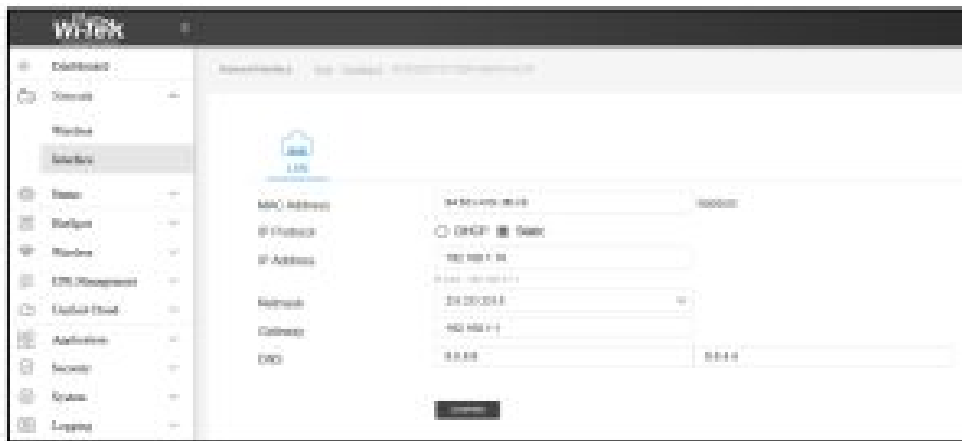
The image shows the login page for the Wi-Tek Communication Solution. It has a dark grey background with the Wi-Tek logo at the top. Below the logo are three input fields: 'Username' with a user icon, 'Password' with a lock icon, and a language dropdown menu currently set to 'English (US)'. To the right of the language dropdown is a link that says 'FORGOT PASSWORD?'. At the bottom is a large blue button labeled 'LOG IN'.

The default username & password is **admin/admin**

You will now be at the dashboard of the controller.



From here the first thing we need to do is change the IP of the cube. To do this, navigate to Network > Interface. Change the IP of the unit to the desired IP, preferably outside of the site networks DHCP range. In this case I have set it to '192.168.1.10'.



Click '**CONFIRM**' to save.

NOTE: Once the IP is changed you will need to navigate to the new IP address and log back into the Cube.

Step 4 – Configure the AC50 Global Parameters

Navigate to Wireless > Overview. From here we can setup a few options on how we want the AC50 Controller to manage the Access Points.

To be able to control the access points they need to know where the AC50 is, to do this we set the Distribute AC Address to Using LAN IP. This will ensure the cube issues its IP to each access point that is connected.

Enable AC-AP Time Sync – This will make sure all the access points are set to the same time & date as the Cube.
 Enable AP Auto Upgrade – This will enable you to remotely upload firmware to the AC50 for it to distribute to the connected access points.

Enable AP Scheduled Reboot – Most WiFi related issues are fixed by a quick reboot, set a Daily / Weekly / Monthly time & day to automatically reboot the WiFi to avoid having to do manual reboots. At minimum we recommend setting this to once a month.

Enable AC Scheduled Reboot – Same as the above but for the controller.

Enable Wireless Optimization – This enables the controller to manage the signal channels from the access points to give optimal performance.

AP Watchdog – This enables you to set an IP of one of the access points, if this IP is unable to be found the APs will start to emit a Rescue SSID for diagnosis.

Set the Country for All AP to United Kingdom.

Once complete you should have something that looks similar to below.

Access Controller	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Distribute AC Address	<input type="radio"/> Disabled <input checked="" type="radio"/> Using LAN IP <input type="radio"/> Custom AC Address
Distribute IP of LAN ports as the AC address	
AC-AP Time Sync	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Auto Upgrade	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Scheduled Reboot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Weekly
	Monday
AP Scheduled Reboot Time	04:30
AC Scheduled Reboot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Weekly
	Monday
AC Scheduled Reboot Time	04:00
Wireless Optimization	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Watchdog	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Country For All AP	United Kingdom
CONFIRM	

Click **CONFIRM** to save.

Navigate to System > System Time and set the correct time and date.

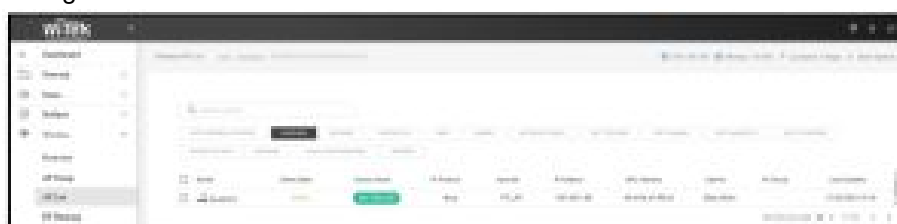
System Time	2021/07/13 16:23:42	
	Sync System Time	
NTP Service	<input checked="" type="checkbox"/> Enable NTP	
Time Zone	Europe/London	
Time Server 1	0.pool.ntp.org	Sync Now
Time Server 2	1.pool.ntp.org	Sync Now
Time Server 3	2.pool.ntp.org	Sync Now
Time Server 4	3.pool.ntp.org	Sync Now
CONFIRM		

Click **CONFIRM** to save.

Step 5 – Connecting the Access Points

Connect the first access point to the PoE switch and wait for it to boot.

From the controller navigate to Wireless > AP List.



Once the AP appears in the list select the tick box and click 'Network Config'. Change the Network Mode to Static IP Address and enter the new desired IP and network details.



Network Config

Network Mode: Static IP Address

IPv4 Address: 192.168.1.20

IPv4 Netmask: 255.255.255.0

IPv4 Gateway: 192.168.1.1

DNS: 8.8.8.8

CONFIRM
CANCEL

Click '**CONFIRM**' to push the new settings to the AP.

Repeat this process for each Access Point until all are configured with the desired IP Addresses. You may also want to rename each access point to make it easier to differentiate between them. For example, Master Bedroom, Kitchen, Lounge etc.

AP	AP Name	AP Type	AP Model	AP IP	AP Subnet	AP Gateway	AP DNS	AP Status
<input checked="" type="checkbox"/>	ap1	Static	Static	192.168.1.20	255.255.255.0	192.168.1.1	8.8.8.8	Online
<input checked="" type="checkbox"/>	ap2	Static	Static	192.168.1.21	255.255.255.0	192.168.1.1	8.8.8.8	Online
<input checked="" type="checkbox"/>	ap3	Static	Static	192.168.1.22	255.255.255.0	192.168.1.1	8.8.8.8	Online

Step 6 – Configuring the WiFi Group Settings

Navigate to AP Group and click Edit for the default group. From here we can set the desired SSID and password details for both 2.4G and 5G signals.

Group Name: default

2.4G 5G

Wireless Template Configuration

SSID: WIFI_2.4G

Encryption: WPA2-PSK

KEY: 88888888

Advanced Features: ☐ Isolate ☐ Hidden ☐ Qrcode

MAX Num of User: 32

AuthType: None

VLAN BINDING: 0

Delete

CONFIRM
CANCEL

Select 2.4G at the top and edit the template for the WiFi.

SSID – This is the name you want the WiFi to show up as.

Encryption – The type of wireless encryption you want to use. Recommended to leave this as WPA2-PSK. If you have devices that only utilise WPA-PSK, set this to WPA-PSK+WPA2-PSK to enable WPA-Mixed encryption.

KEY – This is the desired WiFi Password.

Advance Features

– **Isolate** – Enable/Disable WiFi Isolation.

– **Hidden** – Enable/Disable SSID Hiding.

– **QR Code** – Enable/Disable the use of QRcodes for connecting users.

MAX Num of User – Set the maximum number of clients for the WiFi.

AuthType – If utilising the local portal feature enable it here.

VLAN Binding – If deploying on a managed network with VLANs you can set a VLAN number for the SSID.

Click the Advanced dropdown and enable the 802.11kvr Roaming (make sure to do this under both the 2.4G and 5G settings) everything else can be left default here.

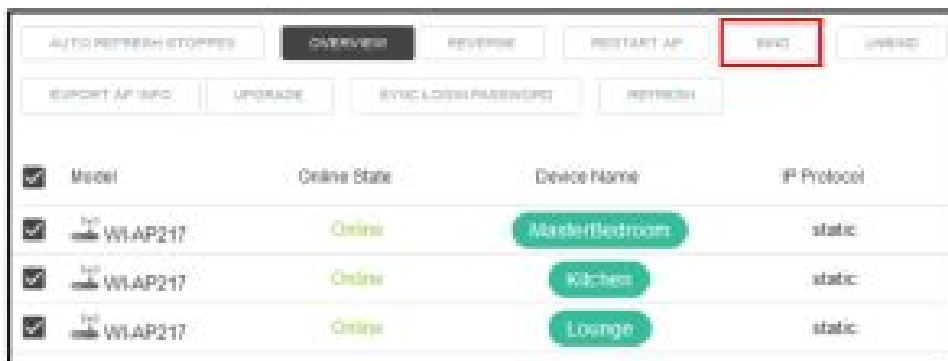


Click **CONFIRM** to save and then repeat for the 5Ghz settings.

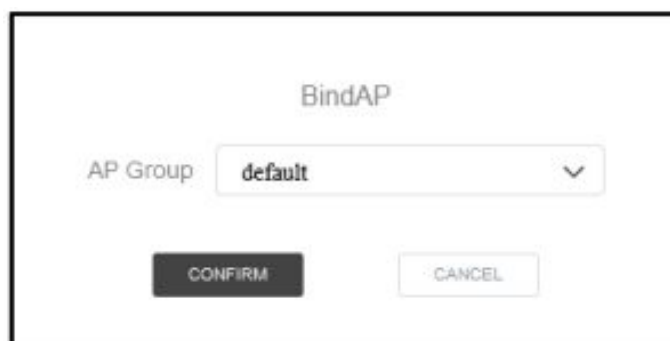
Step 7 – Binding the APs to the WiFi Group

Navigate to Wireless > AP List

Select all the access points, click BIND.



Select the group and click Confirm.



The access points will now reboot and be updated with the WiFi configuration. The group each AP is bound too is

displayed under AP Group to the right.

Connect the switch back into the rest of the network via the Uplink. Connect to the WiFi and if everything is correct you can get online. If you are unable to connect to the Internet, double check your cable connections and that the network gateway is set correctly for the access points.

Deploy the access points in the desired locations.

Step 8 – RF Planning

Once deployed, log back into the controller and navigate to Wireless > RF Planning.

Click Start Scan, this will have all the access points check for the best channels to be used with the least interference.

2.4G AP:0 Dual-Band AP:3 Offline Device:0					
GET CHANNELS START SCAN SAVE RESULT					
Configure	SN	Online State		Plan Status	
View		Online		-	
View		Online		-	
View		Online		-	

2.4G Channel	5G Channel	2.4G Noise	5G Noise	2.4G Interference	5G Interference
11	112	-95	-95	18	3
11	136	-95	-95	15	6
11	168	-95	-95	12	3

Once the scan completes, click Save Results to push the channel changes to the access points.

Note: You may temporarily lose connection to the WiFi during this process.

Step 9 – Unified Cloud Tunnel

Login to your Wi-Tek Cloud Account via cloud.wireless-tek.com. If you don't already have a cloud account, click register and follow the steps to get started.



Sign in your account!

☐ Remember Me

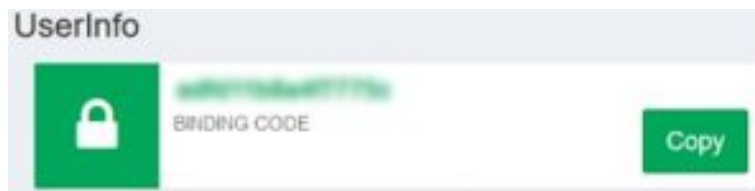
Sign In

[Forgot Password](#)

[Register](#)

[Re-Confirm](#)

Once logged in, click Unique Code in the top bar to see your unique binding code. Click Copy.



From the cloud cube and navigate to Unified Cloud and paste your unique Binding Code.

Serial Number	AC-00000000000000000000
Binding Code	<input type="text" value="0000000000000000"/>
Longitude	<input type="text" value="Input Longitude"/>
Latitude	<input type="text" value="Input Latitude"/>
Description	<input type="text" value="Mast Digital WI-AC50"/>
<input type="button" value="CONFIRM"/>	

Give the device a relevant description to make it easy to identify from the cloud. You can also enter co-ordinates of the location; this will enable you to see the location of the system on the map in your Wi-Tek Cloud account. Click Confirm to save. The WI-AC50 will now show up in your cloud account under 'Gateway'.

Note: It can take around 10-15 minutes to show up in your account.

Once the device is visible in the cloud, click InfoMessage to see more details about the cloud cube. Scroll down and under service click Enable for the 'Tunnel'. This will generate a direct tunnel link to the WI-AC50 to enable remote monitoring and management.

Note: The tunnel connection can take from 15 minutes up to 24 hours to become fully operational.

Service

Server Type	Domain Port	Description	Creation Time
Tunnel	<input type="text" value="0000000000000000"/>	Tunnel service for remote access the device via internet	<input type="button" value="Enable"/>
Configuration		Backup device configuration to cloud server	<input type="button" value="Enable"/>

Other Operate

Using this tunnel, you can access the cloud cube and manage the access points remotely in the same manner as you can whilst onsite.

Mast Digital (UK) LTD
Unit A Station Road Industrial Estate, Station Road, Epworth, Doncaster, DN9 1JZ
Company Number: 09009545 | VAT Number: GB193301816

Documents / Resources



[MAST DIGITAL AC50 Wi-Tek Smart Cloud Cube Mini AP Controller](#) [pdf] User Guide
AC50, Wi-Tek Smart Cloud Cube Mini AP Controller