

AccessMyLAN

Setup Guide for Hotspots



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.)
 - **Create a whitelist to** 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 [Group Plans](#) 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 [additional exceptions](#).

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 > Creating Domestic Plan (Domestic)

1 Group Name / Add Devices 2 Standard Policy 3 Add Limits 4 Restricted Policy

GROUP NAME
e.g. Design Team

Test Group Plan

DEVICES AVAILABLE (97) Find Devices

DEVICE	CURRENT GROUP	ADD
(+1)993688390 (+1)993688390	Default Group	+
(+1)985760858 (+1)985760858	Default Group	+
(+1)971093176 (+1)971093176	Default Group	+
(+1)966877537 (+1)966877537	Default Group	+
(+1)960714587 (+1)960714587	Default Group	+

DEVICE IN THIS GROUP (1) Find Devices

DEVICE	NEW (1)	REMOVE
(+1)993757260 (+1)993757260	★	-

< First < Previous 1 Next > Last > Devices 250

Showing 1 to 97 of 97

< First < Previous 1 Next > Last > Devices 250

Showing 1 to 1 of 1

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 existing 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 > Creating Domestic Plan (Domestic)

1 Test Group Plan / Devices (1) 2 Standard Policy 3 Add Limits 4 Restricted Policy

STANDARD POLICY
Applies from the start of your 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 the data speed to save on data consumption. E.g setting 750 kb/s will let emails through but limit video streaming.

100 kb/s Unlimited 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 Plan (Domestic)

Test Group Plan / Devices (1)
 Standard Policy Default Policy
 Add Limits Alert: 15 GB
 Restricted Policy Default Policy

REVIEW YOUR SETTINGS

STANDARD POLICY *(Applies from the start of your billing cycle)*

GROUP NAME: Test Group Plan

DEVICES: 1

PLAN: Domestic

STANDARD POLICY: Default Policy

DATA SPEED: Unlimited

LIMITS

RESET: Monthly

DEVICE ALERT: 15 GB

GROUP ALERT: -

RESTRICTED POLICY *(Applies after the 15 GB device alert)*

RESTRICTED POLICY: Default Policy

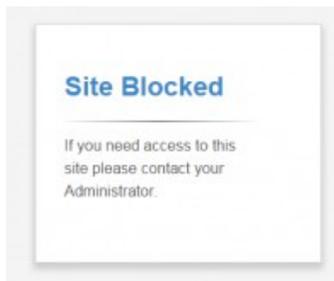
DATA SPEED: Unlimited

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 [cached in the mobile device](#). 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.

<input type="checkbox"/>	NUMBER	DESCRIPTION	DEVICE SETUP	CONNECTION
<input type="checkbox"/>	(+1)993688390	(+1)993688390	Controlled	

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

- Make sure the device is **not** currently connected to Wi-Fi
- Select the  **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: attsupport@accessmylan.com 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

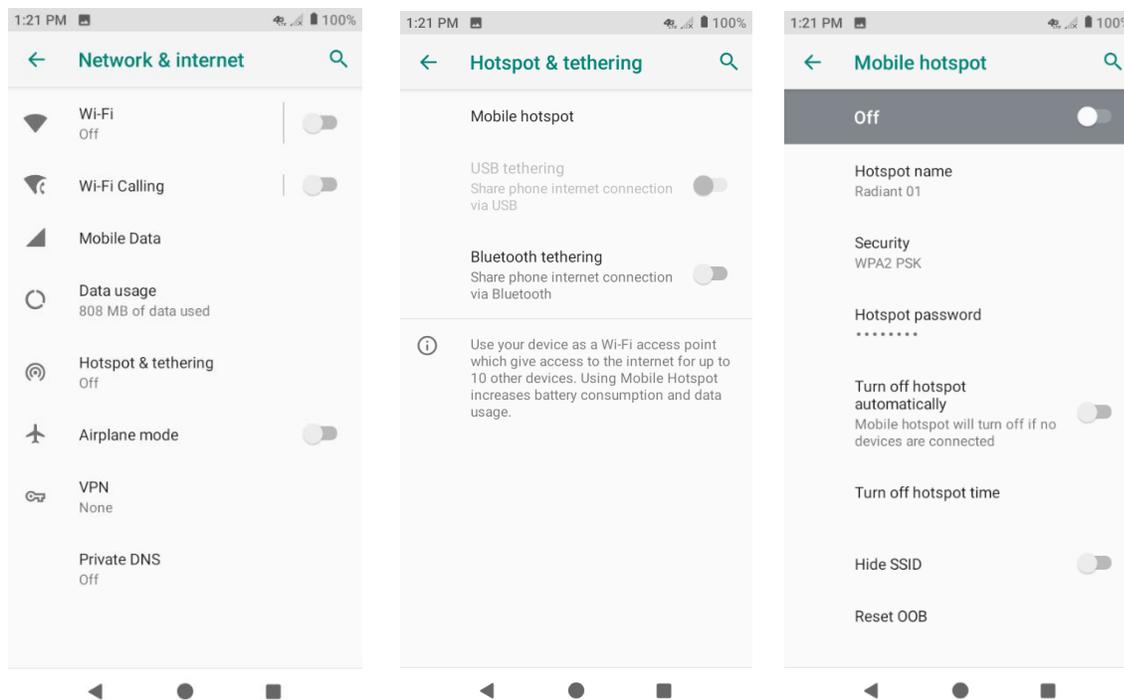
It is important to note that the device will not have access to the internet via the Radiant Core Browser as this functionality is not supported. The device has been designed to only allow internet connectivity via the hotspot.

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

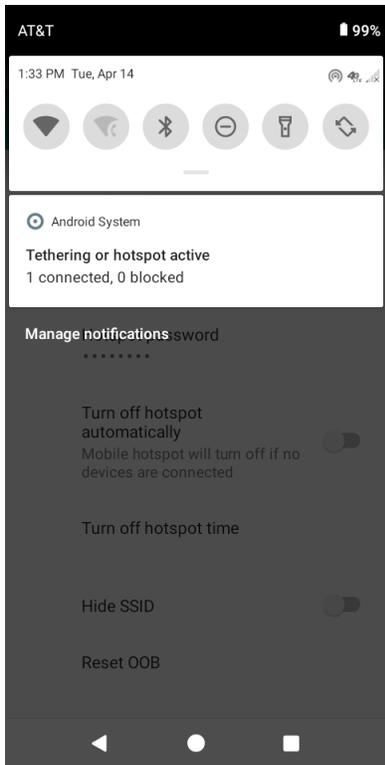
Radiant Core Hotspot



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.

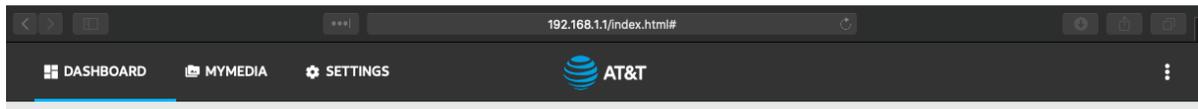


How to connect your end-user device to the Nighthawk Mobile Hotspot

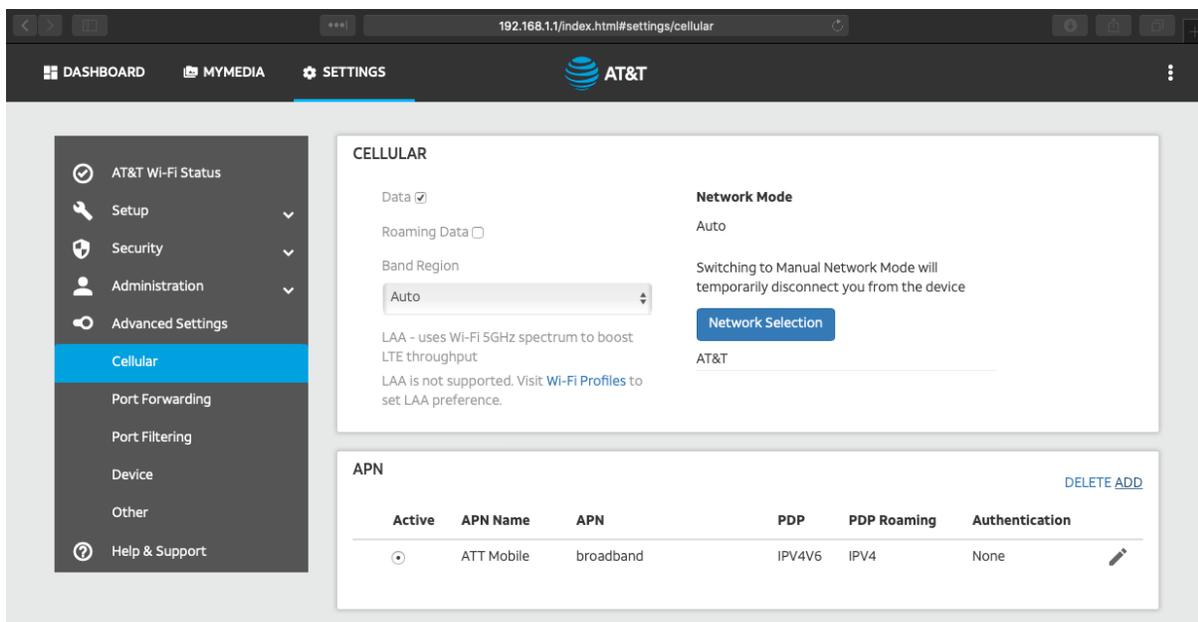
Make sure you are connected to the Wi-Fi on the modem before proceeding.

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.

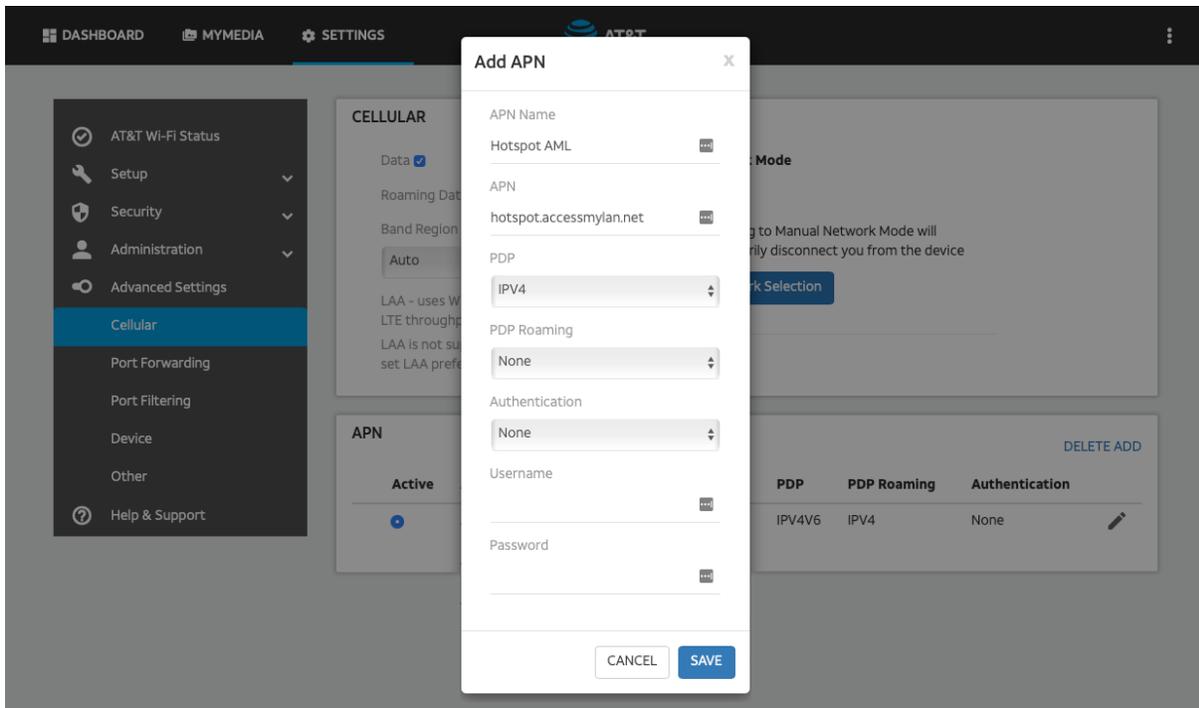


3. Select Settings > Advanced Settings > Cellular.

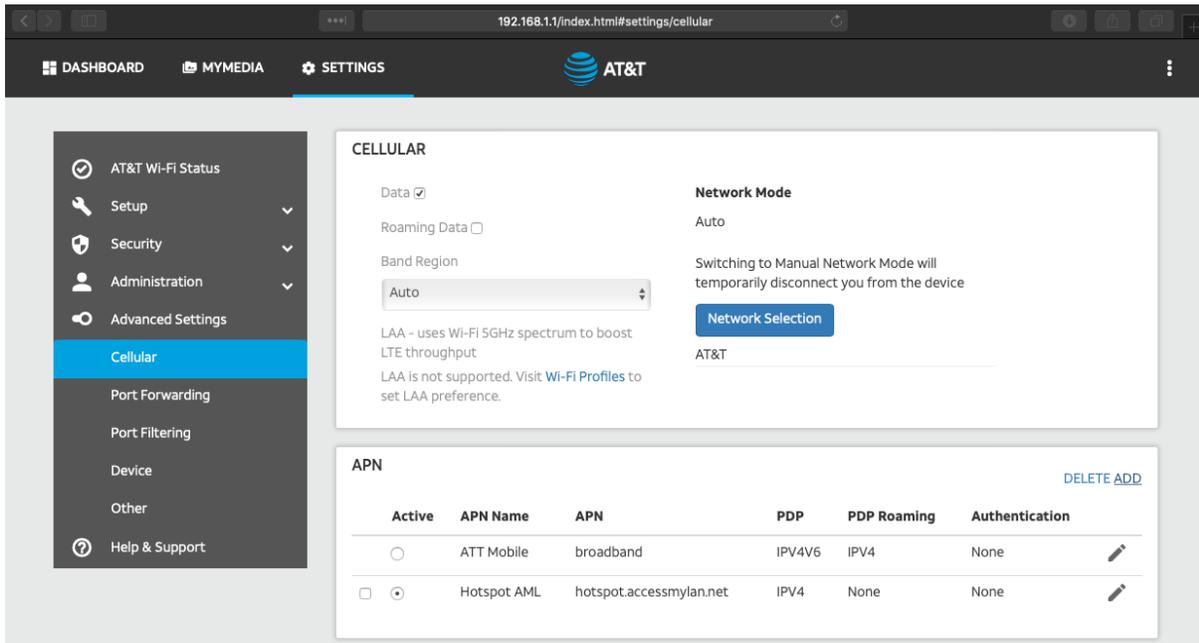


4. Click the blue **ADD** button and complete the fields as follow:

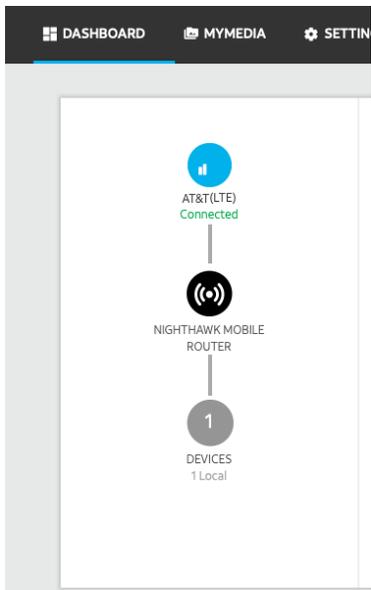
- APN name: **Hotspot AML**
 - APN: **hotspot.accessmylan.net**
 - PDP: **IPV4**
 - PDP Roaming: **None**
 - Authentication: **None**
- Leave username and password blank, and click **SAVE**



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



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

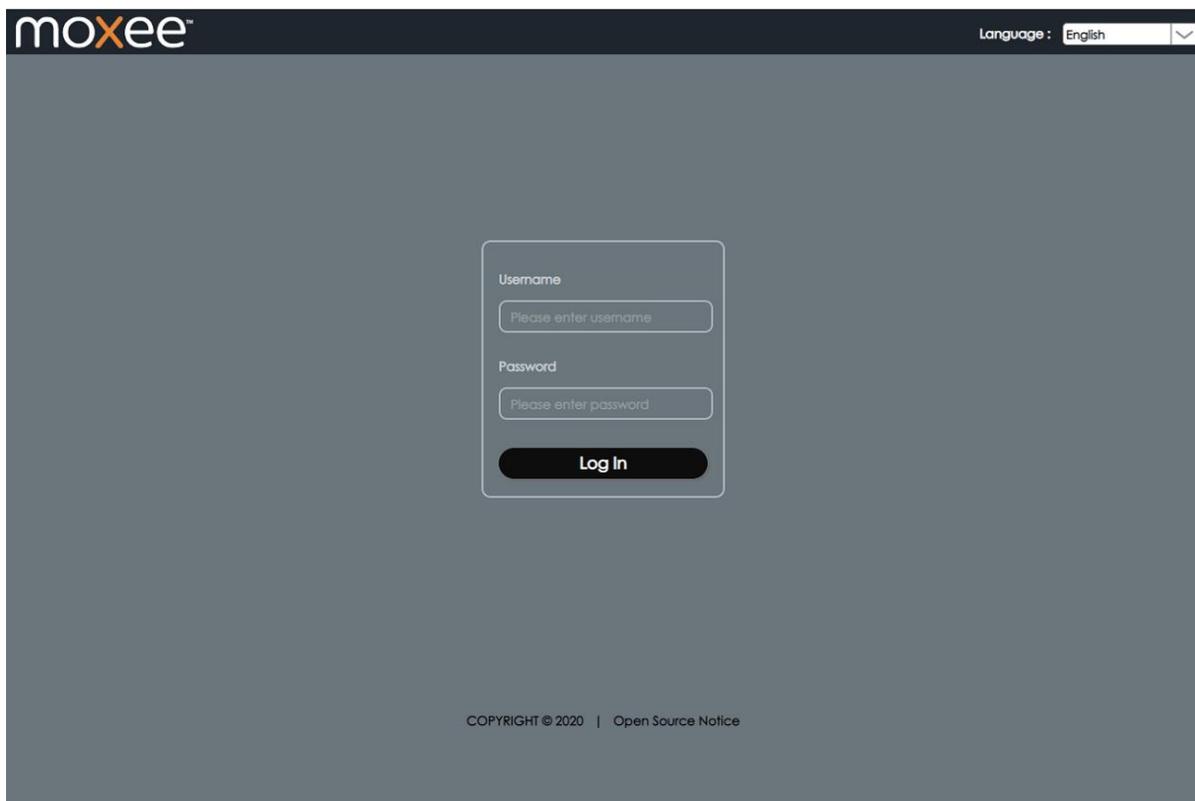


How to connect your end-user device to the Moxee Mobile Hotspot

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.
3. 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.



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.

moxee Home SMS Settings Logout English

Internet
Mobile Connection
Wireless
Network
Features
Management

Mobile Connection

Mobile Data: On
Data Roaming: Enable
Carrier Name:
Authentication Type:
APN:
User Name:
Password:
IP Type:
MCC:
MNC:
GID1:
APN Type: Default
Bear:

+ New Profile Apply

Network Mode: 4G LTE
Network Operator: Auto

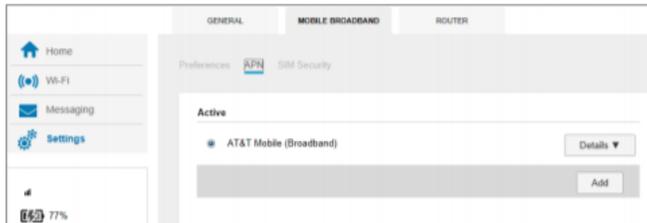
Apply

COPYRIGHT © 2020 | Open Source Notice

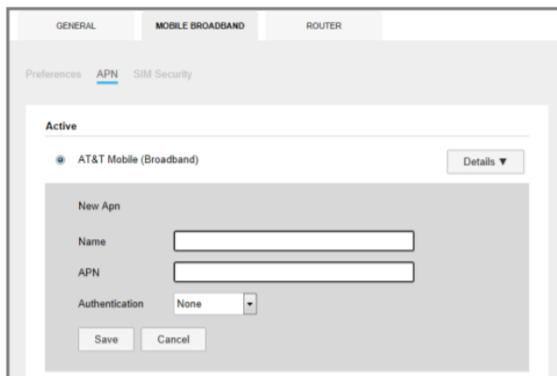
How to connect your end-user device to the AT&T Unite Express

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.
2. Enter **http://attwifimanager** or **http://192.168.1.1**.
A login screen displays.
3. Enter the password in the **Sign In** field.
The default password is **attadmin**. The password is case-sensitive.
4. Select **Settings > MOBILE BROADBAND > APN**.



5. Click the **Add** button.



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.

