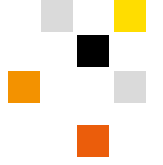


Figure 32: Representation of grounding and voltage tapping cabling

5. OPERATIONS & TROUBLESHOOTING



5.1 POWERING ON

Once the hyperSPROUT™ smarthub or hyperHUB™ access point is installed properly on the pole/wall, the hyperSPROUT™ smarthub or hyperHUB™ access point front LED will glow **RED** during boot up. After boot-up, once the below conditions are satisfied, the LED will glow **GREEN**:

- Internet connection established
- Communicating with cloud server
- Wi-Fi radios are up

Further, the device can be accessed through cloud application. Refer to the subsequent *Local GUI* section for device accessibility and configuration.

5.2 OPERATION

The below *Table 4* shows the LED indication of the unit and it's a glowing pattern.

Table 4: LED Indications

Item	State	LED Color	Glowing Pattern	Duty Cycle
1	During board boot-up	Red	Always active	Not applicable
2	Backhaul down and Wi-Fi manager started	Red	Blinking (moderate)	ON - 500ms OFF - 500ms
3	Backhaul up and radios are down	Blue	Always active	Not applicable
4	OTA upgrade status	Blue	Blinking (moderate)	ON - 500ms OFF - 500ms
5	Internet connection down and radios are up	Green	Blinking (moderate)	ON - 500ms OFF - 500ms
6	Internet connection established, communicating with cloud server and radios are up (normal operation)	Green	Always active	Not applicable
7	Cloud connectivity down but Internet connected	Red/ Blue	Toggling between red and blue colors	Red active - 1000ms Blue active - 1000ms

5.3 TROUBLESHOOTING

If the hyperSPROUT™ smarthub or hyperHUB™ access point does not function properly, use the troubleshooting functions in the collectionENGINE™ asset management system before resetting in the field. The device can be reset either manually in-field or remotely by using the collectionENGINE™ asset management system.

To reset the hyperSPROUT™ smarthub or hyperHUB™ access point manually:

- Remove the M32 end cap as shown in *Figure 33*.
- Perform a reboot by pressing the reset switch for 0-10sec.
- If a reboot does not restore functionality, perform a factory reset by pressing the reset switch for 10-20sec.
- Reinstall the end cap as shown in *Figure 33* and *Figure 34*.
- If the reset does not correct the function, contact the supplier or agent, or replace the hyperSPROUT™ smarthub or hyperHUB™ access point directly.

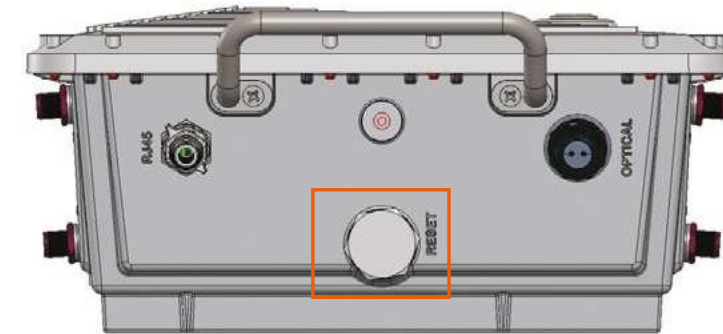


Figure 33: M32 end cap

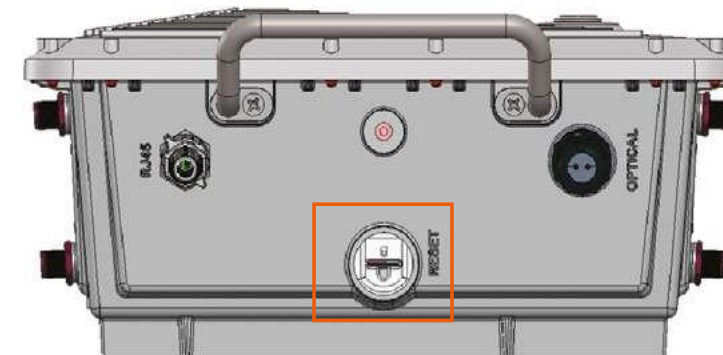
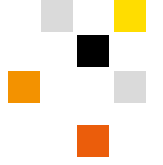


Figure 34: Uncovered reset switch

6. LOCAL GUI



6.1 LOCAL GUI

This section explains the Local GUI interface details for the hyperSPROUT™ smarthub and the hyperHUB™ access point.

IMPORTANT: Upon initial commissioning of the hyperSPROUT™ smarthub or hyperHUB™ access point using the local GUI, the installer is strongly advised to lock the device’s local GUI interface using the collectionENGINE™ asset management system. This locking prevents any unauthorized user from gaining local control of the device via the Local GUI. Note that configuration changes to the hyperSPROUT™ smarthub or hyperHUB™ access point may still be processed remotely using the collectionENGINE™ asset management system after performing this lock.

6.2 HYPERSPROUT™/HYPERHUB™

Follow below instructions to login to the Local GUI interface.

- Connect a laptop with default provisioning SSID (e.g.: HyperSprout_06:03:7f: 63:23:21).
- Type the device default br-lan IP address in the browser https://192.168.20.1
- After giving the br-lan IP address, the browser will redirect to the login page as shown in *Figure 35*.
- Enter the following user name and password to login to the device. Note that all devices may be “locked” after set-up via use of the collectionENGINE™ asset management system. This locking procedure prevents others from accessing these devices in-field using the device’s default br-lan IP address. All devices should be locked upon initial commissioning.
 - User Name: **root**
 - Password: **delta123**
- After entering the *User Name* and *Password* press the *LOGIN* button.

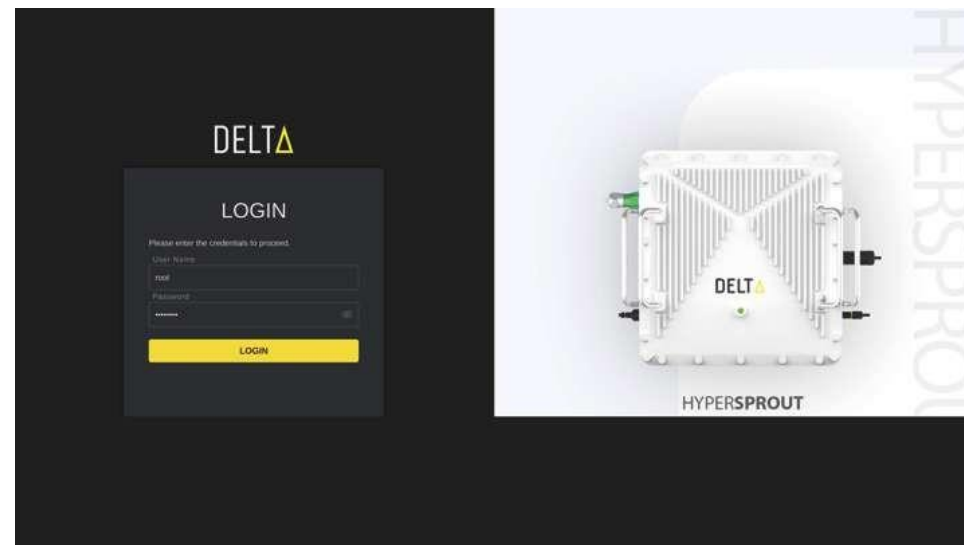


Figure 35: Login Page

- Logging in with the correct user name and password will redirect to the set-up page.

6.2.1 Set-Up Page

Follow below instructions to set up the system and access system information.

- Once in the set-up page, select the appropriate *Country* and *Time Zone* from the drop-down menus and click *SAVE*, as shown in *Figure 36*.

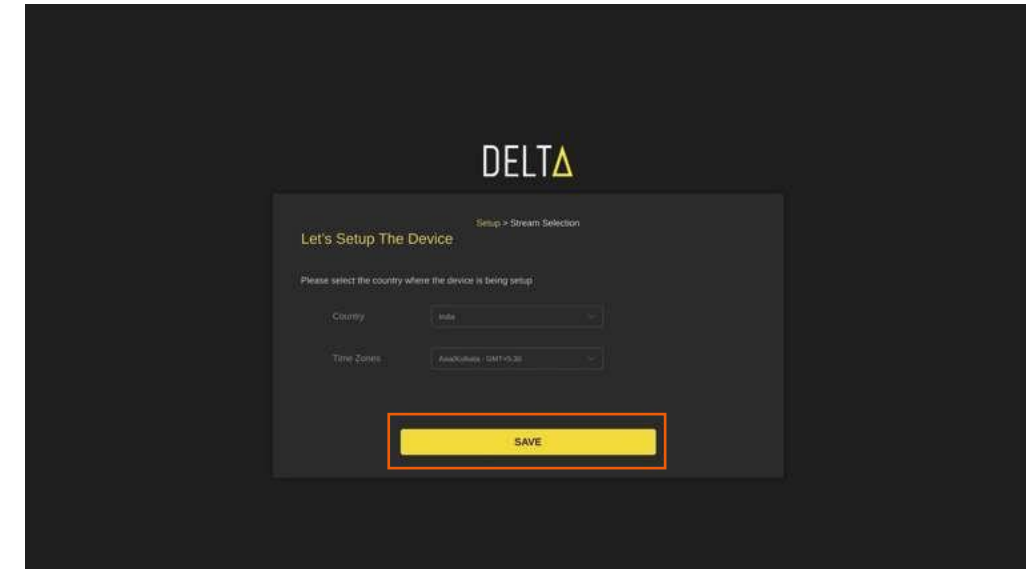


Figure 36: Setup Page

- Then GUI will redirect to the *Stream Selection* page. From the dropdown, select the *Stream* as either *4x4* or *8x8*. See *Figure 37*.

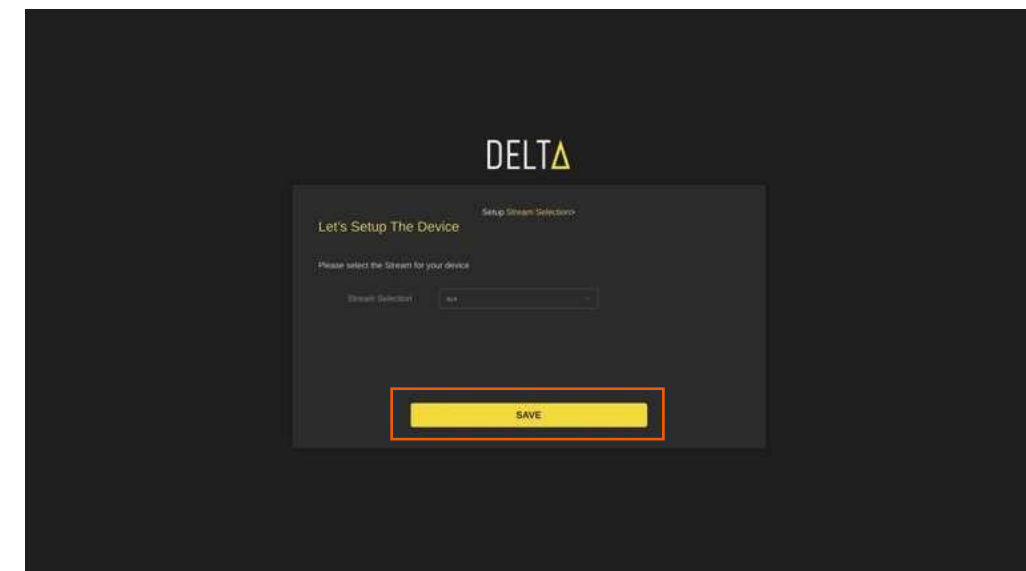
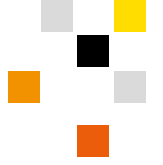


Figure 37: Stream Selection



- c. If stream selection is selected as **8x8**, upon clicking on **SAVE** the system will reboot.
- d. If stream selection is selected as **4x4**, upon clicking on **SAVE** the GUI will redirect to the **System Information** page.
- e. The **System Information** page will show the device **IPv4 Address**, **System Name**, **Ethernet MAC Address**, **Wireless MAC Address**, **Cloud Status**, **Current Firmware Version** number, device **UpTime**, and both the **Ethernet** and **Cellular** status. See **Figure 38**.

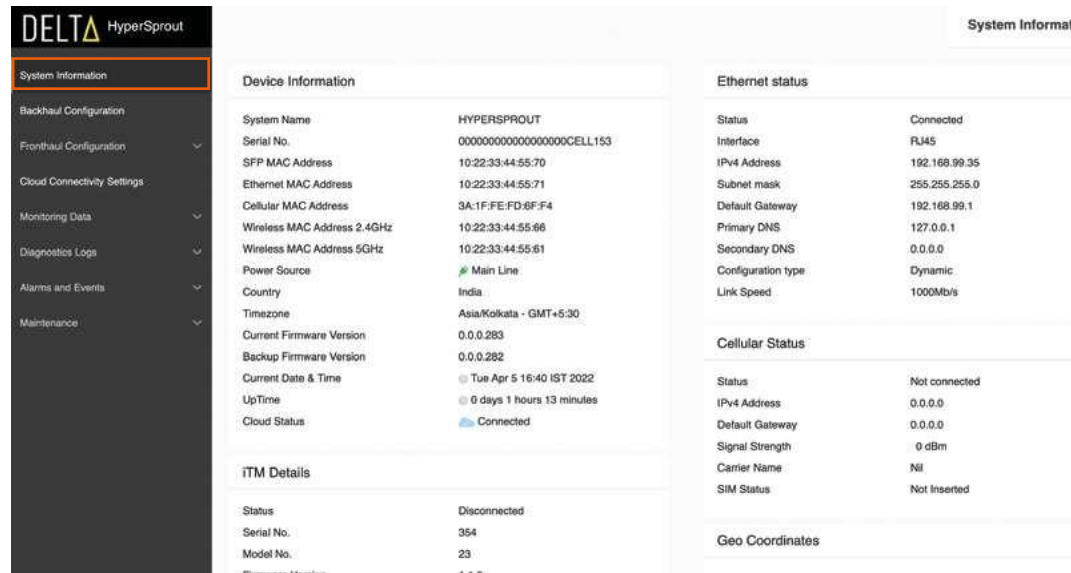


Figure 38: System Information - 1

- f. In the **System Information** page, we will be able to see the remaining board details such as **Wireless Settings**, **Geo Coordinates**, and **iTM Details**. See **Figure 39**.

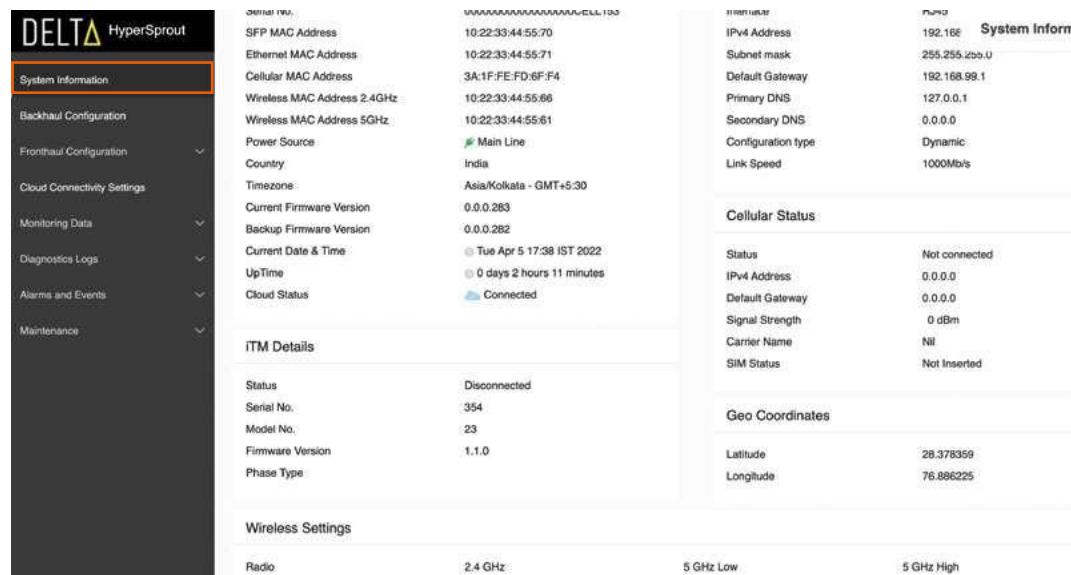


Figure 39: System Information - 2

6.2.2 Backhaul Selection

Follow below instructions to configure the backhaul settings.

- a. Navigate to the **Backhaul Configuration** page for configuring both the **Cellular** and **Ethernet**.
- b. For cellular operation, an authorized and activated SIM card must already be included in the device's SIM card port. An authorized and activated SIM card is an optional accessory for the device.
- c. For Ethernet operation, an appropriate Ethernet or fiber-optic terminated device must be connected to one of the two external ports (one for RJ-45 hook-ups and one for fiber-optic hook-ups).
- d. In the **Cellular** section, provide the **Username**, **Password**, **SIM PIN**, and **Network Selection** as either **Auto** or **Manual** as shown in **Figure 40**.

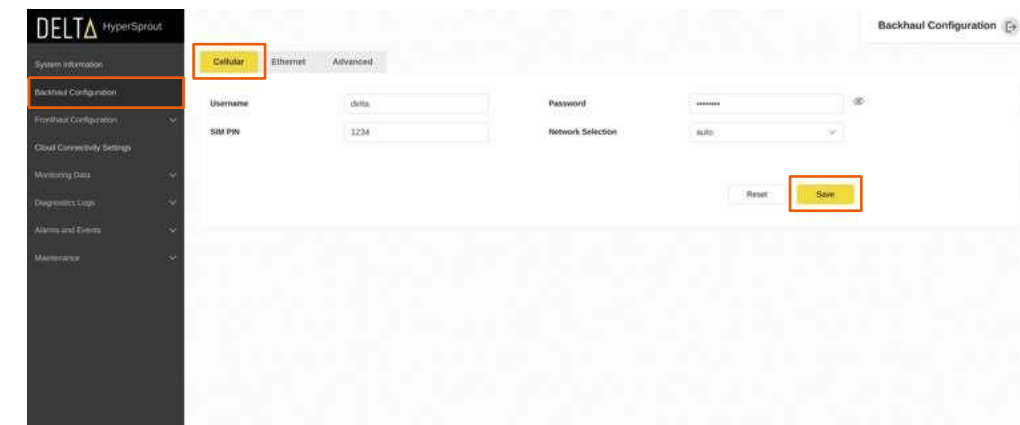


Figure 40: Backhaul - Cellular

- e. Under **Ethernet**, users can configure the **Static IP** or **Dynamic IP** for the Ethernet backhaul as shown in **Figure 41**.
- f. In the **Advanced** configuration, a user may configure the **Primary Backhaul** link and an **Auto Switch-over** to the secondary in the event that the primary backhaul is non-responsive. Note that two backhauls must be established for this functionality to be present, i.e. a primary **Ethernet** backhaul and a secondary **Cellular** backhaul, or vice-versa.

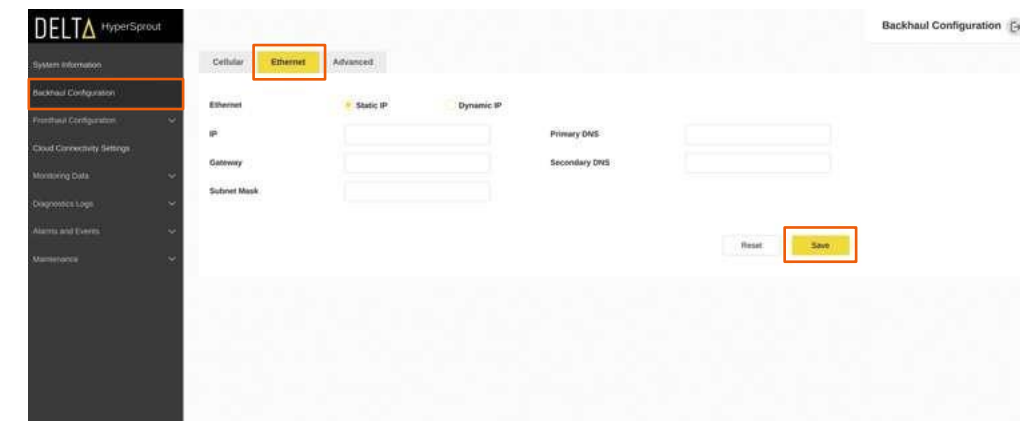
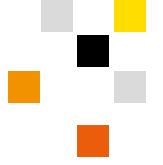


Figure 41: Backhaul - Ethernet



- g. **Auto switch over** will switch the backhaul connection from the primary backhaul to the secondary backhaul in case of any failure in the primary backhaul connection, as shown in *Figure 42*.

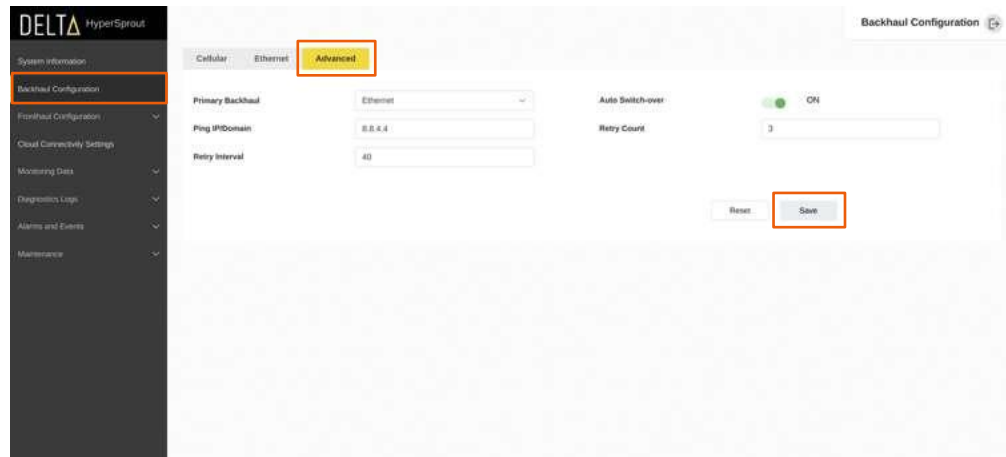


Figure 42: Backhaul - Advanced

6.2.3 Radio Configuration

To view or modify the **Radio configuration**, navigate to the **Fronthaul Configuration** and then select the **Radio Configuration** page to configure radio-related parameters such as **Radio Mode**, **Channel Width**, **Channel**, and **Transmit Power** under the corresponding radio tab **2.4GHz**, **5GHz (Low)**, and **5GHz (High)** and click the **Save** button when complete, as shown in *Figure 43*.

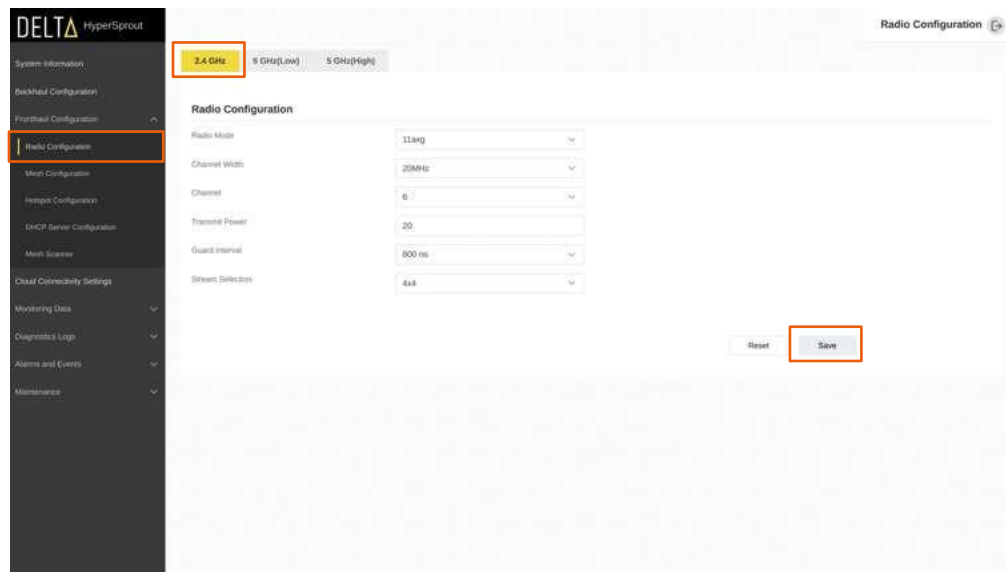


Figure 43: Radio - 2.4Ghz

6.2.4 Mesh Configuration

Follow below instructions to configure the mesh settings.

- a. To perform 2.4GHz mesh-related configurations, navigate to **Fronthaul Configuration** and then select **Mesh Configuration** and **2.4GHz**, where the **Mesh ID**, **Security Type**, and the pre-shared key can be configured. Once the configurations are done, click the **Save** button to save the required changes in 2.4GHz. See *Figure 44*.

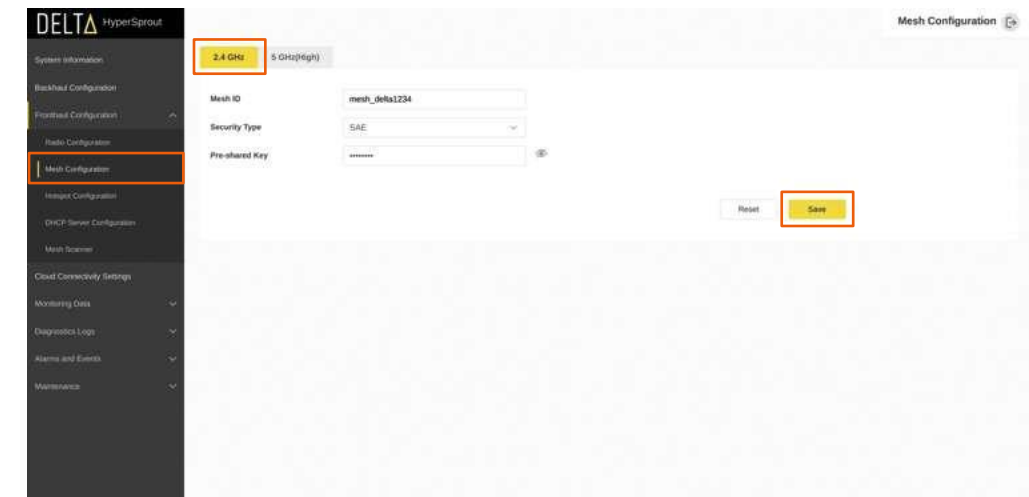


Figure 44: Mesh - 2.4Ghz

- b. To perform 5GHz mesh-related configurations, navigate to **Fronthaul Configuration** and then select **Mesh Configuration** and **5GHz (High)**, where we can configure **Mesh ID**, **Security Type**, and pre-shared key. Once the configuration is done, click the **Save** button to save the required changes in 5GHz. See *Figure 45*.

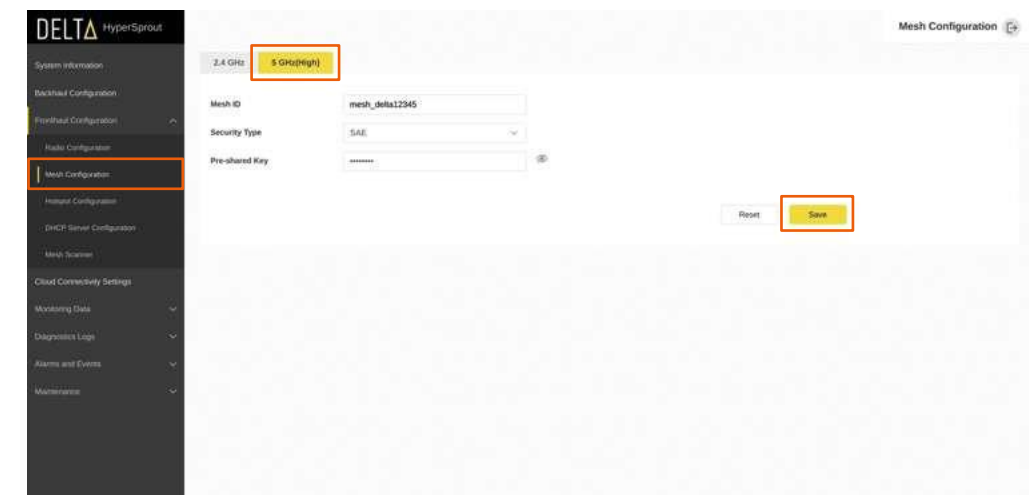


Figure 45: Mesh - 5Ghz

6.2.5 Hotspot Configuration

Follow below instructions to configure the hotspot settings.

- By default, hotspot configuration is set at 2.4GHz for SSID provisioning. Note that 5GHz may also be set, after configuring 2.4GHz.
- A new SSID is created by clicking the '+' icon, configuring the *SSID* and *Wireless Security* mode (OPEN / WPA2-PSK), and then pressing the *Save* button to apply the configuration. The hyperSPROUT™ smarthub or hyperHUB™ access point will now start broadcasting the configured SSID.
- Provisioning of the 5GHz band for hotspot operation follows a similar procedure as for 2.4GHz. See *Figure 46*, *Figure 47*, *Figure 48*, *Figure 49*.

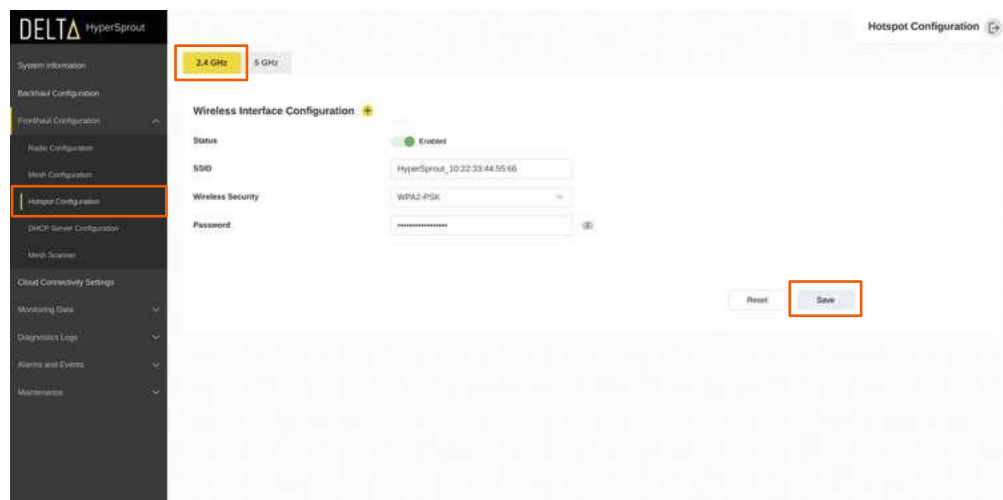


Figure 46: Hotspot - 2.4Ghz - Representation - 1

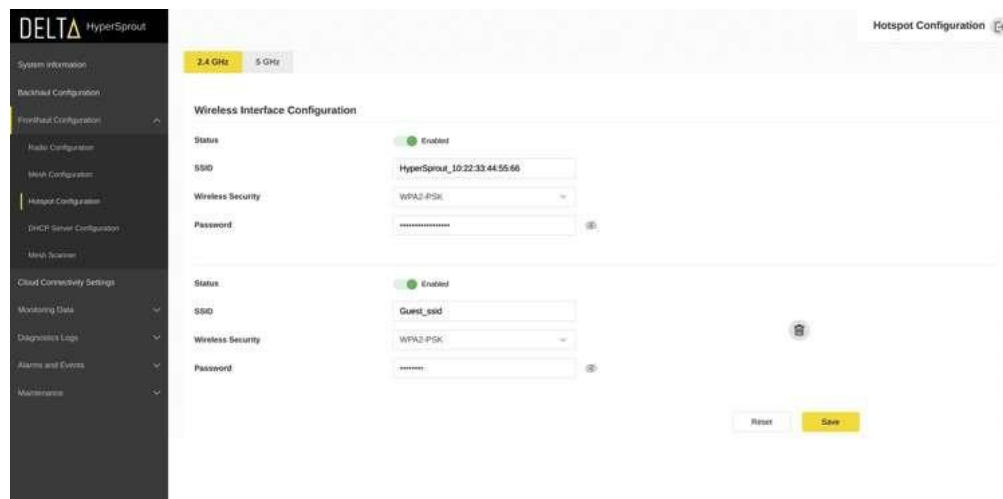


Figure 47: Hotspot - 2.4Ghz - Representation - 2

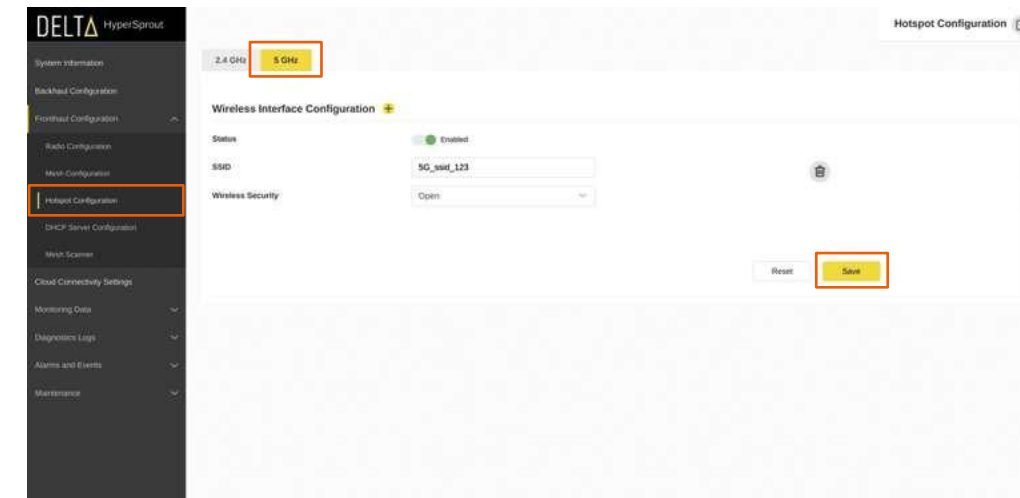


Figure 48: Hotspot - 5Ghz - Representation - 1

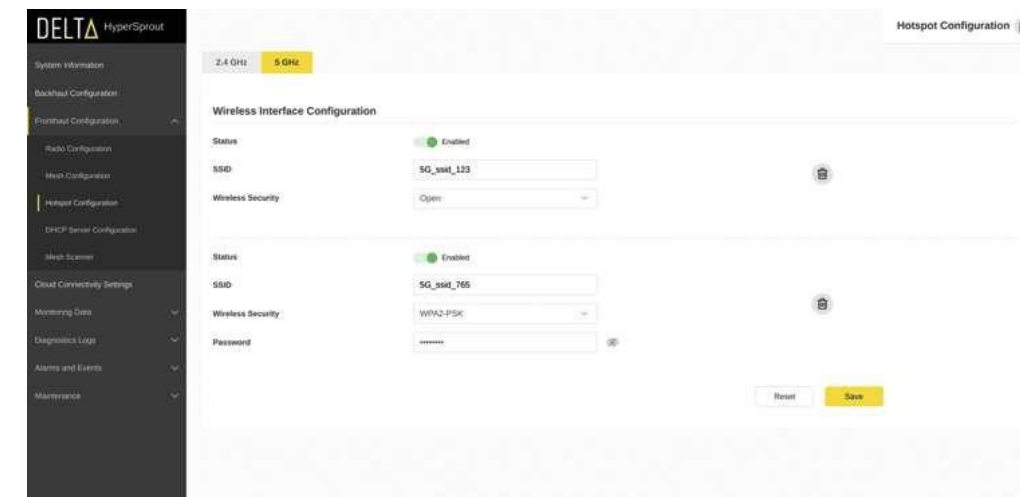
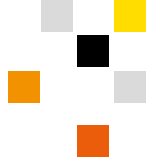


Figure 49: Hotspot - 5Ghz - Representation - 2

6.2.6 DHCP Server Configuration

Follow below instructions to configure the DHCP server.

- To configure the IP address for hotspots/mesh peering devices, navigate to *Fronthaul Configuration* and then select *DHCP Server configuration*. From this page, first select the appropriate configuration in the following two parameters:
 - Select the *Type* to properly set the *Hotspot* or *Mesh DHCP* server configuration.
 - Then select the appropriate *DHCP* button. Either *Enable* or *Disable* the server. If the server is disabled, then user devices will connect using a static IP configuration.



- b. If the **DHCP** button has been enabled, set the following parameters:
- Start Address
 - End Address
 - Subnet Mask
 - Default Gateway
 - Primary DNS
 - Secondary DNS
- c. Then click the **Save** button to save the settings. See *Figure 50* and *Figure 51*.

Note: Please keep a different subnet for **Hotspot** and **Mesh** server configurations.

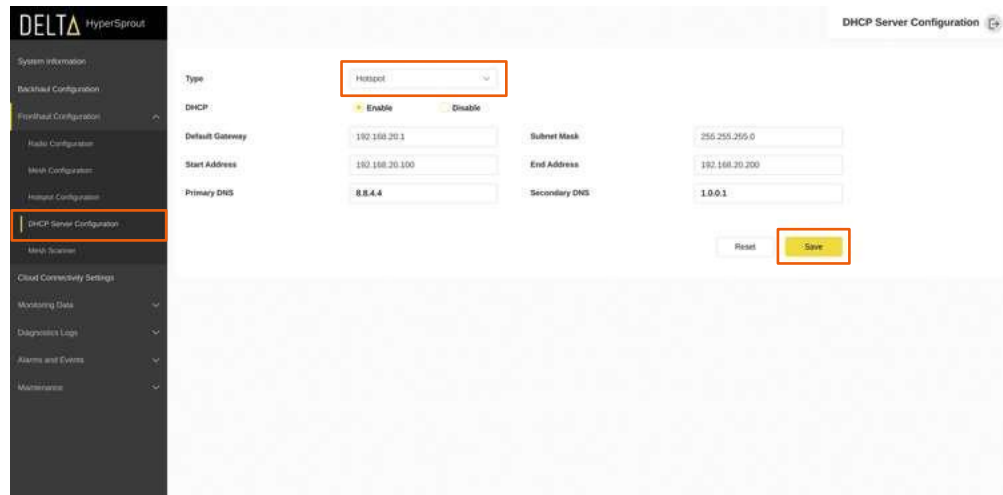


Figure 50: DHCP - Hotspot

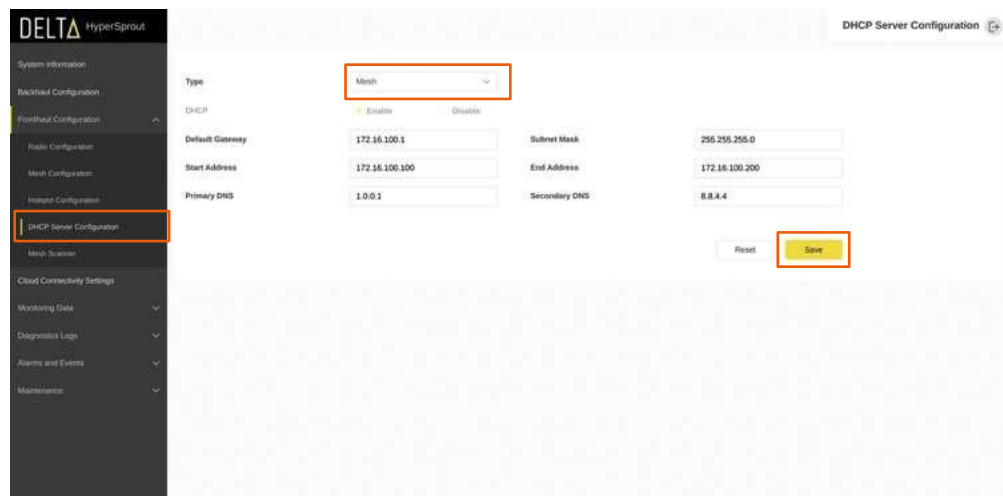


Figure 51: DHCP - Mesh

6.2.7 Mesh Scanner

Follow below instructions to scan and verify available mesh profiles.

- The **Mesh Scanner** page may be used to verify the available mesh profiles, **Device Types**, **RSSI**, and **Encryption** status. See *Figure 52*.
- Selection of the **Scan** button will repeat the scan of the local area.

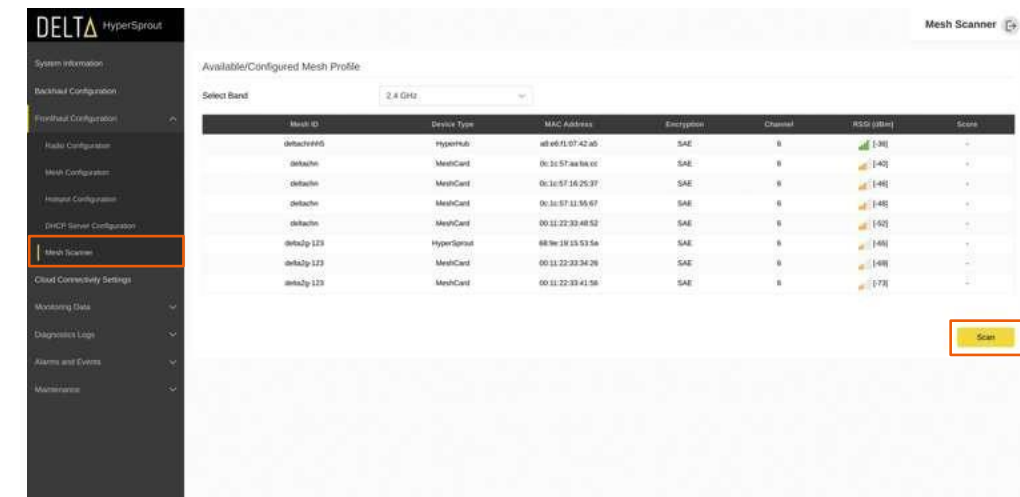


Figure 52: Mesh Scanner

6.2.8 Cloud Configuration

Follow below instructions to configure the appropriate device cloud access.

- First, select the **Cloud Connectivity Settings**.
- Next, provide the **Hostname**, **Shared Access Key**, and upload the appropriate **Certificate** in the **Cloud Connectivity Settings**. This process will configure the cloud details in the device. When complete click **Save**. See *Figure 53*.

Note: **Hostname** and **Shared Access Key** credentials need to be taken from the Microsoft Azure portal.

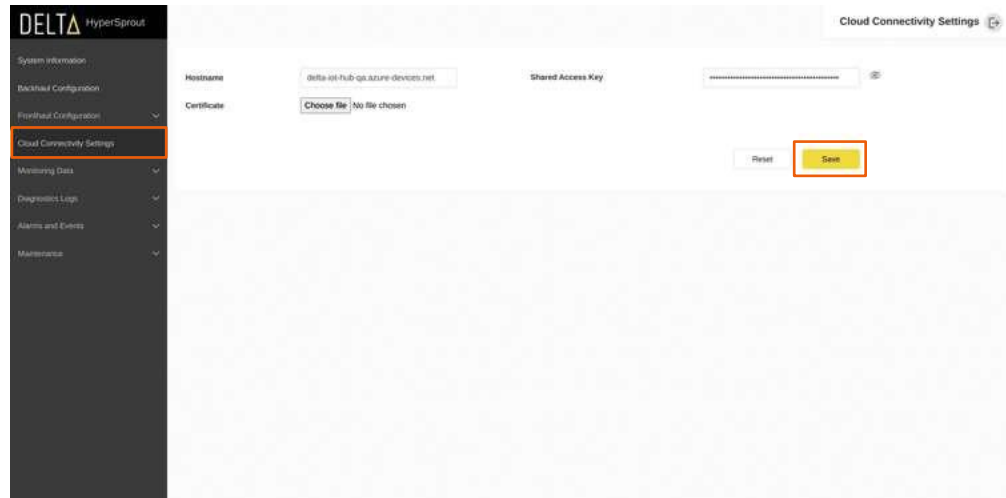
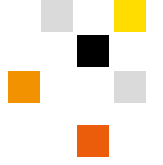


Figure 53: Cloud Connectivity

6.2.9 Transformer Monitor

Navigate to *Monitoring Data* and, select *Transformer Monitor*, and click *Run Diagnostics* to verify the transformer diagnostics. See *Figure 54*.

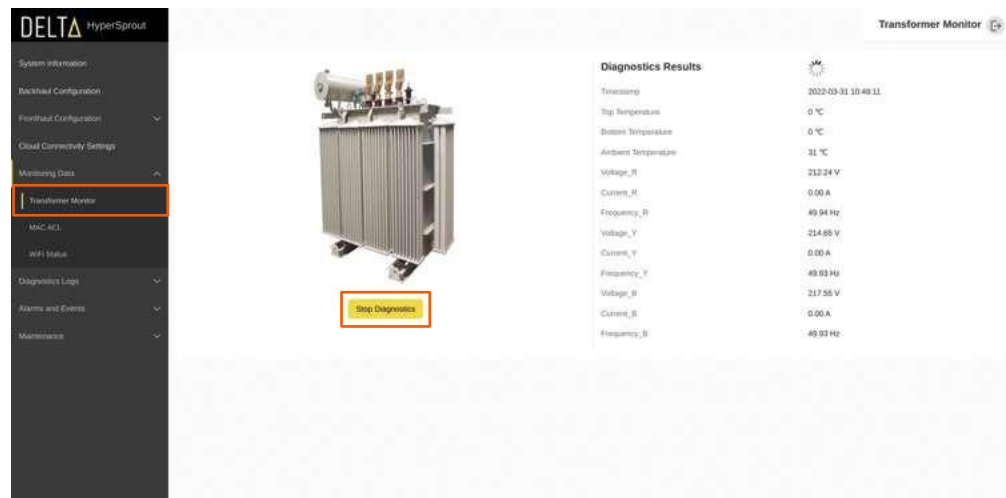


Figure 54: Transformer Monitor

6.2.10 Hotspot MAC-ACL

The Hotspot MAC-ACL is a security feature that allows or denies a digital endpoint client's connection to the hyper-SPROUT™ smarthub or hyperHUB™ access point. By default, the Hotspot MAC-ACL feature is disabled. Follow below instructions to enable and configure the MAC-ACL feature.

- Navigate to *Monitoring Data* and select *MAC ACL*.
- From the *MAC ACL* page, click the *Enable* icon and select *Save*. See *Figure 55*.

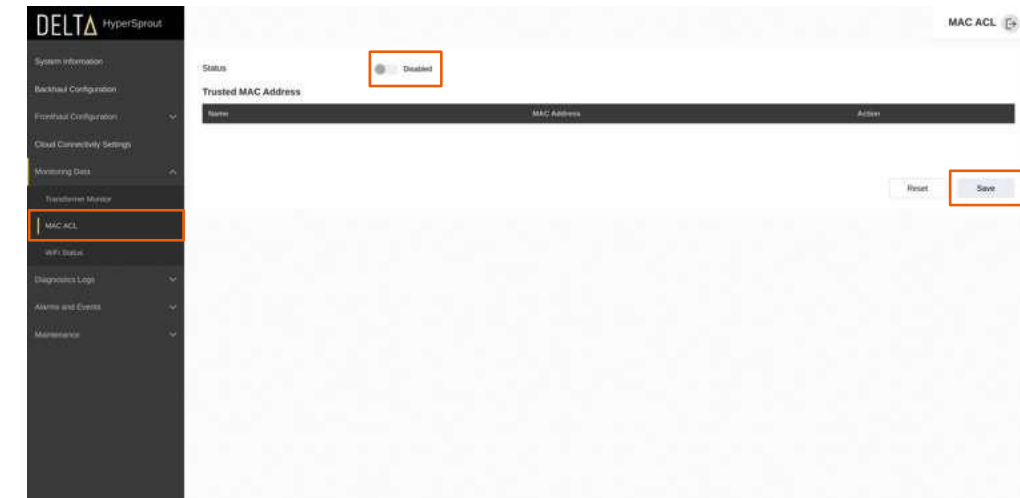


Figure 55: MAC ACL – Representation - 1

- Click the '+' icon and add a specific client's digital device *MAC Address* along with the user's name and click *Save*. See *Figure 56*.

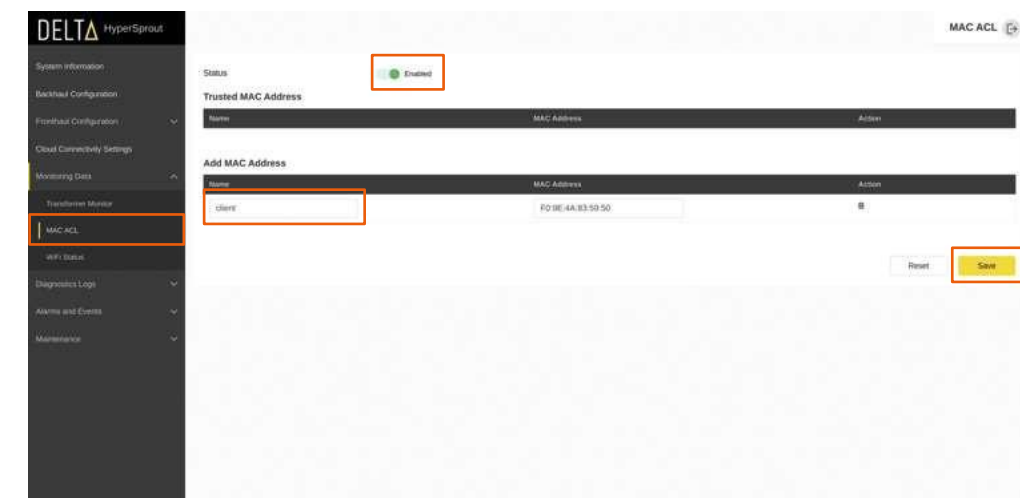


Figure 56: MAC ACL – Representation - 2

- After selecting *Save* and saving the *MAC Address* it will be listed in the *Trusted MAC Address* list as shown in *Figure 57*.

Note that this operation can also be addressed via the collectionENGINE™ asset management system. This system allows for the remote authorization of a specific MAC address across the entirety of a specific distribution transformer circuit. Additional details may be found in the collectionENGINE™ asset management system manual.

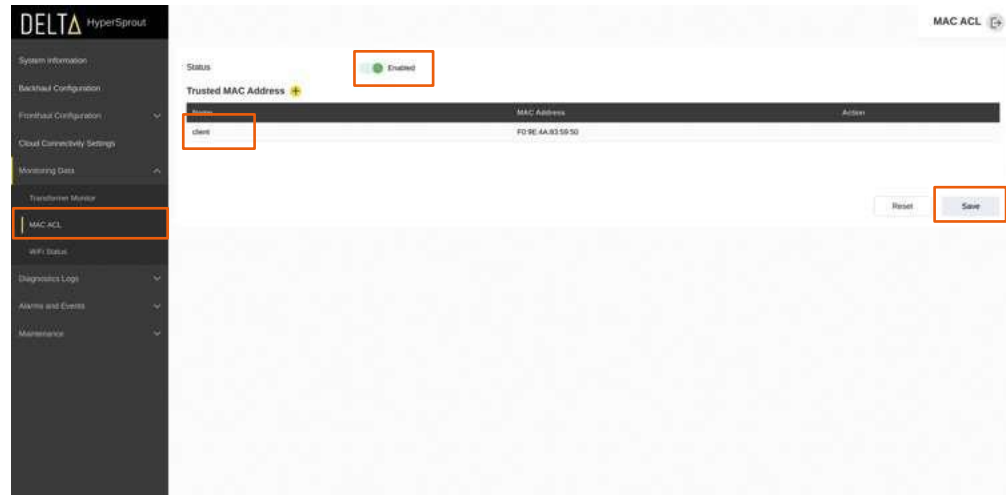
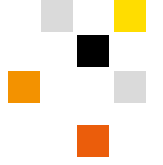


Figure 57: MAC ACL - Representation - 3

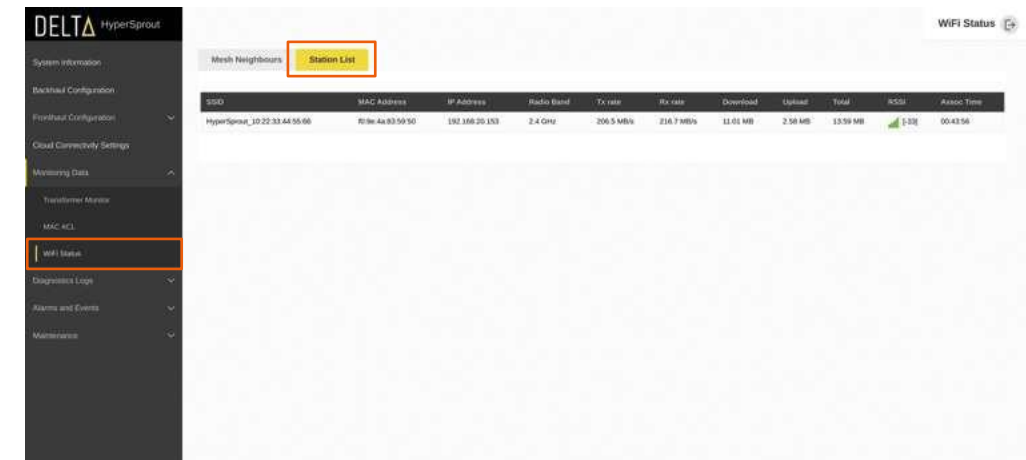


Figure 59: Wi-Fi Status Station

6.2.11 Wi-Fi Status

Follow below instructions to check for connected mesh neighbors.

- First, navigate to "Monitoring data" and then select *Wi-Fi status*.
- Any mesh neighbors will be noted under the *Mesh Neighbors* tab as shown in *Figure 58*.

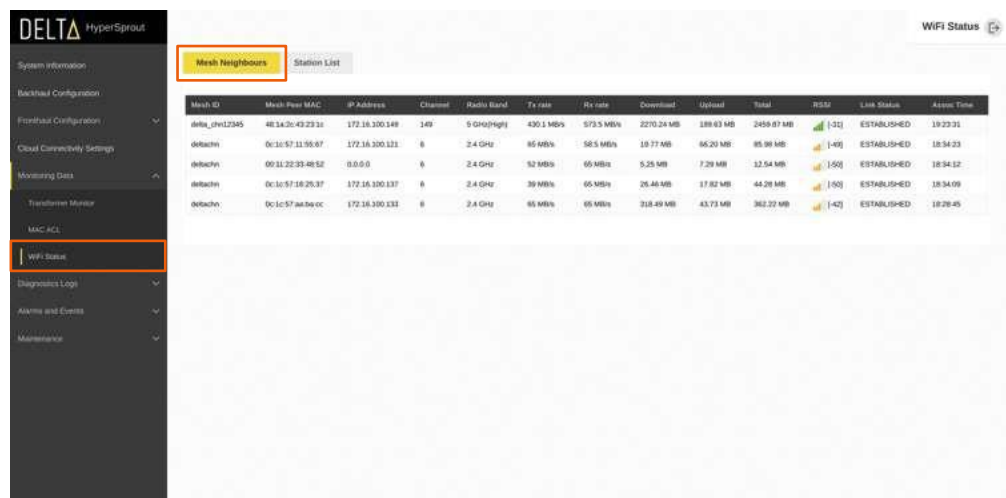


Figure 58: Wi-Fi Status Mesh

- To check the status of connected digital endpoint clients, navigate to *Monitoring Data* and then select *Wi-Fi Status*.
- Any connected digital endpoint clients will be noted under the *Station List* tab as shown in *Figure 59*.

6.2.12 Diagnostics Logs

The Diagnostics Logs section contains options to access the device logs and debugging tools relevant to understanding and validating ongoing device functionalities and operations in real-time.

6.2.12.1 System logs

Follow below instructions to access system logs.

- To view the Delta running applications of Wpa Supplicant Logs (mesh) and Hostapd Logs (hotspot), navigate to *Diagnostics Logs* and then select *System Log*.
- Next, select the appropriate log from the dropdown menu as shown in *Figure 60*.

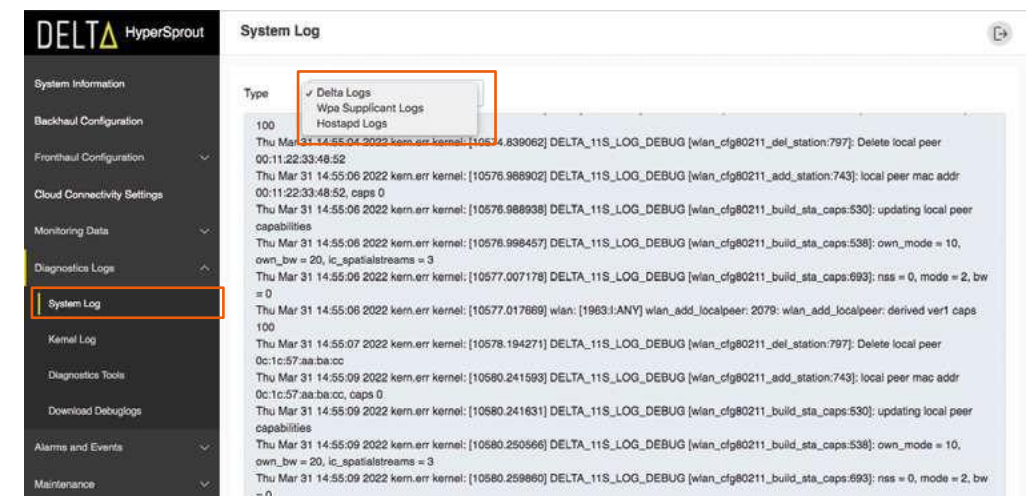


Figure 60: System Logs

6.2.12.2 Kernel logs

To view the appropriate Kernel Logs, navigate to *Diagnostics Logs* and then select *Kernel Log* as shown in *Figure 61*.

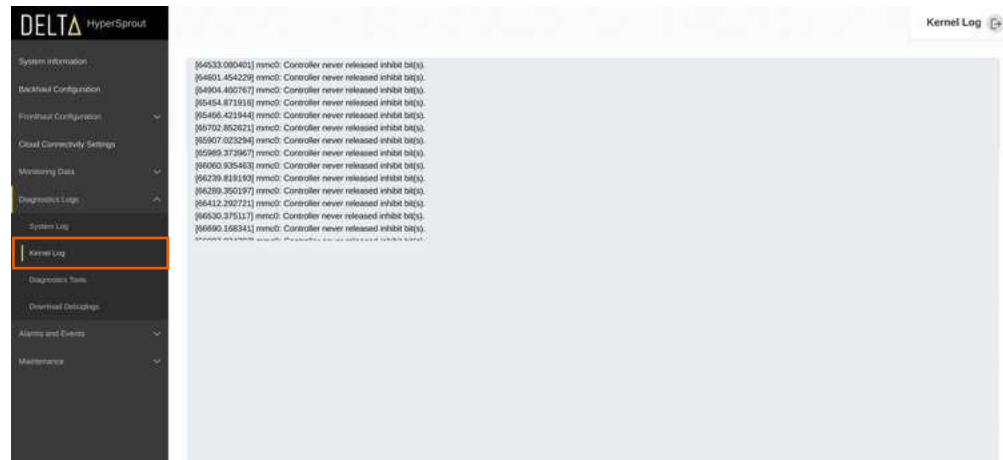


Figure 61: Kernel Logs

Debug logs may be downloaded by following the instructions below.

- Navigate to *Diagnostics Logs* and then select *Download Debug Logs* as shown in *Figure 63*.
- Click the *Download Debug Logs* button to download the device logs in ".tar" format.

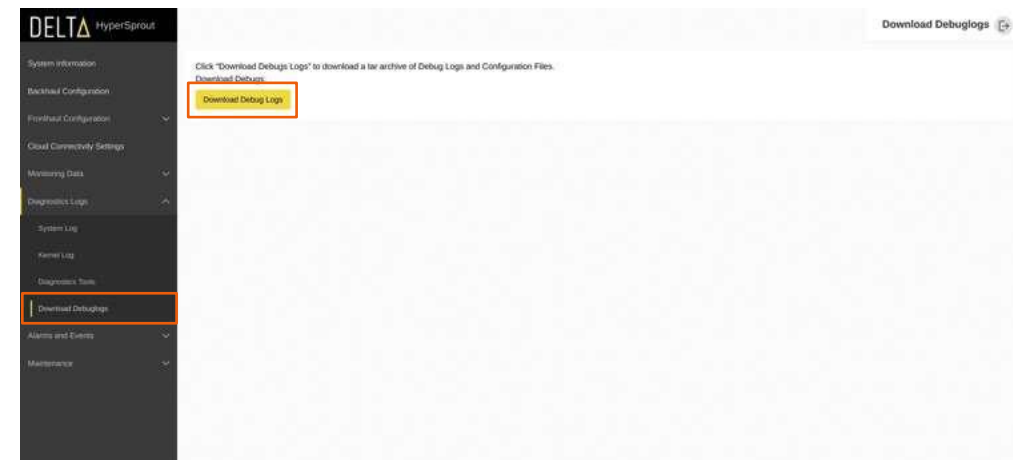


Figure 63: Download - Debug Logs

6.2.12.3 Diagnostics Tools

Follow below instructions to access diagnostic tools to address connectivity and network performance.

- Navigate to the *Diagnostics Logs* and then select *Diagnostics Tools* to verify the below network functionalities in the device. See *Figure 62*.
 - Ping* will ping an IP address/hostname.
 - Traceroute* will locate an IP address.
 - Nslookup* will find the IP address of a specific domain name (e.g. google.com)

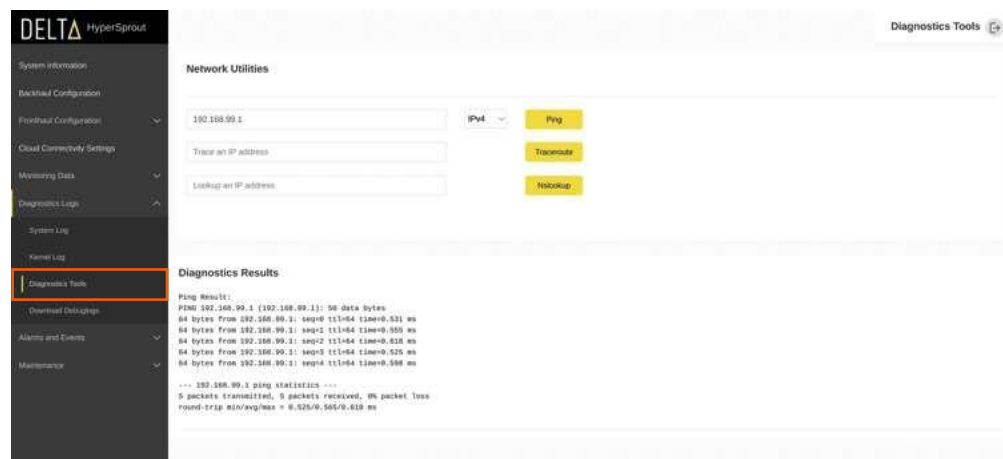


Figure 62: Diagnostic Logs

6.2.13 Alarms and Events

Follow below instructions to view active alarms and historical alarm details for a specific device.

- To view active alarms, navigate to *Alarms and Events* and then select *Active Alarms* to view a listing of the currently active alarms.
- The alarm table will show the alarm details like *Time Stamp*, *Alarm* type, *Severity*, and *Alarm Information* for that particular alarm as shown in *Figure 64*.

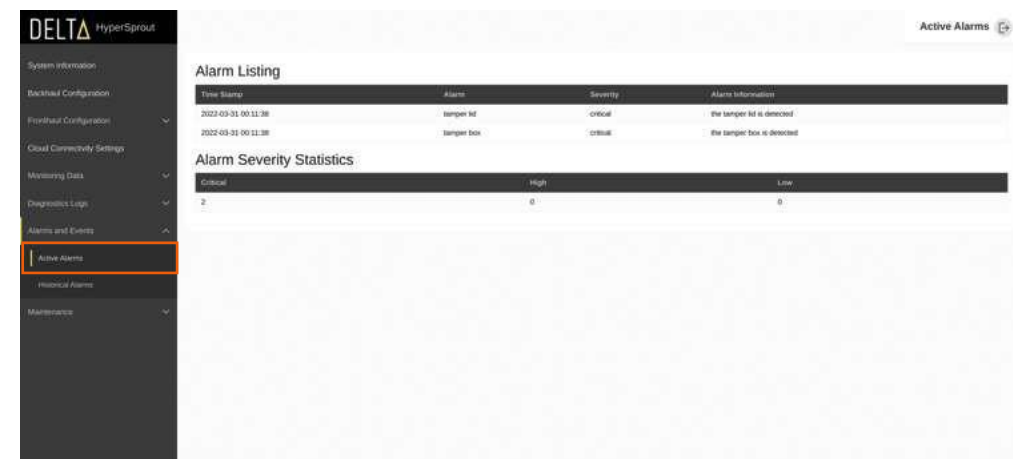
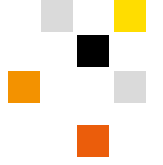


Figure 64: Active Alarms



- c. To view a listing of historical alarm activity, navigate to *Alarms and Events* and then select *Historical Alarms* to view a listing of these historical alarms.
- d. Similar information is noted as in the active alarms. See *Figure 65*.

Time Stamp	Alarm	Severity	Alarm Information
2022-03-31 04:30:43	CT Open	High	Alarm is cleared
2022-03-31 04:30:45	CT Open	High	Alarm is set
2022-03-31 04:31:00	CT Open	High	Alarm is cleared
2022-03-31 04:31:18	CT Open	High	Alarm is set
2022-03-31 04:31:57	CT Open	High	Alarm is cleared
2022-03-31 04:32:12	CT Open	High	Alarm is set
2022-03-31 04:33:00	CT Open	High	Alarm is cleared
2022-03-31 04:33:07	CT Open	High	Alarm is set
2022-03-31 04:34:57	CT Open	High	Alarm is cleared
2022-03-31 04:35:00	CT Open	High	Alarm is set
2022-03-31 04:36:00	CT Open	High	Alarm is cleared
2022-03-31 04:36:07	CT Open	High	Alarm is set
2022-03-31 04:36:48	CT Open	High	Alarm is cleared
2022-03-31 04:37:08	CT Open	High	Alarm is set
2022-03-31 04:37:28	CT Open	High	Alarm is cleared
2022-03-31 04:37:50	CT Open	High	Alarm is set
2022-03-31 04:38:18	CT Open	High	Alarm is cleared
2022-03-31 04:38:18	CT Open	High	Alarm is set
2022-03-31 04:41:30	CT Open	High	Alarm is cleared

Figure 65: Historical Alarms

6.2.14 Maintenance

The maintenance section provides device maintenance activity such as *Firmware Upgrade*, *System Settings*, *Reboot*, *Factory Reset*, and *Backup and Restore*.

6.2.14.1 Firmware Upgrade

Follow below instructions to perform a firmware upgrade.

- a. To upgrade the device to a new firmware image, navigate to *Maintenance* and then select *Firmware Upgrade Wizard*. Next, follow the steps outlined below.
 - i. *Select* the device type in the dropdown menu. See *Figure 66*.
 - ii. Click the *Choose File* button and select the required firmware file from the laptop/PC. Then, click the *Upload Image* button as shown in *Figure 66*.
 - iii. Note that this activity may also be conducted remotely using the collectionENGINE™ asset management system.

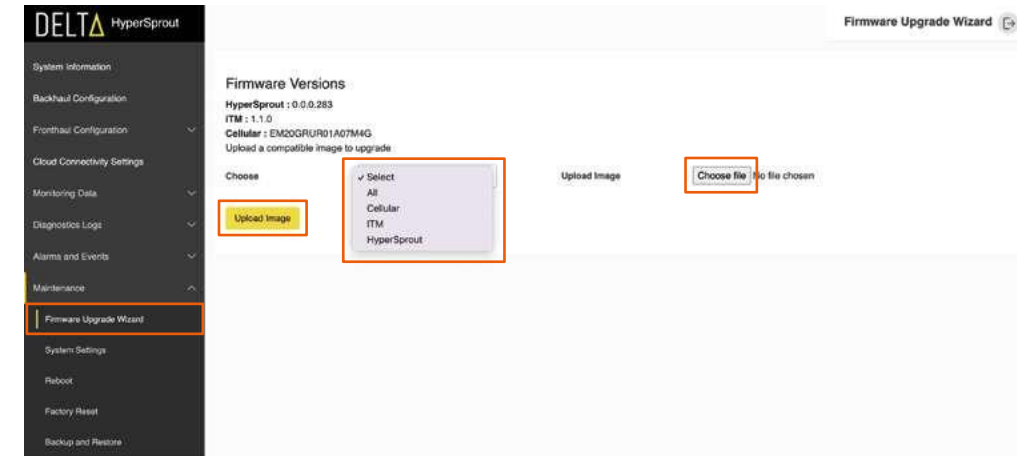


Figure 66: Firmware Upgrade

- b. Upon successful image upload, the user will be redirected to the *Firmware Upgrade* page as shown in *Figure 67*. This page will provide details of the upload image and will provide the user with a *Proceed* or *Cancel* button selection. The user may click the *Proceed* button to upgrade the device, as shown in *Figure 67*.
- c. Upon successful upgrade, the device will reboot and restart with the newly upgraded image.

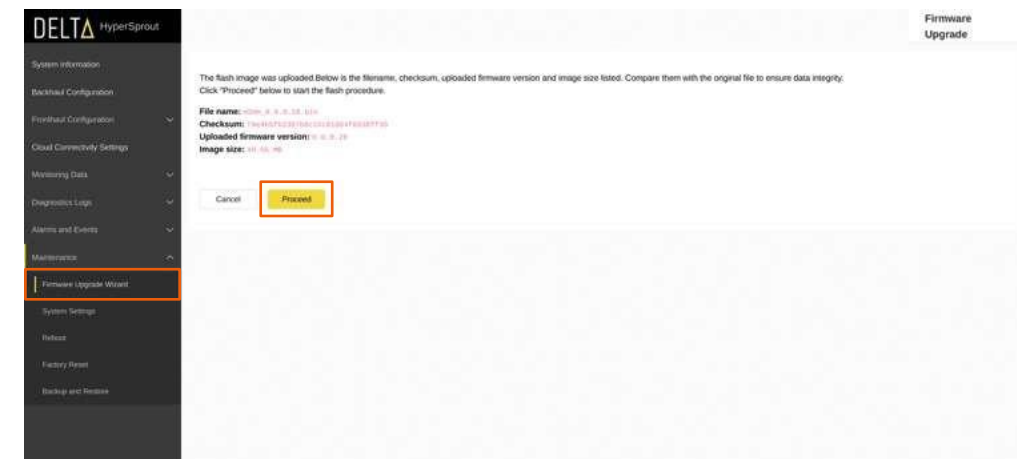


Figure 67: Firmware Upgrade Finish

6.2.14.2 System Settings

To access the system settings, navigate to *Maintenance* and select *System Settings*. Following items can be viewed and configured. See *Figure 68*.

- *System Name*
- *Country* of device operation
- *Time Zone* of device operation

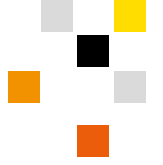


Figure 68: System Settings

6.2.14.3 Reboot

Follow below instructions to reboot the device.

- To reboot the device, navigate to **Maintenance** and then select **Reboot** as shown in *Figure 69*.
- Next, click the **Perform Reboot** button to reboot the device.
- The reboot procedure, as executed from this screen, will simply restart the device. There will be no change in the configurations applied to the device.

Note that this feature and other reboot options are also available remotely from the collectionENGINE™ asset management system.



Figure 69: Reboot

6.2.14.4 Factory Reset

Follow below instructions to factory reset the device.

- To conduct a factory reset, navigate to **Maintenance** and then select **Factory Reset** as shown in *Figure 70*.
- Next, click the **Perform Factory Reset** button to execute a full factory reset of the device.
- The factory reset procedure, as executed from this screen, will reset the device and will return the device to the factory default configurations. All other configurations will be erased.

Note that this feature and other reset options are also available remotely from the collectionENGINE™ asset management system.

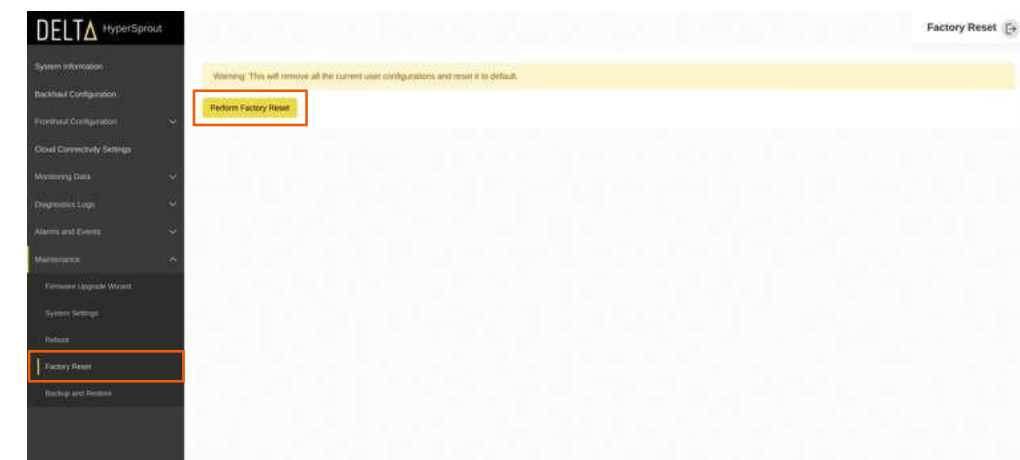


Figure 70: Factory Reset

6.2.14.5 Backup and Restore

The **Backup and Restore** page provides options to either take a current device configuration backup or restore the device configuration to a prior backup taken earlier. See below instructions and *Figure 71* for an example of each selection.

- To create a backup of a current configuration, the following procedure is used.
 - Navigate to **Maintenance** and then select **Backup and Restore**.
 - Click the **Generate Archive** button under the **Backup** section to download the device's current configuration in ".tar" format.
 - The backup file name will be the device name and the MAC address of the device along with the date of downloading the file. Note the following example.
(E.g.: Debuglogs-HyperSprout-98ae710024c4-2022-02-22-09-54-14.tar.gz)
- To restore from a prior backup, the following procedure is used.
 - Navigate to **Maintenance** and then select **Backup and Restore**.
 - Click the **Choose file** option and select the configuration backup file to upload from the laptop/PC.
 - Click the **Upload archive** option to restore the configuration.
 - Once the backup file is restored, the device will reboot and restart with the updated backup configuration.

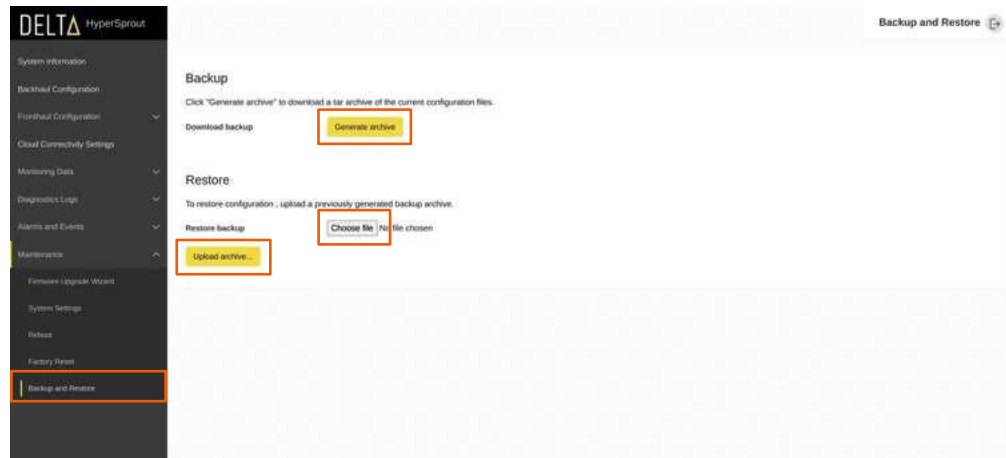
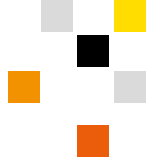


Figure 71: Backup & Restore

7. HARDWARE LIMITED WARRANTY



A SCOPE OF MANUFACTURER'S WARRANTY

(i) Express Warranty – Warranty Periods and Remedies

Subject to the terms and conditions herein, including the limitations in Section A(ii), and the exclusions in Section A(iii) and Section C below, Delta warrants the hardware in this product against defects in materials and workmanship under normal use for the Warranty Period (as defined below). A claim under this warranty is only eligible if it is made within the Hardware Warranty Period.

The Hardware Warranty Period begins on the later of (i) the date of purchase by the original end-user purchaser or (ii) the date of installation of the product on the end-user electrical grid, and lasts for a period of one (1) year.

If you make an eligible hardware claim under this limited warranty, Delta will honor this warranty by doing one of the following (at its option):

- a. repairing the product with new or refurbished parts;
- b. replacing the product with a reasonably available equivalent new or refurbished Delta product;
- c. refunding the actual purchase price of the product less any rebates and discounts, or
- d. paying the cost of repair of the product.

The foregoing is the sole remedy for breach of the limited warranties set forth herein.

Be aware that goods presented for repair may be replaced by refurbished goods of the same type rather than the defective goods being repaired. Alternatively, refurbished parts may be used in the repair. Any repaired or replacement products or parts are warranted for the remainder of the original Hardware Warranty Period or 30 days, whichever is longer, and such warranty is subject to the same exclusions set forth herein. All products and parts that are replaced become the property of Delta.

Subject to the terms and conditions herein, including the limitations in section (ii) and the exclusions in Section A(iii) and Section C below, Delta additionally warrants that any firmware or other software contained in the product will be free from defects in materials and workmanship under normal use for the Software Warranty Period, as defined below. A claim under this warranty is only eligible if it is made within the Software Warranty Period. The Software Warranty Period is a period of ninety (90) days from the date of original purchase by the end user-purchaser. If you make an eligible software media claim under this manufacturer's warranty, Delta will honor the warranty by replacing the software media.

No Delta employee, distributor, agent or reseller can make any verbal or written modification, extension or addition to this limited warranty.

This limited warranty is granted to the original end user purchaser who is the Customer of the qualifying and applicable product and is not transferable. Any such transfer shall void the limited warranty.

Note: The rights and remedies outlined above are the only rights and remedies available under this manufacturer's limited warranty. However, a defect which gives rise to a claim under this limited warranty may also give rise to rights under local laws, and different or additional remedies may be available under those laws. Further, rights and remedies

may be available under local laws even for defects, goods or services that are not covered by this limited warranty at all. YOU ARE ADVISED TO CONSULT APPLICABLE STATE OR COUNTRY LAWS FOR A FULL DETERMINATION OF YOUR RIGHTS.

(ii) Express Warranties NOT Given

Delta does not give any express warranty:

- a. with respect to any damage that occurs as a result of your failure to follow the instructions intended for this product;
- b. with respect to performance factors attributable to backhaul methodology, topographical features, wireless network capacity, data throughput rate, speed, range, coverage, signal propagation, interference, environmental conditions, and / or supported product mix;
- c. in relation to software or services provided by Delta with the product, whether factory loaded on the product or contained on media accompanying the product, except for the limited warranties given in section A(i) above;
- d. in relation to any third party software or service offerings which may be included in, or bundled with the product;
- e. that the operation of the product, software or services will be uninterrupted or error-free;
- f. in relation to interoperability with third party hardware, software or service offerings which you may attempt to operate with the product;
- g. that the product, software or services, or any equipment, system or network on which the product, software or services are used will be free of vulnerability to intrusion or attack; or
- h. as to the continued availability of a third party's service which this product's use or operation may require.

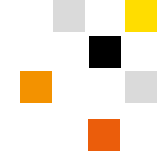
Note: Although these warranties are not expressly given by Delta they may be implied or otherwise given under local laws.

(iii) Circumstances in Which This Limited Warranty Does Not Apply

This manufacturer's limited warranty does not apply if:

- a. the product assembly has been opened or tampered with in any way;
- b. the product has been altered or modified, except by Delta or its agents;
- c. the product damage was caused by use with non-Delta products, except as expressly described in these instructions supplied by Delta;
- d. the product has not been stored, installed, commissioned, operated, used, repaired, or maintained in accordance with these instructions supplied by Delta;
- e. the product has been subjected to abnormal physical or electrical stress, misuse, abuse, tampering, negligence, or accident;
- f. damage occurs in shipment, due to act of God, or due to power surge;
- g. the serial number on the product has been altered, defaced, or removed; or
- h. the product is supplied or licensed for beta, evaluation, testing or demonstration purposes for which Delta does not charge a purchase price or license fee.

Note: Although this manufacturer's limited warranty does not apply in the above circumstances, you may still have rights and remedies under local laws.



B OBTAINING SERVICE UNDER THIS MANUFACTURER'S WARRANTY

If you have a question about this product or experience a problem with it, please contact Delta at info@deltaglobalnetwork.com. If you have any questions about the product or return process, you can contact Delta at info@deltaglobalnetwork.com.

If the product proves defective during the Hardware Warranty Period or Software Warranty Period (as applicable), you may lodge a warranty claim as set forth herein. You must provide your product serial number and invoice number when lodging a warranty claim. If you are requested to return your product by post, you will be given a Return Materials Authorization (RMA) number. Along with the RMA number, you will be given the appropriate shipping address.

Delta is not liable for a breach of the warranties set forth herein unless: (i) you give written notice of the defective products or services, as the case may be, reasonably described, to Delta within thirty (30) days of the time when you discover or ought to have discovered the defect; (ii) if applicable, Delta is given a reasonable opportunity after receiving the notice of breach of the warranty to examine such products and you (if requested to do so by Delta) return such products to Delta's place of business for the examination to take place there; and (iii) Delta reasonably verifies your claim that the products or services are defective. Delta shall not be liable for a breach of the limited warranties set forth herein if you make any further use of the products after giving such notice.

You are responsible for properly packaging and shipping your product at your own cost and risk, and you are responsible for all shipping and handling charges, unless noted otherwise, in addition to any applicable customs duties, VAT or other associated taxes or charges when returning your product. Transfer of the products may be covered by export controls issued by the United States or other governments. You must include the RMA number supplied by Delta when returning your product. Products received without a RMA number will be rejected. Do not include any other items with the product you are returning.

Defective product covered by this manufacturer's warranty will be repaired or replaced and returned to you without charge. Repairs or replacements not covered under this manufacturer's warranty or your statutory consumer rights will be subject to charge at Delta's then-current rates.

C GENERAL EXCLUSIONS AND LIMITATIONS OF LIABILITY

IN SOME JURISDICTIONS AND CIRCUMSTANCES IT IS POSSIBLE FOR A MANUFACTURER TO CHANGE OR EXCLUDE WARRANTIES, CONDITIONS OR GUARANTEES IMPLIED OR IMPOSED BY LAW, AND TO OTHERWISE LIMIT ITS LIABILITY TO CONSUMERS. IN THOSE JURISDICTIONS WHERE IT CAN LAWFULLY DO SO, AND TO THE FULL EXTENT THAT IT IS ALLOWED BY LAW TO DO SO:

- EXCEPT FOR THE WARRANTIES EXPRESSLY SET FORTH HEREIN, DELTA MAKES NO WARRANTY WHATSOEVER, EXPRESS OR IMPLIED, WITH RESPECT TO THE PRODUCTS OR SERVICES. DELTA HEREBY EXCLUDES AND EXPRESSLY DISCLAIMS, TO THE EXTENT ALLOWED BY APPLICABLE LAW, ALL EXPRESS, IMPLIED, OR STATUTORY CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED

WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR RESULTING FROM A COURSE OF DEALING, LAW, CUSTOM, USAGE, OR TRADE PRACTICE, EXCEPT FOR THE LIMITED WARRANTIES SPECIFIED HEREIN;

- TO THE EXTENT THAT ANY OF THE SAME CANNOT BE EXCLUDED, SUCH IMPLIED CONDITION, REPRESENTATION AND/OR WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD REFERRED TO IN SECTION A(i) ABOVE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY IN SUCH JURISDICTIONS.
- DELTA EXCLUDES ALL LIABILITY FOR THE LOSS OF, OR DAMAGE TO, DATA CAUSED BY USE OF A DELTA PRODUCT, OR ITS REPAIR;
- TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT SHALL DELTA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OF USE, REVENUE OR PROFIT, LOSS OF DATA OR DIMINUTION IN VALUE, INCONVENIENCE OR DAMAGES OF ANY KIND OR CHARACTER, OR FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR PUNITIVE DAMAGES (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, ANTICIPATED SAVINGS, WORK SLOW-DOWN OR STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, LOSS OF THE ABILITY TO USE ANY THIRD PARTY PRODUCTS, SOFTWARE OR SERVICES, DAMAGE TO OR FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH DELTA'S PRODUCT IS CONNECTED, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO DELTA FOR WARRANTY SERVICE, OR THIRD PARTY CLAIMS) WHETHER ARISING OUT OF BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY) OR OTHER LEGAL OR EQUITABLE THEORY, REGARDLESS OF WHETHER SUCH DAMAGES WERE FORESEEABLE AND WHETHER OR NOT DELTA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND NOTWITHSTANDING THE FAILURE OF ANY AGREED OR OTHER REMEDY OF ITS ESSENTIAL PURPOSE.
- IN NO EVENT SHALL DELTA'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER ARISING OUT OF OR RELATED TO BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, EXCEED THE TOTAL OF THE AMOUNTS PAID TO DELTA FOR THE PRODUCTS AND SERVICES SOLD HEREUNDER. THIS LIMITATION SHALL NOT APPLY TO (I) LIABILITY RESULTING FROM DELTA'S FRAUD OR WILLFUL MISCONDUCT AND (II) DEATH OR BODILY INJURY RESULTING FROM DELTA'S ACTS OR OMISSIONS.

TO THE EXTENT ALLOWED BY APPLICABLE LOCAL LAW, THESE TERMS AND CONDITIONS CONSTITUTE THE COMPLETE AND EXCLUSIVE WARRANTY AGREEMENT BETWEEN YOU AND DELTA REGARDING THE PRODUCT YOU HAVE PURCHASED. THESE TERMS AND CONDITIONS SUPERSEDE ANY PRIOR AGREEMENTS OR REPRESENTATIONS—INCLUDING REPRESENTATIONS MADE IN DELTA SALES LITERATURE OR ADVICE GIVEN TO YOU BY DELTA OR AN AGENT OR EMPLOYEE OF DELTA—THAT MAY HAVE BEEN MADE IN CONNECTION WITH YOUR PURCHASE OF THE PRODUCT. NO CHANGE TO THE CONDITIONS OF THIS LIMITED WARRANTY IS VALID UNLESS IT IS MADE IN WRITING AND SIGNED BY AN AUTHORIZED REPRESENTATIVE OF DELTA.

RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

FCC PART 15 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.

This equipment has been verified to comply with the limits for a class B computing device, pursuant to FCC Rules. In order to maintain compliance with FCC regulations, shielded cables must be used with this equipment. Operation with non-approved equipment or unshielded cables is likely to result in interference to radio and TV reception. The user is cautioned that changes and modifications made to the equipment without the approval of manufacturer could void the user's authority to operate this equipment.

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. See 47 CFR Sec. 15.105(b). 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.

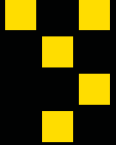
However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to 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.

FCC CAUTION STATEMENT FOR MODIFICATIONS

CAUTION: Any changes or modifications not expressly approved by Delta Energy and Communication, Inc. could void the user's authority to operate the equipment





Vertical text consisting of mathematical summation formulas and the number 8760, repeated multiple times.

CONTACT

UNITED STATES

Delta Energy & Communications, Inc.
29975 Technology Drive, Suite 101
Murrieta, CA 92563
Phone +1 951 816 6338
info@deltaglobalnetwork.com

Standard Disclaimer on Data Rate speeds.

Theoretical maximum performance derived from IEEE Standard 802.11 specifications. Actual performance may vary, including lower wireless network capacity, data throughput rate, speed, range, and coverage. Performance depends upon many factors, conditions, and variables, including but not limited to, building materials and construction, the volume of network traffic, the mix of wireless products used, interference, and other adverse conditions. Actual data throughput will vary and may depend upon the mix of wireless products used, quantity of wireless products used, and external factors. Product specifications are subject to change without notice.

Data rates described, communicated, and quoted represent top-end, theoretical capacity for the referenced IEEE specifications and devices, and in all cases, are subject to system configurations and, importantly, the backhaul methodologies used. Using a fiber connection, the theoretical maximum is 4.8Gbps. Using a 4G/LTE cellular connection, the average typically achievable data rate ranges from 3Mbps to 10Mbps. Theoretical maximum speeds are in the range of 100 Mbps (download) and 50Mbps (upload).

