ZOLL Mobile Hotspot

Operator Guide
Rev 1.0

The issue date for the ZOLL Mobile Hotspot (REF 8016-000117-01 Rev. A) is **May, 2021.**

ZOLL Medical Corporation
269 Mill Road
Chelmsford, MA USA
01824-4105

EC REP ZOLL International Holding B.V.
Newtonweg 18
6662 PV ELST
The Netherlands

Contents:

A. About the Device

Figure 1 Front of Device

Figure 2 Back of device

B. Inserting the SIM Card & Battery

Step 1: Remove the six screws on the bottom of the Mobile Hotspot.

Figure 3 ZOLL Mobile Hotspot.

Figure 4 Turn the unit over & remove the six pads (marked in figure by Orange circles) to reveal the screws.

Figure 5 With screwdriver, remove the six screws.

Step 2: Place SIM card in Tray 1 (Primary) and Tray 2 (Optional)

Figure 6 To insert the SIM card into the tray, unlock the tray by sliding the lock to the left, insert the SIM, and then slide the lock to the right to lock the SIM into place

Step 3: Slide the battery towards battery contact in the Mobile Hotspot

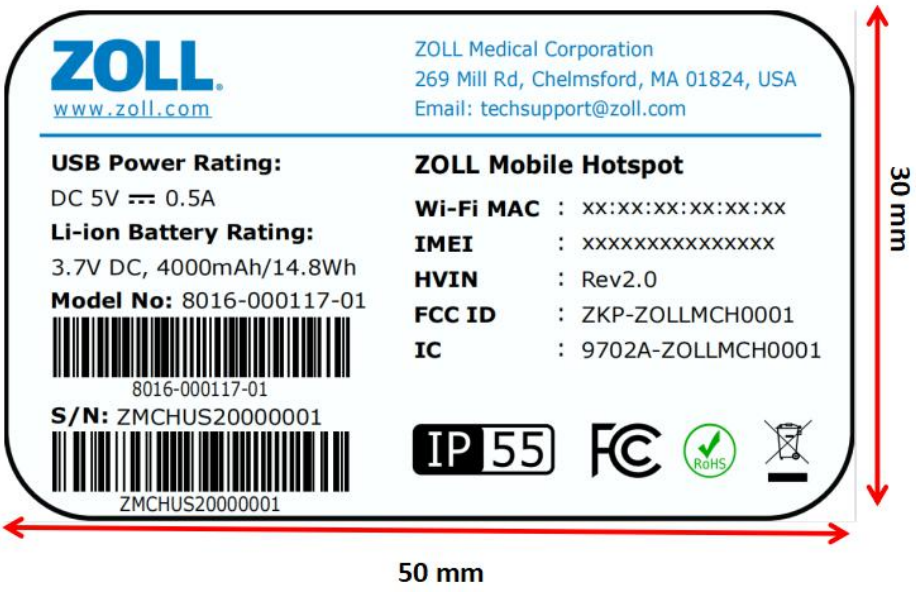
Figure 7 Slide battery

Figure 8 Insert battery in Mobile Hotspot unit, contacts facing downward.

Step 4: Replace the screws and pads.

Step 5: Charge the Mobile Hotspot using a USB Type C Cable.

Step 6: ZOLL Product Label detail for US Variant.



C. Power-up & Connection Instructions:

Step 1: Press the Power button once and wait for the system to boot (minimum time to boot is 55 seconds).

Power Button Functionality:

- Short press to power ON.
- Long press (>5 Secs) to power OFF.
- Note: To power on again, wait ~5 Secs after power OFF.

LED Indications:

- All LEDs will light up once upon power ON to confirm successful power on cycle.
- Once the device has booted up, LEDs will illuminate to show the status of the device. The following table shows LED status in different power modes:

Time	LED	LED Pattern	Significance
Upon Booting	All LEDs	Upon pressing the power button, all LEDs will briefly appear. During the booting process, only the power LED will illuminate.	
While Operating	Power LED	Blinking	System Running Normally
	Signal RGB LED 	Green Continuous On	Good/Excellent Signal Strength
		Blue Continuous On	Moderate Signal Strength
		Red Blinking	Initiating connection to the network and turning data connection ON
		Red Continuous On	Network not registered/ Network not reachable/ No clients connected to the modem for more than 5 minutes
	Battery LED 	Green Continuous On	Battery percentage between 60% and 100%
		Amber Continuous On	Battery percentage between 20% and 59%
		Red Continuous On	Battery percentage between 5% and 19%
		Red Blinking	Battery percentage between 0% and 4%
	LTE Data LED	Continuous On	Connected to network and inactive data usage

		Blinking	Connected to network and active data usage
		Continuous Off	Network not available/ Data connection is disabled/ No clients connected to the modem for more than5 minutes
	Wi-Fi LED 	Continuous On	Wi-Fi/Hotspot active and inactive data usage
		Blinking	Wi-Fi/Hotspot active and active data usage
		Continuous Off	Initiating Wi-Fi/Hotspot
Power Save Mode	Power LED	Constant	System Running Normally
	Signal RGB LED 	Red Continuous On	Network not available/ Data connection is disabled/ No clients connected to the modem for more than 5 minutes
		Red Blinking	Modem exiting Power Save Mode
	Battery LED 	Green Continuous On	Battery percentage between 60% and 100%
		Amber Continuous On	Battery percentage between 20% and 59%
		Red Continuous On	Battery percentage between 5% and 19%
		Red Blinking	Battery percentage between 0% and 4%
	LTE LED	Continuous Off	LTE OFF due to modem in Power Save Mode
	Wi-Fi LED	Continuous On	Wi-Fi/Hotspot active and inactive data usage (No clients connected to the modem)

Table 1: LED Indication

Step 2: On your mobile phone, tablet, or PC, go to Wi-Fi settings, and find Wi-Fi SSID "ZWCH_xxxx" (as given on the bottom cover of the Mobile Hotspot and connect using the password **"zollmifi".**

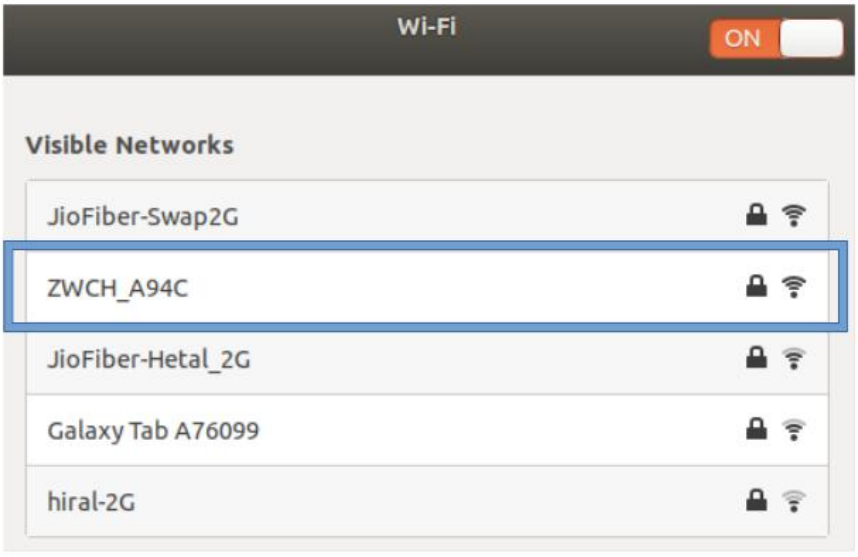


Figure 9 Available Wi-Fi Display Menu in the Mobile/PC/Laptop to connect

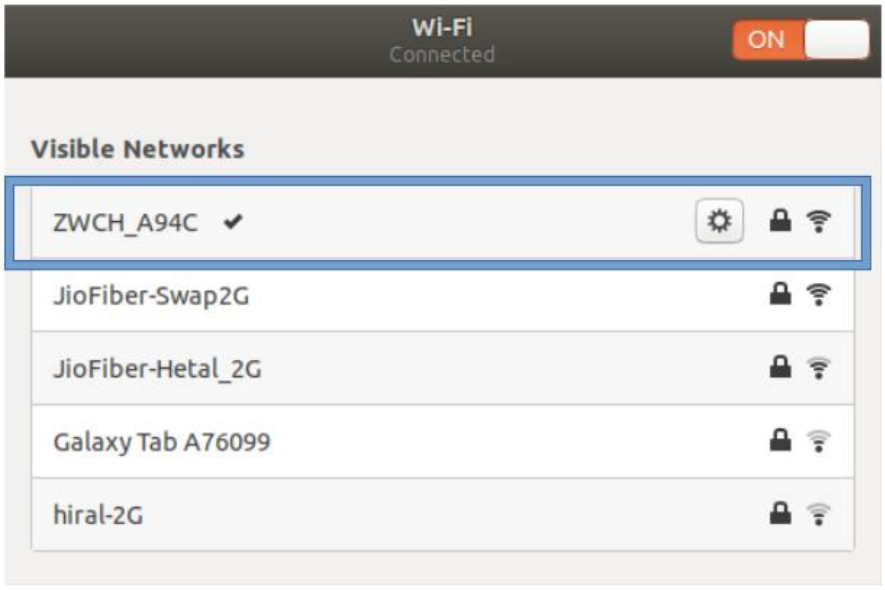


Figure 10 Wi-Fi connection status on Display

Step 3: After a connection to Mobile Hotspot is initiated using the Wi-Fi SSID, load the following web page using a web browser using the link: **http://192.168.56.1**

Figure 11 Enter Web Page Address bar

Tip: (Use Google Chrome in Incognito Mode and keep mobile data off.)

Step 4: Log in to the page with username, “root”. You will see the following screen:

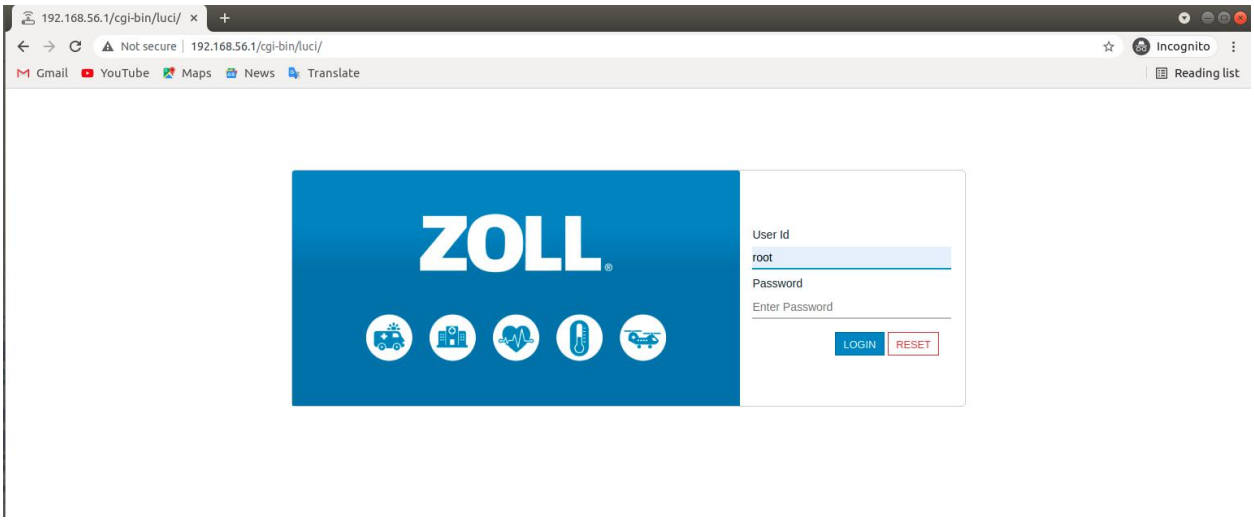


Figure 12 Fill Login page Credential details

Note: Username “root” (with no default password) is required here to login.

D. WebUI Page Hierarchy:

The WebUI allows users to configure the device and monitor device status. The WebUI sidebar (left pane) menu has the following options:

1. **Device Overview**: Contains basic device information.
2. **System Settings**: Allows users to update device time, language, and download logs.
3. **Backup and Restore**: Allows users to download device configuration backup and restore the backup.
4. **Factory Reset Instructions**: Allows users to factory reset the device.
5. **Reboot the Device**: Allows users to reboot the device.
6. **Sleep Mode Configuration**: Allows user to configure the “Time to Sleep” mode.
7. **Wi-Fi Settings**: Allows users to configure the SSID, password, band selection, static lease, etc.
8. **Cellular Settings**: Allows users to configure the SIM selection, data enable/disable, network type, APN, etc.
9. **Change WebUI admin password**: Allows users to change the WebUI admin password.
10. **Domain Whitelisting**: Allows users to configure a Whitelist of URLs.
11. **Firmware Upgrade:** Allows users to upgrade the firmware using drag and drop or OTA methods.
12. **Data Counter Configuration**: Allows users to manually clear Data Consumption Counters or use the Billing Cycle method.
13. **Fetch Cellular Data Plan using USSD Code:** Fetches Data Plan for a SIM card using the USSD Code.

The side pane looks as shown below:

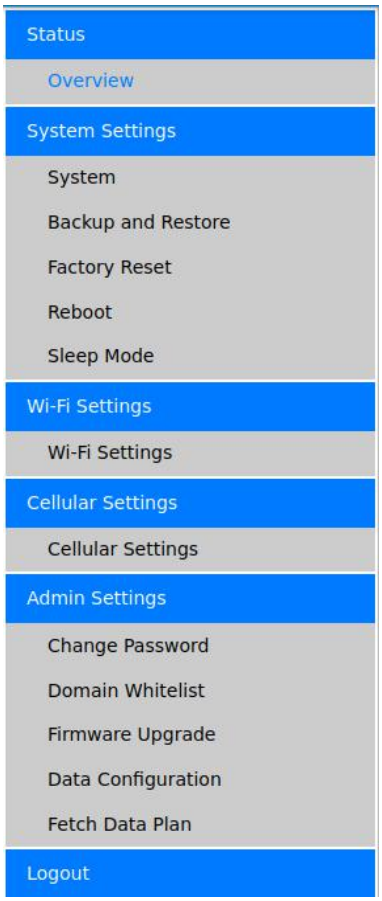


Figure 13 Zoll WebUI side Panel display

The static status bar at the top of the pages looks as shown below:

The status bar shows three different status:

Sr. No.	Status Symbol	Significance
1		Cellular Network Signal Strength
2		Battery Percentage with Charging Status
3		Cellular Data Active/Inactive

Table 2 Status Bar Symbols significance

1. Device Overview:

This page contains basic device information mentioned below:

- Device information: Model, Firmware Version, Hardware Version and Variant, System Time.
- WAN interface information: Cellular IMEI number, Selected SIM Card, Network Connection Status, Signal Strength, IPv4 and IPv6 address of the interface.

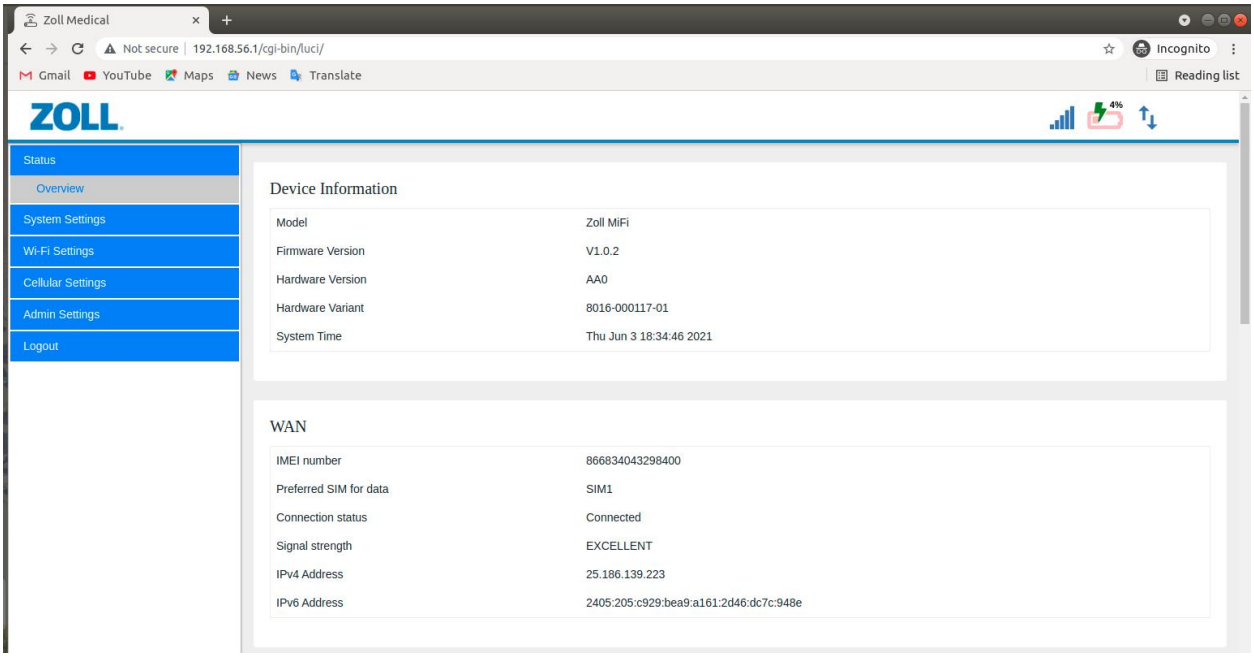


Figure 14 Device Overview

- Data Consumption information: RX and TX data.
- LAN interface information: IP address and subnet mask of the interface.
- List of connected devices with MAC address of all the clients connected and IP address assigned to those clients.

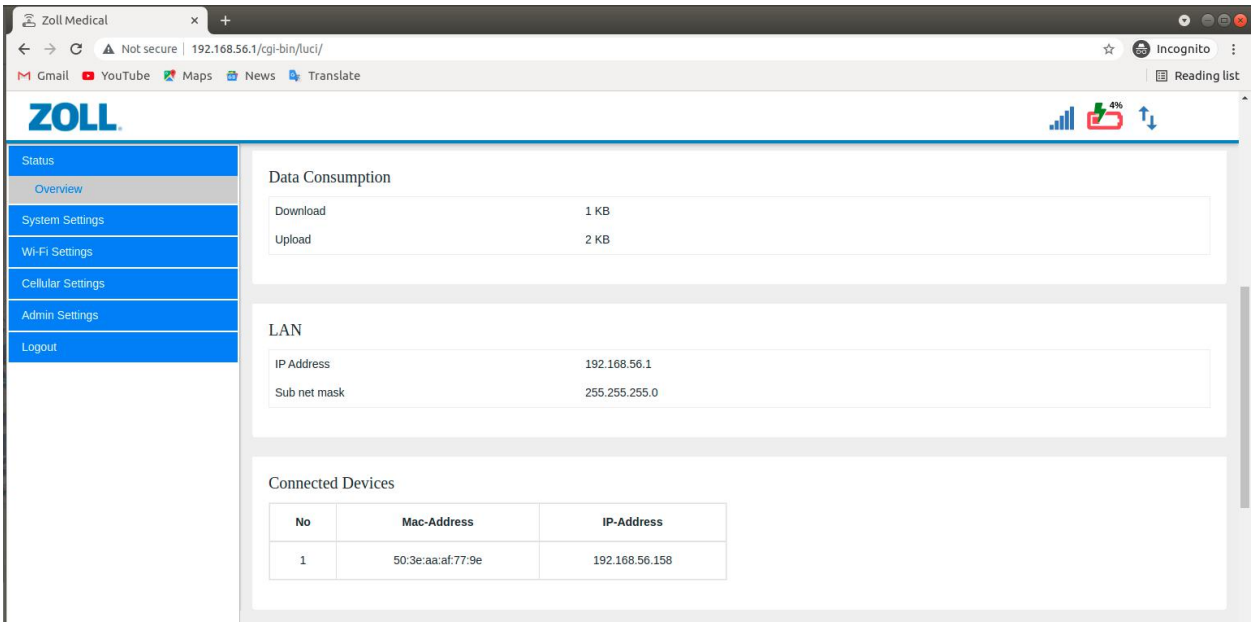


Figure 15 Device Overview

- Data Consumption Chart consists of Download and Upload data per day for a maximum of 30 days. This chart will clear as per Billing Cycle Day configuration or by manually clearing the information in the Data Configuration page. The user can customize the chart as per the start date and end date selection option on the page.

2. System Settings:

This page contains basic device configuration as mentioned below:

2.1 Time Sync

System time synchronization using NTP URL. This page takes at least one NTP URL as input to synchronize the system time. By default, there are 3 NTP URLs set for time synchronization.

Step 1: Go to the left pane and click on “System” in the “System Settings” tab on Web UI. The “Time Sync” tab would be open by default.

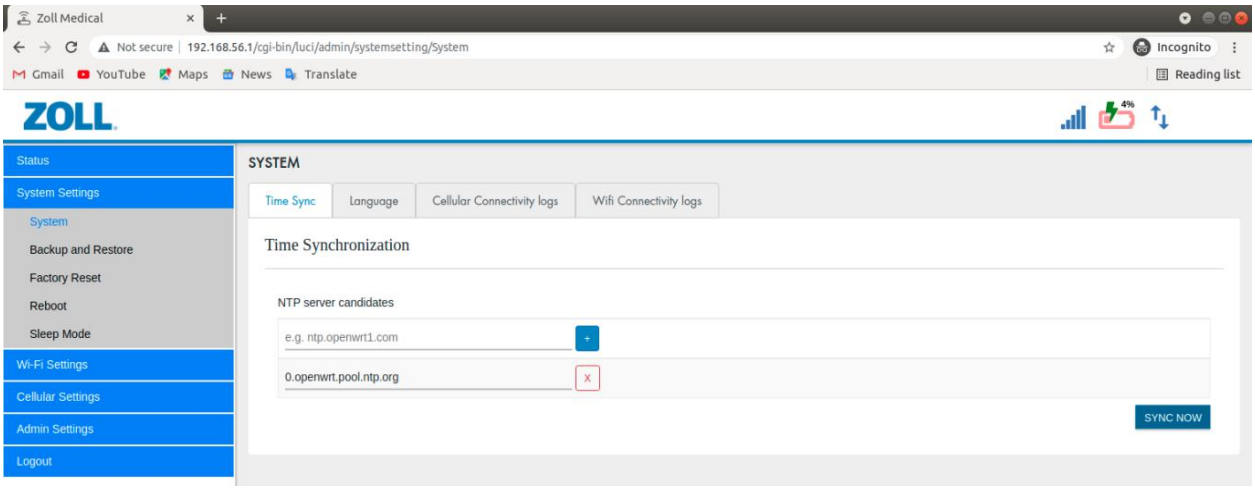


Figure 16 Time Sync under system setting

Step 2: Enter the NTP URL for time synchronization and click the plus sign “+” to add the URL to the list. After entering all the required URLs, click “SUBMIT”.

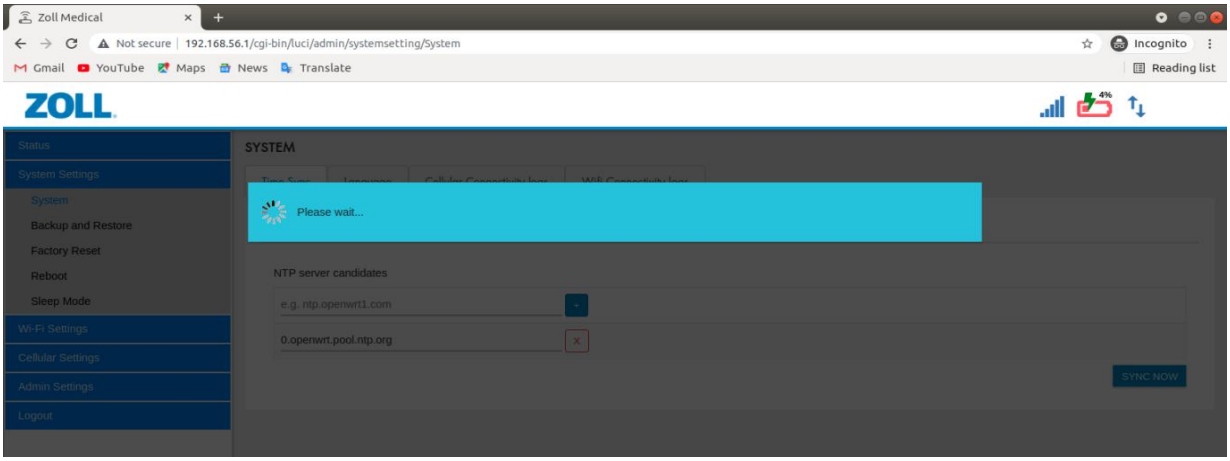


Figure 17 Time sync display after providing details

Step 3: Wait for the device to synchronize the system time. Once the time synchronization is complete, a popup will appear to show the system time before and after the time synchronization.

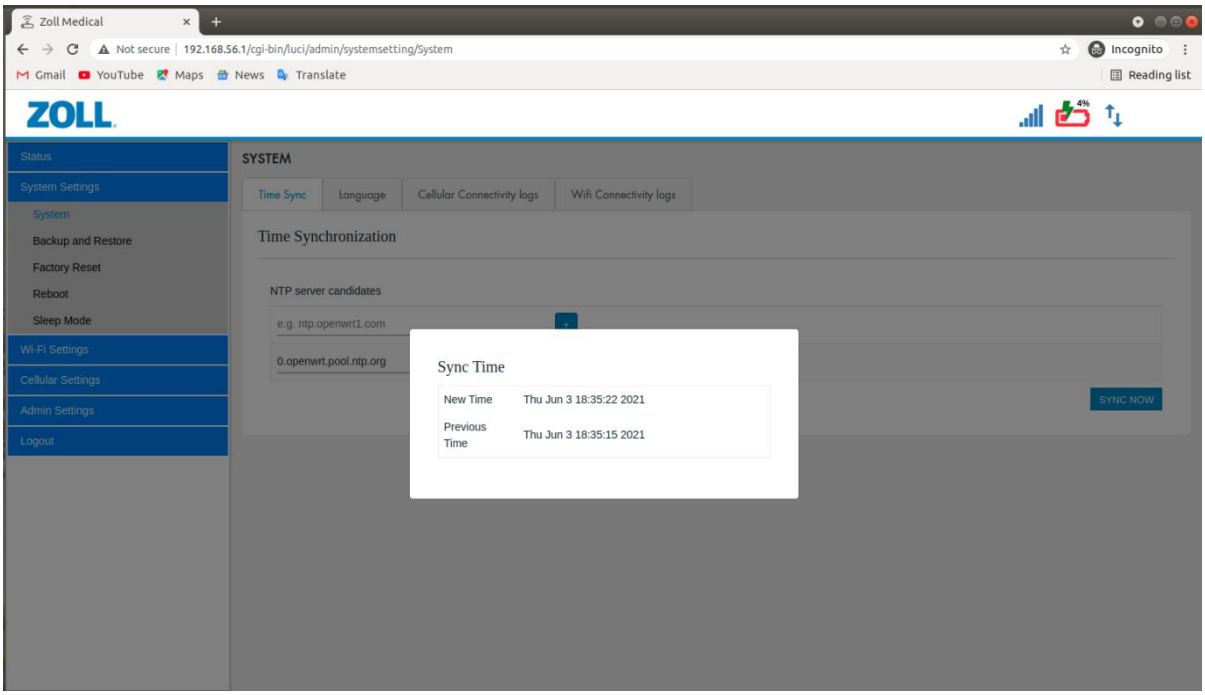


Figure 18 Time Sync Completion Popup

2.1 Language

- System Language selection allows users to set WebUI language. A drop-down menu is available for the users to select a language. By default, *Auto* is selected which uses the browser language for the WebUI. Note: The language selection only translates the static WebUI contents.

Step 1: Go to the left pane and click on “System” in the “System Settings” tab on WebUI. Now click on the “Language” tab selection button on the top of the “Settings” page. Once the tab loads, select the preferred language from the drop-down menu.

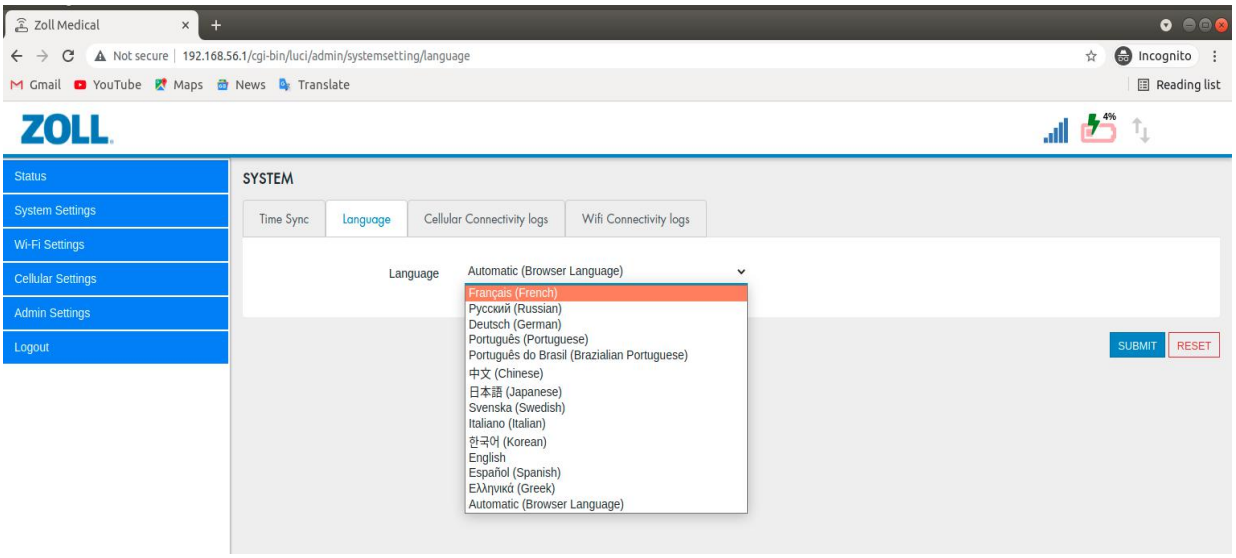


Figure 19 Language selection under system setting

Step 2: Click on the “SUBMIT” button to apply the language on the WebUI.

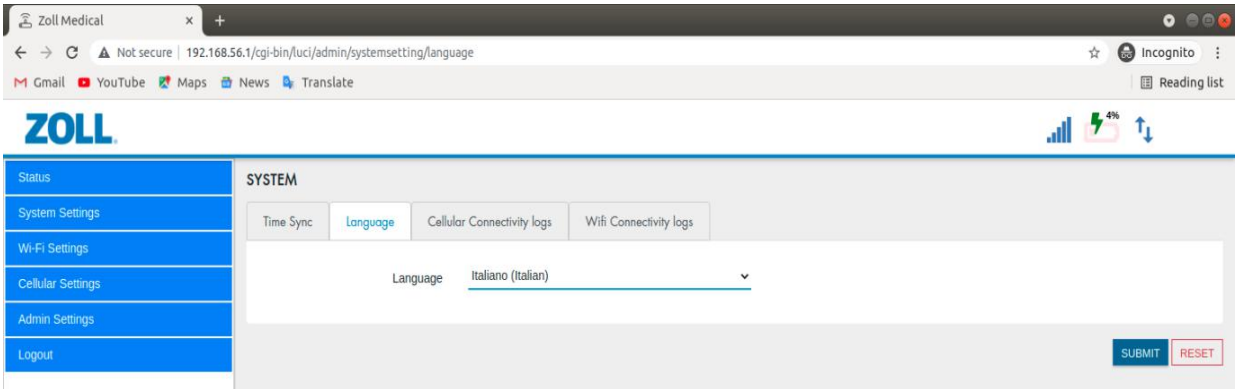


Figure 20 Submit option for language selection

Step 3: Once the submission is complete, the WebUI content will appear as per the selected language.

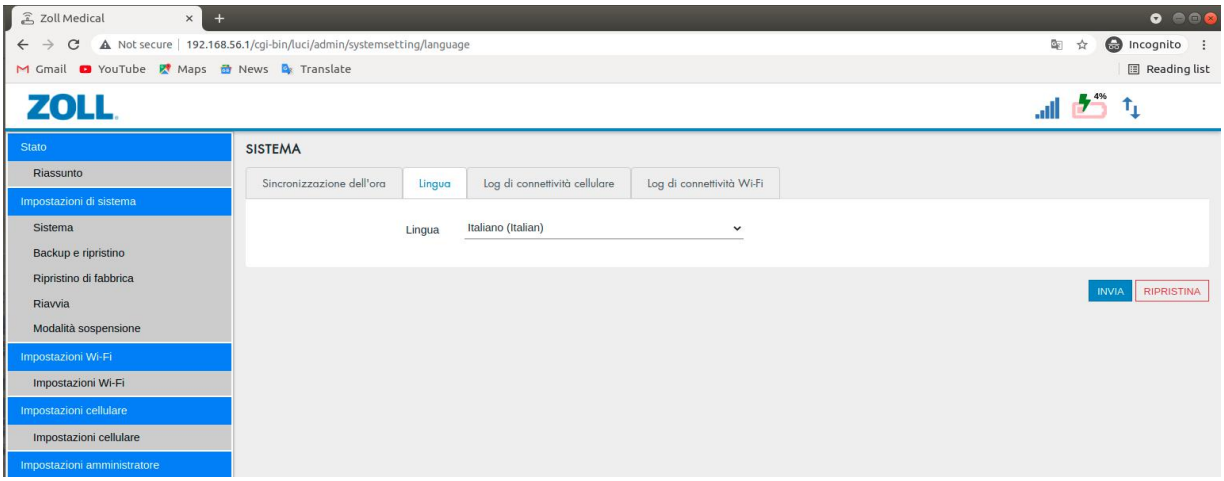


Figure 21 Language selection completion display

2.2 Cellular Connectivity Logs

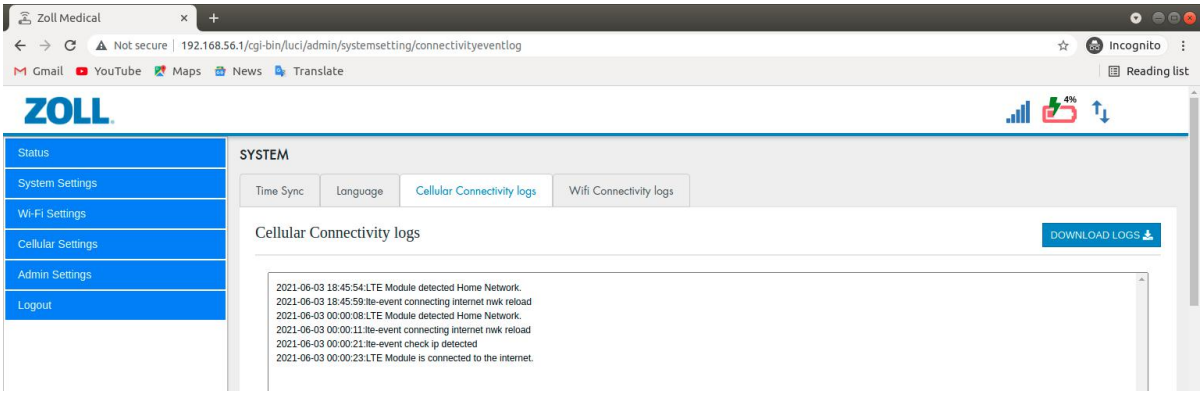


Figure 22 Cellular connectivity logs under system setting

- LTE Connectivity Logs page displays the LTE network connectivity logs. This log will clear after 30 days have elapsed since the first log or after 100 logs have appeared. “DOWNLOAD LOGS” button is also available, which will download a LTEConnectivityLogs.tar file, containing all log files.

Step 1: Go to the left pane and click on “System” in the “System Settings” tab on Web UI. Now click on the “Cellular Connectivity Logs” tab selection button on the top of the “Settings” page. The page also allows the user to download the logs (click “DOWNLOAD LOGS”).

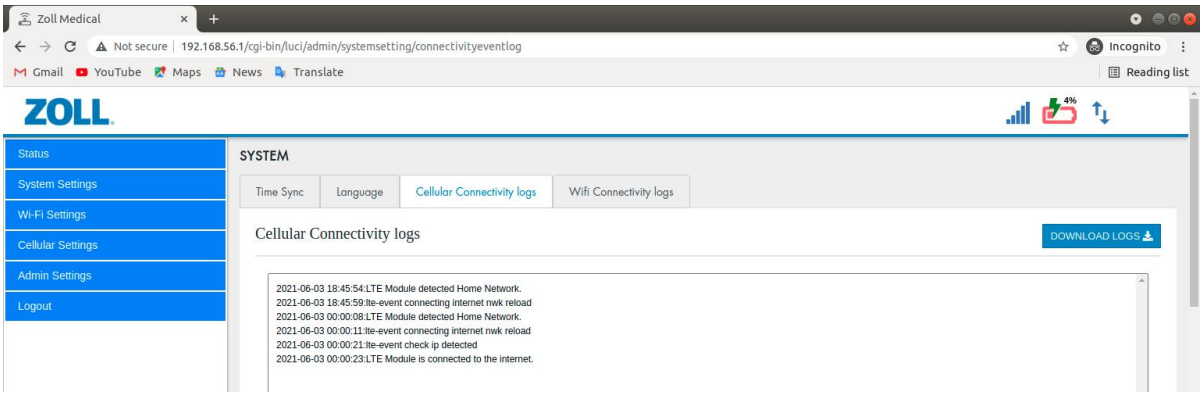


Figure 23 Download option for cellular connectivity logs

2.3 Wi-Fi Connectivity Logs

- Wi-Fi Connectivity Logs page display the Wi-Fi client's connectivity (connection/disconnection) logs with TX/RX rates. This log will be cleared if 30 days have elapsed since the first log, or 100 logs have appeared. "DOWNLOAD LOGS" button is also available, which will download a Wi-FiConnectivityLogs.tar file containing all log files.

Step 1: Go to the left pane and click on "System" in the "System Settings" tab on Web UI. Now click on the "Wi-Fi Connectivity Logs" tab selection button on the top of the "Settings" page. The page also allows the user to download the logs (click "DOWNLOAD LOGS").

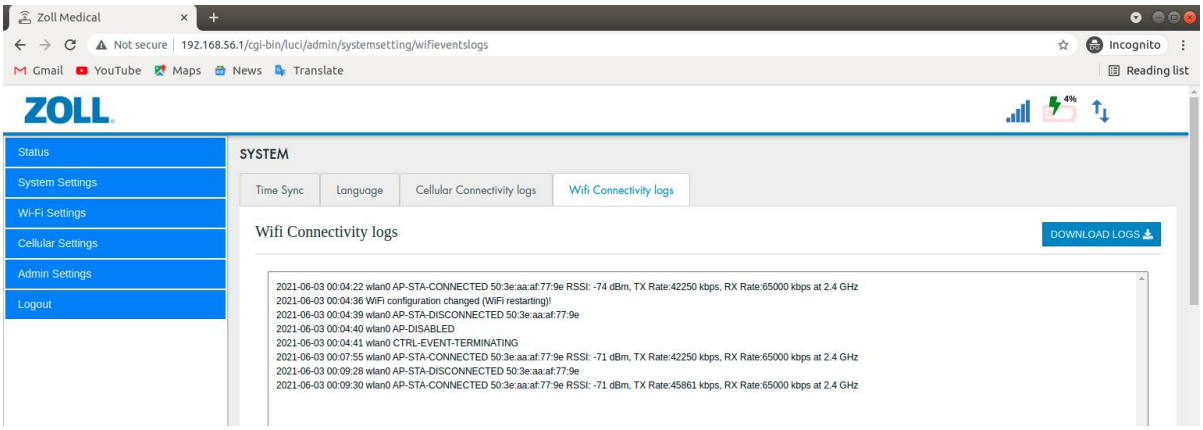


Figure 24 Wi-Fi connectivity logs

3. Backup and Restore:

Users can back up the device configurations and restore these backups if required. An option to include the SSID and password in the backup is available.
The backup file will be available as a Backup.tar file.

Backup:

Step 1: Go to the left pane and click on “Backup and Restore” in the “System Settings” tab on Web UI.

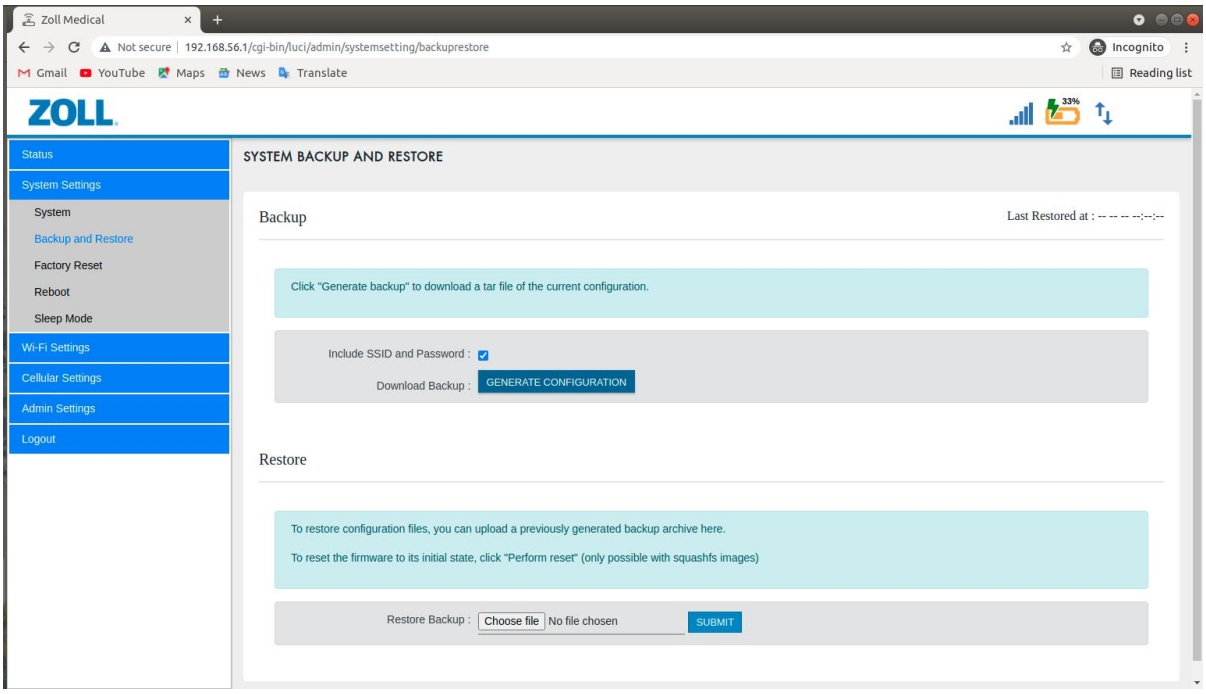


Figure 25 Backup and Restore under system setting

Step 2: Select “Include SSID and Password” option, to include the SSID and Password of the Mobile Hotspot to be included in the backup. For creating a backup file click on the “SUBMIT” button. The backup file will then download to the local storage.

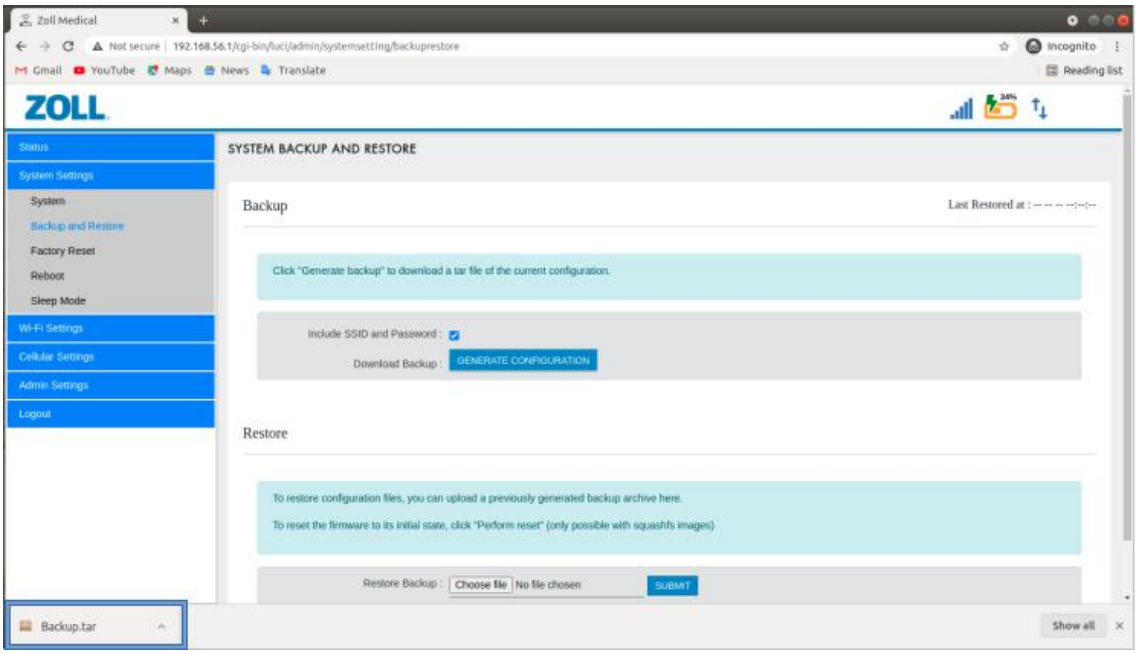


Figure 26 Download backup file

Note: If SSID and Password are included in the backup, the SSID and Password in the backup file will continue to be used on the devices, once this backup is restored.

Restore:

Step 1: Go to the left pane and click on “Backup and Restore” in the “System Settings” tab on Web UI.

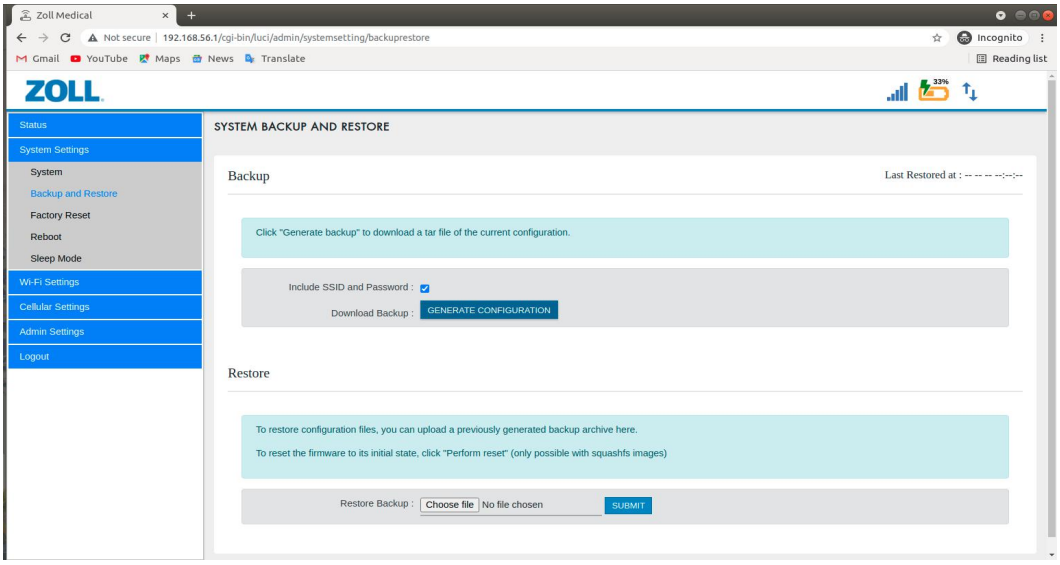


Figure 27 Restore option in WebUI

Step 2: Click the “Choose file” button in the “Restore” section of the page. Select the backup file from the local storage for restoration.

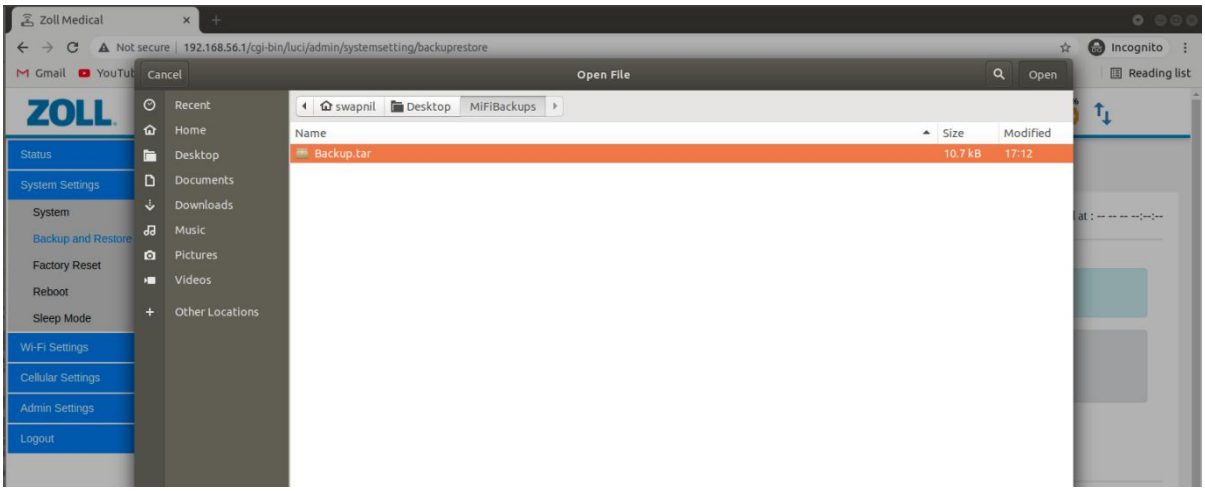


Figure 28 Backup file selection for Restore

Step 3: Click the “SUBMIT” button to restore the device with the backup configuration file submitted.

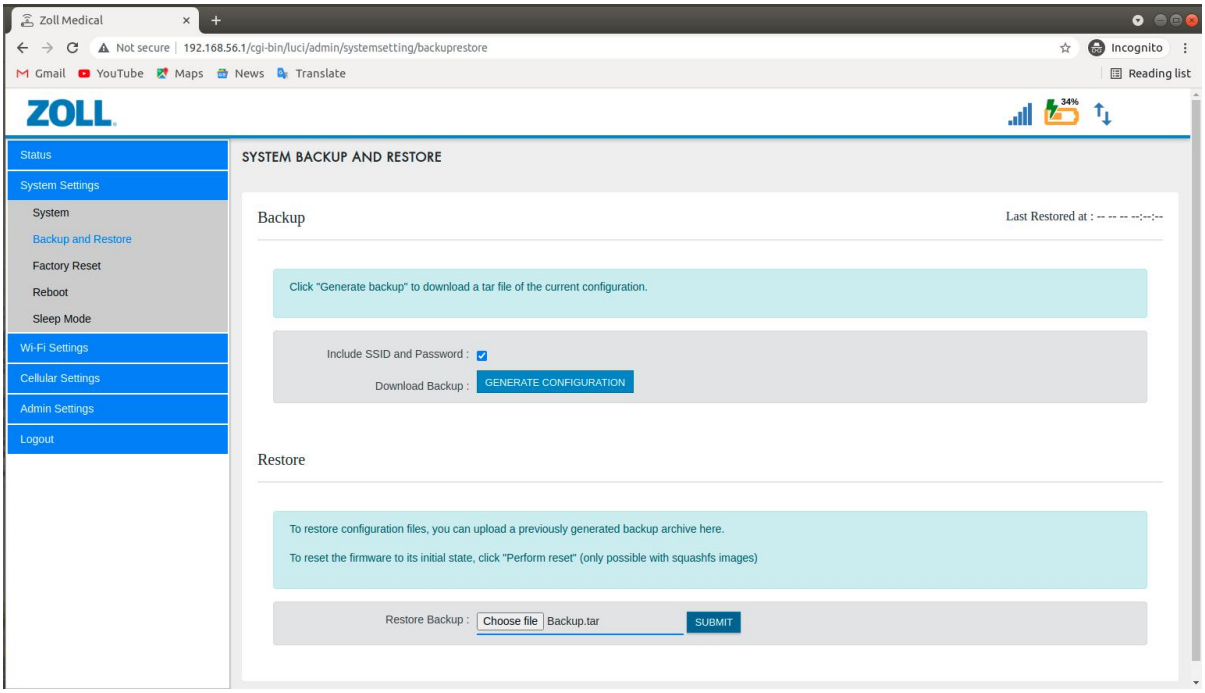


Figure 29 Submit option after File selection

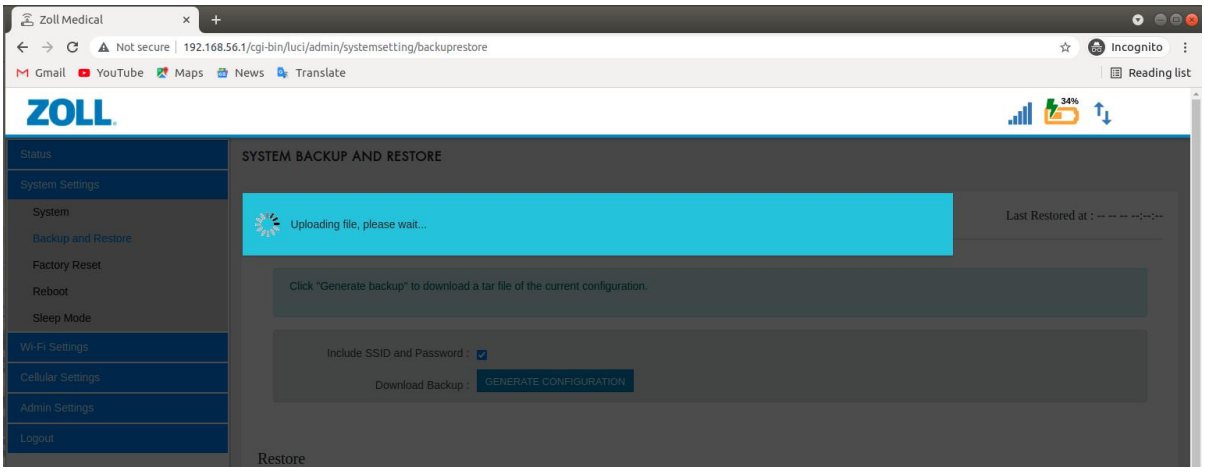


Figure 30 backup file uploading in progress

Step 4: Once the restore is complete, the device will reboot with the restored configurations.

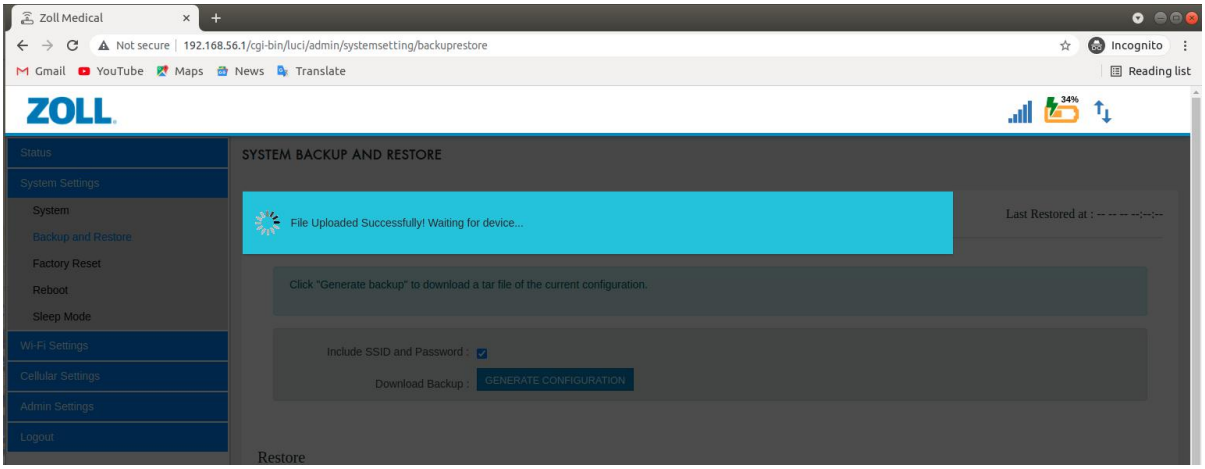


Figure 31 Pop-up of successfully File upload

4. Factory Reset Instructions:

Users can reset the device to its factory settings using the “Factory Reset” option. After clicking “Factory Reset” on the WebUI, a popup will appear to ask the user to create a backup before opting for factory reset. If the user selects to backup, they will be directed to the “Backup and Restore” page. When “Factory Reset” is pressed, the device will reboot with factory settings applied.

The page will also show the date and time when the last factory reset occurred.

Step 1: Go to the left pane and click on “Factory Reset” in the “System Settings” tab on Web UI. Click on the “PERFORM RESET” button to reset the device to factory settings.

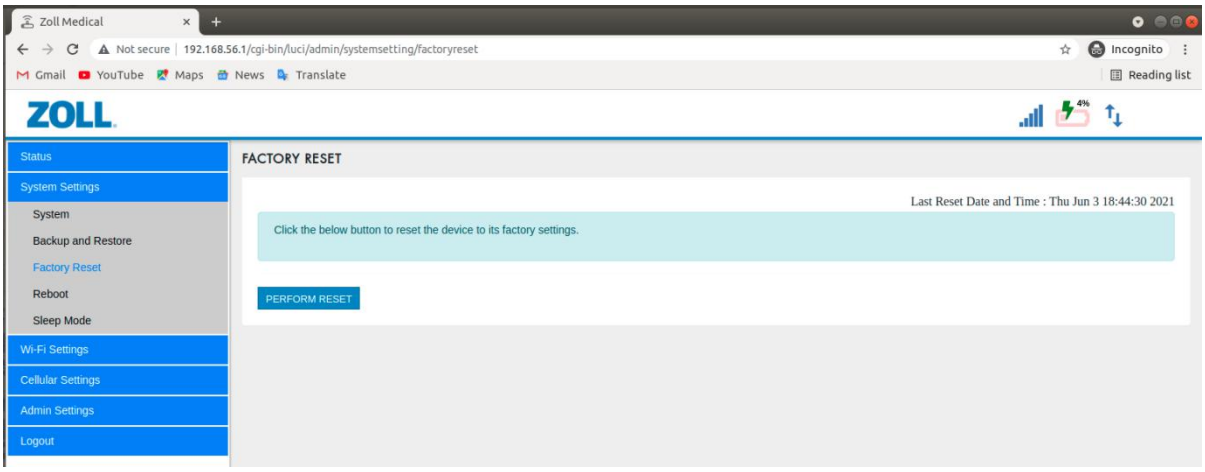


Figure 32 Factory Reset under system setting

Step 2: Once the “PERFORM RESET” button is clicked, a pop-up will appear to ask the user to create a backup of the configuration before factory reset. If “YES” is clicked for backup generation, the user will be redirected to the “Backup and Restore” page.

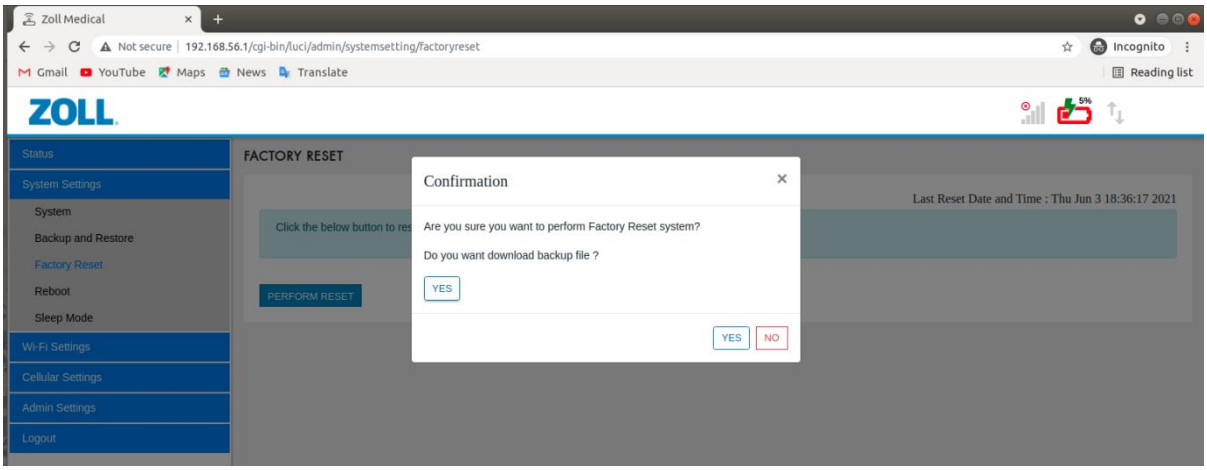


Figure 33 Pop-up after clicking on perform Reset

Step 3: Once the “YES” button is clicked for factory reset, the device will reboot with factory settings applied.

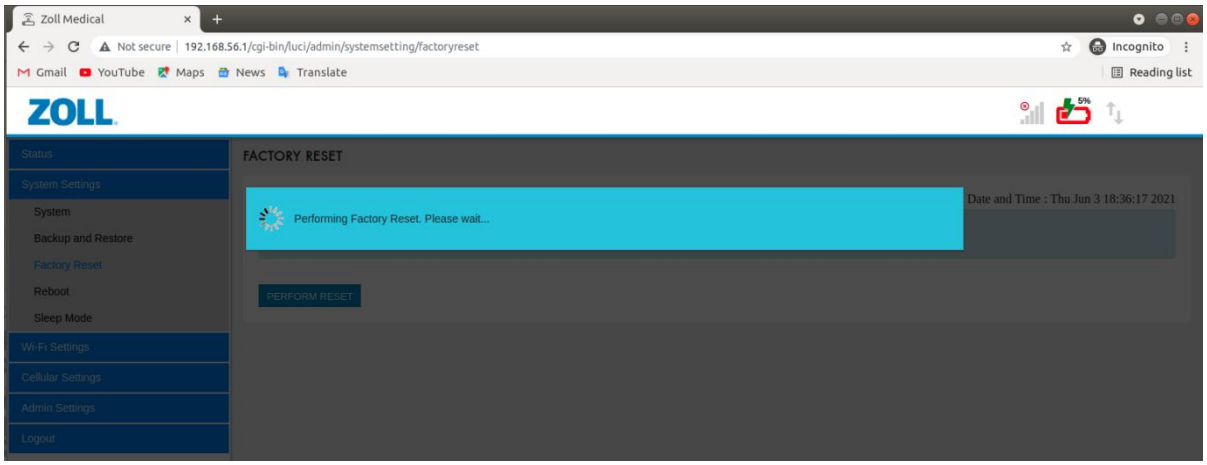


Figure 34 Pop-up for performing factory reset

5. Reboot the Device:

Users can reboot the device using this option on the WebUI.

Step 1: Go to the left pane and click “Reboot” in the “System Settings” tab on WebUI. Click on the “PERFORM REBOOT” button to reboot the Mobile Hotspot.

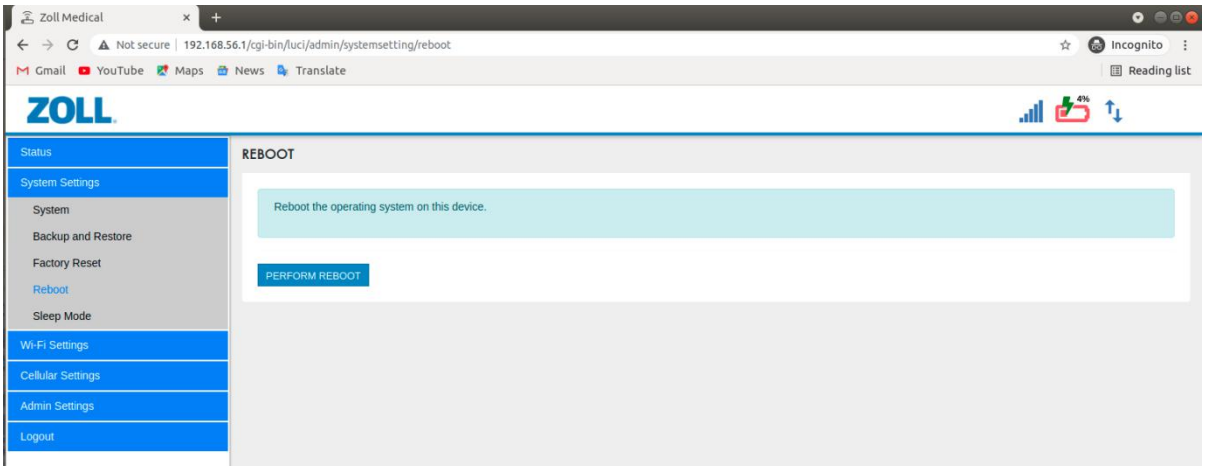


Figure 35 Device reboot option under system setting

Step 2: Once the “PERFORM REBOOT” button is clicked, a pop-up will appear to prompt the user to confirm the reboot.

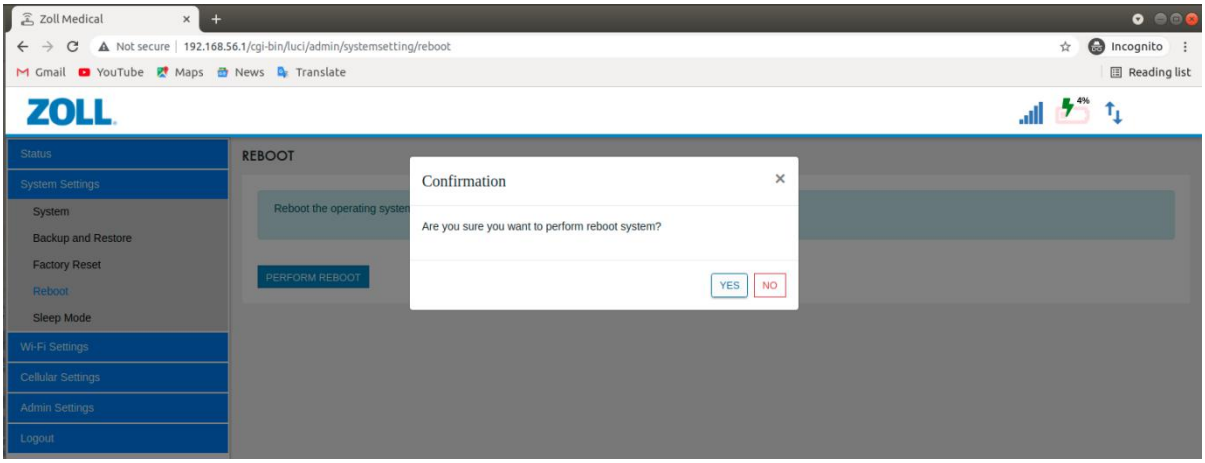


Figure 36 Reboot confirmation Pop-up

Step 3: Once the “YES” button is clicked, the Mobile Hotspot will reboot. Reconnect the clients to the Mobile Hotspot to access the WebUI.

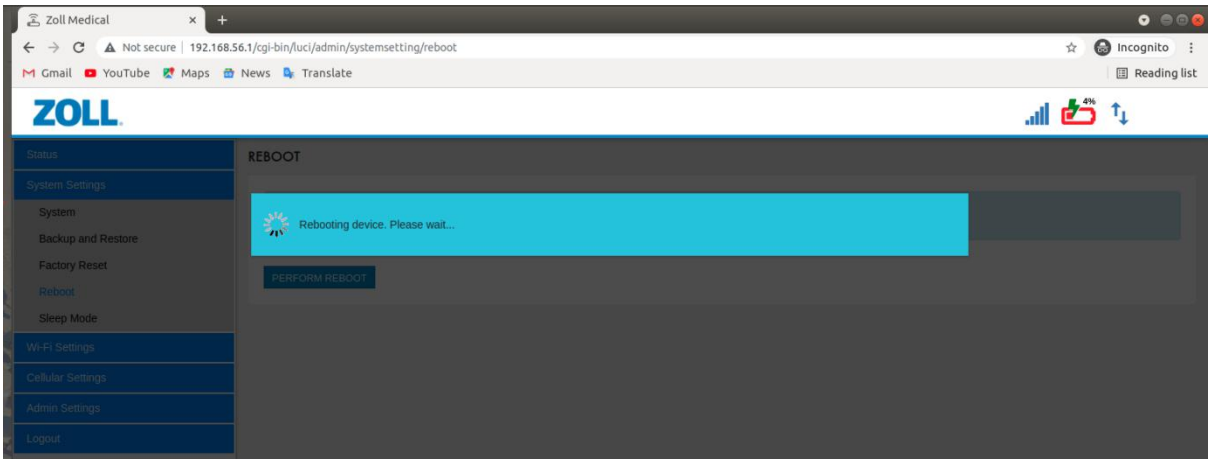


Figure 37 Device Rebooting

6. Sleep Mode Configuration:

This page allows users to configure Time to Sleep for the modem. The modem will enter sleep mode (power saving mode) if no clients are connected to the modem Wi-Fi for the specified Time to Sleep period.
There is also an option to select “Never” to disable the sleep mode.

Step 1: Go to the left pane and click on “SLEEP MODE” in the “System Settings” tab on Web UI. Select the “Sleep mode” (Time to Sleep) from the drop-down list available.

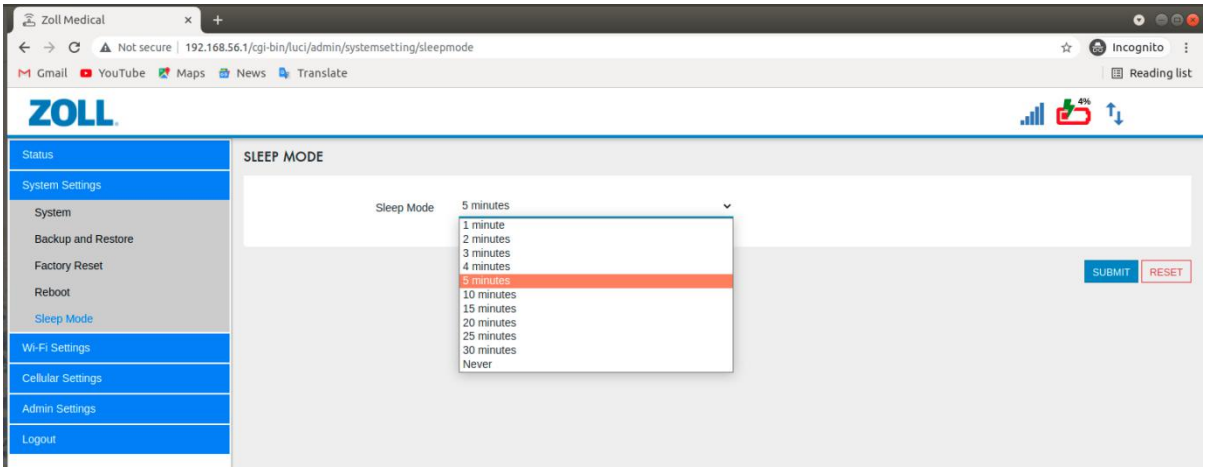


Figure 38 sleep mode selection under system setting

Step 2: Click on the “SUBMIT” button to set the Time to Sleep for the Sleep mode

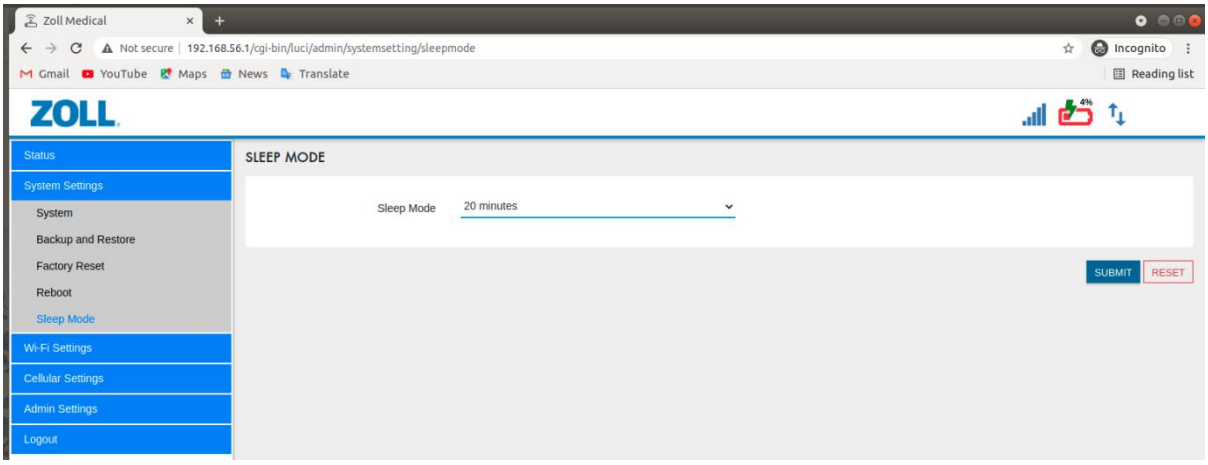


Figure 39 Sleep mode time setting

7. Wi-Fi Settings:

Wi-Fi interface configurations can be changed in the “Wi-Fi Settings” page in the “Wi-Fi Settings” tab on the WebUI. Users can configure the following settings for the Wi-Fi interface:

- SSID for the AP/Hotspot of the Modem.
- Encryption type for the security of the Hotspot.
- Password to allow only trusted clients to access the Hotspot.
- AP band selection allows two options, 2.4GHz or 5GHz. Select the band as per client device specifications.
- Static Lease assignment allows users to assign specific IP addresses to clients as per MAC address provided.

Step 1: Go to the left pane and click on “Wi-Fi Settings” in the “Wi-Fi Settings” tab on WebUI.

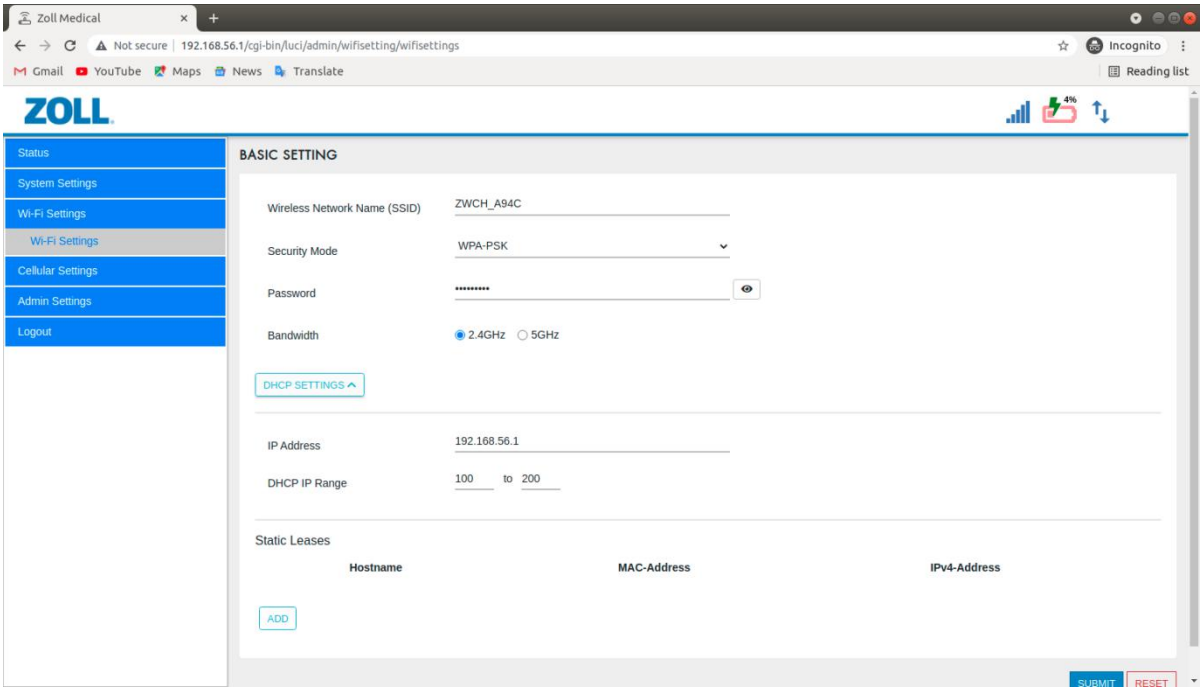


Figure 40 Wi-Fi Setting

Step 2: Change any of the available Wi-Fi settings and click on the “SUBMIT” button to apply the changes. All devices connected to the Mobile Hotspot will disconnect for the changes to apply. Once the changes are applied, the clients should be able to connect back to the Mobile Hotspot.

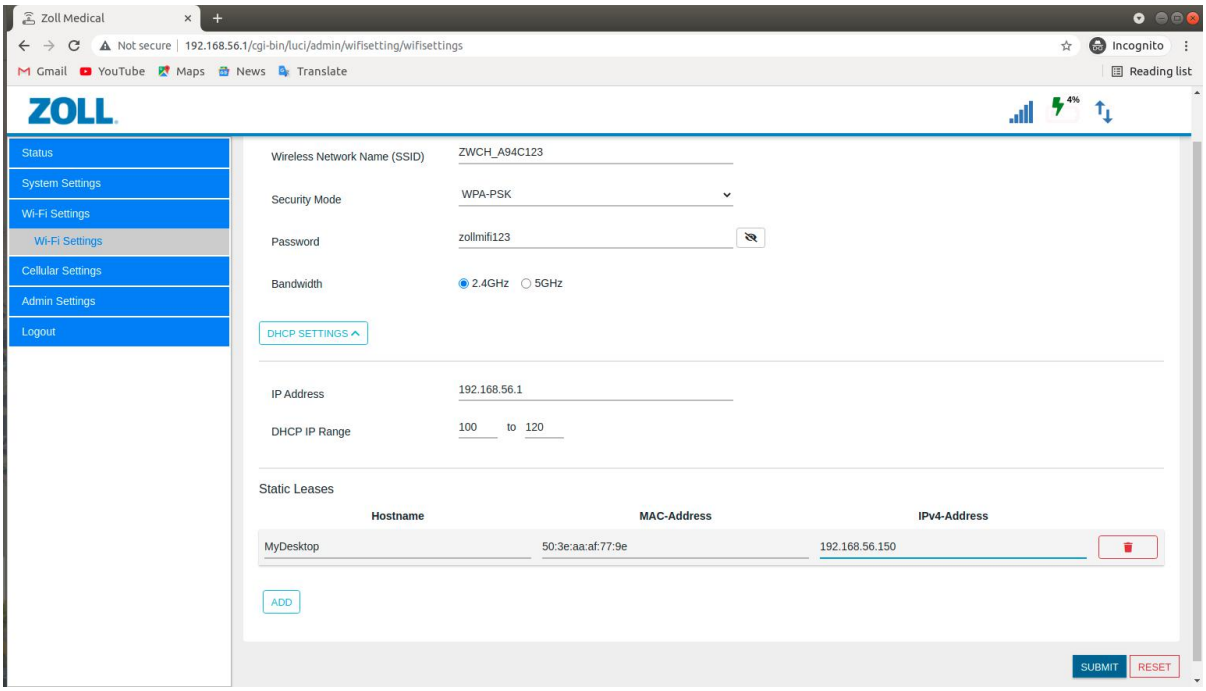


Figure 41 WebUI for available Wi-Fi settings

Note: If a password change is applied, clients will need to reconnect to the Mobile Hotspot with the new password. (Check Network Settings for Laptop/PC/Mobile/Tablet etc.).

8. Cellular Settings:

Cellular configurations can be changed in the “Cellular Settings” page in the “Cellular Settings” tab on the WebUI.

Step 1: Go to the left pane, and click on “Cellular Settings” in the “Cellular Settings” tab on WebUI.

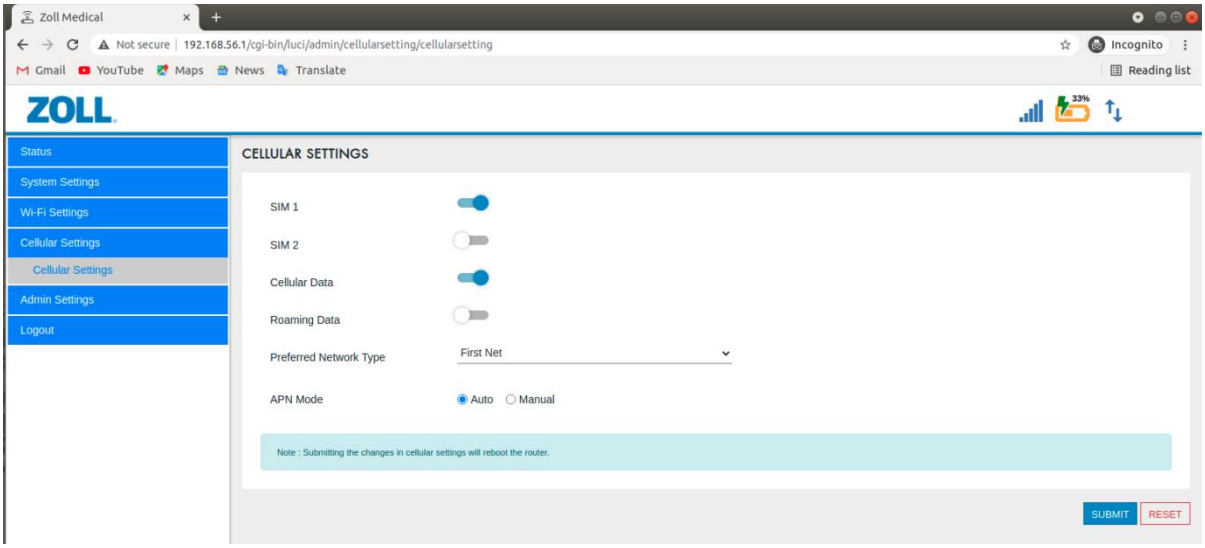


Figure 42 Cellular Setting option

The users can configure the following settings:

- SIM 1 / SIM 2 selection (Only one SIM can be selected at a time)
- Cellular Data Enable/Disable
- Network Type Selection: Available options are FirstNet, 4G, 3G, 2G. Fallback capability is enabled if the selected option is not available.

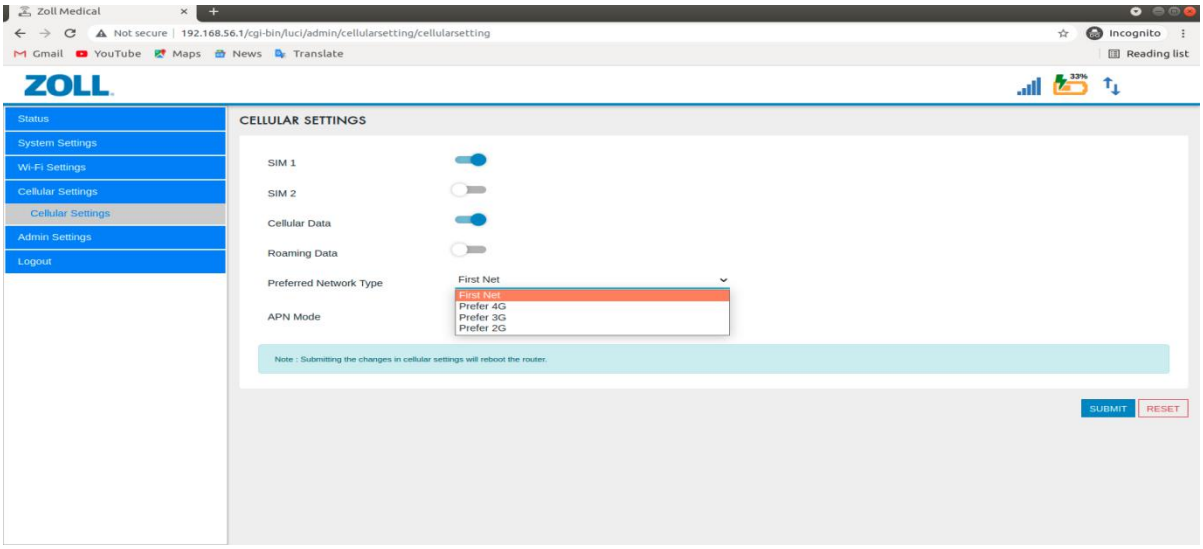


Figure 43 APN Mode selection under cellular settings

- APN Mode: Auto or Manual. If Manual is selected, an APN profile must be selected from the drop-down menu. The new profile can be added using the “ADD NEW PROFILE” button.

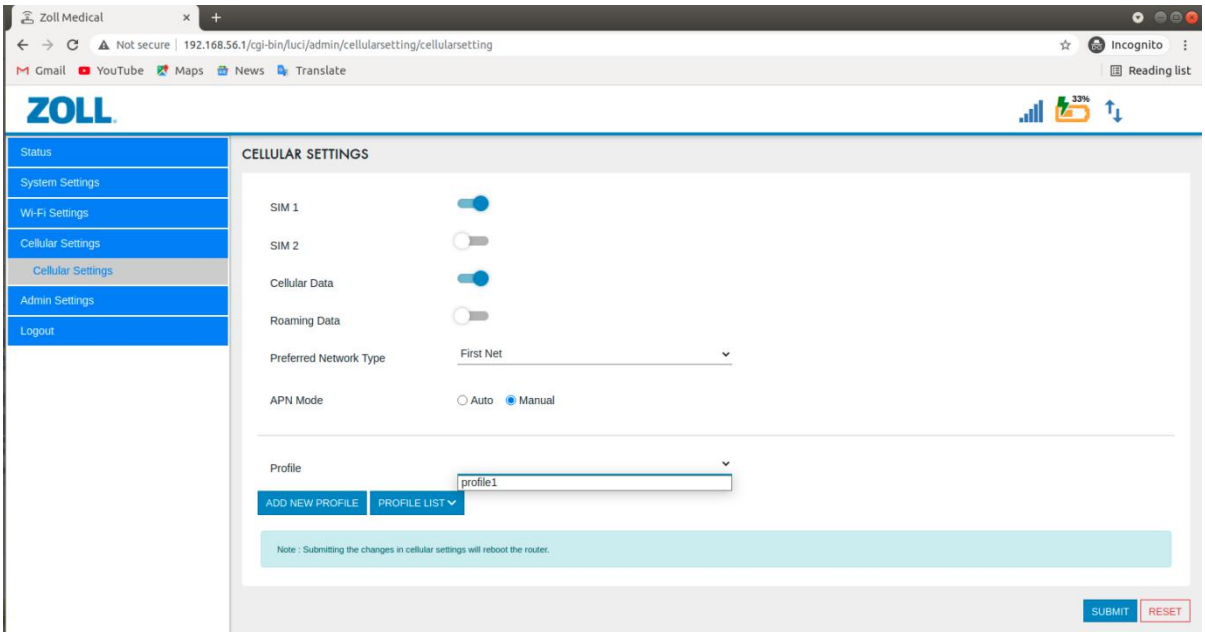


Figure 44 Adding profile

- For Manual profile, complete the Profile Name*, APN*, User Name, Password, APN Protocol*, and APN Roaming Protocol* (Fields marked with an “*” are required).

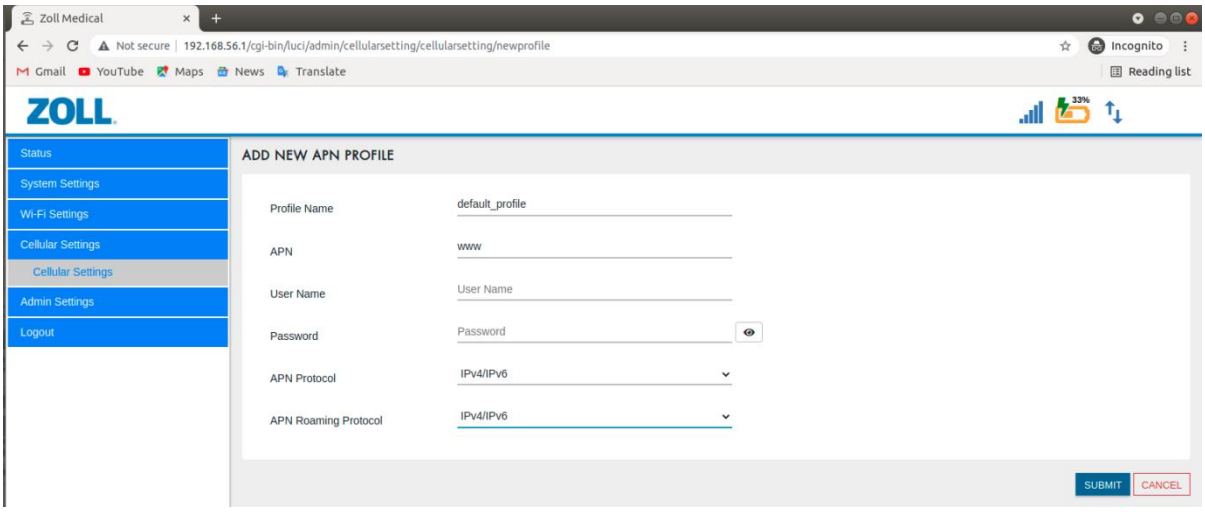


Figure 45 Adding new APN profile

- APN profiles can also be deleted. Click on “PROFILE LIST” to display a list of all available profiles. Profiles can then be deleted as desired. Synced profiles cannot be deleted.

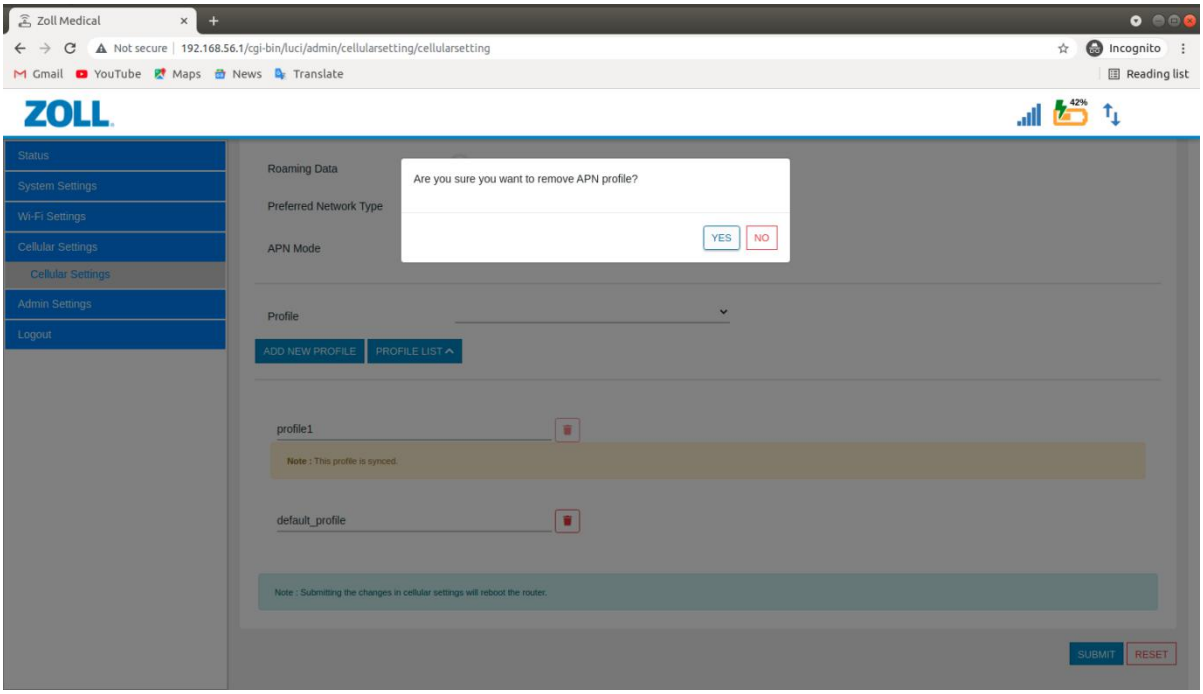


Figure 46 Pop-up for APN profile

Step 2: After making the necessary changes, click on “SUBMIT” to apply the new cellular settings. If changes are made, (except for cellular data enable/disable) the Mobile Hotspot will reboot with new settings applied.

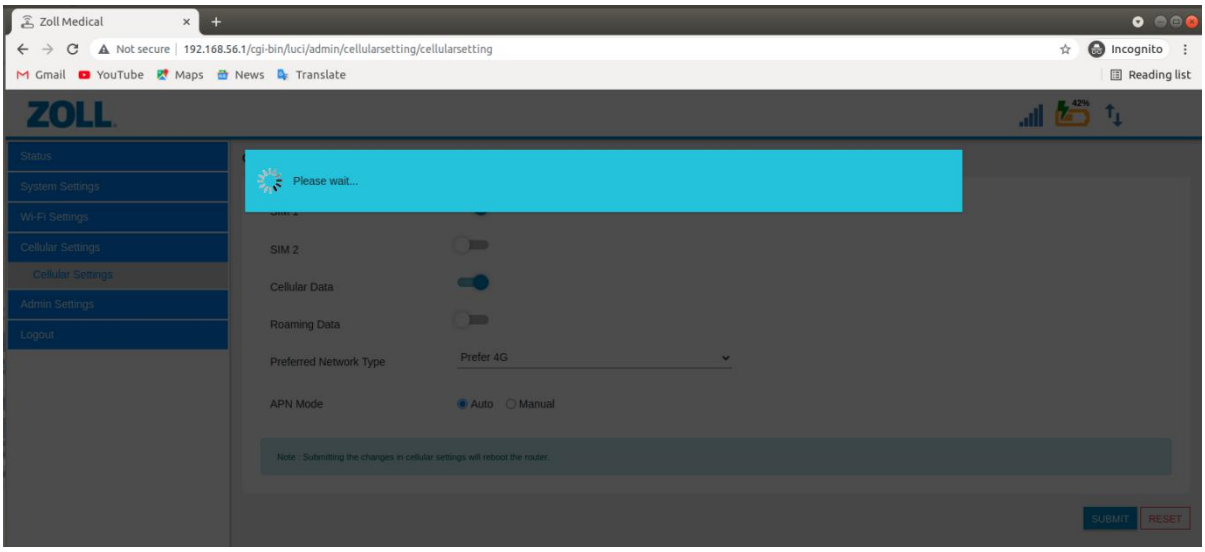


Figure 47 pop-up after submitting new APN profile

9. Change WebUI admin password:

This page allows users to set up or change the WebUI default user password of **“root”**. For security purpose, user will be forced to change password for the first time after logging into the WebUI.

Step 1: Go to the left pane and click on “Change Password” in the “Admin Settings” tab on WebUI. Enter the password in the “New Password” and “Confirm Password” fields and hit the “SUBMIT” button.

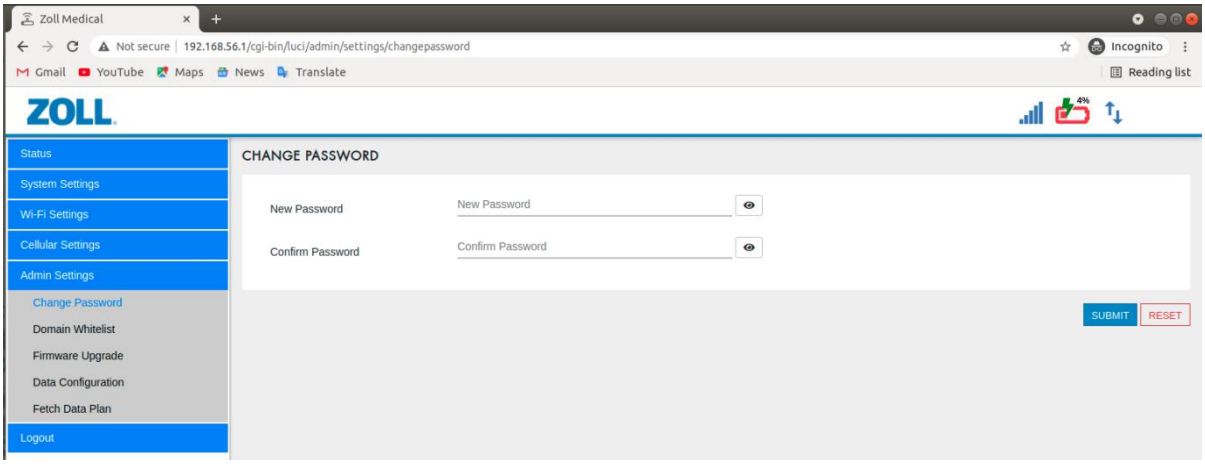


Figure 48 WebUI admin password change to update

Step 2: Ensure the “New Password” and “Confirm Password” fields match. Once the password is submitted, a confirmation message will appear as shown below.

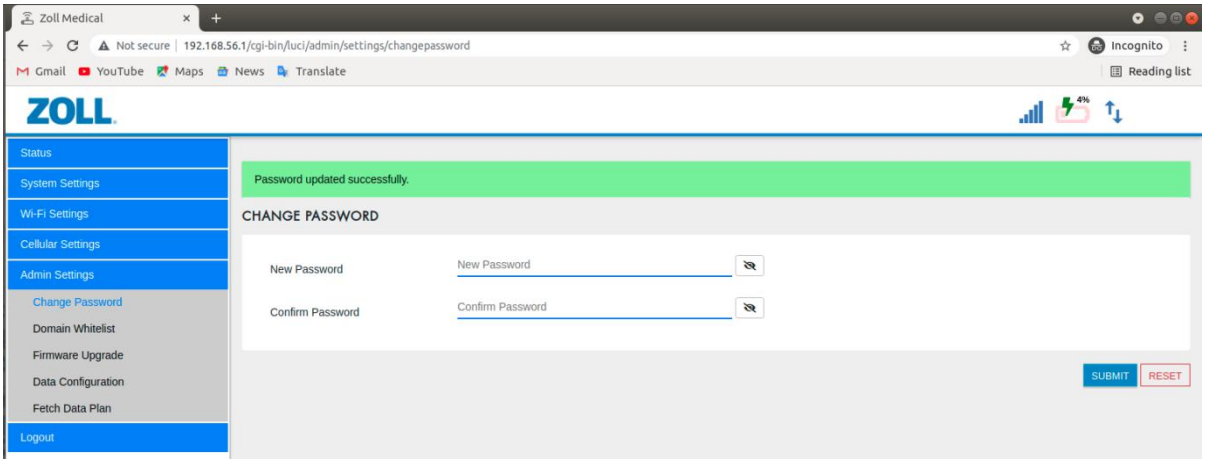


Figure 49 successfully password update display

Step 3: The user will be logged out of the current session and will be able to log in with the username “root” and new password.

Figure 50 login page to login with new credentials

Note: If an incorrect password is entered, the user will receive the error message below.

Figure 51 Error message display for incorrect credentials

10. Domain Whitelisting:

Admin can configure limited access to the internet by providing URLs for whitelisting. If configured, the connected clients will only be able to access the whitelisted URLs. Disable whitelisting to whitelist all URLs.

Step 1: Go to the left pane and click on “Domain Whitelist” in the “Admin Settings” tab of WebUI.

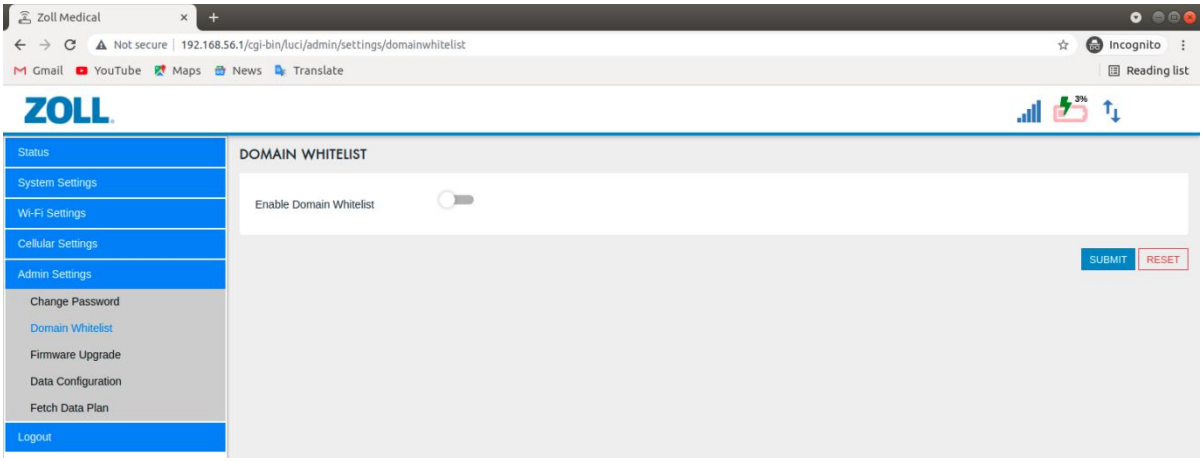


Figure 52 Domain whitelisting under Admin settings

Step 2: Toggling the “Enable Domain Whitelist” option will enable/disable whitelisting. To enter URLs for whitelisting, enter the URL into the “Domain Whitelist” field and click on the “+” after entering every URL. “Enable Domain Whitelist” must be toggled to the on position in order to limit the accessible URLs to the Whitelist only.

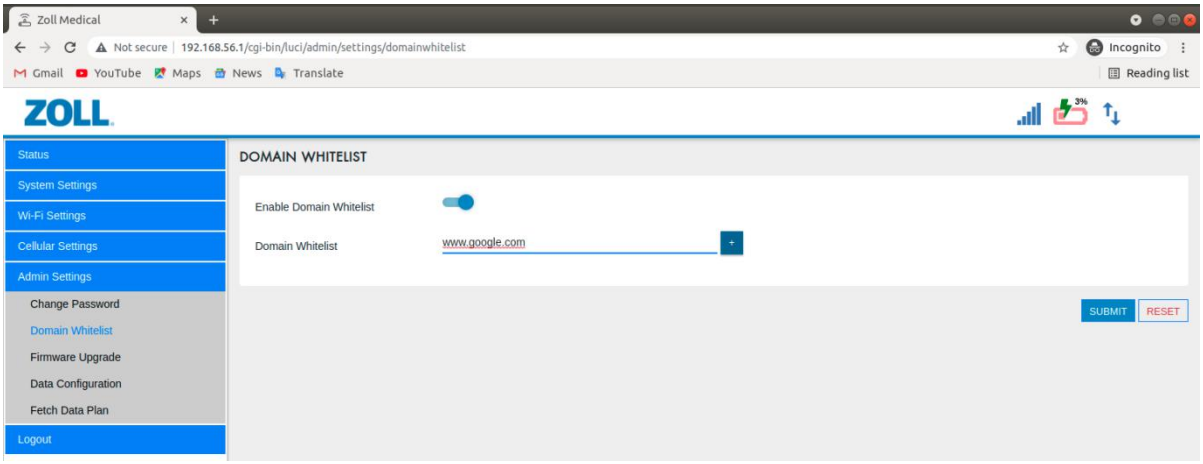


Figure 53 Enable Domain Whitelist option

Step 3: URLs can be removed from the Whitelist by clicking the trash can symbol next to an added URL. After entering all required URLs, click on the “SUBMIT” button.

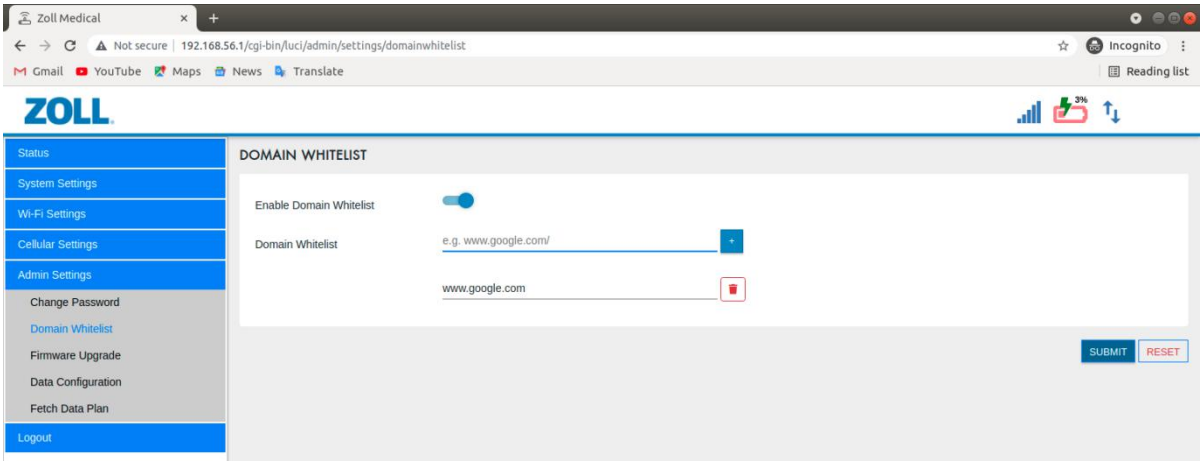


Figure 54 Domain remove option

Note: If no URLs are entered and “SUBMIT” is clicked with “Enable Domain Whitelist” in the on position, all URLs will be blacklisted.

11. Firmware Upgrade:

Step 1: Check the existing firmware version on the “Overview” page. Verify that the firmware file to be uploaded is a newer version, delineated by a higher version number.

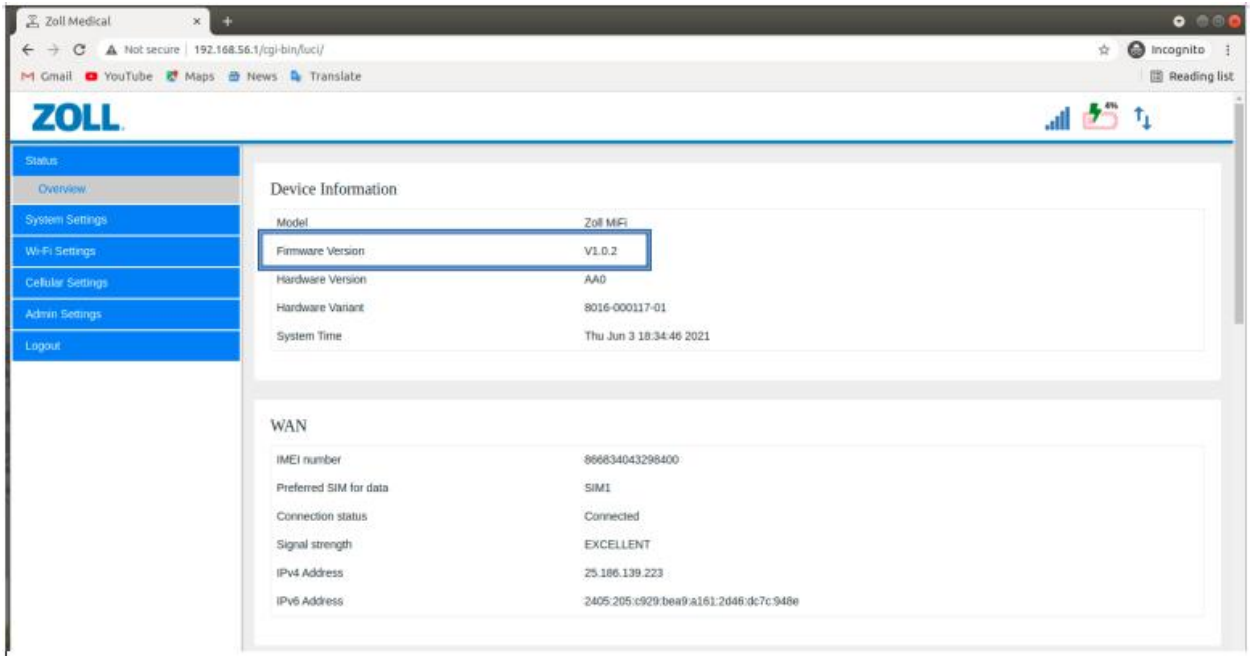


Figure 55 Firmware upgrade

Step 2: Go to the left pane and click on “Firmware Upgrade” in the “Admin Settings” tab on WebUI.

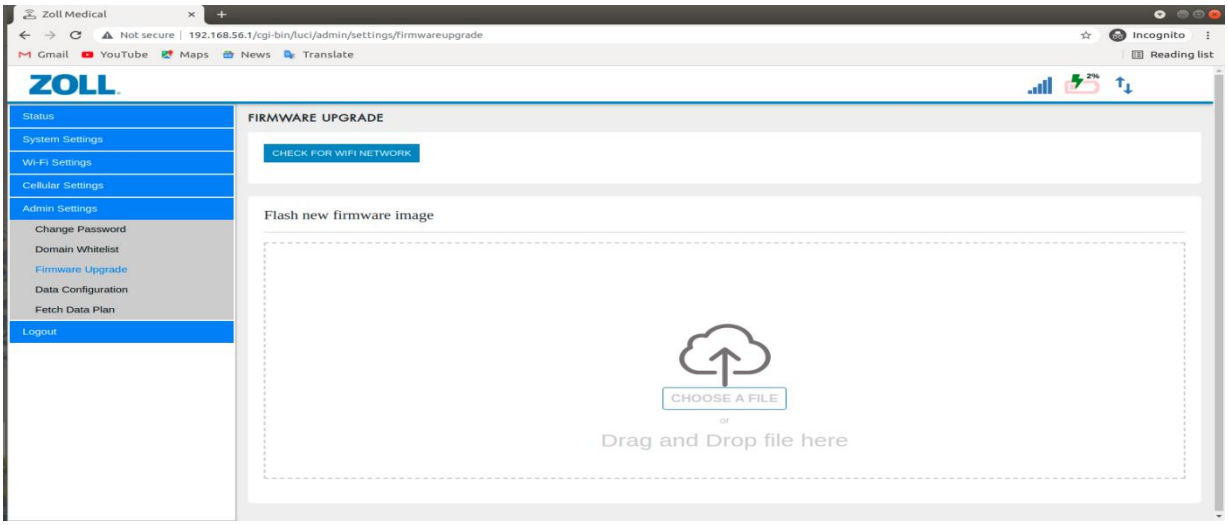


Figure 56 Firmware upgrade display under Admin settings

Step 3: Click on “CHOOSE A FILE”, and then select the firmware file from the local storage.

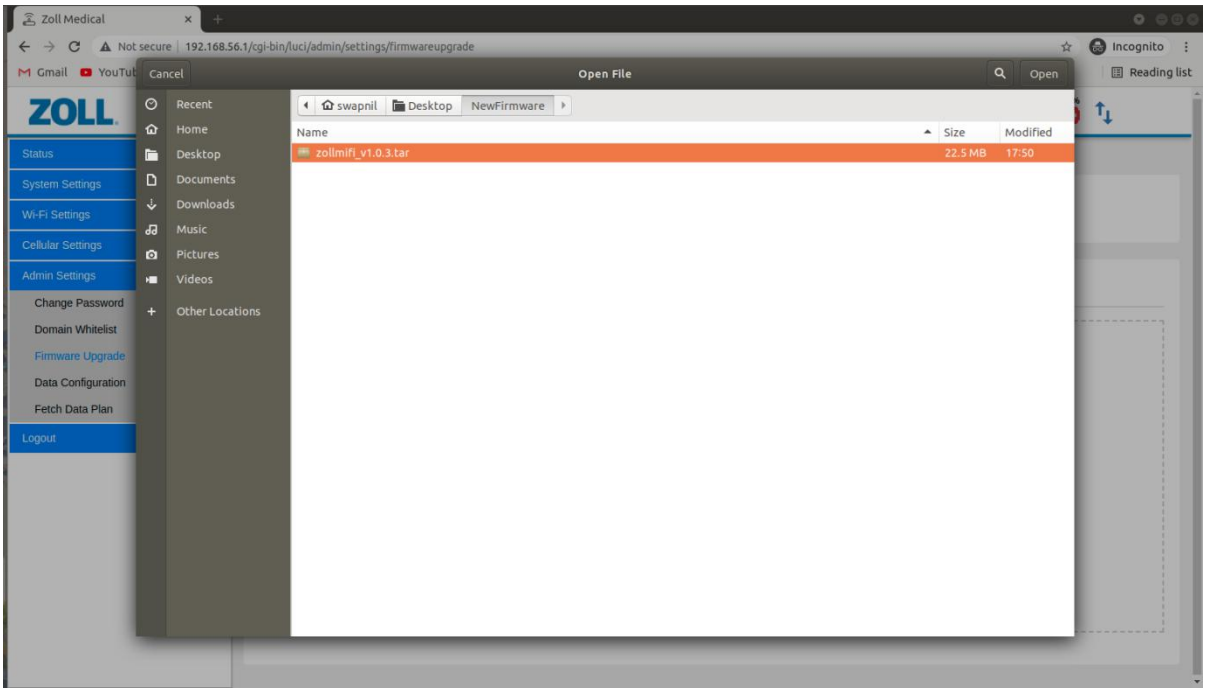


Figure 57 File selection for firmware upgrade

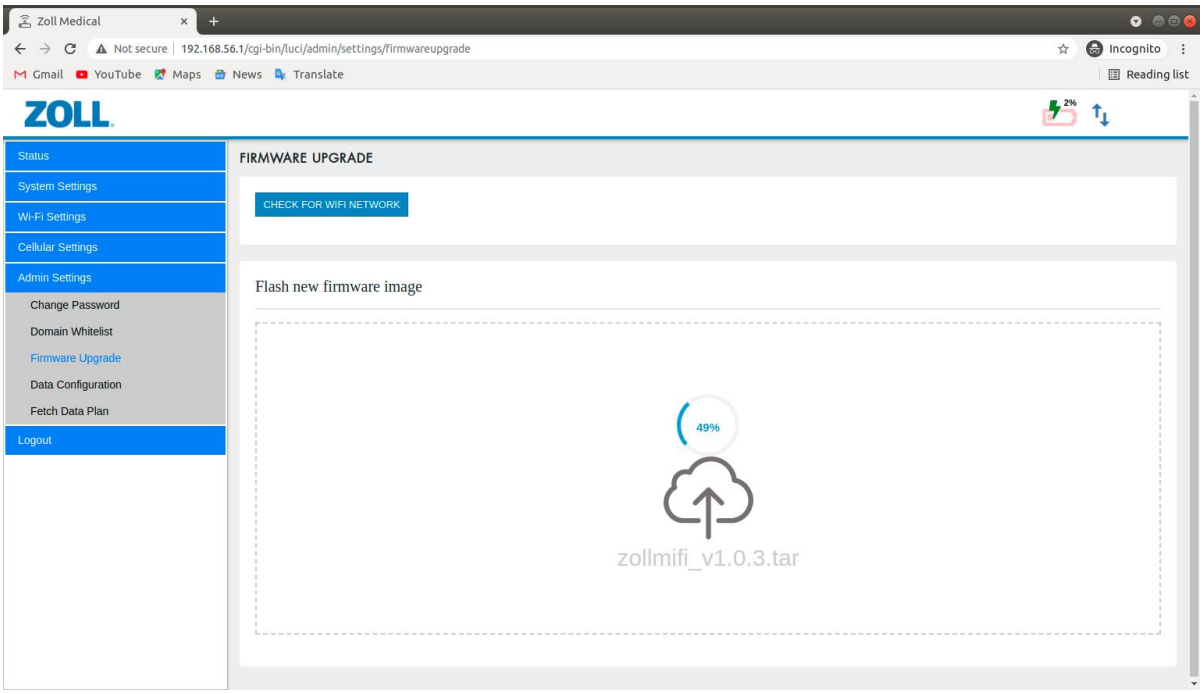


Figure 58 percentage display for firmware upgrade

Step 4: Wait for the firmware to upload and then extract.

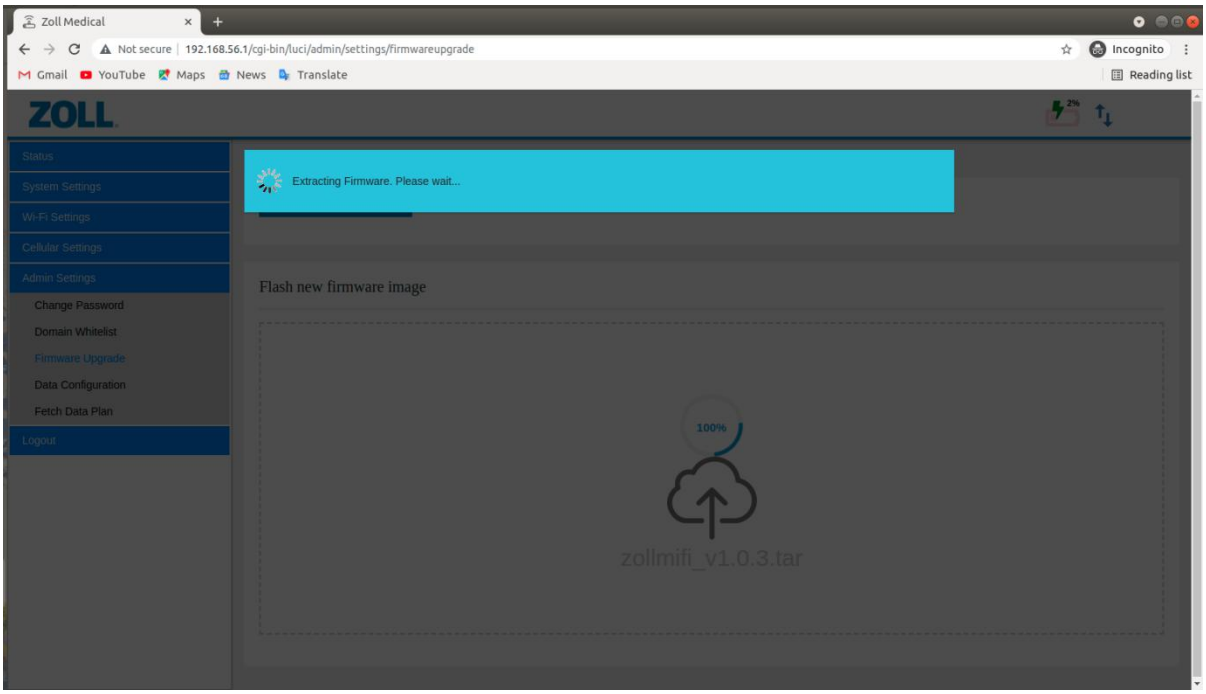


Figure 59 Firmware extracting

Step 5: Once the firmware is extracted, a popup will prompt the user to confirm the upgrade with the uploaded file.

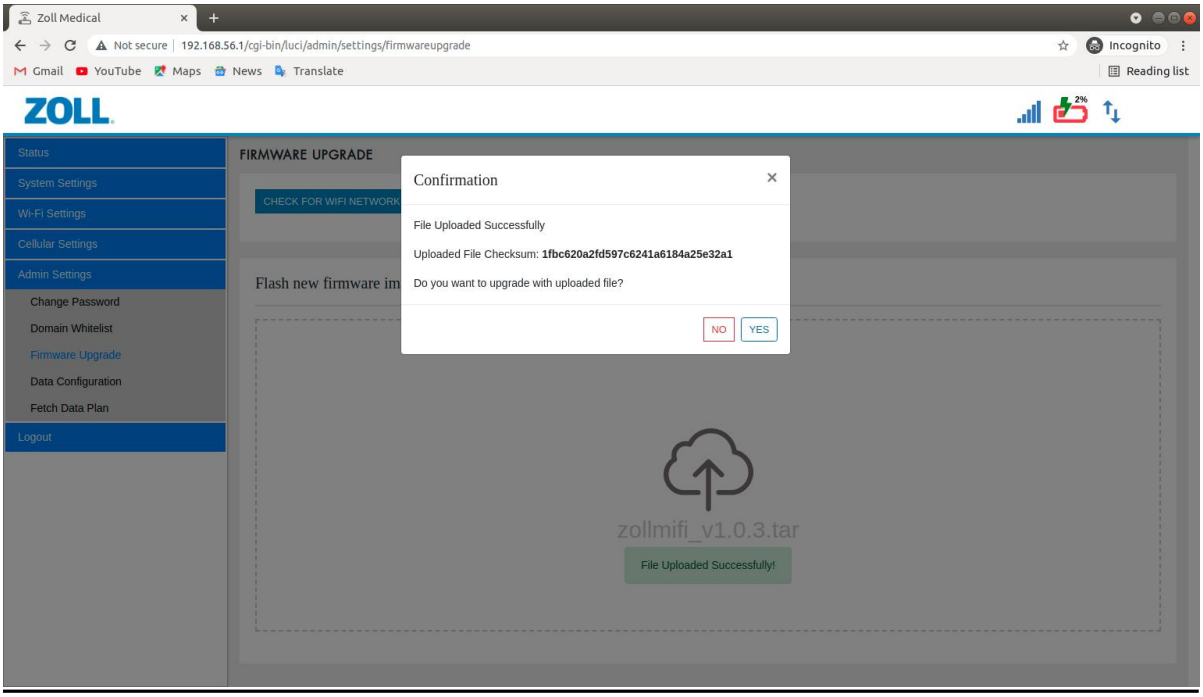


Figure 60 confirmation Pop-up for firmware upgrade

Step 6: Click the “YES” button to proceed with the firmware update process. The user should click “NO” if the file checksum (as seen on the WebUI popup window) does not match the uploaded firmware file checksum

Note: The firmware file checksum would be available with firmware file. Open the test file containing checksum and compare the checksum with the one shown on the WebUI. Checksum file (md5sum_zollmifi_vx.x.x) contents are as shown below:

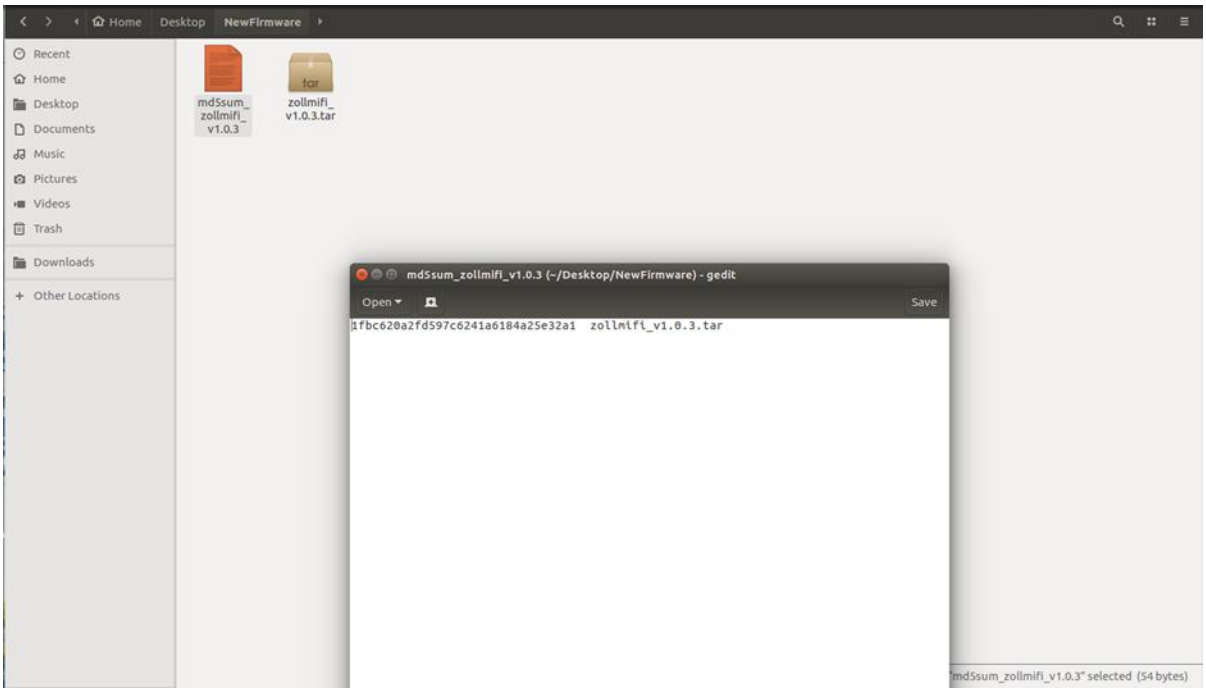


Figure 61 checksum process

Once “YES” is clicked, the firmware update process starts, and the Mobile Hotspot will reboot with the new firmware.

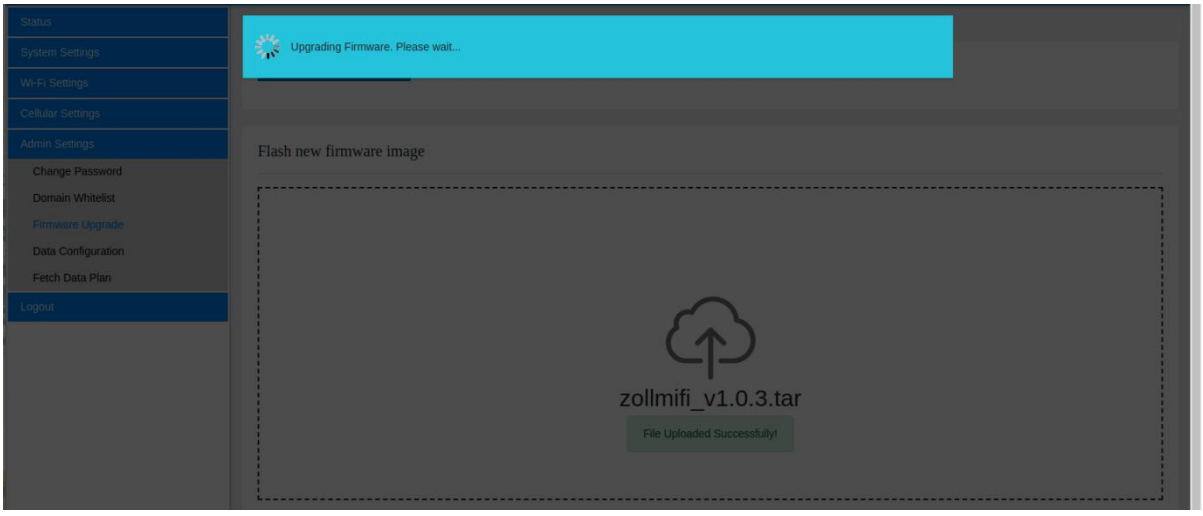


Figure 62 Firmware update process starts display

Firmware upgrade using OTA update method

Note: Firmware download will only start if a newer version of the firmware is available on the server specified by the URL.

Step 1: Go to the left pane and click on" Firmware Upgrade" in the "Admin Settings" tab on Web UI. Click on the "CHECK FOR WI-FI NETWORK" to see the list of all available Wi-Fi networks.

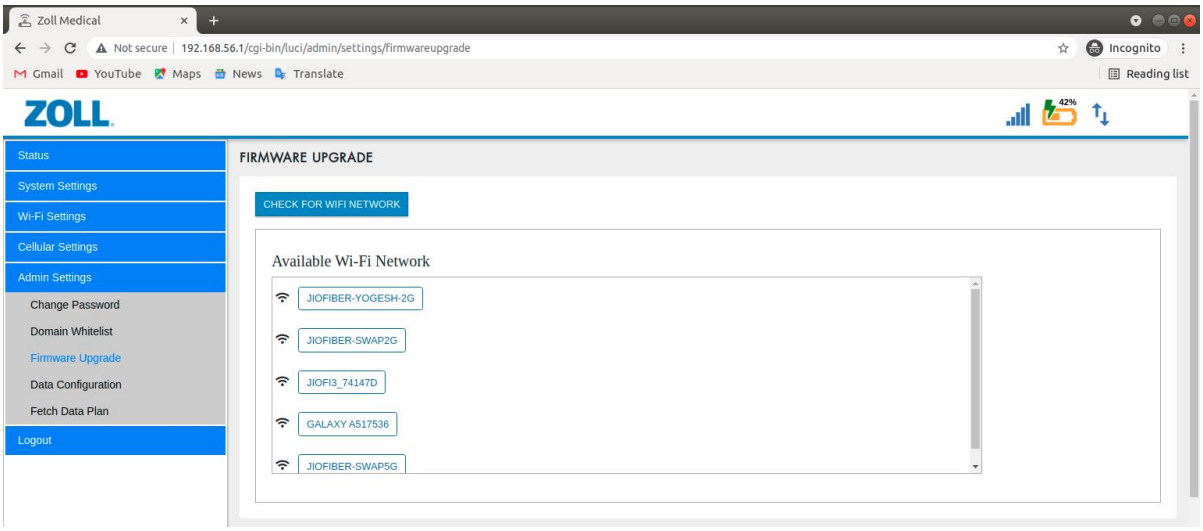


Figure 63 Firmware update using OTA method

Step 2: Select any your Wi-Fi network to proceed with the download. Enter the "Password" for the external Wi-Fi network and the URL where the firmware file is available. Click the "SUBMIT" button to proceed.

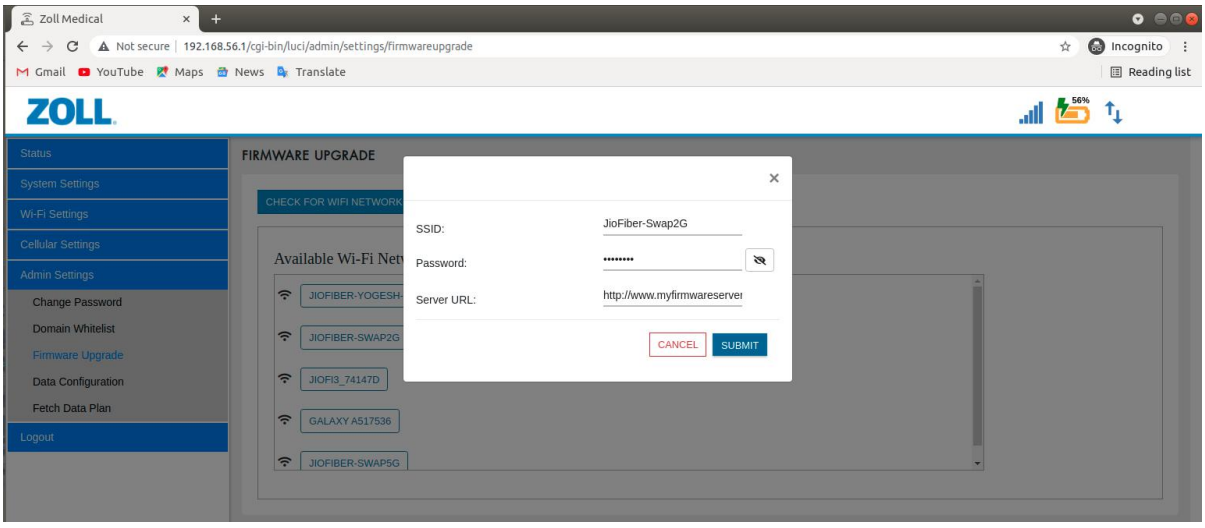


Figure 64 Firmware update using OTA method to Submit

Step 3: Once the firmware file is available on the URL, the firmware download process will begin. Download percentage will be shown on the page.

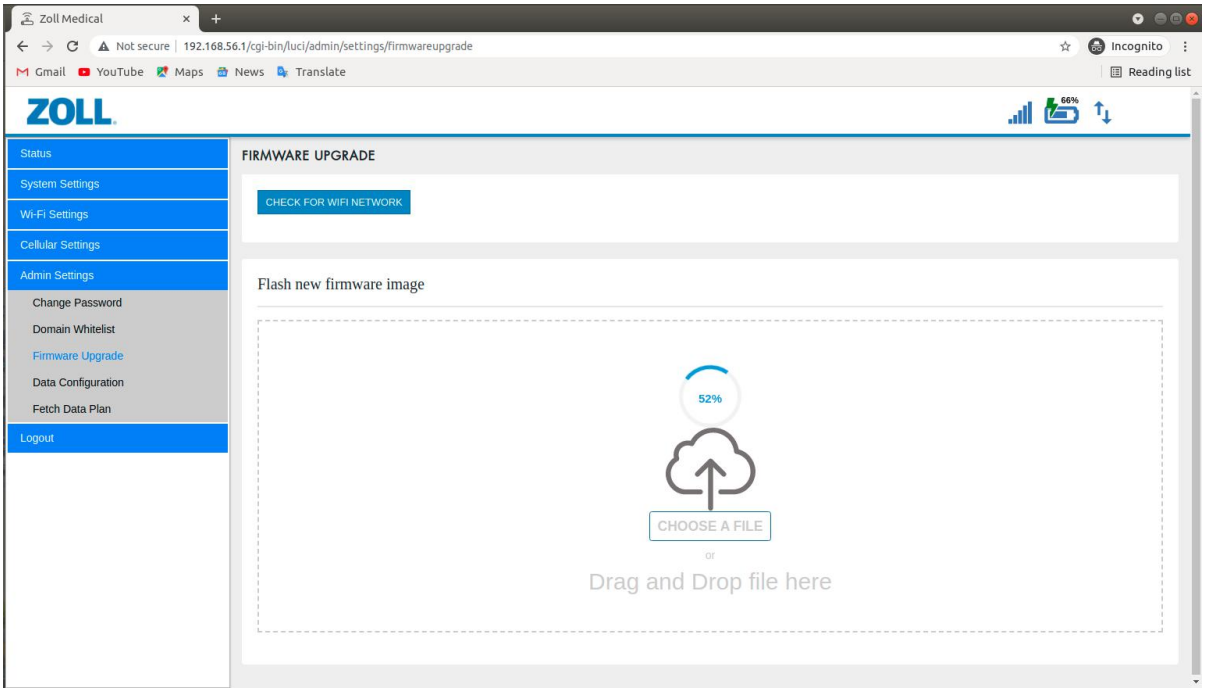


Figure 65 Firmware download process

Step 4: Once the download is complete, the user will be asked whether they want to upgrade with the uploaded file.

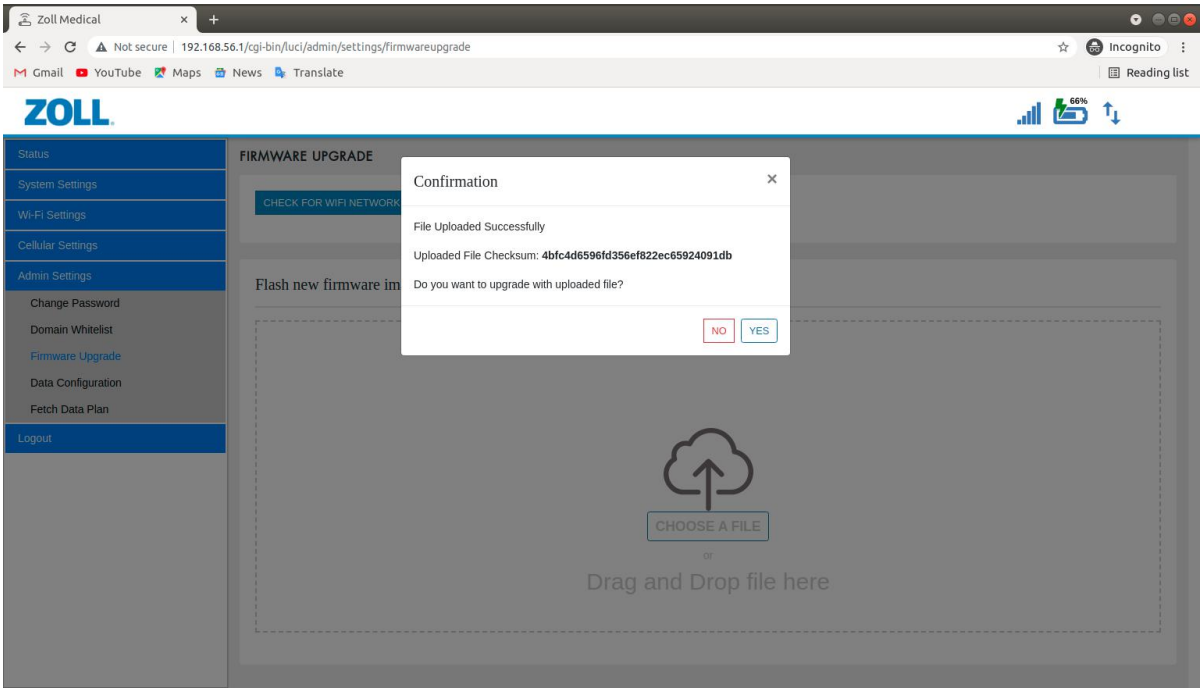


Figure 66 confirmation pop-up for firmware upgrade

Step 5: Click on the “YES” button to proceed with the installation of the new firmware. The Mobile Hotspot will reboot with the new firmware installed.

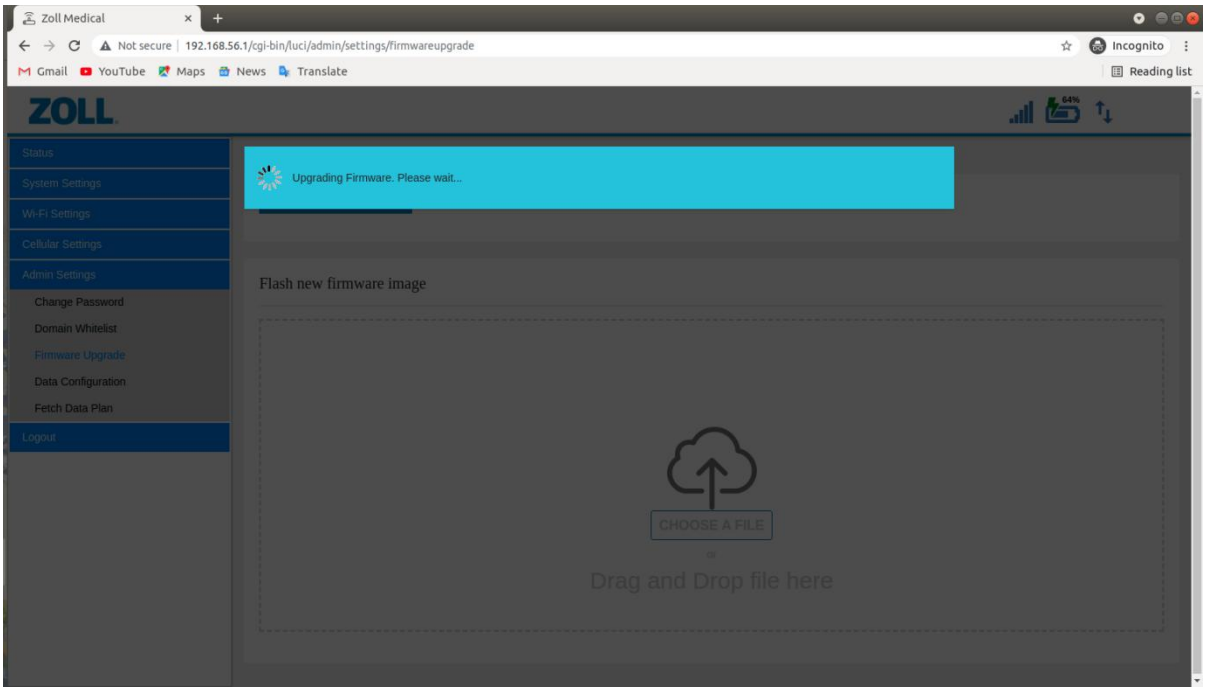


Figure 67 Firmware upgrading display

12. Data Counter Configuration:

The Data Consumption for the cellular interface is shown on the “Overview” page. This consumption information is cleared as per the Billing Cycle Day (specified day of the month in the billing cycle start date) configured in the “Data Configuration” page. The consumption information can be cleared manually using the “RESET DATA” button on this page.

Clear Data Consumption Manually

Step 1: Go to the left pane and click on” Data Configuration” in the “Admin Settings” tab on the WebUI. Click on the “RESET DATA” to clear all Data Consumption information.

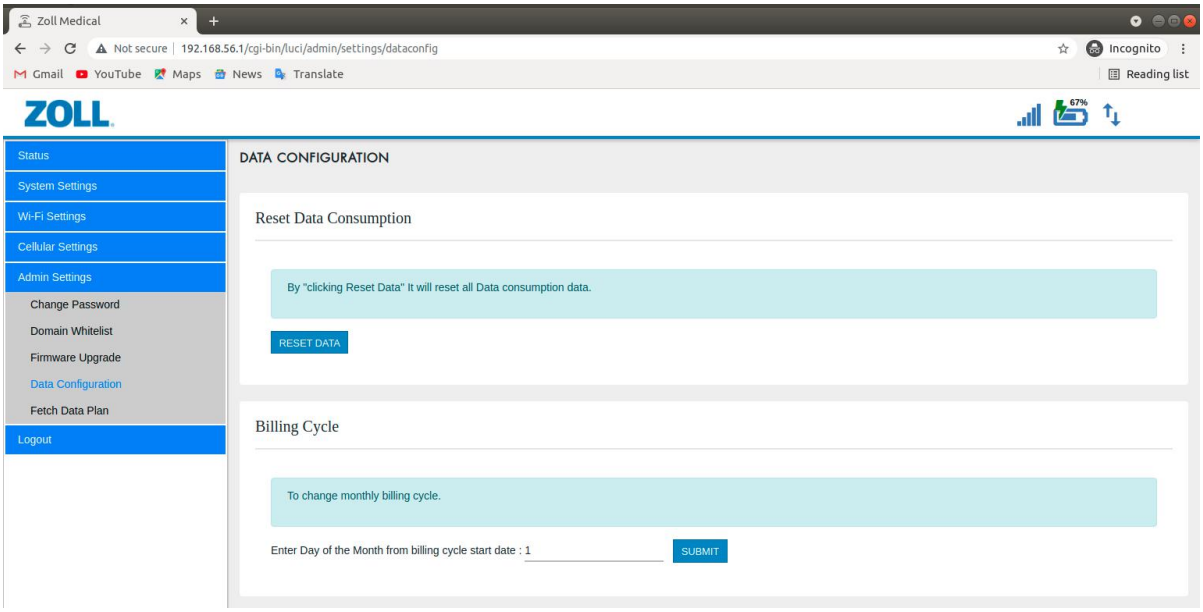


Figure 68 Data counter configuration reset

Step 2: Verify the changes by observing the Data Consumption on the “Overview” page.

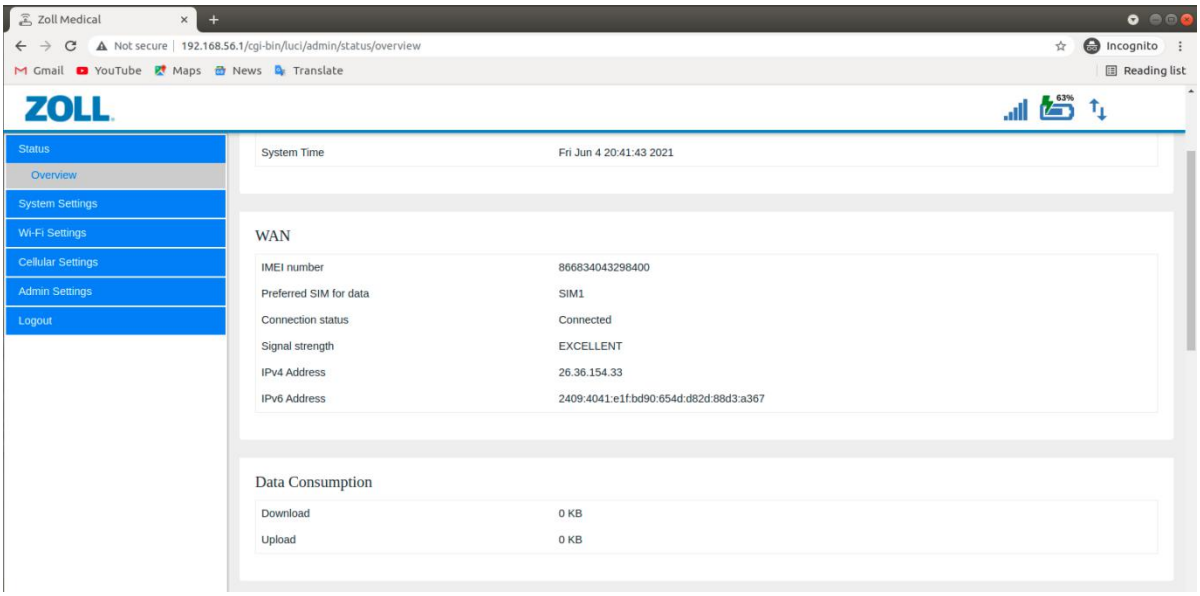


Figure 69 verifying data consumption on overview page

Configure Billing Cycle Day

Step: Go to the left pane and click on" Data Configuration" in the "Admin Settings" tab on the WebUI. Enter the Day of the Month from the cellular billing cycle start date for the SIM card in the "Billing Cycle" section of the page. Click on the "SUBMIT" button to apply the changes.

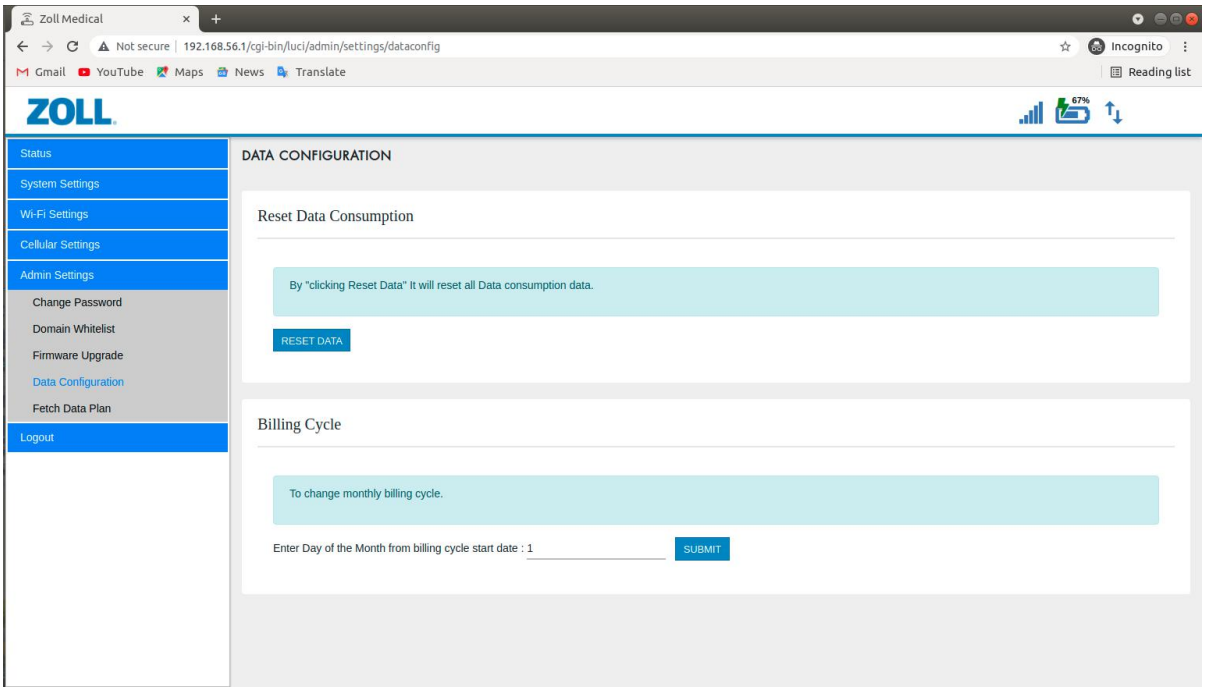


Figure 70 Billing cycle configuration

13. Fetch Cellular Data Plan using USSD Code:

This page allows the user to fetch the selected SIM card's active data plan using the USSD code available from the SIM card user manual. Special USSD codes for all telecom companies for fetching active data plans are available.

Step 1: Go to the left pane and click on "FETCH DATA PLAN" in the "Admin Settings" tab on WebUI.

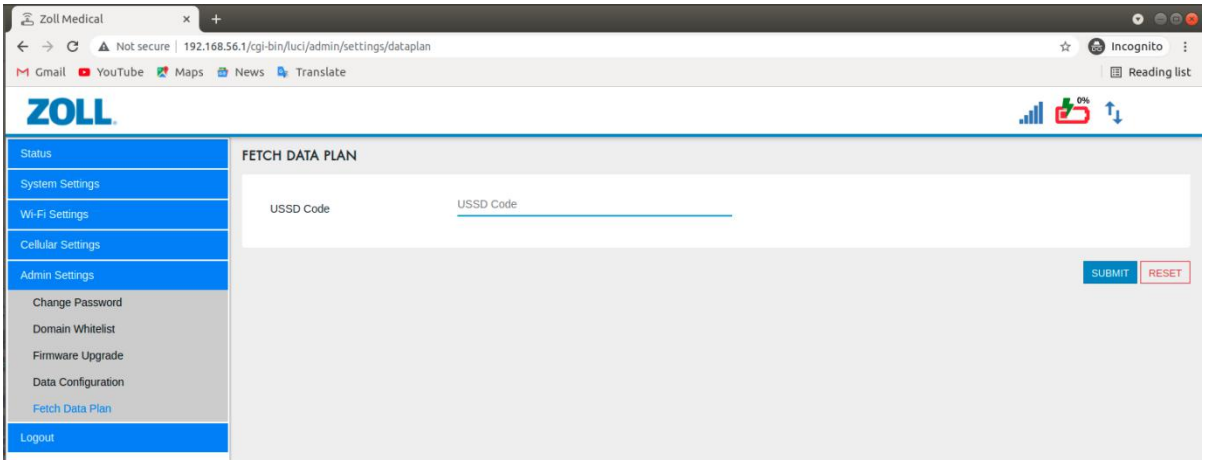


Figure 71 Fetching cellular data plan using USSD code

Step 2: Enter the USSD code available for the selected SIM card to checking the active data plan and click the "SUBMIT" button.

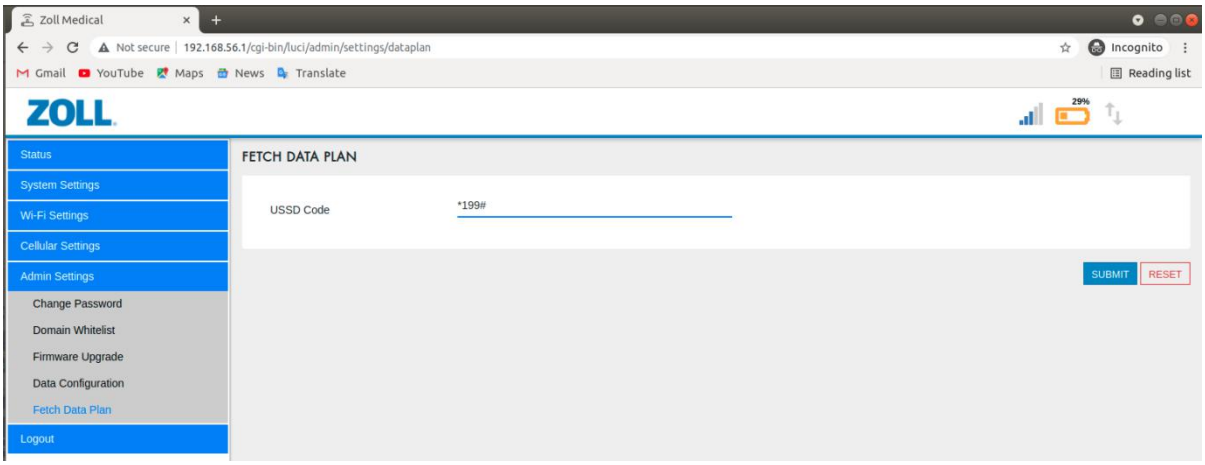


Figure 72 Display for adding USSD code

Step 3: Wait for the Mobile Hotspot to fetch the data plan. This may take a while.

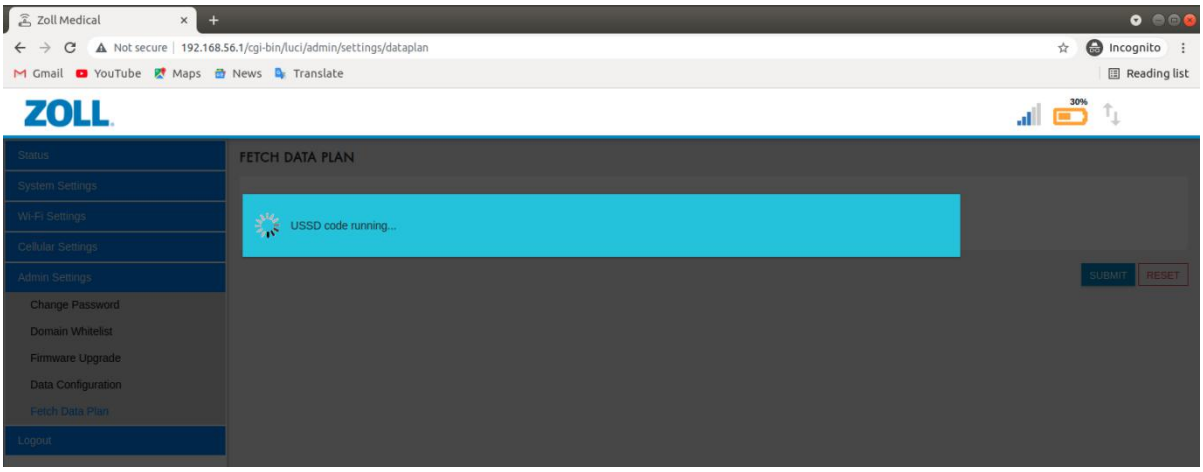


Figure 73 USSD code fetching

Step 4: The response for the USSD code will be displayed as below.

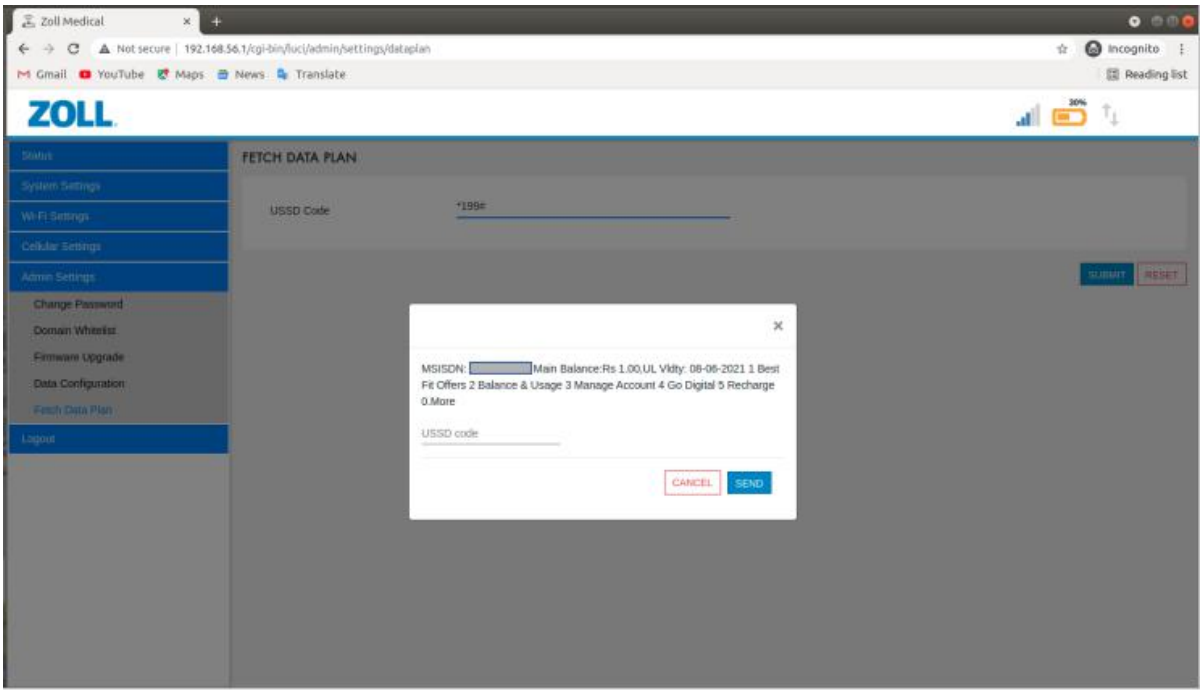


Figure 74 USSD code response

Step 5: To utilize the menu options in the response, enter the item number and click “SUBMIT”.

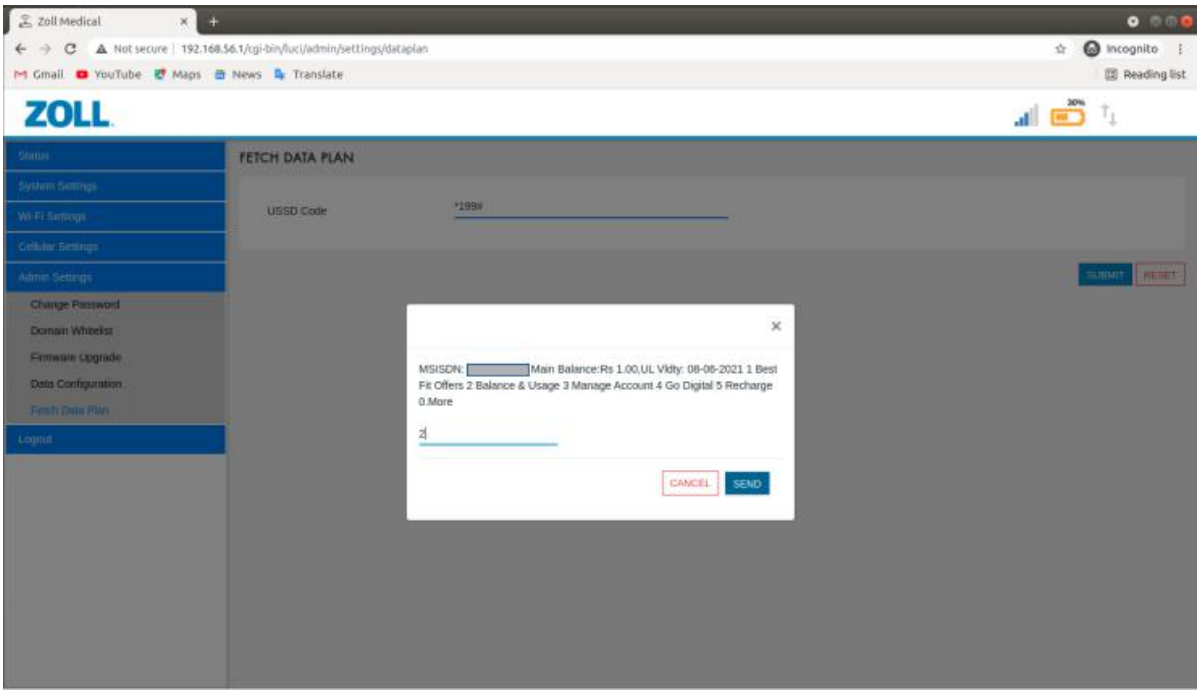


Figure 75 Utilize the menu options in the response example 1

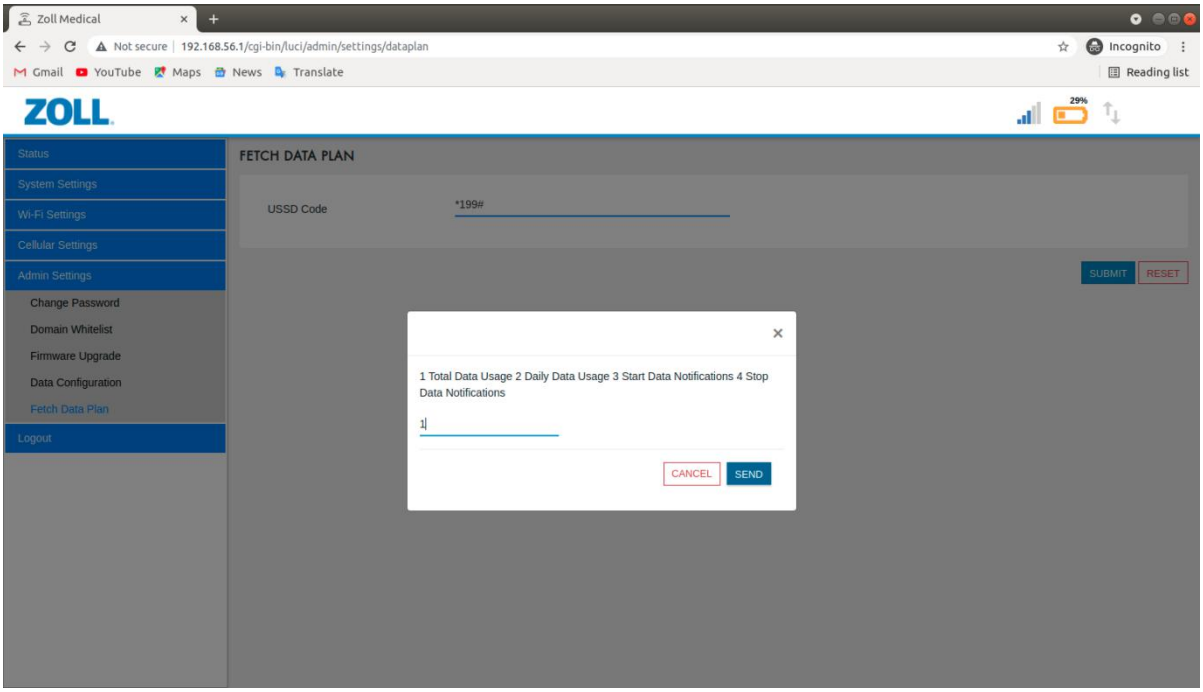


Figure 76 Utilize the menu options in the response example 2

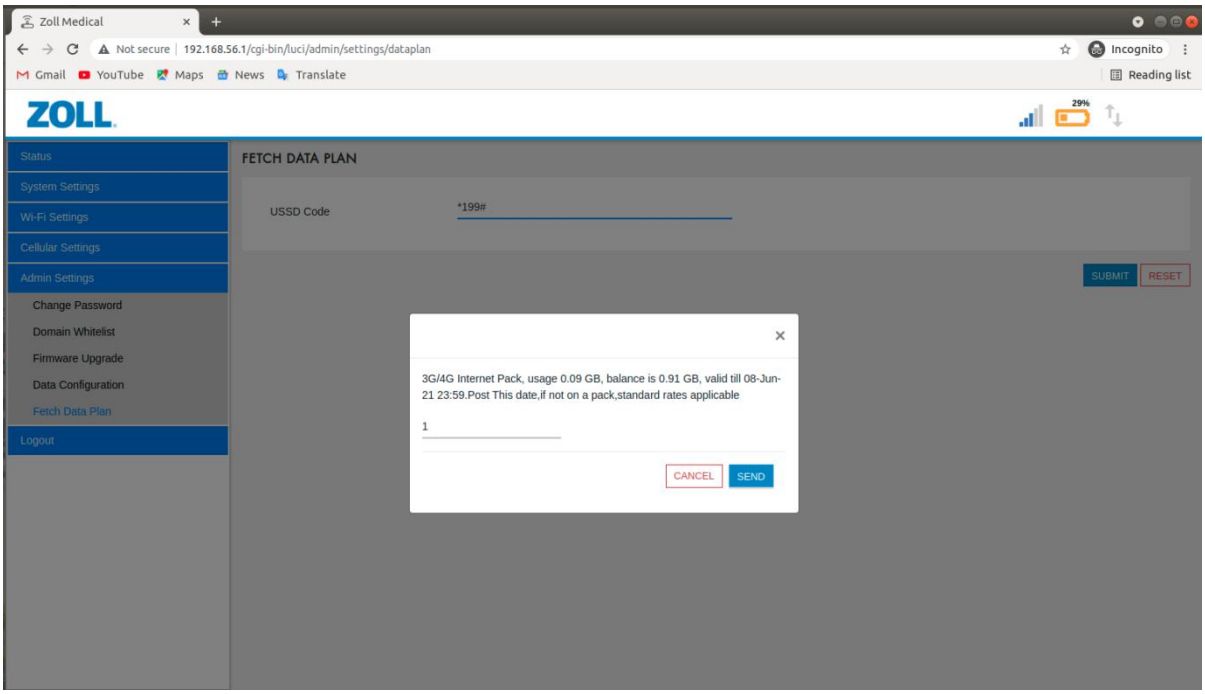


Figure 77 Utilize the menu options in the response example 3

E. Device Specification

Below are the device specifications:

Particulars	Details
Size	134.2mmx80.7mmx27.9mm
Weight	280 grams Approx.
Data Rate	Download: Up to 150Mbps Upload: Up to 50Mbps
Wi-Fi	802.11ac/a/b/g/n 1x1
Cellular	LTE CAT-4 Module integrated with chip Antenna
Power	5 VDC 0.5A by USB Type C cable
Battery	3.7V Li-ion, 4000mAH
Temperature	-10°C to 50°C
Humidity	15% to 95% RH (non-condensing) (per IEC 60601-1-12)
Vibration	Sinusoidal Vibrations (EN 1789 for ambulance per EN60068-2-6)
	RTCA/DO-160G (multiple helicopter frequencies)
	Broadband Random Vibrations (per IEC 60069-2-64)
Shock	15g/11ms half sine & 30g/6ms half sine (per IEC 60068-2-27)
Bump	IEC 60068-2-29
Drop	EN 1789, 30-inch functional drop
Altitude	-170 m to 4572 m (-557 feet to 15,000 feet)
Transportation & Storage	-20°C to 70°C
Ingress Protection	IP-55 (per EN60529)

Table 3 Device Specification

F. Device RF Support Details

This device supports Wi-Fi and Cellular for wireless data transmission. The frequency, band and power support details are as follows,

Wi-Fi:
Band Supported: 2.4GHz, 5GHz
Chip Antenna Gain: 2.2dBi, 5.2dBi
Maximum Power Level settings to support for Wi-Fi 2.4GHz transmitter:
Mode b: 13dBm
Mode g: 16dBm
Mode n: 16dBm
Maximum Power Level settings to support for Wi-Fi 5GHz transmitter:
Mode a: 12dBm to 14dBm
Mode n: 11dBm to 15dBm
Mode ac: 11dBm to 16dBm

LTE:
US Variant:
Contains Radio transmitter FCC ID: XMR201808EC25AF
Contains Radio transmitter IC: 10224A-2018EC25AF

Band Supported: LTE: 2, 4, 5, 12, 13, 14, 66, 71
WCDMA: WCDMA II, WCDMA IV, WCDMA V
Antenna Gain:

Antenna Type	Frequency Range (MHz)	Antenna Gain (dBi)
Chip Antenna	617 - 698	0.81
	698 - 960	1.1
	1710 - 2690	2.4
External/ Diversity Antenna	617 - 698	-1.1
	698 - 806	1.8
	824 - 960	2.8
	1427 - 1518	1.6
	1710 - 2200	3.0
	2300 - 2690	4.7

G. Regulatory Information

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.
Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Product FCC ID: ZKP-ZOLLMCH0001

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 operated in conjunction with any other antenna or transmitter.

This device is integrated with certified cellular module which contains following FCC ID and IC:
Cellular module contains FCC ID: XMR201808EC25AF
Cellular module contains IC: 10224A-2018EC25AF

RF Radiation Exposure Statement

To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with a minimum distance of 20 cm from your body.

IC Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) This device may not cause interference, and (2) This device must accept any interference, including interference that may cause undesired operation of the device. This device complies with RSS-247 of Industry Canada. Operation is subject to the condition that this device does not cause harmful interference. This Class B digital apparatus complies with Canadian ICES-003 (Cet appareil numérique de la Classe B conforme à la norme NMB-003 du Canada).
Product IC: 9702A-ZOLLMCH0001

This equipment complies with 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.
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.
Cet équipement est conforme aux limites IC d'exposition aux radiations définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et votre corps. Cet émetteur ne doit pas être situé ou opérant en conjonction avec une autre antenne ou émetteur.