

ND100

USER GUIDE

By :



Index

Contents

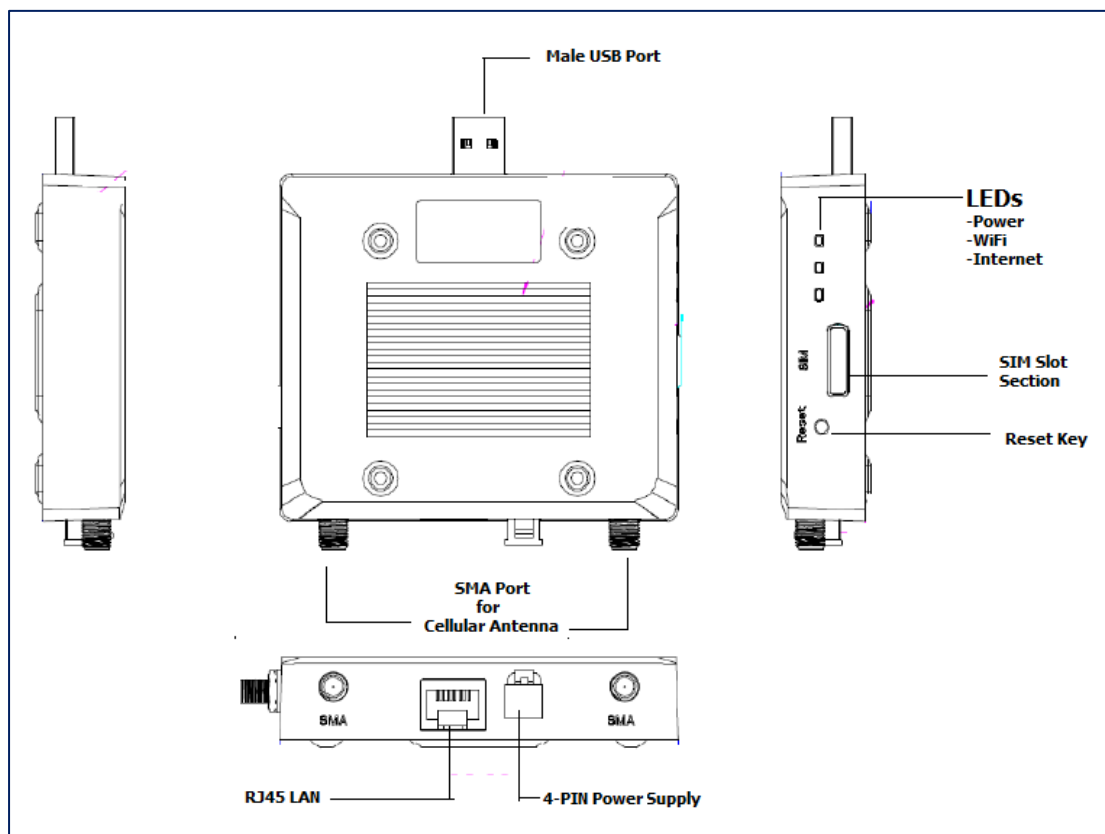
About Product.....	3
Interfaces	3
Power on the ND100:.....	4
Configure ND100.....	4
Homepage	5
Manage WIFI User.....	6
Settings.....	7
Advance Settings	14

About Product

ND100 is a Mini Router is a CAT-4 device which can support high download and upload throughput as per the 3GPP standards with following features :

- Supports FDD-LTE on band
- Supports WCDMA on band
- Supports WIFI 802.11b/g/n on 2.4GHz & 802.11ac on 5GHz with Internal Antennas.
- Max 8 users can connect over WIFI
- 1 x RJ45 Port for LAN (10/100 BaseT support)
- SIM Slot with 3FF MICRO SIM standard
- 2x RP-SMA connectors for Cellular Antennas

Interfaces



Let's start using ND100

1. Insert SIM card with 3FF (MICRO SIM) into SIM slot section.
2. Connect both antennas provided with packaging.

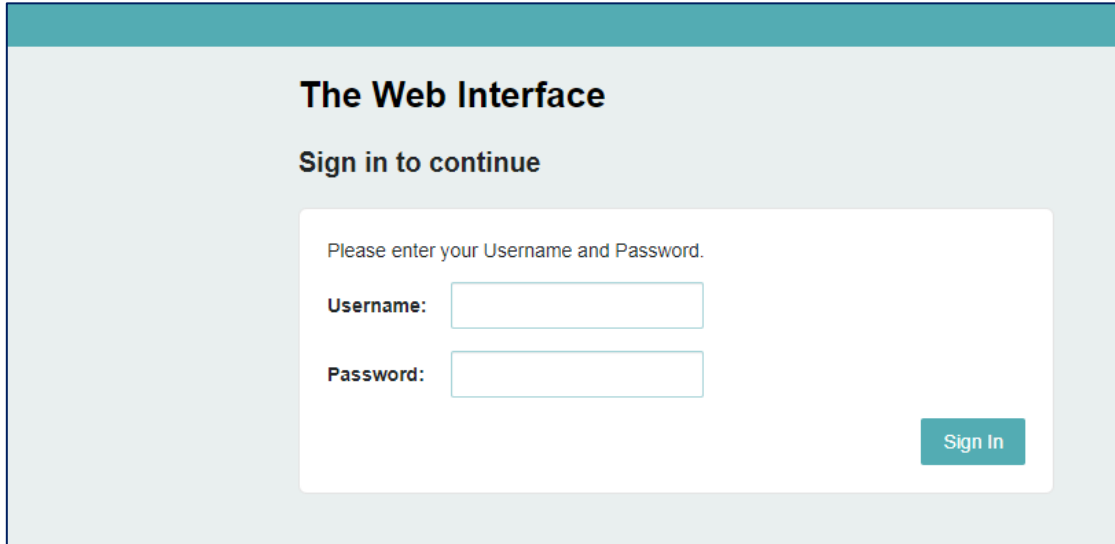
Power on the ND100:

- ND100 can be power on using USB, Just connect USB to your PC.
OR
Using 4 PIN Molex connector for Power Supply (Ref. Interface section). Kindly use the adaptor & cables provided with packaging.
- Power Led will be turned out Green, which indicates that device is powered on successfully and it is ready to use or setup the device configurations if required.

Configure ND100

- Turn ON the device and connect LAN port with your PC .

- Device support webGUI management. Which means it can be setup using any web browser which makes this device so easy to configure
- Once your PC recognized this device , you can open any web browser
- Input <http://192.168.0.1> on address bar and hit enter.
- User will get login window for ND100 as below



User needs to enter admin/admin for Username/Password.

NOTE:

- Default password is admin but it can be modify.
- After press reset switch or select factory default function from webGUI, Password will be again as default (admin) with all the default configurations.

- After input correct credentials, click on Sign In tab.
User can login to web management page.

Homepage

- After log-in , User can see **homepage** where all the basic details about ND100 are displayed like:

IMEI

Firmware & Hardware version

SIM card ICCID

Network Status and Signals information

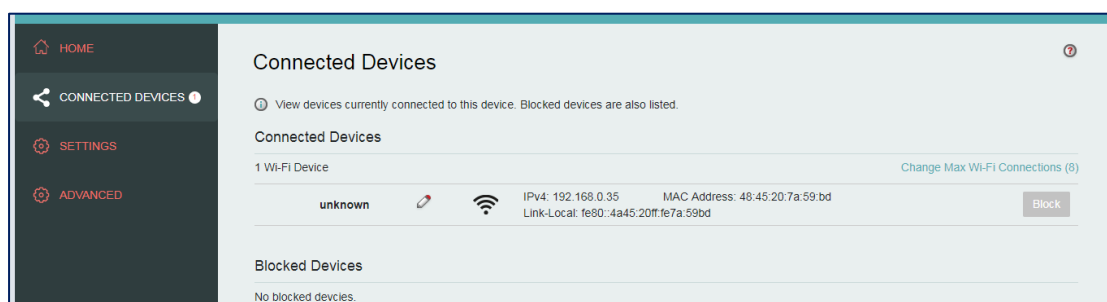
WIFI Status with SSID, Password and connected users

Internet status with available WAN IP, connected time and data usage.



Manage WIFI User

- On **Connected Devices** page, User can see all the connected devices details like IP & MAC address and if required, user can block any unwanted or suspicious connected device by simply click on **Block** tab.



All the blocked devices can be seen under Blocked devices. Where user can also unblock them if required.

Settings

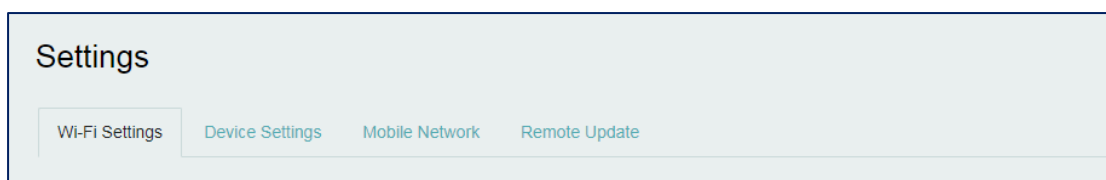
- On this section, User can see different important configuration settings like:

WIFI Setting

Device Settings

Mobile Network

Remote Update (Firmware over the Air feature)



WIFI Settings

- On this page, User can configure the WIFI feature like SSID, Security , Password, Transmission mode & channel etc. (ref. image)

 A screenshot of the "Wi-Fi" settings page. At the top, there's a toggle switch labeled "Wi-Fi" with the text "Turn On to allow Wi-Fi devices to connect to this device." and an "ON" button. Below this is a "Settings" section with several fields: "Wi-Fi Name (SSID)" with the value "default_CC9980" and a description "This is the name of the Wi-Fi network."; "Security" set to "None" with a warning: "Warning: Anyone can use this Wi-Fi network and your data plan. WPA2 is strongly recommended."; "Wi-Fi Password (Key)" with an empty field and a note: "Wi-Fi security is disabled. All users can connect to this Wi-Fi network without needing a password (not recommended)."; "802.11 Mode" set to "802.11bgn"; and "Channel" set to "Automatic". Below the settings is an "Options" section with "Broadcast Wi-Fi Name (SSID)" checked, "Wi-Fi Privacy Separation" checked with a note "If turned on, connected devices cannot communicate with each other.", and "Max Wi-Fi Connections" set to "8". At the bottom, there's a warning icon and text: "Devices connected to this device use data from your data plan. Performance may vary with the number of devices." and a "Save Changes" button.

WiFi Name (SSID): Subscriber set identity; User can define this field as per their requirement. Default SSID is “**default_XXXXXX**”(last six characters for WIFI MAC address)

Security: available options are None (as Default), WAP2 Personal (AES) & WPA/WPA2 Mixed Mode

WIFI Password (Key): User can setup password **8~ 63 ASCII characters** for password. By Default , There is no password.

802.11 Mode: Supports **802.11 bgn** (as default) & 802.11ac.

Channel: Supports **Automatic** channel (as default) and manual channel from 1 ~ 9 for 802.11bgn
Supports **Automatic** channel (as default) and manual channel from 36, 40, 44, 48, 149, 153, 157, 161& 165 for 802.11ac.

Broadcast Wi-Fi Name (SSID): Enabled as default. If disabled, SSID name will not be visible during WIFI AP scan.

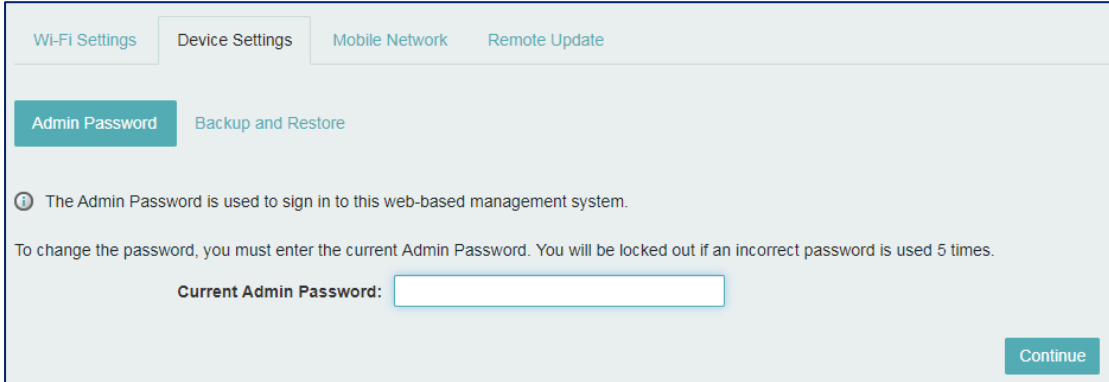
Wi-Fi Privacy Separation: Enabled as default, User can uncheck it wants to disable this security function.

Max WIFI connections: Default is **8**, user can defined the number of devices (1~8) which can connect to ND100 over WIFI

NOTE: After change any configuration, User needs to click on Save Changes tab on below to save the modify configurations.

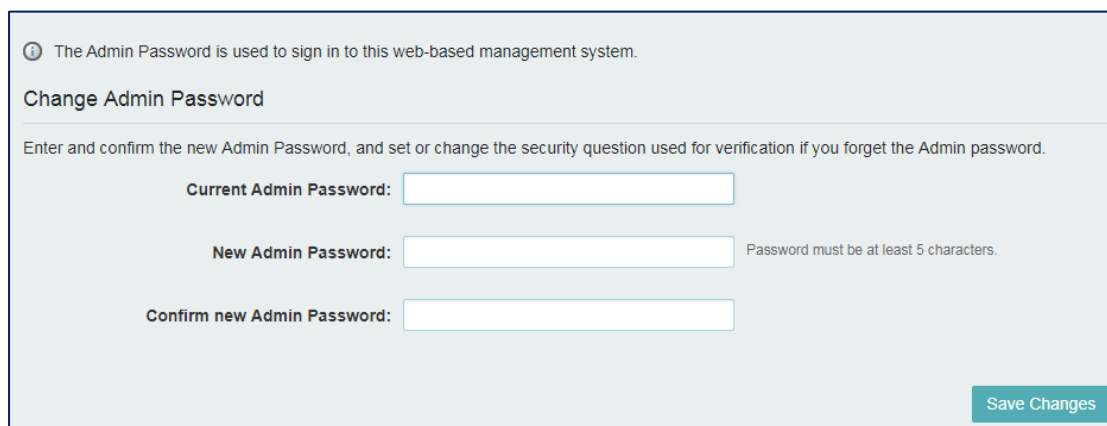
Device Settings

Admin Password: on this page, user can change the default password if required.
User need to first input existing password and click on continue as below



The screenshot shows the 'Device Settings' tab selected in a web interface. Below the tabs, there are two buttons: 'Admin Password' (highlighted in teal) and 'Backup and Restore'. A message states: '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.' Below this message is a text input field labeled 'Current Admin Password:' and a teal 'Continue' button in the bottom right corner.

New page will open and then user needs to put current admin password and then only User can define new password , ref below image



The screenshot shows a web-based management system interface for changing the admin password. At the top, an information icon and text state: "The Admin Password is used to sign in to this web-based management system." Below this is the section header "Change Admin Password". A sub-instruction reads: "Enter and confirm the new Admin Password, and set or change the security question used for verification if you forget the Admin password." The form contains three input fields: "Current Admin Password:", "New Admin Password:", and "Confirm new Admin Password:". A note next to the "New Admin Password" field specifies "Password must be at least 5 characters." A "Save Changes" button is located in the bottom right corner of the form area.

To make change into effect, user must need to click on **Save Changes** tab.

Backup and Restore: On this section, User can get many important features like backup/Restore, Reboot/Reset.

The screenshot shows the 'Backup and Restore' tab selected in the top navigation bar. Below the navigation bar, there is an information icon and a note: 'Back up your settings and preferences to your computer. Please note that the backup file will only work with this particular MiFi.' The page is divided into three main sections: 'Backup', 'Restore', and 'Restore to Factory Defaults'. The 'Backup' section has the instruction 'Save your settings to your computer.' followed by an 'Admin Password:' label and a text input field. A 'Download' button is located to the right of the password field. The 'Restore' section has the instruction 'Upload a previously saved backup file from this device to restore your settings.' followed by an 'Admin Password:' label and a text input field. Below the password field is a 'Select a file:' label with two buttons: 'No file selected' and 'Browse'. A 'Restore Now' button is located to the right of the 'Browse' button. The 'Restore to Factory Defaults' section has the instruction 'Restore all settings to the factory default values.' followed by a 'Restore Factory Defaults' button. At the bottom of the page, there are two buttons: 'Restart' and 'Download Mode'.

Admin Password Backup and Restore

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

Backup

Save your settings to your computer.

Admin Password:

Download

Restore

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

Admin Password:

Select a file:

Restore Now

Restore to Factory Defaults

Restore all settings to the factory default values.

Restore Factory Defaults

Restart Download Mode

- To backup the current configuration, User needs to input admin password and then click on **Download** tab to the PC connected to device. (ref. below image)

This screenshot shows a zoomed-in view of the 'Backup' section of the settings page. It includes the information icon and note at the top, the 'Backup' heading, the instruction 'Save your settings to your computer.', the 'Admin Password:' label, and the text input field. The 'Download' button is visible in the bottom right corner.

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

Backup

Save your settings to your computer.

Admin Password:

Download

- To restore any saved configuration of ND100 from local PC, User needs to input admin password first then click on **browse** and then select the correct file from the local connected

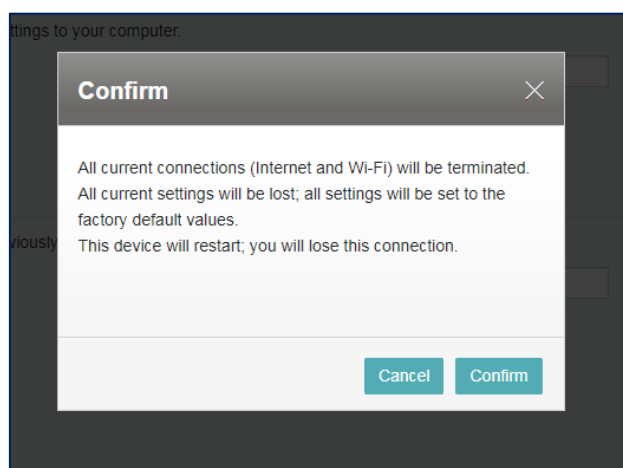
PC and click on **Restore Now** tab to get saved configuration over ND100. (ref. below image)

Reset to Factory Defaults & Reboot:

- User needs to click on **Restore Factory Defaults** tab to make all the configurations as factory settings. This is important feature sometimes useful during debugging where you want have factory settings on device.

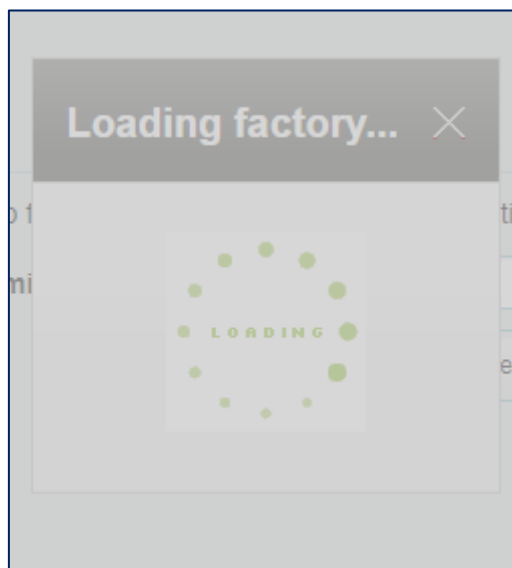
When Restore factory default tab is clicked , User can the below message on webpage for confirm .

To continue , confirm tab needs to be clicked. Else click cancel to avoid this function.

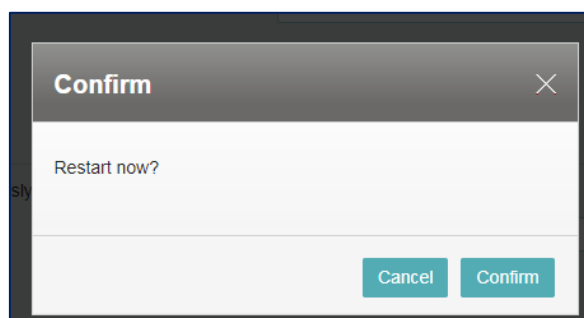


When clicked on confirm, User can see below information on webpage. This shows that Loading

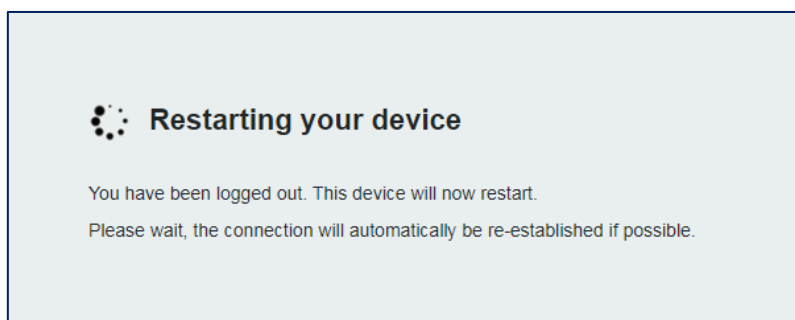
factory settings process is going on. So ensure , no power failuer while doing this.It may cause problem to device.



- In case, where Restart/Reboot is requyired for the device. User can select the **Restart** tab. User can get below message on Prompted window to confirm.



Once confirm, below message on webpage appears to show about restart procedure & User needs to ensure uninterupted power supply to device while doing this.



Mobile Network Under this setting page, User will have ability to configure cellular and SIM related configurations.

Mobile Settings: User can turn off/On the cellular data by sliding On/Off tab.
Under advance setting, User can define the APN manually. (ref. below image)

Wi-Fi Settings Device Settings **Mobile Network** Remote Update

Mobile Settings SIM Lock

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

Advanced Settings

APN: Obtain the APN value from your service provider.

Authentication: NONE

Username:

Password:

Save Changes

SIM Lock: on this page, User can see the SIM status, PIN Lock status.
User can also enable the SIM PIN lock. (ref. below image)

Mobile Settings **SIM Lock**

ⓘ 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.

Save Changes

Remote Update

FOTA URL Link: This page is for about FOTA feature, User needs to modify/Input URL for FOTA server to get SW upgrade remotely.

Wi-Fi Settings Device Settings Mobile Network Remote Update

FOTA URL Link

FOTA URL Link

Save Changes

Advance Settings

On this section, user can find some important industrial and useful features related to VPN, MAC Filter, LAN setting, Port filtering and forwarding .

Firewall On this page, user can configure below feature

VPN passthrough : **Enable**(as default) /Disable by simply slide On/Off button

DMZ(IPv4) : Enable / **Disable**(as default)

To enable DMZ function, tick the DMZ box and input the destination IP address and click on **Save Changes** tab to takes affect.

Advanced Settings

Firewall MAC Filter LAN Port Filtering 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.

Save Changes

MAC filter This feature is disabled (OFF) as default. If User wants to allow specific MAC address only, then user need to click on new device and input the allowed MAC address and click on Save Changes tab to takes affect.

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 devices.

☐ OFF

Type	Name	MAC Address	Status	MAC Address Filter	Delete
Laptop	unknown	48:45:20:7a:59:bd	Your device	<input type="checkbox"/>	

0 0

LAN

On this page, User can configure the local area network (LAN) as per the requirements for below options available on webGUI .

Local IPv4 : **192.168.0.1** (as default)

Subnet mask: **255.255.255.0** (as default)

DHCP Server: **Enabled** (as default)/ Disabled

DHCP lease time: **43200** min (as default)

DHCP IPv4 Range: **192.168.0.20 ~ 192.168.0.60** (as default)

Local IPv6: **Enabled** (as default)/ Disabled

Advanced Settings

[Firewall](#)[MAC Filter](#)[LAN](#)[Port Filtering](#)[Port Forwarding](#)

IPv4

IP Address:

192.168.0.1

Subnet Mask:

255.255.255.0

MAC Address:

34:BA:98:12:34:70

DHCP server:

☒

DHCP Lease Time:

43200

minutes.

Start DHCP Address Range at:

192.168.0.20

DHCP Address Range:

192.168.0.20 - 192.168.0.60

IPv6

Turn on IPv6:

☒

When on, connected devices can make IPv6 connections to the Internet.

Link-Local Address:

fe80::a81e:4cff:fe11:5462

Save Changes

Port Filtering

On this page, User can configure application to access the internet as required. By default, this feature is **Off** (disabled)

Advanced Settings

[Firewall](#)[MAC Filter](#)[LAN](#)[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.

 [Add a Custom Application](#)

Save Changes

Port Forwarding

On this page, User can define the specific incoming traffic to specific connected device/IP address. This feature is **OFF** (disbaled) by Default.

Firewall
MAC Filter
LAN
Port Filtering
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
<input type="checkbox"/>	DNS	0.0.0.0
<input type="checkbox"/>	FTP	0.0.0.0
<input type="checkbox"/>	HTTP/HTTPS	0.0.0.0
<input type="checkbox"/>	NNTP	0.0.0.0
<input type="checkbox"/>	POP3/POP3S	0.0.0.0
<input type="checkbox"/>	SMTP/Secure SMTP	0.0.0.0
<input type="checkbox"/>	SNMP	0.0.0.0
<input type="checkbox"/>	Telnet	0.0.0.0
<input type="checkbox"/>	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.

Add a Custom Application

Save Changes

Logout webGUI

In case if user wants to log out from the webGUI, User needs to click on SIGN OUT option available on Top corner of webGUI page. Webpage will be redirected to login page.



Discontinue transmission

In case if absence of information or operational failure, the device will automatically discontinue transmission by software control.

FCC statement

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help
- This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

This equipment complies with FCC and IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter

IC statement

This device complies with RSS-247 of Industry Canada. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

5G Wi-Fi Restriction information

The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.