



This guide provides key information to setup the AccessMyLAN service, enroll devices and create usage policies on the online portal.

Contents

What is AccessMyLAN?	. 3
How to access the AccessMyLAN portal	. 3
Pre-configured policies	.3
How to customize configurations	.4
How to create new policies	.4
Onboarding your devices	.8
How can the admin check if the phone is ready to use AccessMyLAN?	.8
How to turn on the mobile hotspot on your devices	.9
How to connect your end-user device to the Radiant Core Personal Hotspot	10
How to connect your end-user device to the Nighthawk Mobile Hotspot	12
How to connect your end-user device to the Moxee Mobile Hotspot	15
How to connect your end-user device to the AT&T Unite Express	17

What is AccessMyLAN?

AccessMyLAN from AT&T is a mobility service that helps protect data and devices from hackers and malware attacks and can implement policies to protect devices from being used for non-permitted purposes.

How to access the AccessMyLAN portal

Once your organization signs up for the AccessMyLAN service, you, as the administrator, will receive a welcome email that contains the link to login to the online portal.

You can also login by clicking on the link below. If you can't click on it, copy and paste it into your browser directly:

https://att.accessmylan.com/apps/datacontrol/login

Note: The first time you log-in you will see an ACCOUNT SETUP page and you will need to check your time zone settings are correct, set a Company/School Name, and agree to the Terms and Conditions.

Pre-configured policies

AccessMyLAN is one tool you can use to help implement your CIPA compliance responsibilities. We have pre-configured your AccessMyLAN account with a set of defaults that can help you and your devices comply with CIPA regulations. Before you hand over the phones to students, you will need to whitelist the specific websites and services (i.e. K12 reference sites, productivity tools, online classroom).

The pre-configured policies include **blocking** of the following content categories:

- Anonymizers
- Malicious websites
- Adult content
- Social networking
- Chat
- Online ads
- Business and Finance
- Shopping
- Entertainment
- Lifestyle
- Sport
- Travel
- Religion
- Streaming audio (Spotify, Tidal, Primephonic, etc.)
 - Create a whitelist to allow specific audio services
- Streaming video (Netflix, Hulu, YouTube, etc.)
 - <u>Create a whitelist to</u> allow specific training services
 - Create a whitelist to allow specific K12 educational services

How to customize configurations

You can customise your configuration by creating additional Policies or <u>Group Plans</u> to reflect the needs of your organization. You can also create additional policies to customise the types of websites that are allowed/denied. You can remove the "example.com" exception if you want to allow access to this website and add <u>additional exceptions</u>.

Example:

In a Policy, you may want to deny access to social media and streaming video categories.

You may also want to create a specific Policy for the certain teams with fewer restrictions (e.g. allow teachers access to social media).

You can also Manage a Devices attributes.

How to create new policies

As mentioned above, AccessMyLAN comes with a default policy called **Default Group Plan**. You can create additional Group Plans to manage data allowances and usage restrictions for different groups in your organization.

You can create a new Group Plan as follows:

- 1. Select **Data Control > Group Plans** and select **Create new Group Plan** on top right hand corner.
- 2. Enter GROUP NAME : Test Group Plan, and select Continue.
- 3. Move your device to the new group plan, and select Next.

GROUP PLANS > C	reating Domestic Pla	n (Domestic)					
	1	2		3	4		
	Group Name / Add Devices		ý	Add Limits	Restricted Policy		
GROUP NAME .g. Design Team							
Test Group Plan			×				
DEVICES AVAILABLE (97)	Find Davisor	0	DEVICE IN THIS GROUP (1)		Find Davisor	
0.00		Plild Devices	~	page	101/20	Find Devices	
(+1)993688390 (+1)993688390	Default Group	•	^	(+1)993757260 (+1)993757260	*		
(+1)985760858 (+1)985760858	Default Group	0					
(+1)971093176 (+1)971093176	Default Group	٥					
(+1)966877537 (+1)966877537	Default Group	0					
(+1)960714587 (+1)960714587	Default Group	Θ					
«First «Previous <u>1</u> Showing 1 to 97 of 97		Dev 250	ices	« First « Previous <u>1</u> Ne Showing 1 to 1 of 1		Dev 25	vic O
Cancel						Next	

The very first time you create a group plan, the wizard invites you to customise your Default Policy. In order to test the service, we recommend configuring your policy as follows:

- 1. Select **Continue** to view the NETWORK SECURITY categories (leave all categories as **Deny**).
- 2. Select **Continue** to view the INTERNET ACCESS categories.
- 3. Scroll down to *Device Access to Specific Websites* section, enter **example.com** in the field and choose **deny** to test the service.
- 4. Select Save.

Tip: If you want to edit policies later, you can always go **to Data Control > Policies** to find all your exisiting policies.

Group Plans also allow you to the *Add Limits* and *Alerts* per device or group and assign a different Restricted Policy after the Alert threshold. You can also throttle the *Data Speed* to limit data heavy content.

1. Under STANDARD POLICY, choose the *Default Policy*, and then click **Next**.

GROUP PLANS > Cr	eating Domestic Pl	an (Domestic)			
	 Image: A start of the start of	2	3		
	Test Group Plan / Devices (1)	Standard Policy	Add Limits		cy
STANDARD POLICY Applies from the start of y	our billing cycle				
Select existing Policy	Add New				
POLICY NAME	WEBSITE CATEGORY	ACCESS	SPECIFIC WEBSITE ACCESS	DETAILS	
Default Policy	146 ALLOWED	0 DENIED	0 ALLOWED 1 DENIED	View	
DATA SPEED					
You may also throttle th E.g setting 750 Kb/s will	e data speed to save on o let emails through but lin	lata consumption. hit video streaming.			
		Unlimited			
100 Kb/s		Unlimited			
Cancel	Previous				Next

- 2. Under ADD LIMITS TO THE PLAN, choose *No, I want to add an unlimited plan*, then click **Continue**.
- 3. Under DATA ALLOWANCE RESET TIME, choose *Monthly*, then click **Continue**, and in the bottom right, select **Next** leaving all fields as default.

GROUP PLANS >	Creating Domestic Pla	an (Domestic)			
	Ø		3		
	Test Group Plan / Devices (1)	Standard Policy Default Policy	Add Limits	Restricted Policy	
ADD LIMITS TO THE PL	LAN				
Do you want to add a	CUT-OFF point?				
○ Yes ● No, I v	vant an unlimited plan				
DATA ALLOWANCE RE Choose the reset time	SET TIME				
Monthly	Daily				
ALERT Receive an alert for devi	ice with high usage. Alert valu	e must he less than your device	cut-off		
DEVICE ALERT	GROUP ALERT	,,			
15 GB	•	GB 👻			
	🖌 Don't set a gr	oup alert			
EMAIL You will receive alerts to	the following email address				
appledemo@asavie.co	om Email me 📝	SMS device			
Cancel	Previous				Next

4. Under RESTRICTED POLICY leave all as default and select **Review your settings** button.

GROUP PLANS > C	reating Domestic Pla	an (Domestic)			
	~		⊘	4	
	Test Group Plan / Devices (1)	Standard Policy Default Policy	Add Limits Alert 15 GB	Restricted P	blicy
RESTRICTED POLICY					
Do you wish to appl	y a restrictive policy after	the 15 GB device alert fo	r a more restricted plan?		
Select existing Polic	y Add New				
POLICY NAME	WEBSITE CATEGORY	ACCESS S	PECIFIC WEBSITE ACCESS	DETAILS	
Default Policy	146 ALLOWED	0 DENIED 0	ALLOWED 1 DE	NIED View	
DATA SPEED					
You may also throttle th E.g setting 750 Kb/s will	e data speed after the 15 let emails through but lin	GB device alert to save on the save of t	on data consumption.		
		Unlimited			
100 Kb/s		Unlimited			
Cancel	Previous				Review your settings

5. Under REVIEW YOUR SETTINGS, select **Save**.

You should now see a **Test Group Plan** with one device.

Note: For more information on Group Plan configurations, visit our guide <u>here</u>.

	Image: A start of the start	⊘	⊘	⊘	
	Test Group Plan / Devices (1)	Standard Policy Default Policy	Add Limits Alert 15 GB	Restricted Policy Default Policy	
REVIEW YOUR S	ETTINGS				
STANDARD PO	LICY (Applies from the start of your b	illing (ycle)			
GROUP NAME: Tes	t Group Plan				
DEVICES: 1					
PLAN: Domestic					
STANDARD POLICY	: Default Policy				
DATA SPEED: Unlin	nited				
LIMITS					
RESET: Monthly					
DEVICE ALERT: 15	GB				
GROUP ALERT: -					
RESTRICTED PO	LICY (Applies after the 15 GB device	alert)			
RESTRICTED POLIC	Y: Default Policy				
DATA SPEED: Unlin	nited				

Test the Policy

With your newly created *Test Group Plan* we will test the policy on the test device.

- 1. From your *device* open a browser.
- 2. Try access the *example.com* website.

You should now see the Site Blocked message.

Note: If you are making the same test with an HTTPS website, they will return an empty webpage. If you are trying to run an application that requires internet access, such as the Netflix mobile app, the app will open, but you will get an error message like "internet connection problem".

Congratulations!

You have now proved that the "Test Group Plan" works on your device.

Tip:

If you find that you are still able to access the blocked website, it could be due to the website being <u>cached in the mobile device</u>. In this case, put your device into airplane mode or reboot and try again.

Please ensure the Wi-Fi is turned *off* and that you are browsing the web over your mobile connection.

Onboarding your devices

We have also pre-loaded a list of your devices onto the portal to make it easier for you to start managing them straight away.

Once you receive your devices you need to follow the next steps to onboard them onto the AccessMyLAN service:

- 1. Power up the device
- 2. Leave it up and running. This will allow the configuration to be pushed onto the device
- 3. The service will automatically replace the "nextgenphone" APN with "**ent.accessmylan.net**" APN as the default APN on the phone. This process only takes a few minutes.
- 4. Turn on the hotspot on the phone to validate functionality.

Note: If the device starts a firmware update before the new APN is configured, the former request will take priority and the APN change will be ignored. Once this process is complete, a second attempt will be made.

How can the admin check if the phone is ready to use AccessMyLAN?

On the AccessMyLAN portal, navigate to **Devices > Device Overview** and search for the device you just connected. The *DEVICE SETUP* field should now show **Controlled** when viewing the phone in list.

NUMBER	DESCRIPTION	DEVICE SETUP	CONNECTION
(+1)993688390	(+1)993688390	Controlled	at

Tip: If the phone does not show a status of Controlled:

- Make sure the device is **not** currently connected to Wi-Fi
- Select the C refresh icon in top right-hand.

Please check periodically to ensure your users have not initiated a factory reset. That would happen if the devices you have Controlled, no longer are. If you see devices that are no longer Controlled, contact Asavie Support one of the ways below:

- Email: <u>attsupport@accessmylan.com</u> To be used Monday through Friday from 9-5:30pm EST. Email is also checked on the weekends 3 times daily – Morning, Afternoon and Night or via
- Phone: 866-570-4483 Used in and out of hours above. In hours for escalation. Out of hours customer will be asked if they want to talk to an "on call" person.

How to turn on the mobile hotspot on your devices

It is important to note that the device will not have access to the internet via the Radiant Core Browser as this functionality is not supported. The device has been designed to only allow internet connectivity via the hotspot.

The purpose of the information below will guide end users to set up their phones into mobile hotspots.

- 1. From the home screen, swipe up to access **Apps**, and tap **Settings**.
- 2. Tap Network & Internet > Hotspot & tethering > Mobile hotspot.
- 3. Slide the Mobile hotspot switch to the **On** position to turn on Wi-Fi hotspot.
 - Hotspot name: Tap to set the hotspot name.
 - Security: Tap to select security mode.
 - Hotspot password: Tap to set hotspot password.
 - **Turn off hotspot automatically:** Slide the switch to the **On** position to turn off hotspot automatically if no devices are connected.
 - Turn off hotspot time: Tap to select a time for your hotspot to turn off.
 - Hide SSID: Slide the switch to the **On** position to hide the SSID.
 - **Reset OOB**: Tap to reset the network SSID, security and password to the default settings.
 - Maximum connection: Tap to set the number of maximum connected users.
 - **Connected users:** View your connected users.
 - Blocked users: View your blocked users.

How to connect your end-user device to the Radiant Core Personal Hotspot

Radiant Core Hotspot



Once the mobile hotspot on the Core Radiant device has been enabled, students can connect their devices such as laptops or tablets in the following manner:

- 1. On a Windows device, open Settings > Network & Internet > Wi-Fi
- 2. Click Show available networks and browse to find the network your phone has just created.
- 3. Select the network and click **Connect.** Then input the password as displayed on your phone.

The connection will establish after a moment. The device will show you how many laptops or tablets are connected to the hotspot.

AT&T	∎ 99%
1:33 PM Tue, Apr 14	@ 49
Android System	
Tethering or hotspot active 1 connected, 0 blocked	
Manage notifications sword	
Turn off hotspot automatically Mobile hotspot will turn off if no devices are connected	
Turn off hotspot time	
Hide SSID	
Reset OOB	
• •	

How to connect your end-user device to the Nighthawk Mobile Hotspot

Make sure you are connected to the Wi-Fi on the modem before proceeding.

- 1. Launch a web browser and enter 192.168.1.1
- 2. Enter the administrator login password. You may need to RESET the modem if you forgot by pressing the RESET button where the battery is located using a paperclip.

You are now on the Dashboard of your device.

$\langle \rangle$				192.168.1.1/index.html#				
DASHBOARD	🖻 MYMEDIA 🛛 😫			😂 AT&T				:
3. Select S	Settings > A	Advanced Se	ettings >	Cellular.				
			192.168.1	.1/index.html#settings/c	ellular			
DASHBOARD	🖻 MYMEDIA 🛛 🗯	SETTINGS		🚔 AT&T				:
 AT&T Wi-Fi S Setup Security Administrat Advanced S Cellular Port Forwar 	status v ion v ettings ding	CELLULAR Data @ Roaming D Band Regit Auto LAA - uses LTE throug LAA is not set LAA pro	ata on WI-Fi 5GHz spect hput supported. Visit N eference.	¢ trum to boost Wi-Fi Profiles to	Network Mode Auto Switching to Manual temporarily disconne Network Selection AT&T	Network Mode will ct you from the devic	e	
Device	y	APN						
Other		Active	APN Name	APN	PDP	PDP Roaming	Authentication	n
🕜 Help & Supp	oort	۲	ATT Mobile	broadband	IPV4V6	IPV4	None	1

- 4. Click the blue **ADD** button and complete the fields as follow:
 - APN name: Hotspot AML
 - APN: hotspot.accessmylan.net
 - PDP: **IPV4**
 - PDP Roaming: None
 - Authentication: **None** Leave username and password blank, and click **SAVE**

DASH	BOARD 🖻 MYMEDIA	\$	ETTINGS	Add APN	×				
				Add APN	~				
⊘ ∢	AT&T Wi-Fi Status Setup	v	CELLULAR Data 🕑	APN Name Hotspot AML APN		: Mode			
♥	Security Administration	× ×	Band Region	hotspot.accessmylan.net PDP		g to Manual N rily disconnec	etwork Mode will t you from the devic	ce	
•	Advanced Settings Cellular		LAA - uses W LTE throughp	IPV4	\$	rk Selection			
	Port Forwarding		LAA is not su set LAA prefe	None	÷				
			APN	None	\$				DELETE ADD
	Other		Active	Username	_	PDP	PDP Roaming	Authenticatio	n
0	Help & Support		0	Password		IPV4V6	IPV4	None	1
				CANCEL	SAVE				

5. Click the round radio button on the left to activate the APN profile under Active.

Ø	AT&T Wi-Fi Status	CE	LLULAR						
•	Setun		Data 🗹		N	etwork Mode			
 Setup Security Administration 			Roaming D	ata 🗌	Au	Jto			
			Band Region			Switching to Manual Network Mode will			
			Auto	*		temporarily disconnect you from the device			
•	Advanced Settings			Wi-Ei 5GHz spectr	Ei EGHz spectrum to boost		Network Selection		
	Cellular		LTE throug	hput	AT	r&T			
	Port Forwarding		LAA is not set LAA pr	supported. Visit <mark>N</mark> eference.	/i-Fi Profiles to				
	- Port Filtering								
			N						
	Device		N.					DE	LETE <u>AD</u>
	Other		Active	APN Name	APN	PDP	PDP Roaming	Authentication	
0	Help & Support	_	0	ATT Mobile	broadband	IPV4V6	IPV4	None	1
		_			h - t t		News	N	

This APN is now the active. If you go back to the DASHBOARD, you should now see your device Connected in green.

::	DASHBOARD	MYMEDIA	SETTIN
-		ATAT(LTE) Connected	
		DEVICES 1 Local	

How to connect your end-user device to the Moxee Mobile Hotspot

To configure the device, open a web browser on the terminal and input the default URL:

- 1. Make sure to connect your terminal (e.g. tablet, PC, etc.) to the hotspot via Wi-Fi or MicroUSB cable.
- 2. Log in to http://192.168.1.1 or http://device.WebUI in your browser.
- The default username is: admin.
 The default password is: 12\$ followed by the last 3 digits of the device IMEI (for example: 12\$123).

It is suggested to change the default login and password of the WebUI to prevent unauthorized users from changing the hotspot's settings.

moxee ⁻	Language: En	glish 🗸
	Username Please enter username Password Please enter password Log In	
СОР	YRIGHT © 2020 Open Source Notice	

Congratulations! You have successfully logged in to the hotspot. Once you have logged in to your hotspot via your web browser, you can see the Home page for the hotspot.

- 4. Go to Settings > Internet > Mobile Connection
- 5. In this menu, you can configure your mobile data, click on + NEW PROFILE enter the following settings:
 - a. APN: hotspot.accessmylan.net
 - b. Authentication: None
- 6. Click APPLY

The new APN is added.

Internet Mobile Connection Wreless Network Peatures Management Management <	ee		Home	SMS	Settings	Logout English	
Internet Mobile Connection Wrevex Network Peatures Management Muthentication Type: APN: User Name: Password: IP Type: MCC: MRC: GIDI: APN Type: Default McC: MRC: GIDI: APN Type: Default McC: McC:							• 🕾 •
Mobile Connection Wireless Network Peatures Management Management <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>							
Michele Connection Wireles Mobile Data: Network Data Roaming: Enable V Management Carrier Name: Authentication Type: V APN: V User Name: V Password: V IP Type: V MCC: MCC: MIC: GIDI: Bear: Default Bear: V Network Mode: 4G LTE Network Coperator: Auto	Internet	w.	Mobile Connecti	on			
Wireless Mobile Data: On Network Data Roaming: Enoble Features Cartier Name: Image: Cartier Name: Authentication Type: Image: Cartier Name: Image: Cartier Name: Authentication Type: Image: Cartier Name: Image: Cartier Name: User Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: Image: Cartier Name: <	Mobile Connectio	n			11		
Network Peatures Patrones Carrier Name: Carrier Name: Authentication Type: APN: User Name: User Name: Password: IP Type: Password: GiD1: APN Type: Default Bear: Carrier Auto Vetwork Mode: Auto Vetwork Mode: Auto Vetwork Coperator: Auto Vetwork Co	Wireless	•	Mobile Data:	On	~		
Features Cartier Name: Management Cartier Name: Authenflication Type: Image: Cartier Name: User Name: Image: Cartier Name: User Name: Image: Cartier Name: Brasword: Image: Cartier Name: IP Type: Image: Cartier Name: IP Type: Image: Cartier Name: IP Type: Image: Cartier Name: APN: Image: Cartier Name: IP Type: Image: Cartier Name: APN Type: Default Bear: Image: Cartier Name: Network Mode: Image: Cartier Name: Network Mode: Image: Cartier Name: Network Coperator: Auto	Network	•	Data Roaming:	Enable	~		
Management Authenlication Type: Authenlication Type: Password: Password:	Features	*	Carler Name:				
Authentication Type: APN: User Name: Password: Password: IP Type: MCC: MNC: GID 1: APN Type: Default Bear: Composition Composition Metwork Mode: Network Mode: Auto	Management	*	Collier Hume.				
APN: User Name: Password: IP Type: MCC: MNC: GID1: Bear: Default Bear: APN Type: Default Bear: APN Type: CCC/ Bear: APN Type: CCC/ Bear: CCC/ Bear: CCC/ Bear: CCC/ CCC/ CCC/ CCC/ CCC/ CCC/ CCC/ CC			Authentication Type:		\sim		
User Name: Password: IP Type: MCC: MNC: GiD1: APN Type: Default Bear: Metwork Mode: Network Operator: Muto			APN:	<u>f</u>			
Password:			User Name:	1			
Pasword. IP Type: MCC: MNCC: GID 1: APN Type: Default Bear: Metwork Mode: Acoly Network Operator: Auto			Barrowards				
IP Type: MCC: MNC: GID1: APN Type: Default Bear: Network Mode: 4G LTE Network Operator: Auto V			Password.				
MCC: MCC: GID1: GID1: APN Type: Default Bear: Metwork Mode: Network Operator: Auto			IP Type:		~		
MNC: GID 1: APN Type: Default Bear: Network Mode: 4G LTE Network Operator: Auto			MCC:				
GID1: APN Type: Default Bear: Metwork Mode: 4G LTE Network Operator: Auto			MNC:				
Network Mode: Auto							
APN Type: Default Bear: Network Mode: 4G LTE Network Operator: Auto			661.				
Bear: (+ New India) Activ Network Mode: 40 LTE V Network Operator: Auto V			APN Type:		Default		
Network Mode: 40 LTE V Network Operator: Auto V			Bear:				
Network Mode: 40 LTE V Network Operator: Auto V					+ New Profile Ac	phy	
Network Operator:			Network Mode:	4G LTE			
			Network Operator:	Auto	~		
			COPYRIGHT @ 2020 Open Sour	ce Notice			
COPYRIGHT © 2020 Open Source Notice							

How to connect your end-user device to the AT&T Unite Express

To add an APN for another network:

- 1. Launch a web browser from a computer or Wi-Fi device that is connected to the network.
- Enter http://attwifimanager or <u>http://192.168.1.1</u>. A login screen displays.
- Enter the password in the Sign In field.
 The default password is attadmin. The password is case-sensitive.
- 4. Select Settings > MOBILE BROADBAND > APN.

	GENERAL MOBILE BROADS	AND ROUTER	
🟫 Home	Desfacement ATAL City Councils		
(•)) WI-FI	Preferences APR Sim Security		
Messaging	Active		
Settings	 AT&T Mobile (Broadband) 		Details ¥
			Add
-			

5. Click the **Add** button.

GENERAL	MOBILE BROADBAND	ROUTER		
Preferences APN	SIM Security			
Active				
AT&T Mobile	e (Broadband)		Details 🔻	
New Apn				н
Name				
APN				
Authenticati	on None 💌			
Save	Cancel			

- 6. Enter the following settings:
 - c. Name: Hotspot AML
 - d. APN: hotspot.accessmylan.net
 - e. Authentication: **None**
- 7. Click the **Save** button.

The new APN is added.



© 2020 AT&T Intellectual Property. AT&T, Globe logo, and DIRECTV are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.