ATEL™
PASSION FOR INNOVATION

Arch™ W01

Mobile Hotspot by ATEL

User Manual

Version 7.0

Contents

Overview

Thank you for choosing the W01 Arch, an LTE Mobile Hotspot by ATEL!

Having the W01 Arch at your fingertips will allow you to access the LTE network for fast uploads and downloads on your own Wi-Fi Hotspot. You can also connect up to 15 Wi-Fi capable devices to the Internet at once - laptops, tablets, Smartphones and more.

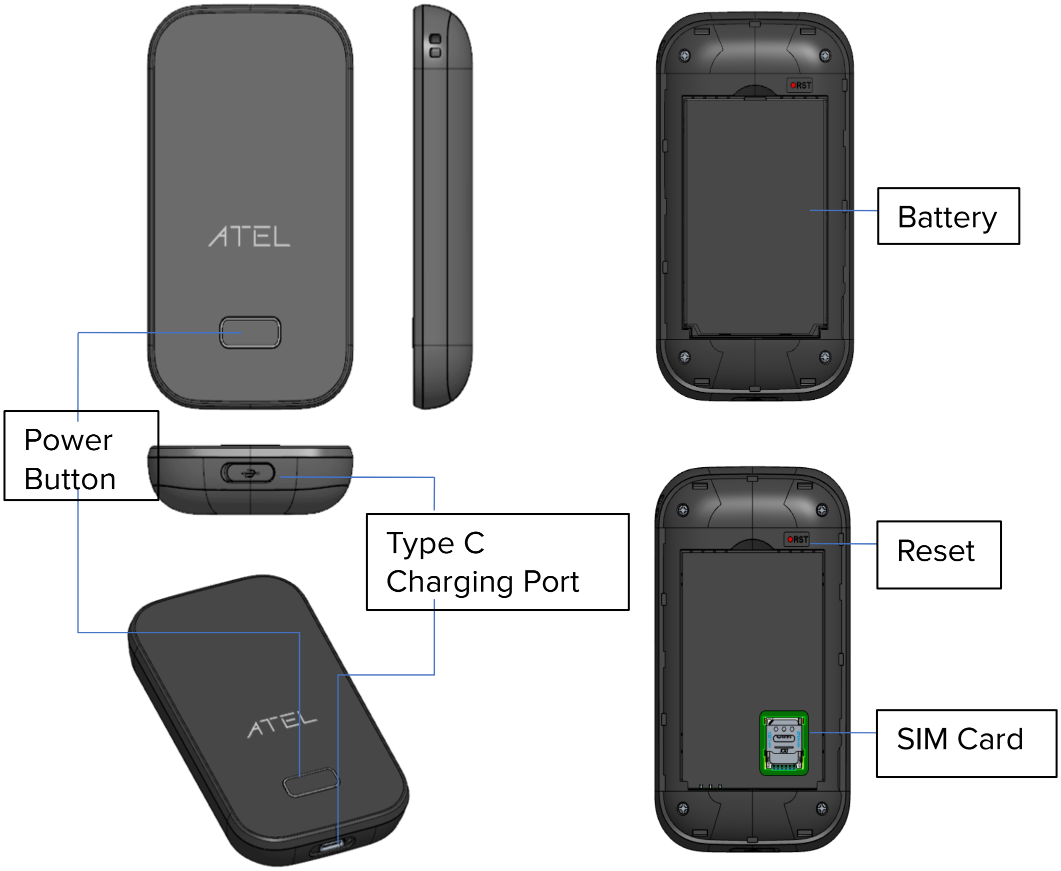
Network Bands supported:
4G LTE Bands: B2/4/5/12/13/66/71
3G Bands: B2/4/5

System Requirements

- Compatible with all IEEE802.11b/g/n/ac Wi-Fi enabled devices.
- Works with the latest versions of most browsers*.

* It is recommended to use the latest versions of Internet browsers. Outdated versions may not be compatible with the W01 Arch Online Device Management Portal, http://192.168.0.1 or https://192.168.0.1.

Components



Key

Power Button

Power on/off for the W01 Arch. Press power key twice quickly to wake up Wi-Fi from the Sleep mode.

Type C Charging Port

The USB charger connects here.

Battery

Insert the battery to align with the battery contacts.

Reset Pin Hole

To perform reset of your device, use a unfolded paperclip, insert into the RST pin hole, and push down for 3 seconds, then release.

SIM Card

Remove the battery cover from the back of your W01 Arch and remove the battery.
Slide the SIM door open and insert your SIM. Makre sure the SIM is placed properly before sliding the door back up to close the SIM door.

LED Indicator

LED	Color	Action	Function Description
Power/Battery	Green	On	Battery level _ high, capacity > 65%
	Green	Blinking	Charging, Battery level _ high
	Blue	On	Battery level _ Mid, , capacity 35%~65%
	Blue	Blinking	Charging, Battery level_Mid
	Red	On	Battery level _ Low capacity < 35%
	Red	Blinking	Charging, Battery level _ Low
		Off	No battery
	White	Blinking	Power off Charging
	White	On	Power off charging full
WiFi	Green	On	WiFi connected with a WiFi Client
		Off	WiFi not connected
	Green	Blinking	On 1S, off 1S, during WPS is enabled
SMS	Green	Always on	Unread SMS
		Off	No unread SMS
LTE/3G	Green	On	Represents 5-bar signal strength
	Blue	On	Represents 4-bar signal strength
	Cyan(B+G)	On	Represents 3-bar signal strength
	Purple(R+B)	On	Represents 2-bar signal strength
	Yellow	On	Represents 1-bar signal strength
	Red	Blinking	Means error, no SIM or no internet connection
		Off	No Signal

Upgrading	All above LED	On	Power and LTE LED light white, WiFi and SMS LED light green during F/W upgrading

Battery Management

Your W01 Arch is equipped with a replaceable and rechargeable battery. It works from the charged battery alone, or when the device is plugged into a power source. Charge the battery with the charger provided with your Hotspot. If you are logged on to your W01 Arch Online Portal, the battery charging icon 🔋 is displayed at the top right corner while the battery is charging.

Note: Please do not attempt to open or disassemble your Hotspot and the battery pack. Doing so may cause damage that voids your warranty.

IMPORTANT! Please use only an approved charger to charge your Hotspot. Improper handling of the charging port, as well as the use of an incompatible charger, may cause damage to your device and void the warranty.

Accessing the Network

Work effectively outside the home or office with the reliable broadband speed that the LTE service provides. You can connect to the internet at speeds fast enough to keep up-to-date on all your email correspondence, download attachments, and access your corporate internet.

Using Your W01 Arch for the First Time

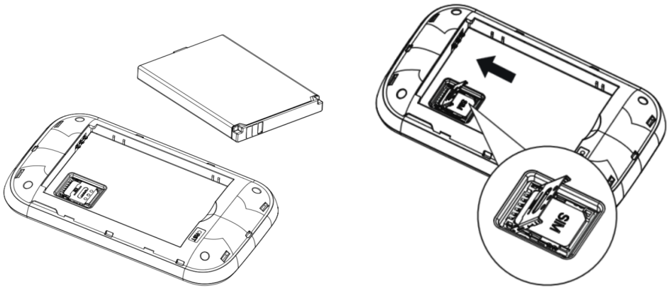
System Requirements

Your computer, tablet, or other wireless devices need Wi-Fi capability and Internet browser software only. Your W01 Arch is compatible with most major operating systems and the latest versions of browsers.

Installing the LTE Nano SIM Card

If not already inserted, follow the instructions below to install your LTE Nano SIM card.

- Remove the back cover of your device and take the battery out.
- Slide the SIM door open and insert your SIM. Make sure the SIM is placed properly before sliding the door back up to close the SIM door as the image shows below.
- Properly install the battery and put the back cover on**.**



IMPORTANT! Do not bend or scratch your Nano SIM card. Avoid exposing your Nano SIM card to static electricity, water, or dirt. Whenever you insert or remove the SIM card, ensure your W01 Arch is powered off and is not connected to any power source. Never use tools, knives, keys, or any type of object to force the door open or to remove the Nano SIM card. Doing so might void the warranty.

Charging the Battery

Before using your Mobile Hotspot, ensure that the battery is fully charged. Be sure to use the charger that came with your device.

NOTE: Your W01 Arch is equipped with a replaceable, rechargeable battery. When handling the battery or SIM card, please make sure the device is not connected to any power sources. Do not use any tools, sharp objects or any utensils when handling the battery. Doing so may cause damage that voids your warranty.

- It normally takes 3 to 5 hours, depending on your power sources and device status to fully charge the battery.
- The battery discharges faster as additional devices connect to your Hotspot.
- Battery life depends on the network, signal strength, temperature, features, and active connection time.
- When charging, keep your device near room temperature.
- Never leave the W01 Arch in an unattended vehicle due to uncontrolled temperatures that may be outside the desired operating and storage temperatures for your device.
- It is normal for batteries to gradually wear down and require longer charging time.

Using Your W01 Arch after Setup is Complete

Mobile Hotspot to Share Connections

You can use your W01 Arch as a wireless Mobile Hotspot to connect to a total of 15 Wi-Fi capable devices to the mobile broadband network.

Wi-Fi and Mobile Hotspot (http://192.168.0.1) Security and Password

The W01 Arch comes from the factory with security turned on. To access the Online Portal,
a) For T-Mobile and all other users, "admin" is the default for both username and password.
b) For Verizon users, "admin" is the username. For password, please check your device label for the unique Online Portal password.

You can create your own Mobile Hotspot password by signing into the Mobile Hotspot Online Portal. Once the password is changed, you will need to use the new password to logon.

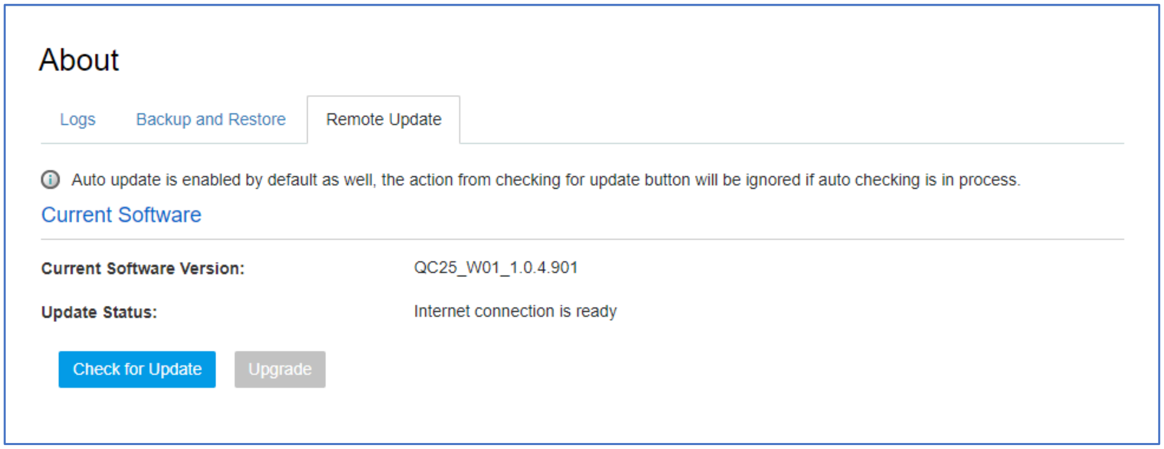
To change your Mobile Hotspot Online Portal password:

- Connect your Wi-Fi capable device to your W01 Arch.
- Open a web browser and enter https://192.168.0.1 or http://192.168.0.1.

Updating Your W01 Arch Software

Your W01 Arch checks for software upgrade availability every 24 hours. When a new version is detected, the device will download the new version and begin the upgrade automatically.

You can also check for software upgrade availability manually through your W01 Online Portal > About > Remote Update. Note: Prior to a manual upgrade, please make sure the battery level is higher than 35%. Loss of power during the upgrade could damage the device.



About

Auto update is enabled by default as well, the action from checking for update button will be ignored if auto checking is in process.

Current Software

Current Software Version: QC25_W01_1.0.4.901

Update Status: Internet connection is ready

Click the “Check for Update” button. If a new software version is detected, the “Upgrade” button will become active (blue color).

Click the “Upgrade” button to launch the software upgrade manually. Once the upgrade is completed, the device will reboot and the new software version will display.

Note: “Check for Update” button is only active (blue color) every 6 hours.

Managing Your Mobile Hotspot

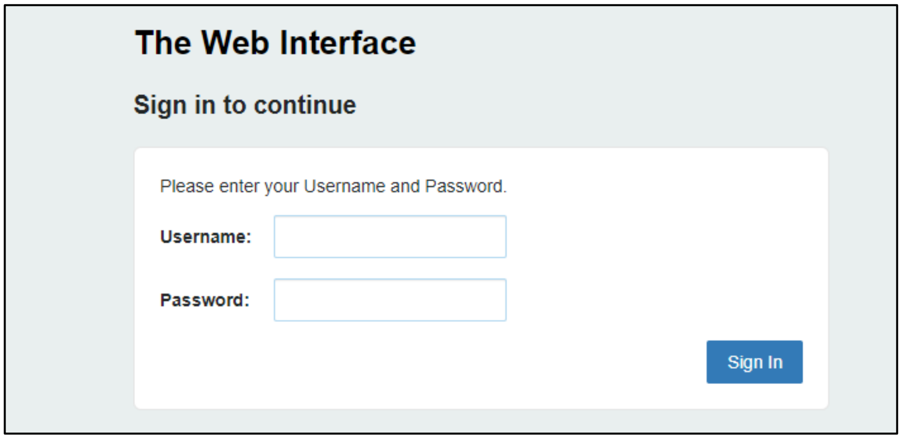
You can access the W01 Arch Mobile Hotspot Online Device Management Portal (Online Portal) using an internet browser.

If there is a firmware upgrade in the future, the Online Portal may be changed without notice.

To access W01 Arch Mobile Hotspot using a browser:

- Connect your Wi-Fi capable device to the W01 Arch.
- Open a web browser on your connected device and enter either https://192.168.0.1 or http://192.168.0.1 in the URL address bar.
- Enter the Username/Password and Click Login. If you entered the correct password, the Online Portal screen appears.

NOTE:
a) For T-Mobile and all other users, "admin" is the default for both username and password.
b) For Verizon users, "admin" is the username. For password, please check your device label for the unique Online Portal password.



The Web Interface

Sign in to continue

Please enter your Username and Password.

Username:

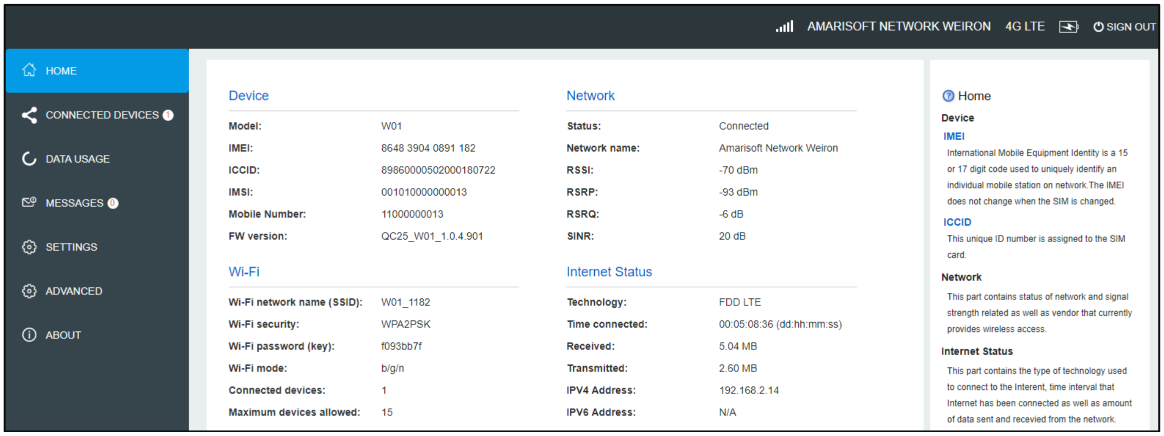
Password:

Home

The W01 Arch Mobile Hotspot Online Device Management Portal (Online Portal) allows you to quickly access all menu options for your W01 Arch.

- HOME
- CONNECTED DEVICES
- DATA USAGE
- MESSAGES
- SETTINGS
- ADVANCED

- ABOUT



Device

Model:	W01
IMEI:	8648 3904 0891 182
ICCID:	89860000502000180722
IMSI:	001010000000013
Mobile Number:	11000000013
FW version:	QC25_W01_1.0.4.901

Wi-Fi

Wi-Fi network name (SSID):	W01_1182
Wi-Fi security:	WPA2PSK
Wi-Fi password (key):	f093bb7f
Wi-Fi mode:	b/g/n
Connected devices:	1
Maximum devices allowed:	15

Network

Status:	Connected
Network name:	Amarisoft Network Weiron
RSSI:	-70 dBm
RSRP:	-93 dBm
RSRQ:	-6 dB
SINR:	20 dB

Internet Status

Technology:	FDD LTE
Time connected:	00:05:08:36 (dd:hh:mm:ss)
Received:	5.04 MB
Transmitted:	2.60 MB
IPV4 Address:	192.168.2.14
IPV6 Address:	N/A

Home

Device

IMEI

International Mobile Equipment Identity is a 15 or 17 digit code used to uniquely identify an individual mobile station on network.The IMEI does not change when the SIM is changed.

ICCID

This unique ID number is assigned to the SIM card.

Network

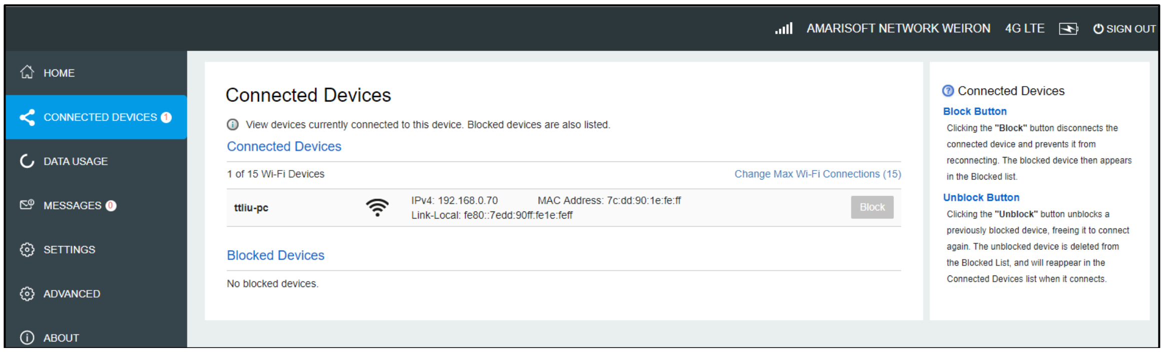
This part contains status of network and signal strength related as well as vendor that currently provides wireless access.

Internet Status

This part contains the type of technology used to connect to the Interent, time interval that Internet has been connected as well as amount of data sent and recevied from the network.

Connected Devices

On this page, you can see Connected Devices, **Blocked Devices** and **Change Max Connections**.



Connected Devices

View devices currently connected to this device. Blocked devices are also listed.

Connected Devices

1 of 15 Wi-Fi Devices — Change Max Wi-Fi Connections (15)

ttliu-pc — IPv4: 192.168.0.70 — MAC Address: 7c:dd:90:1e:fe:ff — Link-Local: fe80::7edd:90ff:fe1e:feff

Blocked Devices

No blocked devices.

Connected Devices

Block Button

Clicking the **"Block"** button disconnects the connected device and prevents it from reconnecting. The blocked device then appears in the Blocked list.

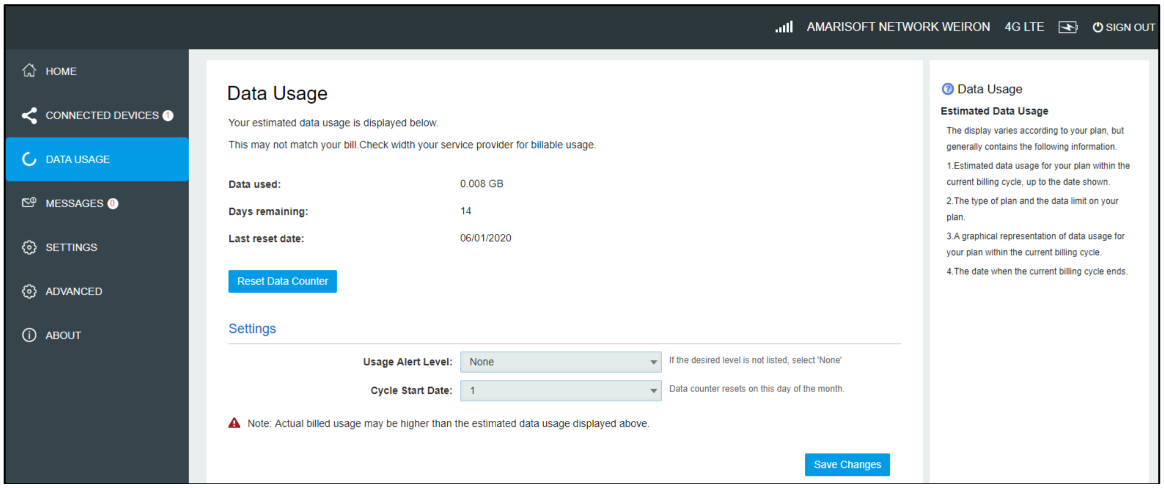
Unblock Button

Clicking the **"Unblock"** button unblocks a previously blocked device, freeing it to connect again. The unblocked device is deleted from the Blocked List, and will reappear in the Connected Devices list when it connects.

- **Connected Devices**: This field lists the device(s) connected to your W01 Arch.
- **Change Max Connections**: The default max connection is 15. Click this button and it will take you to the Wi-Fi Settings where you can change the Max Wi-Fi Connections.
- To block a device, choose a desired device and click the Block button. The Wi-Fi connection to the blocked device will be disconnected and the blocked device will appear in the Blocked Devices list.
- Blocked Devices shows the devices that are blocked. Choose a blocked device and click Unblock button, this device will disappear from the “Blocked Devices” list. It will show in the “Connected Devices” again after it connects to your W01 Arch .

Data Usage

Your estimated data usage is displayed below.
This may not match your bill. Check with your service provider for billable usage.



Data Usage

Your estimated data usage is displayed below.

This may not match your bill.Check width your service provider for billable usage.

Data used:	0.008 GB
Days remaining:	14
Last reset date:	06/01/2020

Settings

Usage Alert Level: None — If the desired level is not listed, select 'None'

Cycle Start Date: 1 — Data counter resets on this day of the month.

Note: Actual billed usage may be higher than the estimated data usage displayed above.

Data Usage

Estimated Data Usage

The display varies according to your plan, but generally contains the following information.

1.Estimated data usage for your plan within the current billing cycle, up to the date shown.

2.The type of plan and the data limit on your plan.

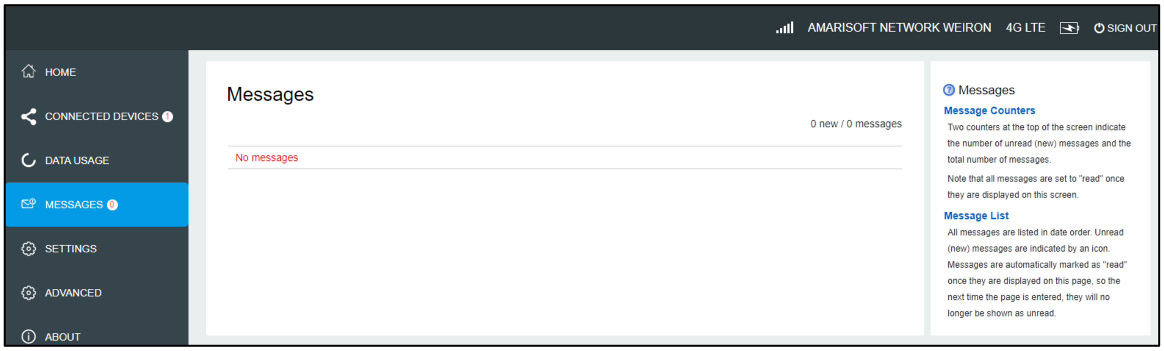
3.A graphical representation of data usage for your plan within the current billing cycle.

4.The date when the current billing cycle ends.

Choose Day of Month, Usage Limit and Click Save Changes to save your settings.

Messages

Messages page displays SMS messages sent to you by Wireless Carrier.



Messages

0 new / 0 messages

No messages

Messages

Message Counters

Two counters at the top of the screen indicate the number of unread (new) messages and the total number of messages.

Note that all messages are set to "read" once they are displayed on this screen.

Message List

All messages are listed in date order. Unread (new) messages are indicated by an icon. Messages are automatically marked as "read" once they are displayed on this page, so the next time the page is entered, they will no longer be shown as unread.

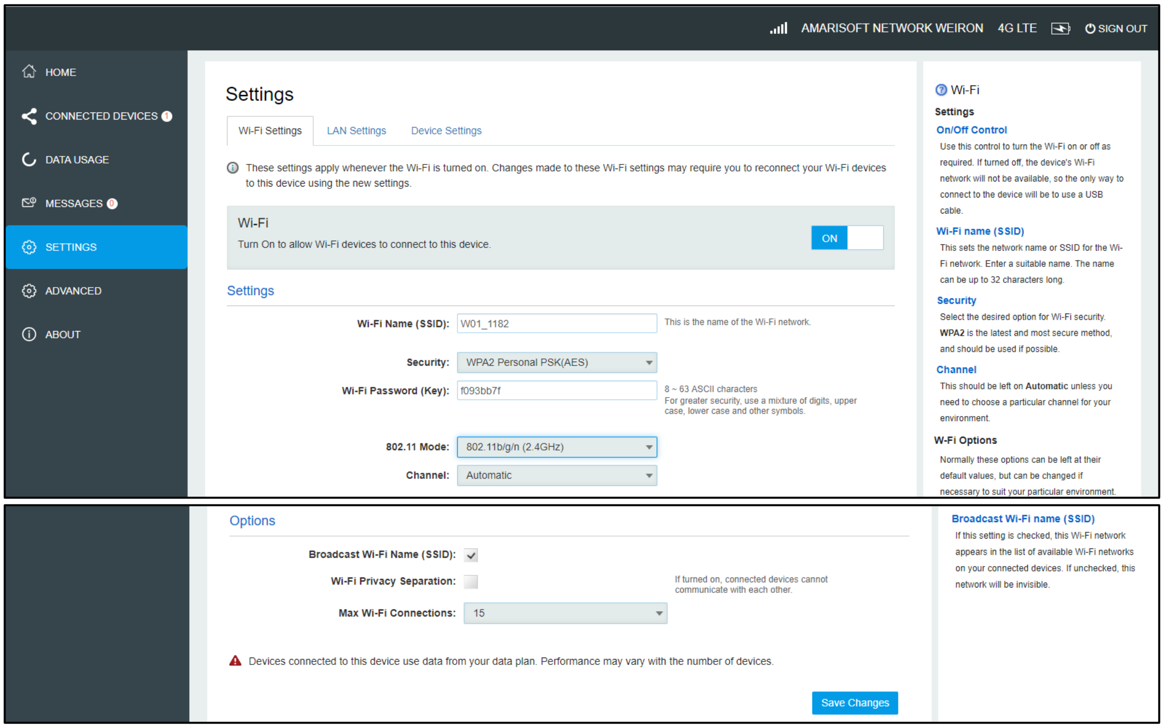
The number of unread messages displays to the right of the message icon.
When a new message arrives, the message icon appears. A maximum of 30 messages can be stored.

You can see the message contents by clicking the Messages menu on your Mobile Hotspot Online Portal. To delete a selected message, click the trash bin icon to the right of the message date and timeline. To delete all messages, click the Delete All Messages button.

Settings

The Settings page has the following menu options.

- Wi-Fi Setting
- LAN Settings
- Device Settings



Settings

These settings apply whenever the Wi-Fi is turned on. Changes made to these Wi-Fi settings may require you to reconnect your Wi-Fi devices to this device using the new settings.

Wi-Fi

Turn On to allow Wi-Fi devices to connect to this device.

Settings

Wi-Fi Name (SSID): W01_1182 — This is the name of the Wi-Fi network.

Security: WPA2 Personal PSK(AES)

Wi-Fi Password (Key): f093bb7f — 8 ~ 63 ASCII characters. For greater security, use a mixture of digits, upper case, lower case and other symbols.

802.11 Mode: 802.11b/g/n (2.4GHz)

Channel: Automatic

Options

Broadcast Wi-Fi Name (SSID): ☑

Wi-Fi Privacy Separation: ☐ — If turned on, connected devices cannot communicate with each other.

Max Wi-Fi Connections: 15

Devices connected to this device use data from your data plan. Performance may vary with the number of devices.

Wi-Fi

Settings

On/Off Control

Use this control to turn the Wi-Fi on or off as required. If turned off, the device's Wi-Fi network will not be available, so the only way to connect to the device will be to use a USB cable.

Wi-Fi name (SSID)

This sets the network name or SSID for the Wi-Fi network. Enter a suitable name. The name can be up to 32 characters long.

Security

Select the desired option for Wi-Fi security. **WPA2** is the latest and most secure method, and should be used if possible.

Channel

This should be left on **Automatic** unless you need to choose a particular channel for your environment.

W-Fi Options

Normally these options can be left at their default values, but can be changed if necessary to suit your particular environment.

Broadcast Wi-Fi name (SSID)

If this setting is checked, this Wi-Fi network appears in the list of available Wi-Fi networks on your connected devices. If unchecked, this network will be invisible.

Wi-Fi settings

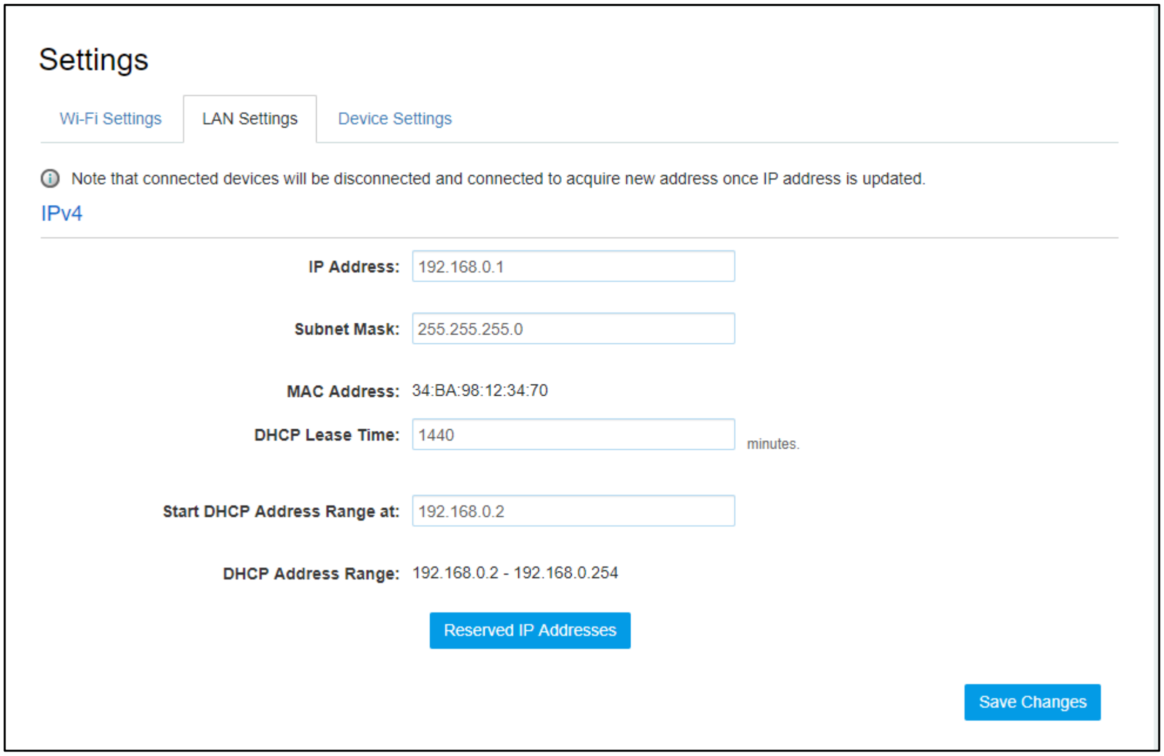
These settings apply whenever the Wi-Fi is turned on. Changes made to these Wi-Fi settings may require you to reconnect your Wi-Fi devices for the new settings to come into effect.

- **Wi-Fi ON/OFF:**
  Turn on to allow Wi-Fi devices to connect to this device. Wi-Fi devices will not connect to this device after it is turned off.
- **Wi-Fi name(SSID):**
  To identify your wireless network, a name called the SSID (Service Set Identifier) is used. You can set a name with a max of 32 characters. Make sure that your SSID is unique if there are other wireless networks operating in your area.
- **Security:**
  You can set the wireless security and encryption to prevent the router from unauthorized access and monitoring. The default security is WPA Personal/PSK. You can also set Security as "None", "WPA Personal/PSK","WPA2 Personal/PSK(AES)", "WPA/WPA2 Mixed Mode".
- **802.11 Mode:**
  The default is"802.11b/g/n". You can also set it as 802.11a/ac (5GHz).
- **Channel:**
  The default "Channel" is "Automatic". You can set it from channel 1 to channel 11.
- **Wi-Fi Options:**
  Wi-Fi Options include Broadcast Wi-Fi name (SSID), Wi-Fi Privacy Separation and Max Wi-Fi Connections.
- **Broadcast Wi-Fi name (SSID):**
  The wireless device can search and connect to the SSID after turning on "Broadcast Wi-Fi name (SSID)". The wireless device must input SSID manually to connect to the SSID after turning off "Broadcast Wi-Fi name (SSID)".

- **Wi-Fi privacy separation:**
  If turned on, connected devices cannot communicate with each other.
- **Maximum Wi-Fi connections:**
  The default maximum Wi-Fi connection is 15. You can set it to any number between 1 and 15.

LAN Settings

From the Online Portal, click Settings > LAN Settings to display the Hotspot WIFI. Information shown in the following figure.



ⓘ Note that connected devices will be disconnected and connected to acquire new address once IP address is updated.

IPv4

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

MAC Address: 34:BA:98:12:34:70

DHCP Lease Time: 1440 minutes.

Start DHCP Address Range at: 192.168.0.2

DHCP Address Range: 192.168.0.2 - 192.168.0.254

- **IP Address:**
  Enter the IP address of your W01 Arch Hotspot (factory default: 192.168.0.1).
- **Subnet Mask:**
  An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
- **MAC Address:**
  It is written to the device at the time of manufacture.
- **DHCP lease time:**
  The Lease Time is the amount of time a network user will be allowed connection to the router with their current dynamic IP address. Enter the amount of time in minutes and the user will be "leased" this dynamic IP address. After the time is up, the user will be assigned a new dynamic IP address automatically.
- **Start DHCP address range at:**
  Specify an IP address for the DHCP server to start with when assigning IP address. The default start address is 192.168.0.2.
- **Reserve IP Address:**

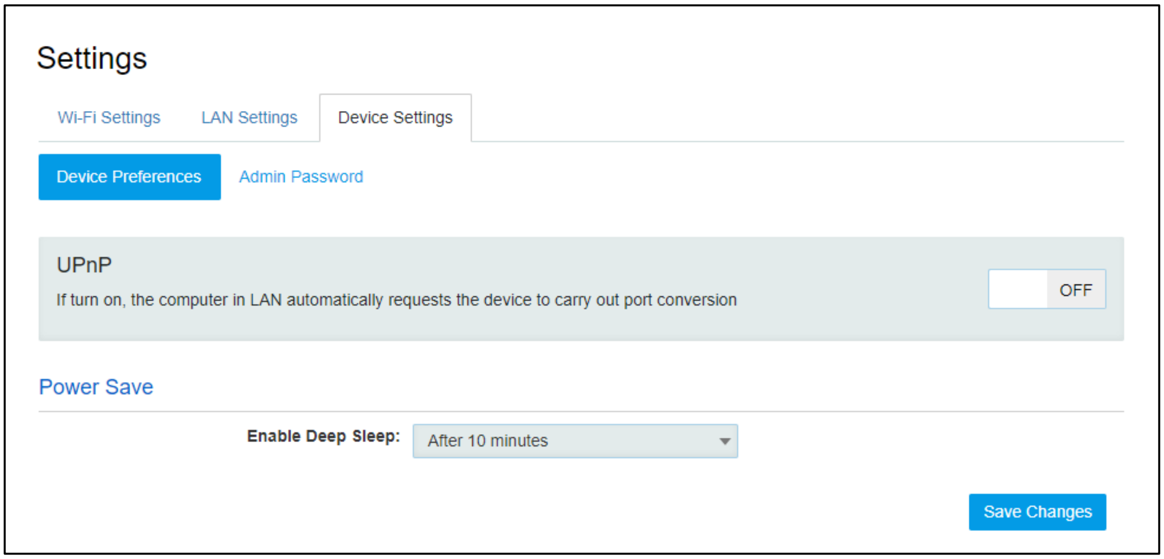
You can reserve an IP address so that it is always assigned to the same connected device. Every reserved IP address must be within the range of IP addresses used by DHCP.

Device Settings

Device Preferences

- **UPnP (Universal Plug and Play):**
  UPnP (which stands for Universal Plug and Play) is a feature that allows the devices on your home network to discover each other and access certain services. If you don't use applications that need port forwarding, such as peer-to-peer applications, game servers, and many VoIP programs, you may be better off disabling UPnP entirely.
- **Enable Deep Sleep:**
  The device will enter deep sleep after a period of inactivity. Select the desired time period to enter deep sleep.

  If no Wi-Fi device connects to your W01 Arch for more than the time set in Power Save, it's required to press the power button to reactivate the Wi-Fi for connection.



UPnP

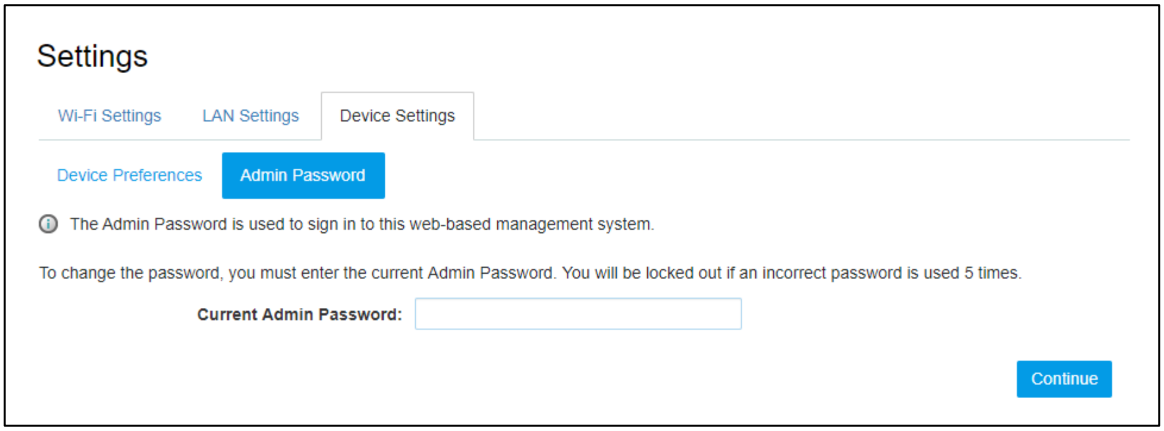
If turn on, the computer in LAN automatically requests the device to carry out port conversion

OFF

Enable Deep Sleep: After 10 minutes

Admin Password

- **Admin Password:**
  The Admin Password is used to sign in to this Online Device Management Portal. To change the password, you must enter the current Admin Password. You will be locked out after 5 incorrect password attempts. You will need to restart the W01 Arch and enter the Online Portal again.



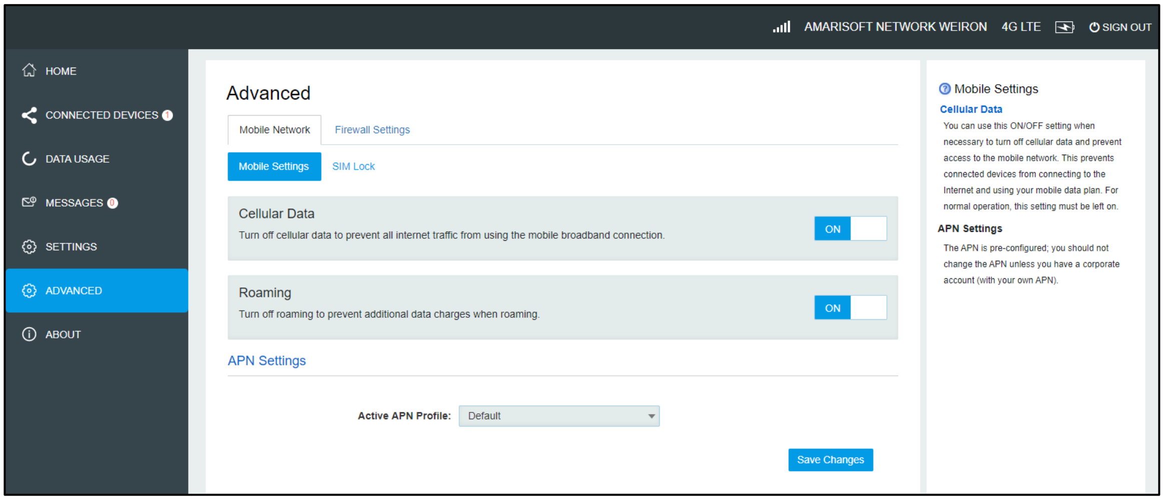
The Admin Password is used to sign in to this web-based management system.

To change the password, you must enter the current Admin Password. You will be locked out if an incorrect password is used 5 times.

Current Admin Password:

Advanced

On this page, you can see two menus: Mobile Network and Firewall Settings.



Cellular Data
Turn off cellular data to prevent all internet traffic from using the mobile broadband connection. ON

Roaming
Turn off roaming to prevent additional data charges when roaming. ON

Active APN Profile: Default

Mobile Settings

Cellular Data

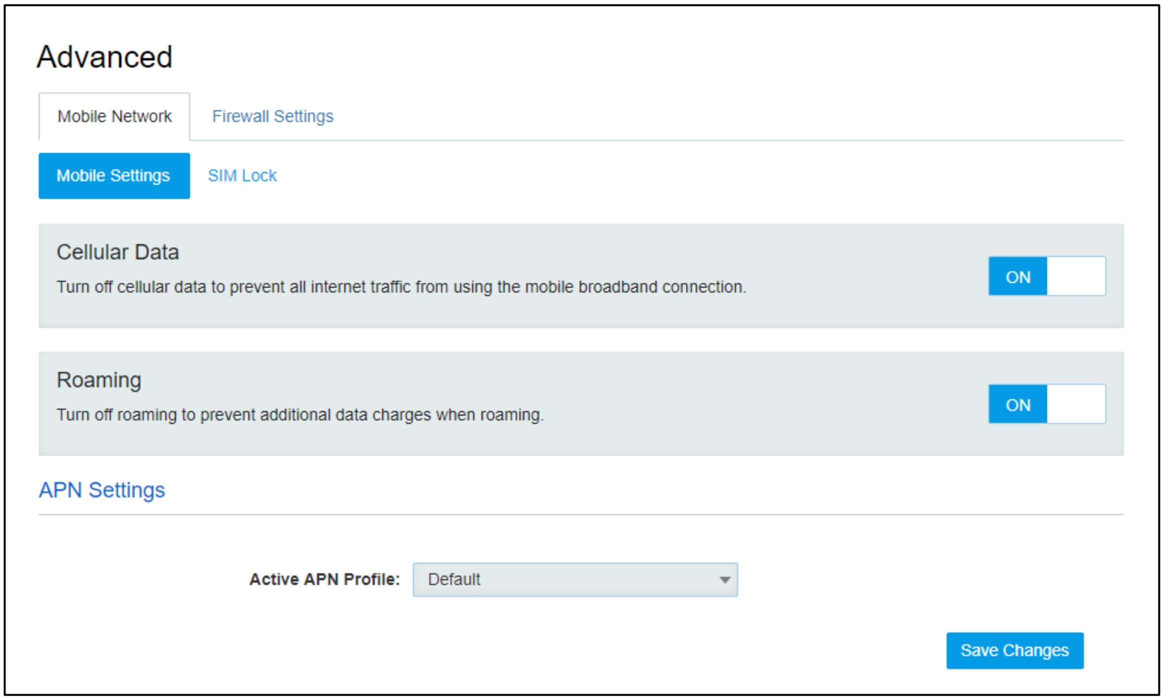
You can use this ON/OFF setting when necessary to turn off cellular data and prevent access to the mobile network. This prevents connected devices from connecting to the Internet and using your mobile data plan. For normal operation, this setting must be left on.

APN Settings

The APN is pre-configured; you should not change the APN unless you have a corporate account (with your own APN).

Mobile Network

From this page, you can see two menus: Mobile Settings and SIM Lock.



Cellular Data

Turn off cellular data to prevent all internet traffic from using the mobile broadband connection. ON

Roaming

Turn off roaming to prevent additional data charges when roaming. ON

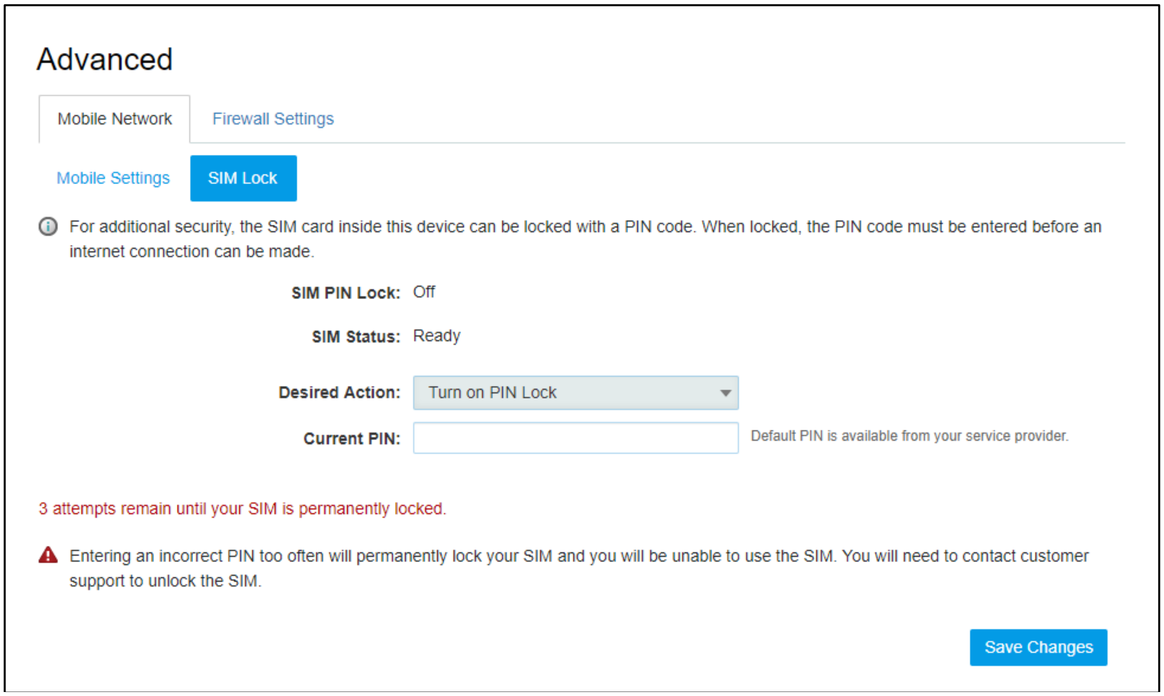
Active APN Profile: Default

Mobile Settings

- **Cellular Data**
  Turn off cellular data to prevent all internet traffic from using the mobile broadband connection.
- **Roaming**
  Turn Data Roaming on or off. Turn it ON to require confirmation before connecting to the roaming network.
- **APN Settings**
  You can use the default APN to connect to the Internet. You can also add new APNs.

SIM Lock

For additional security, the SIM card inside your W01 Arch Hotspot may be locked with a PIN code. When locked, the PIN code must be entered before the W01 Arch will connect to the internet. The default PIN is available from your service provider.
If the PIN Lock feature is ON, you will need to enter the SIM PIN every time the W01 Arch is powered on.



For additional security, the SIM card inside this device can be locked with a PIN code. When locked, the PIN code must be entered before an internet connection can be made.

SIM PIN Lock: Off

SIM Status: Ready

Desired Action: Turn on PIN Lock

Current PIN:

Default PIN is available from your service provider.

3 attempts remain until your SIM is permanently locked.

Entering an incorrect PIN too often will permanently lock your SIM and you will be unable to use the SIM. You will need to contact customer support to unlock the SIM.

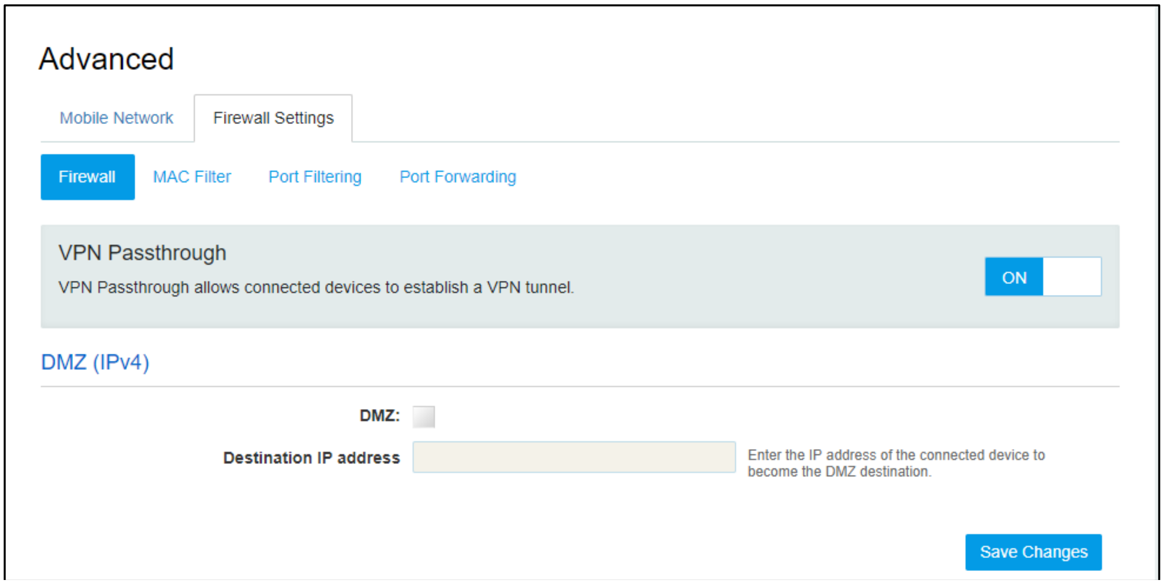
When you enter the right PIN code, the status of SIM will change to “Ready”, and you can connect to the internet.

Note:

Entering an incorrect PIN more than 3 times will permanently lock your SIM and you will need to enter the PUK code to unlock. You will need to ask your Service provider to get the PUK code.

Firewall Settings

On this page, you can see four menus: Firewall, MAC Filter, Port Filtering and Port Forwarding.



VPN Passthrough

VPN Passthrough allows connected devices to establish a VPN tunnel. ON

DMZ (IPv4)

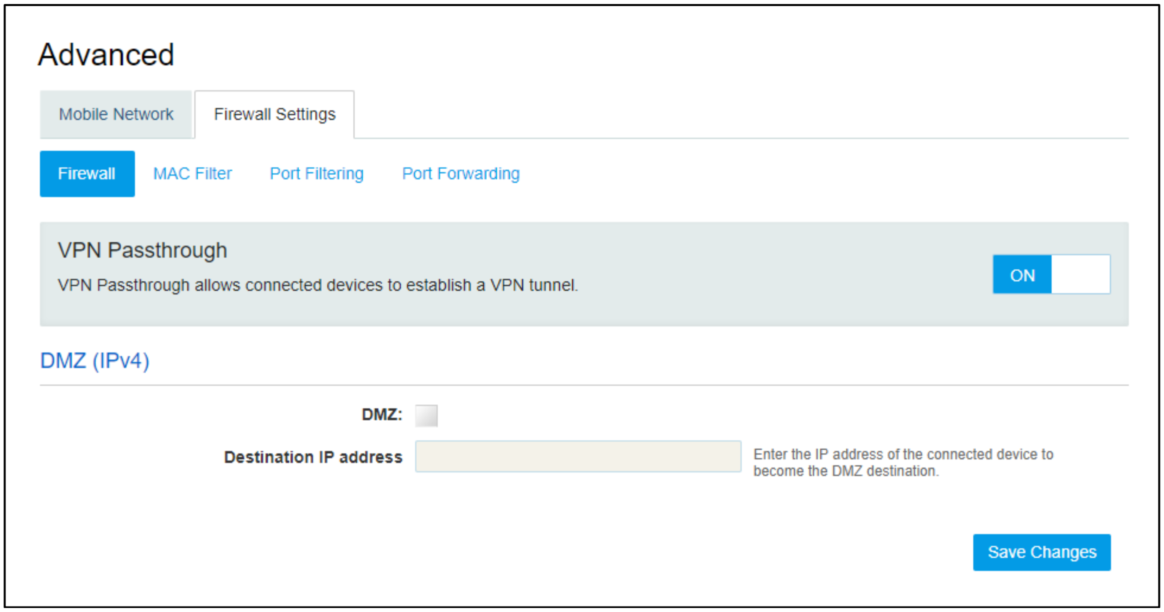
DMZ: □

Destination IP address

Enter the IP address of the connected device to become the DMZ destination.

Firewall

This page contains Firewall-related settings:



VPN Passthrough

VPN Passthrough allows connected devices to establish a VPN tunnel.

DMZ (IPv4)

DMZ: □

Destination IP address

Enter the IP address of the connected device to become the DMZ destination.

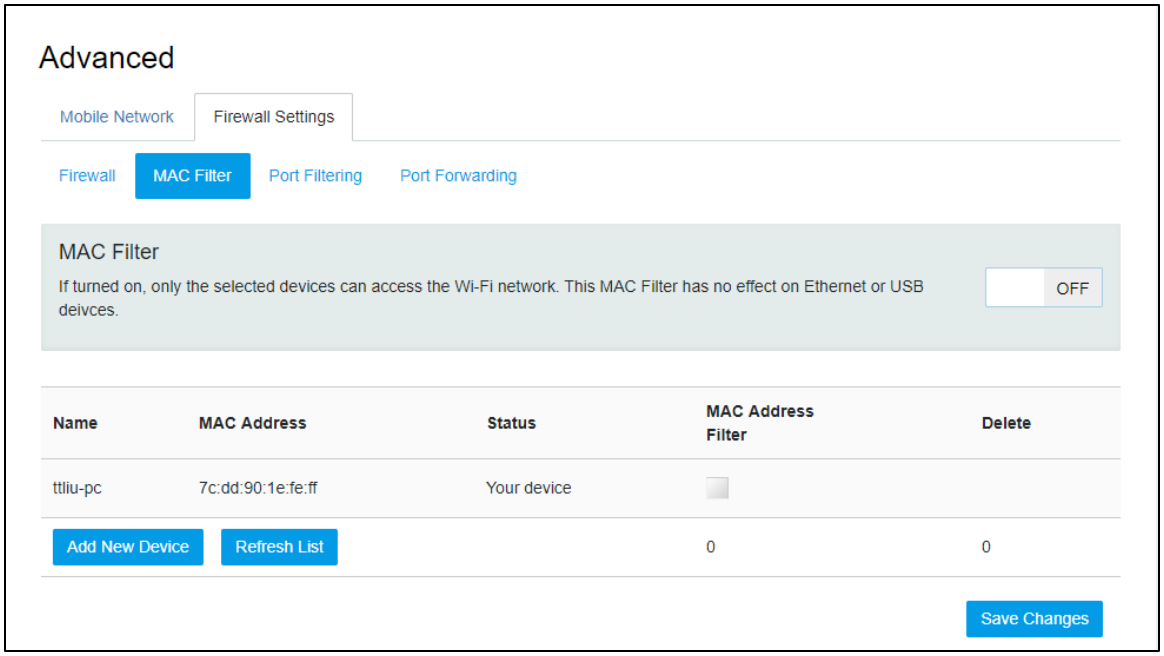
- **VPN Passthrough**

  After turned on, VPN Passthrough allows connected devices to establish a VPN tunnel.

- **DMZ(IPv4)**

  Enter the IP address of the connected device in the Destination IP address input field to become the DMZ destination. After enabling DMZ feature, all the applications of the connected device will be visited.

Mac Filter



Advanced

MAC Filter

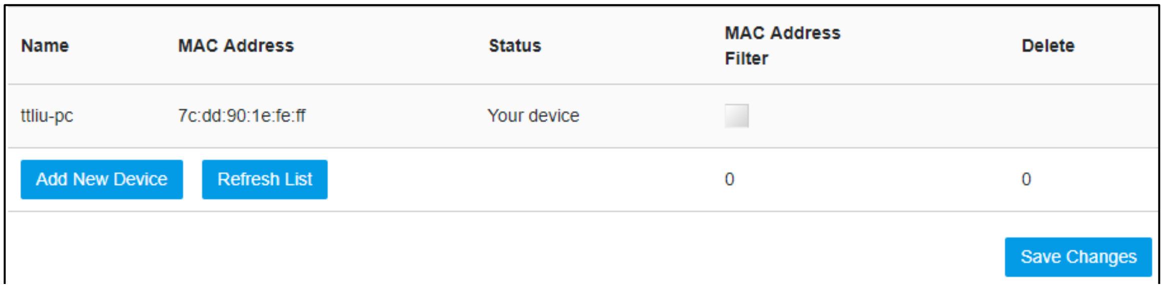
If turned on, only the selected devices can access the Wi-Fi network. This MAC Filter has no effect on Ethernet or USB deivces.

Name	MAC Address	Status	MAC Address Filter	Delete
ttliu-pc	7c:dd:90:1e:fe:ff	Your device	□	
Add New Device Refresh List			0	0

The default “MAC Filter” status is “OFF”. If the MAC Filter is on and devices are listed in MAC Address Filter list, then all of the listed devices will be able to connect to your W01 Arch.
For any given device, the interaction of the MAC Filter with the “Block” feature on the Connected Devices screen is shown on the following table.

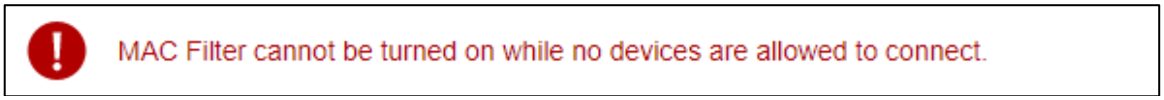
Included in Block List	Included in MAC Filter List	Connection
No	Yes	Allowed
No	No	Not allowed
Yes	Yes	Not allowed
Yes	No	Not allowed

The “Block” (Blacklist) feature is always available. After blocked, the blocked devices will disconnect from the W01 Arch.



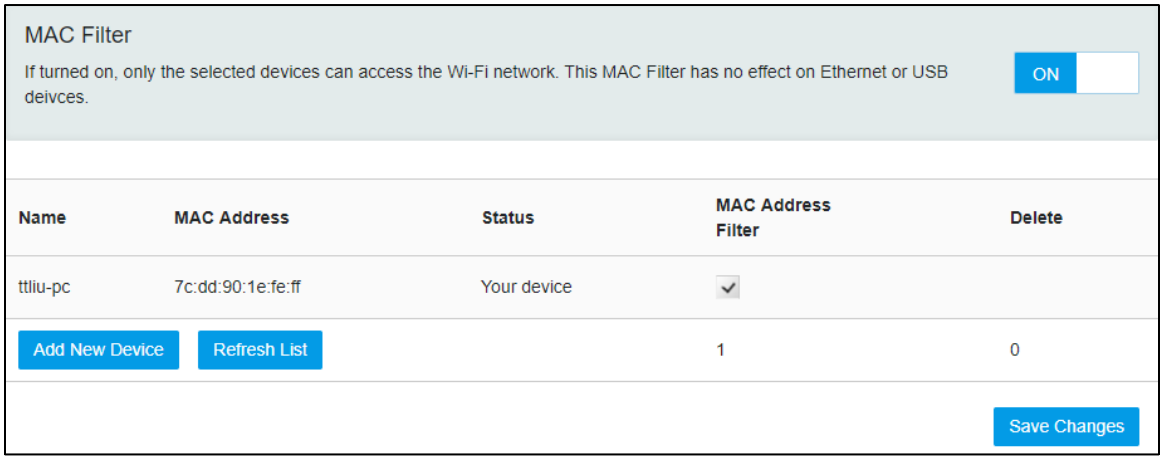
Name	MAC Address	Status	MAC Address Filter	Delete
ttliu-pc	7c:dd:90:1e:fe:ff	Your device	□	
Add New Device Refresh List			0	0

Because enabling the MAC Filter could potentially disconnect all devices, the user needs to populate the “MAC Address Filter” list first while the MAC Filter is OFF. Otherwise when you click the “ON/OFF” button, it will prompt warning information as follows:



MAC Filter cannot be turned on while no devices are allowed to connect.

After changing the “MAC Filter” to “ON”, only the local “MAC Address Filter” listed devices can connect to the W01 Arch, other devices will disconnect from the W01 Arch.

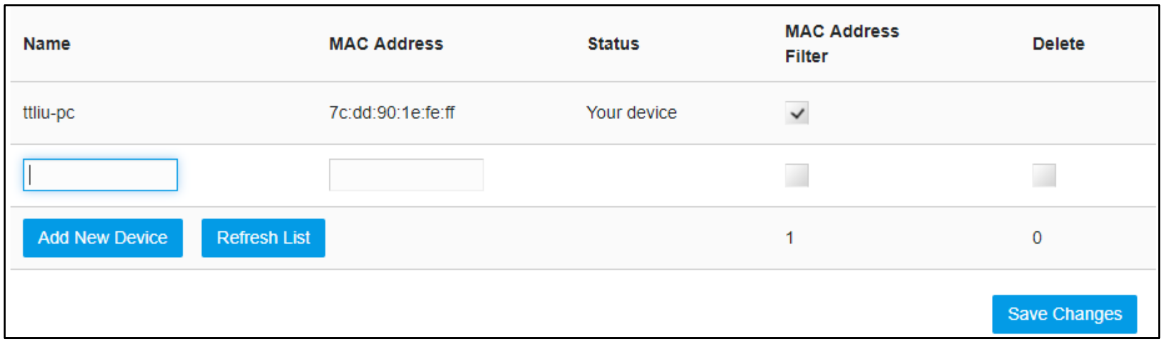


MAC Filter

If turned on, only the selected devices can access the Wi-Fi network. This MAC Filter has no effect on Ethernet or USB deivces.

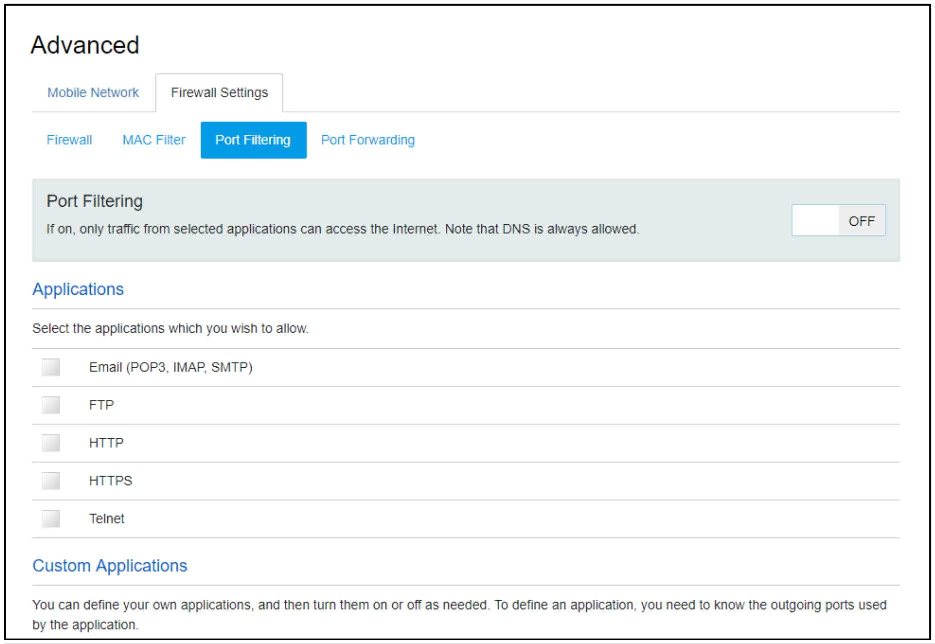
Name	MAC Address	Status	MAC Address Filter	Delete
ttliu-pc	7c:dd:90:1e:fe:ff	Your device	✓	
Add New Device	Refresh List		1	0

You can click “Add Device” button to add the devices. The added devices can connect the W01 Arch.



Name	MAC Address	Status	MAC Address Filter	Delete
ttliu-pc	7c:dd:90:1e:fe:ff	Your device	✓	
			☐	☐
Add New Device	Refresh List		1	0

Port Filtering



Advanced

Port Filtering

If on, only traffic from selected applications can access the Internet. Note that DNS is always allowed.

OFF

Applications

Select the applications which you wish to allow.

□ Email (POP3, IMAP, SMTP)

□ FTP

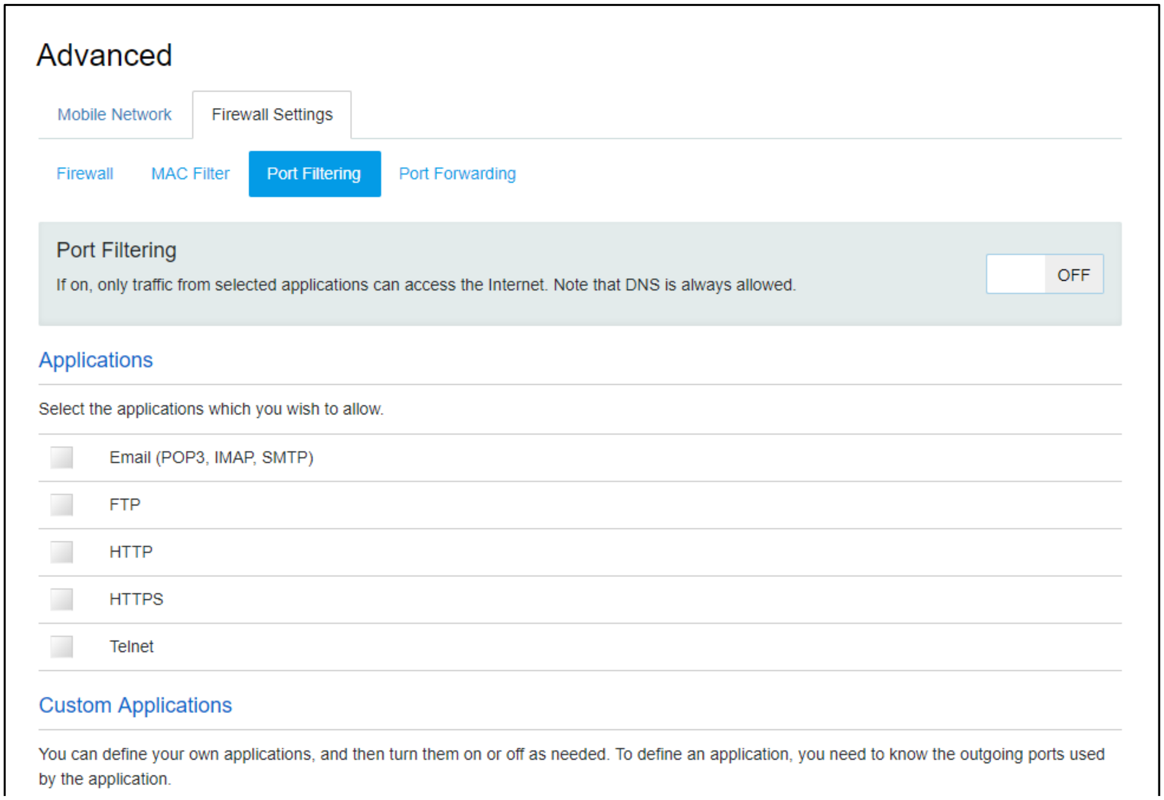
□ HTTP

□ HTTPS

□ Telnet

Custom Applications

You can define your own applications, and then turn them on or off as needed. To define an application, you need to know the outgoing ports used by the application.



Advanced

Mobile Network | Firewall Settings

Firewall | MAC Filter | Port Filtering | Port Forwarding

Port Filtering

If on, only traffic from selected applications can access the Internet. Note that DNS is always allowed.

OFF

Applications

Select the applications which you wish to allow.

□ Email (POP3, IMAP, SMTP)

□ FTP

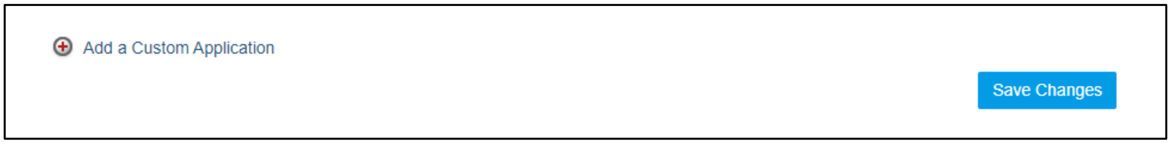
□ HTTP

□ HTTPS

□ Telnet

Custom Applications

You can define your own applications, and then turn them on or off as needed. To define an application, you need to know the outgoing ports used by the application.

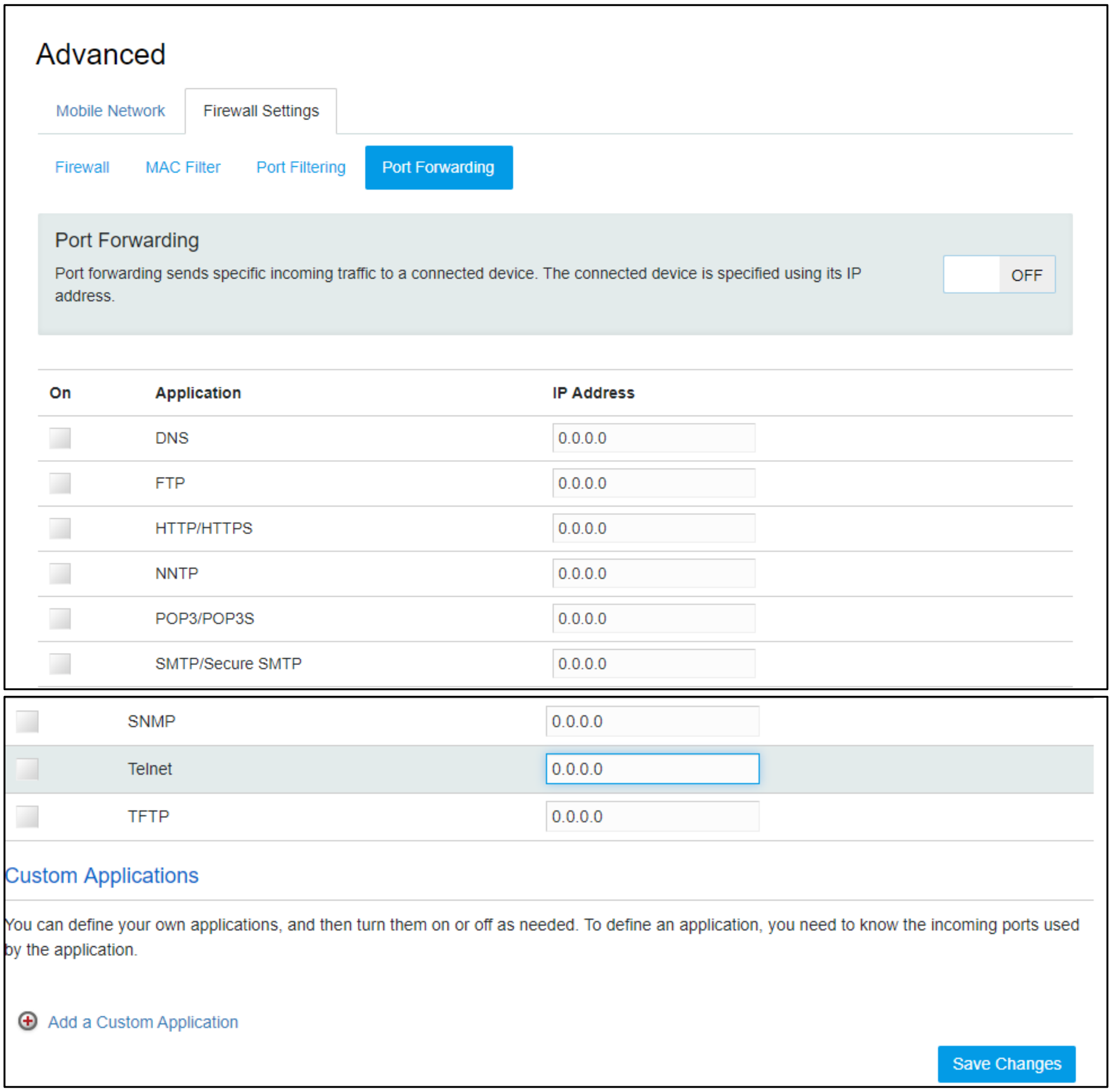


- **Applications**

  The default applications have “Email (POP3, IMAP, SMTP)”, “FTP”, “HTTP”, “HTTPS” and “Telnet”. If port filtering is on, only traffic from selected applications can access the Internet. Note that DNS is always allowed.
- **Custom Applications**

  Click “Add a Custom Application” to define your own applications, and then turn them on or off as needed. To define an application, you need to know the outgoing ports used by the application.

Port Forwarding



Port Forwarding

Port forwarding sends specific incoming traffic to a connected device. The connected device is specified using its IP address.

OFF

On	Application	IP Address
□	DNS	0.0.0.0
□	FTP	0.0.0.0
□	HTTP/HTTPS	0.0.0.0
□	NNTP	0.0.0.0
□	POP3/POP3S	0.0.0.0
□	SMTP/Secure SMTP	0.0.0.0
□	SNMP	0.0.0.0
□	Telnet	0.0.0.0
□	TFTP	0.0.0.0

Custom Applications

You can define your own applications, and then turn them on or off as needed. To define an application, you need to know the incoming ports used by the application.

- **Applications**

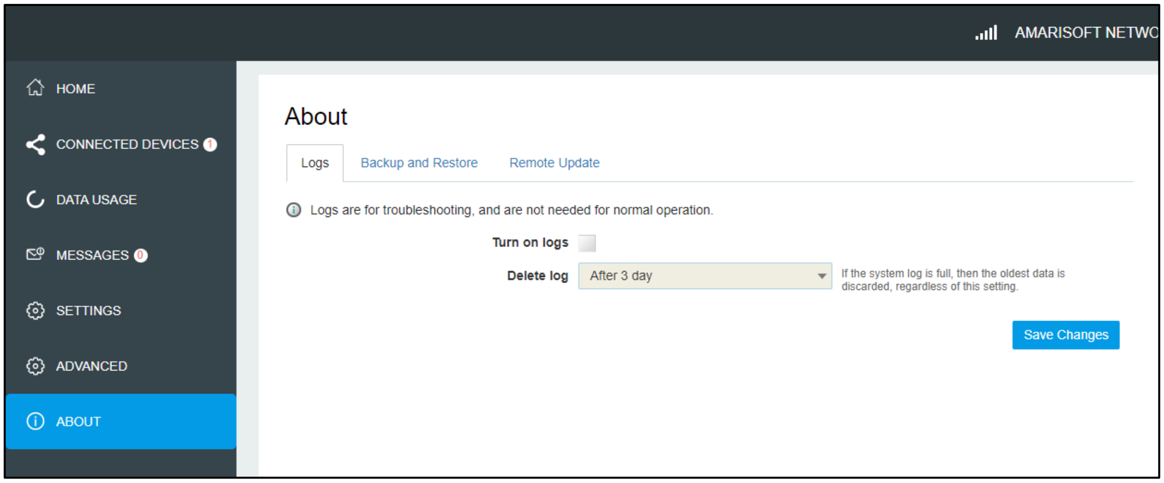
  The default applications have “DNS”, “FTP”, “HTTP”, “POP3”, “SMTP”, “SNMP”, “Telnet” and “TFTP”. Port forwarding sends specific incoming traffic to a connected device. The connected device is specified using the IP address.

- **Custom Application**

Click “Add a Custom Application” to define your own applications, and then turn them on or off as needed. To define an application, you need to know the incoming ports used by the application.

About

From the Online Portal main screen, click the About tab to view the available information.



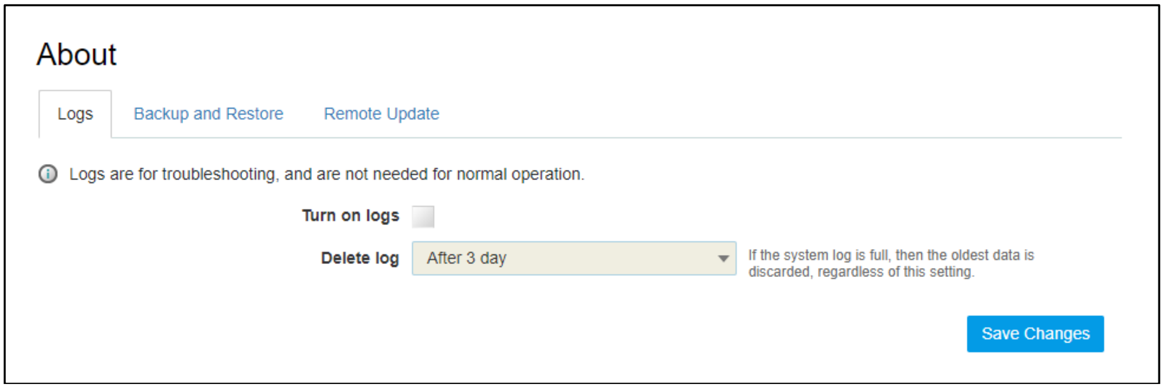
Logs are for troubleshooting, and are not needed for normal operation.

Turn on logs □

Delete log After 3 day

If the system log is full, then the oldest data is discarded, regardless of this setting.

Logs



Logs are for troubleshooting, and are not needed for normal operation.

Turn on logs □

Delete log After 3 day

If the system log is full, then the oldest data is discarded, regardless of this setting.

- **Turn on Logs**

Turn on the logs as needed.

- **Delete log**

This setting determines for how long the log data is retained. Select the desired option. Note that if the log is full, the oldest data is deleted, regardless of this setting.

- **Log**

This log contains data regarding connections to the mobile network.

- **Clear Log**

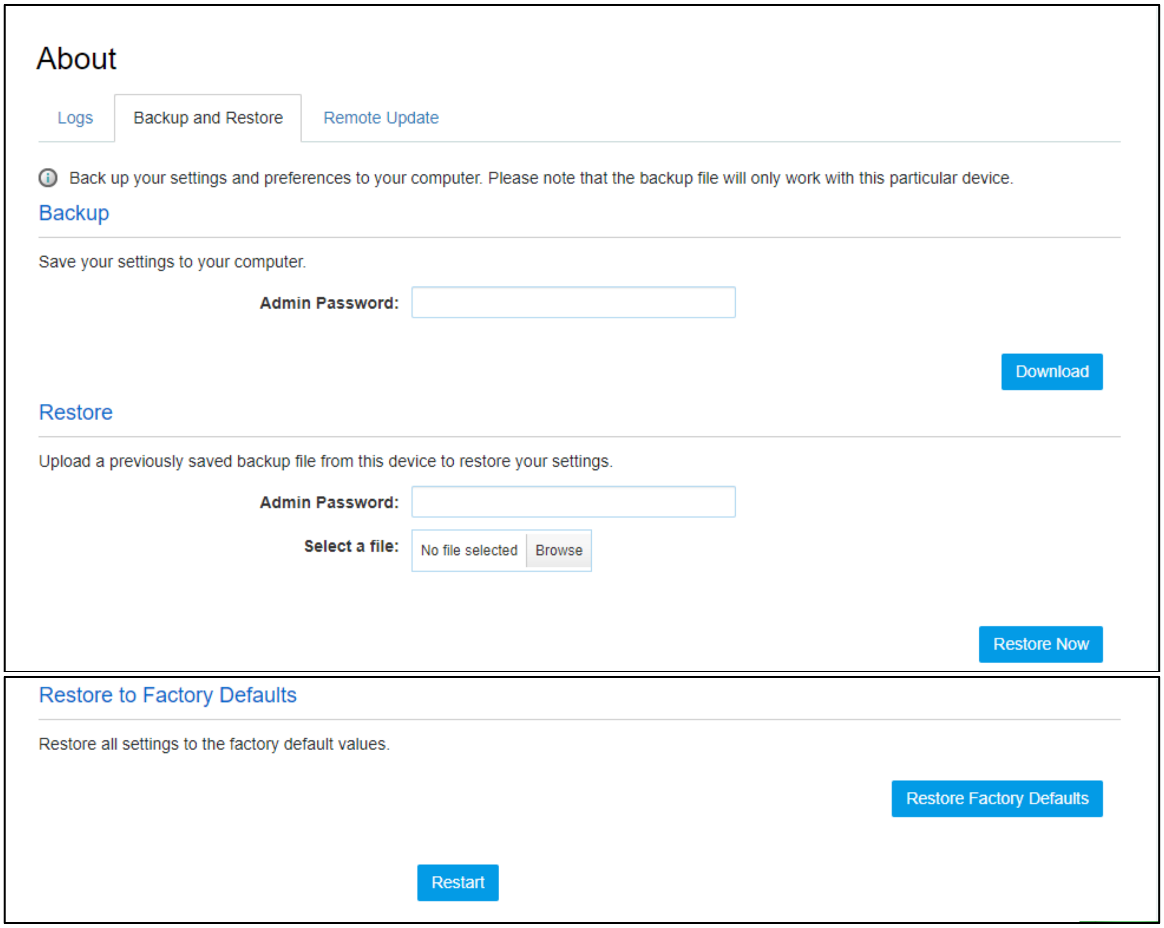
Clicking this button will delete all existing log data. This makes new data easier to read.

- **Refresh**

Use this to update the log data which is displayed.

Backup and Restore

On this page, you can operate Backup, Restore, Restore to Factory Defaults and Restart.



About

Back up your settings and preferences to your computer. Please note that the backup file will only work with this particular device.

Backup

Save your settings to your computer.

Admin Password:

Restore

Upload a previously saved backup file from this device to restore your settings.

Admin Password:

Select a file: No file selected

Restore to Factory Defaults

Restore all settings to the factory default values.

Backup

Backup your W01 Arch Hotspot settings and preferences to your computer.

Note:

- The backup file will only work with this particular W01 Arch.
- You will be locked out if an incorrect password is used too many times.

Restore

Upload a previously saved backup file from this device to restore your settings.

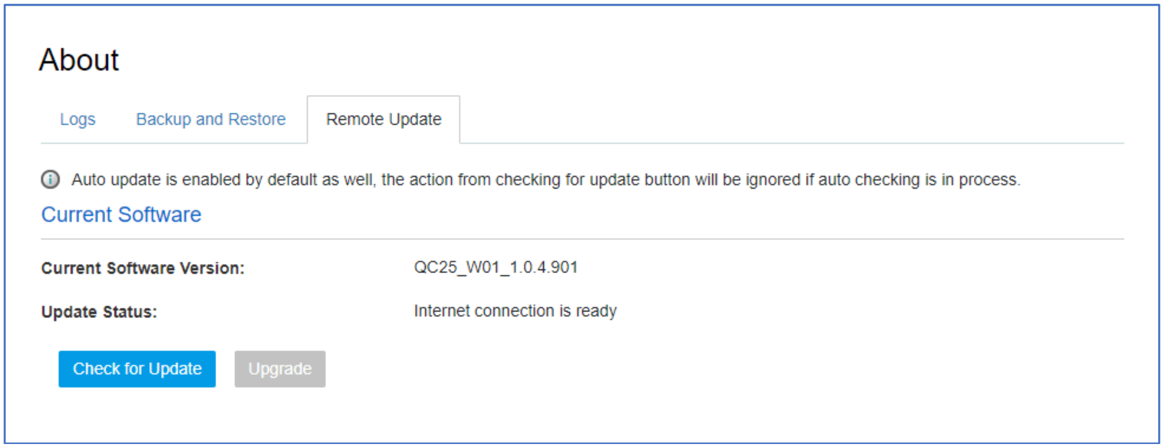
Note:

You will be locked out if an incorrect password is used too many times.

Restore to Factory Defaults

Restore all settings to the factory default values.

Remote Update



About

ⓘ Auto update is enabled by default as well, the action from checking for update button will be ignored if auto checking is in process.

Current Software

Current Software Version: QC25_W01_1.0.4.901

Update Status: Internet connection is ready

Prior to a software upgrade, please make sure the battery level is higher than 35%. Loss of power during the upgrade could damage the device.

- **Check for Update:**

“Check for Update” button is only active (blue color) every 6 hours. When active, you can click the “Check for Update” button to check for new software version. If a new version is detected, the “Upgrade” button will become active (blue color).

- **Upgrade:**

If a software upgrade is available, click the active “Upgrade” button to launch the upgrade manually. Once the upgrade is completed, the device will reboot and the new software version will display.

Question and Answer

The following tips can help solve some common problems encountered while using the W01 Arch.

Before you start

- Make sure you are using your W01 Arch in the correct geographic region (within the wireless coverage area of your service provider).
- Ensure that your wireless coverage extends to your current location by using the interactive wireless carrier’s coverage map tool.
- Ensure that you have an active service plan.
- Restarting your computer and your W01 Arch can resolve many issues.

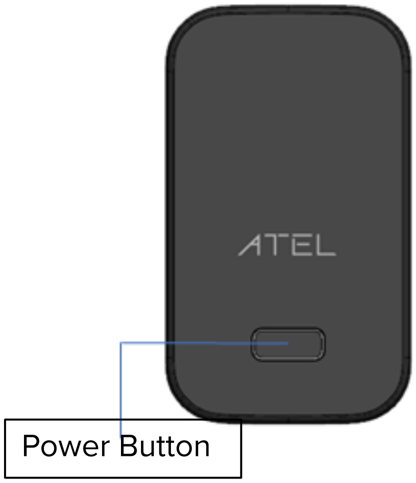
IMPORTANT! Before contacting customer care, be sure to restart both your W01 Arch and any device that is currently connected.

Common Problems and Solutions

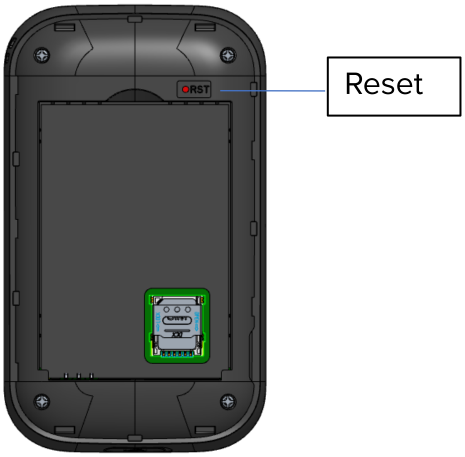
1. **W01 Arch just powered off without pressing the Power/Menu button. Why?**
   This may occur under Battery depletion.
   To restore power, manually press and hold the Power/Menu button to turn on your W01 Arch. If the battery is depleted, charge the battery with the AC charger provided.

IMPORTANT! If the power button will not start your W01 Arch (after charging), please try Power Reset (see How do I perform a Power Reset on W01 Arch? below).

2. **How do I perform a Power Reset on W01 Arch?**
   Using the power button: Press and hold the power button for 10 seconds until the W01 Arch restarts.
   By replacing the battery: If pressing and holding the power button for 10 seconds does not restart the W01 Arch, open the battery cover, take out the battery and re-install the battery after 5 seconds. Put the battery cover back and turn on the W01 Arch by pressing the power button.



3. **How do I perform a Device Reset using the RST pin hole?**
   Using the reset pin hole : Remove the back cover. Make sure the battery is installed and your W01 Arch is powered on. Use a unfolded paper clip, insert it into the RST pin hole and push down for 3 seconds, then release. Your W01 Arch will perform the reset and restart automatically.



4. **How do I perform a Factory Reset via the Online Device Management Portal?**
   Using the Mobile Hotspot Online Device Management Portal: Connect to your W01 Arch and then open the Mobile Hotspot Online Portal (https://192.168.0.1, or, http://192.168.0.1). Select About > Backup and Restore and Click Restore Factory Defaults.

5. **I cannot connect to Wi-Fi after changing Wi-Fi password.**
   Your Wi-Fi devices save the previously used Wi-Fi names associated with the passwords used to access the Wi-Fi name. When you change the Wi-Fi password only for your W01 Arch and keep the same Wi-Fi Name, the devices try to connect to your W01 Arch using the Wi-Fi name and previous Wi-Fi password saved, causing Wi-Fi authentication error.

6. **I cannot access the https://192.168.0.1.**
   Ensure that a Wi-Fi connection is enabled on your device and that you have selected the correct Wi-Fi name (SSID) for your W01 Arch connection. Also, make certain that you are entering the correct full URL address as https://192.168.0.1. If this URL address does not work, try the IP address http://192.168.0.1.

7. **I cannot access the https://192.168.0.1.**
   Ensure that you are entering the correct password for the Device Management Online Portal.
   a) For T-Mobile and all other users, "admin" is the default for both username and password.
   b) For Verizon users, "admin" is the username. For password, please check your device label for the unique Online Portal password.

   If you have forgotten your password, reset your device by following the Device Reset steps with the Reset pin hole.

Regulatory Statements

FCC Equipment Authorization ID: XYO-W01

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

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.

FCC CAUTION: Any changes or modification not expressly approved by ATEL, the party responsible for compliance could void the user's authority to operate this equipment.

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.

RF Exposure Warning Statements:

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons during the normal operations.

NOTE: The Radio Frequency (RF) emitter installed in your modem must not be located or operated in conjunction with any other antenna or transmitter, unless specifically authorized by ATEL.

Safety Hazards

Follow Safety Guidelines

Always follow the applicable rules and regulations in the area in which you are using your device. Turn your device off in areas where its use is not allowed or when its use may cause interference or other problems.

Electronic Devices

Most modern electronic equipment is shielded from radio frequency (RF) signals. However, inadequately shielded electronic equipment may be affected by the RF signals generated by your device.

Medical and Life Support Equipment

Do not use your device in healthcare facilities or where medical life support equipment is located as such equipment could be affected by your device's external RF signals.

Pacemakers

- It is recommended to maintain a minimum separation of six inches between a RF device and a pacemaker in order to avoid potential interference with the pacemaker.
- Persons with pacemakers should always follow these guidelines:
- Always keep the device at least six inches away from a pacemaker when the device is turned on.
- Place your device on the opposite side of your body where your pacemaker is implanted in order to add extra distance between the pacemaker and your device.
- Avoid placing a device that is on next to a pacemaker (e.g., do not carry your device in a shirt or jacket pocket that is located directly over the pacemaker).
- If you are concerned or suspect for any reason that interference is taking place with your pacemaker, turn your device OFF immediately.

Hearing Devices

When some wireless devices are used with certain hearing devices (including hearing aids and cochlear implants) users may detect a noise which may interfere with the effectiveness of the hearing device.

Use of Your Device while Operating a Vehicle

Please consult the manufacturer of any electronic equipment that has been installed in your vehicle as RF signals may affect electronic systems in motor vehicles.
Please do not operate your device while driving a vehicle. This may cause a severe distraction and in some areas, it is against the law.

Use of Your Device on an Aircraft

Don't use your device during flight， it may violate FAA regulations. Because your device may interfere with onboard electronic equipment, always follow the instructions of the airline personnel and turn your device OFF.

Blasting Areas

In order to avoid interfering with blasting operations, your device should be turned OFF when in a blasting area or in an area with posted signs indicating that people in the area must turn off two-way radios. Please obey all signs and instructions when you are in and around a blasting area.

Proper Battery & Adapter Use and Disposal

- Do not disassemble or open crush, bend or deform, puncture or shred.
- Do not modify or remanufacture, attempt to insert foreign objects into the battery, immerse or expose to water or other liquids, expose to fire, explosion or another hazard.
- Only use the battery for the system for which it is specified.
- Do not short circuit a battery or allow metallic conductive objects to contact battery terminals.
- Replace the battery only with another battery that has been qualified with the system per this standard. Use of an unqualified battery may present a risk of fire, explosion, leakage or other hazard. Only authorized service providers shall replace the battery.
- Promptly dispose of used batteries in accordance with local regulations.
- Battery usage by children should be supervised.
- Avoid dropping the battery or the device. Dropping the battery or device, especially on a hard surface, might cause damage. If you suspect damage on the battery or the device, consider replacing them.
- Improper battery use may result in a fire, explosion or another hazard.

Limited Warranty

The full ATEL USA Warranty Policy can be found at www.atel-usa.com/warranty. On this page you can "Start a Warranty Claim", "Check on an Existing Claim" and read our Warranty Policy by clicking on "ATEL's Warranty Policy". Please follow all warranty instructions available and if you have any questions contact us at support@atel-usa.com.

Trademark